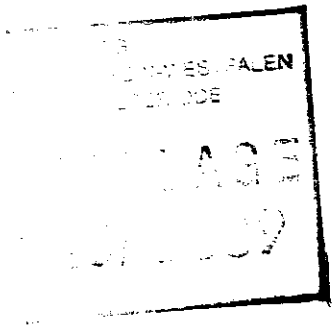
A 1

Der Innenminister
des
Landes Nordrhein-Westfalen

MMV 10/2589

Datenschutz

im nicht-öffentlichen Bereich



1. Bericht der Landesregierung

über die Tätigkeit der für den Datenschutz
im nicht-öffentlichen Bereich
zuständigen Aufsichtsbehörden

A/2

MMV10/2589

Erster Bericht

der Landesregierung Nordrhein-Westfalen

über die Tätigkeit der für den

Datenschutz im nicht-öffentlichen Bereich

zuständigen Aufsichtsbehörden

vorgelegt im Dezember 1989

A/3

MMV10/2589

Herausgeber: Der Innenminister
des Landes Nordrhein-Westfalen
Haroldstraße 5
4000 Düsseldorf 1

A/4

GLIEDERUNG

		Seite
Überblick		1
1.	**Einführung**	3
2.	**Regelungskonzept des BDSG für den Datenschutz im nicht-öffentlichen Bereich; Novellierung**	4
2.1	Geltendes Recht	4
	2.1.1 Verpflichtete Stellen des privaten Rechts	4
	2.1.2 Zulässigkeit der Datenverarbeitung	6
	2.1.3 Rechte des Betroffenen, Pflichten der datenverarbeitenden Stellen	7
	2.1.4 Datensicherung	7
	2.1.5 Aufsichtsbehörden	8
2.2	Novellierung des BDSG	9
	2.2.1 Sachstand	9
	2.2.2 Verfassungsrechtliche Vorgaben für den nicht-öffentlichen Bereich	10
	2.2.3 Erweiterung des Anwendungsbereichs	10
	2.2.4 Erlaubnisnormen auch künftig Generalklauseln	11
	2.2.5 Erweiterung der Rechte des Betroffenen	12
	2.2.6 Erweiterung der Befugnisse der Aufsichtsbehörden	12
3.	**Zuständigkeiten, Organisation und personelle Ausstattung der Datenschutzaufsicht bei den Aufsichtsbehörden**	13

A15 MMV10/2589

		Seite
4.	**Meldungen zum Register der Aufsichtsbehörden**	15
5.	**Übersicht über die Kontrolltätigkeit der Aufsichtsbehörden**	17
5.1	Beschwerden, Anfragen und Beratungsersuchen	18
5.2	Überprüfungen vor Ort	22
5.3	Bußgeldverfahren	24
5.4	Zusammenfassung	25
6.	**Nichteinbeziehung der Akten-Datenverarbeitung in das BDSG: Bedeutung für die Aufsichtspraxis**	27
7.	**Einzelprobleme, Beispielsfälle aus der Kontrolltätigkeit**	29
7.1	Kreditinformationssystem der SCHUFA	29
7.1.1	Organisation, Aufgabe, Verfahren	29
7.1.2	Zulässigkeit des SCHUFA-Verfahrens	31
7.1.3	Mehrfache Verwechselung eines "Unschuldigen" mit Folgen	32
7.1.4	Datenschutz durch Meldung des Geburtsdatums	35
7.1.5	Waffengleichheit: Meldung des Widerspruchs gegen Mahnbescheid	37

A/6

		Seite
7.2	Andere Hinweis- und Warnsysteme	38
	7.2.1 "Schwarzfahrer"-Dateien	38
	7.2.2 Datei über Mietinteressenten	40
	7.2.3 Frauenärzte-Datei	43
	7.2.4 EPOS - Datei zum Schutz gefährdeter Führungskräfte -	44
	7.2.5 Sachschadendatei SAVIS	47
	7.2.6 Weitere Systeme, Zusammenfassung	50
7.3	Wirtschafts- und Handelsauskunfteien	52
7.4	Adressenhandel und Direktwerbung	55
7.5	Markt- und Meinungsforschung	58
7.6	Arbeitnehmerdaten	61
	7.6.1 Fragebogen für Stellenbewerber	61
	7.6.2 Befragung des früheren Arbeitgebers	63
	7.6.3 Geheime Auswahl für Stipendium	66
	7.6.4 Telefondatenerfassung	66
	7.6.5 Personalinformationssysteme	67
7.7	Mieterdaten	68
7.8	Kundendaten	72
7.9	Patientendaten	75
7.10	Mitgliederdaten	78
7.11	Versichertendaten	82

Seite

8. Datensicherung 84

8.1 Allgemeine Erfahrungen 84

8.2 Gespendete Disketten mit Fehlern 86

8.3 Postversand an Nichtadressaten 87

8.4 Daten in der Tonne: Aufsicht auf Spurensuche 88

9. Zusammenarbeit der obersten Aufsichtsbehörden im "Düsseldorfer Kreis" 89

9.1. Entstehung, Funktion, Arbeitsweise 89

9.2 Wesentliche Ergebnisse 92
9.2.1 Vorläufige Verwaltungsvorschriften zum BDSG 92
9.2.2 Bankaufskunftsverfahren 92
9.2.3 SCHUFA-Verfahren 93
9.2.4 Klauseln der Versicherungswirtschaft 94
9.2.5 Novellierung des BDSG 98
9.2.6 Sonstiges 98

9.3 Zusammenfassung 100

10. Grenzüberschreitender Datenverkehr 100

S t i c h w o r t v e r z e i c h n i s 104

MMV10/2589

Der Innenminister
des Landes
Nordrhein-Westfalen

1

Der Innenminister NRW, Postfach 1103, 4000 Düsseldorf 1

Haroldstraße 5, Düsseldorf

Telex 08 58 27 49 imv d
Telefax (0211) 871 3355
Telefon (0211) 8711
Durchwahl 871 2251

An den
Präsidenten des Landtags
Nordrhein-Westfalen
4000 Düsseldorf

LANDTAG
NORDRHEIN-WESTFALEN
10. WAHLPERIODE
VORLAGE
10/2589

Datum 17.12.1989
Aktenzeichen I A 5
(Bei Antwort bitte angeben)

Betr.: 1. Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörden

Die Landesregierung hat in der Kabinettsitzung am 12. Dezember 1989 den 1. Bericht über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörden beschlossen.

Unter Bezugnahme auf § 27 des Datenschutzgesetzes Nordrhein-Westfalen (DSG NW) lege ich namens der Landesregierung den Bericht in 300-facher Ausfertigung vor.

(Dr. Herbert Schnoor)

MMV10/2589

1

Überblick

1. Die Datenschutzaufsicht über den im Bundesdatenschutzgesetz geregelten Datenschutz im nicht-öffentlichen Bereich obliegt in Nordrhein-Westfalen dem Regierungspräsidenten Arnsberg für Westfalen und dem Regierungspräsidenten Köln für das Rheinland; oberste Aufsichtsbehörde ist der Innenminister (1.).

2. Die Konzentration der Datenschutzaufsicht bei zwei Regierungspräsidenten hat sich bewährt (5.4).

3. Die Kontrolltätigkeit der Aufsichtsbehörden hat positive Ergebnisse erbracht; die Zahl der Verstöße, bei denen es zu keiner Einigkeit mit den Aufsichtsbehörden kam, liegt im Bereich von wenigen Prozentpunkten (5.4).

4. Ungeachtet fehlender Kontrollbefugnisse werden die Aufsichtsbehörden in erheblichem Maße von Bürgern hinsichtlich der Zulässigkeit der Datenverarbeitung in Akten in Anspruch genommen (6.).

5. Auch im Bereich der nicht-dateimäßigen Datenverarbeitung in Akten ist eine Reihe von Verstößen gegen das Grundrecht auf Datenschutz festgestellt worden (6.).

6. Die immer zahlreicheren zentralen Warndateien zur Beurteilung wirtschaftlicher Risiken bedürfen besonderer Beobachtung, weil sie insbesondere in kaum kontrollierbarer Weise ungesicherte Verdachtsmomente enthalten können, die wünschenswerte Transparenz für die Betroffenen häufig nicht gewährleisten und vielfach die Systemverantwortlichkeit nicht in einer Hand konzentrieren (7.2).

MMV10/2589

7. Briefkastenwerbung wird unzulässig, wenn der Betroffene ihr widerspricht. Telefonwerbung setzt die vorherige Einwilligung des Betroffenen voraus.(7.4)

8. Bei der Datensicherung bestehen im nicht-öffentlichen Bereich im wesentlichen die gleichen Probleme wie im Bereich der öffentlichen Verwaltung, z.B. beim Einsatz von persönlichen Computern (8.).

9. Die Zusammenarbeit der obersten Aufsichtsbehörden der Länder für den Datenschutz im nicht-öffentlichen Bereich im "Düsseldorfer Kreis" unter Federführung Nordrhein-Westfalens gibt der Aufsichtspraxis unverzichtbare Impulse. Die Verhandlungen des "Düsseldorfer Kreises" mit Spitzenverbänden der Wirtschaft zur Verbesserung des Datenschutzes haben überwiegend zu tragfähigen Kompromissen geführt und müssen trotz z.T. bestehender Meinungsunterschiede fortgesetzt werden. (9.)

10. Vor allem im Zeichen des bevorstehenden EG-Binnenmarkts kann der steigende Transfer personenbezogener Daten ins Ausland nur verantwortet werden, wenn in allen Empfängerstaaten gleichwertiges Datenschutzrecht besteht und fehlende nationale Regelungen so weit wie möglich durch vertragliche Datenschutzverpflichtungen der Wirtschaft im In- und Ausland kompensiert werden (10.).

MMV10/2589

1. Einführung

Das Datenschutzgesetz Nordrhein-Westfalen in der Fassung des Gesetzes zur Fortentwicklung des Datenschutzes vom 15. März 1988 (GV.NW.S. 160) sieht in § 27 erstmals vor, daß die Landesregierung einen Bericht über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörden gibt. Der Bericht ist dem Landtag gleichzeitig mit der Stellungnahme der Landesregierung zu dem Tätigkeitsbericht des Landesbeauftragten für den Datenschutz zu erstatten, den dieser der Landesregierung jeweils für zwei Kalenderjahre hinsichtlich des Datenschutzes im öffentlichen Bereich des Landes vorlegt.

Die allgemeinen Regelungen für den Datenschutz im nicht-öffentlichen Bereich trifft das Bundesdatenschutzgesetz (BDSG). Die externe Datenschutzaufsicht in diesem Bereich wird von den nach Landesrecht zuständigen Aufsichtsbehörden wahrgenommen (§§ 30/40 BDSG). In Nordrhein-Westfalen sind dies

- der Regierungspräsident Arnsberg für die Regierungsbezirke Arnsberg, Detmold und Münster sowie
- der Regierungspräsident Köln für die Regierungsbezirke Düsseldorf und Köln.

Oberste Aufsichtsbehörde ist der Innenminister.

In den anderen Bundesländern besteht eine gesetzliche Verpflichtung zur Erstattung von Tätigkeitsberichten über den Datenschutz im nicht-öffentlichen Bereich bislang nur in Hessen, wo in den Jahren 1988 und 1989 die ersten beiden Berichte dieser Art erschienen.

Der Berichtszeitraum des hier vorgelegten ersten Berichts erstreckt sich (in Orientierung an dem neunten Tätigkeitsbericht des Landesbeauftragten für den Datenschutz) auf die

Jahre 1987 und 1988. In seinen allgemeinen Aussagen erfaßt er darüber hinaus aus früherer Zeit wesentliche Entwicklungslinien des Datenschutzes im nicht-öffentlichen Bereich seit Inkrafttreten des Bundesdatenschutzgesetzes, um den erreichten Stand des Datenschutzes im nicht-öffentlichen Bereich zu verdeutlichen. Ebenfalls im Blick auf grundsätzliche Fragen wird für das Jahr 1989 insbesondere auf die aktuellen Bestrebungen zur Novellierung des Bundesdatenschutzgesetzes eingegangen.

2. Regelungskonzept des BDSG für den Datenschutz im nicht-öffentlichen Bereich; Novellierung

2.1 Geltendes Recht

Das BDSG regelt den Datenschutz im nicht-öffentlichen Bereich im wesentlichen im 3. und 4. Abschnitt. Daneben gelten die allgemeinen Vorschriften des 1. Abschnitts sowie des 5. Abschnitts (Straf- und Bußgeldvorschriften).

2.1.1 Stellen des privaten Rechts

Im nicht-öffentlichen Bereich schützt das BDSG personenbezogene Daten, die von natürlichen oder juristischen Personen, Gesellschaften oder anderen Personenvereinigungen des privaten Rechts

- für eigene Zwecke (3. Abschnitt, §§ 22 bis 30) oder
- geschäftsmäßig für fremde Zwecke (4. Abschnitt, §§ 31 bis 40)

in Dateien gespeichert, verändert, gelöscht oder aus Dateien übermittelt werden.

Der 3. Abschnitt gilt, soweit nicht-öffentliche Stellen personenbezogene Daten als Hilfsmittel für die Erfüllung

ihrer eigenen Geschäftszwecke oder Ziele verarbeiten, beispielsweise für Banken, Handel, Industrie, Wohnungsunternehmen, Versicherungen, freie Berufe, Vereine und Parteien im Hinblick auf Daten etwa von Kunden, Arbeitnehmern, Mietern, Patienten und Vereinsmitgliedern. Der 4. Abschnitt gilt u.a. für Auskunfteien, Adreßhändler, Direktwerbeunternehmen, Markt- und Meinungsforschungsinstitute sowie Service-Rechenzentren.

Die Abgrenzung zwischen dem 3. und 4. Abschnitt kann im Einzelfall problematisch sein. Stellen, die sowohl Zwecke des 3. als auch des 4. Abschnitts verfolgen, müssen beide Abschnitte beachten, soweit diese für ihre Tätigkeit in Betracht kommen. So gilt für den Inhaber einer Videothek hinsichtlich der Verarbeitung der Daten seiner Kunden der 3. Abschnitt; betreibt er zugleich für sich und andere Videotheken eine Warndatei zum Schutz gegen Unterschlagung von Kassetten (s. 7.2.6), findet insoweit der 4. Abschnitt Anwendung.

Vom Geltungsbereich des Gesetzes ausgenommen sind nichtöffentliche Stellen, soweit sie in nicht automatisierten Verfahren personenbezogene Daten, die nicht zur Übermittlung an Dritte bestimmt sind, verarbeiten (sog. interne Datenverarbeitung); insoweit gilt lediglich die Vorschrift über technische und organisatorische Maßnahmen (§ 6). Den Vorschriften des BDSG unterliegen ferner nicht die Unternehmen oder Hilfsunternehmen der Presse, des Rundfunks und des Films, soweit diese personenbezogene Daten ausschließlich zu eigenen publizistischen Zwecken verarbeiten (sog. Presseprivileg); auch hier muß von Gesetzes wegen nur die Datensicherung gewährleistet sein.

2.1.2 Zulässigkeit der Datenverarbeitung

Nach dem 3. Abschnitt ist die Datenverarbeitung zulässig

- im Rahmen der Zweckbestimmung eines Vertragsverhältnisses,
- im Rahmen der Zweckbestimmung eines vertragsähnlichen Vertrauensverhältnisses oder
- soweit es zur Wahrung berechtigter Interessen der datenverarbeitenden Stelle erforderlich ist und dadurch schutzwürdige Belange des Betroffenen (nur natürliche Personen) nicht beeinträchtigt werden.

Der 4. Abschnitt erlaubt die Datenspeicherung, soweit kein Grund zur Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden. Übermittelt werden dürfen Daten, wenn der Empfänger ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat; auch hier bedarf es jeweils einer Gewichtung des in Rede stehenden Eingriffs in das informationelle Selbstbestimmungsrecht.

Für die aus Dateien erfolgende Übermittlung von listenmäßig oder sonst zusammengefaßten Daten bestimmter Art wie Name und Anschrift genügt es nach dem 3. und dem 4. Abschnitt - mit Unterschieden bei den Datenarten -, daß bei summarischer Prüfung kein Grund zur Annahme der Beeinträchtigung schutzwürdiger Belange besteht. "Schwarze Listen" mit Negativangaben über Mitbürger dürfen daher nicht übermittelt werden.

Erlaubt weder das BDSG noch eine andere Rechtsvorschrift die Verarbeitung personenbezogener Daten im nicht-öffentlichen Bereich, so ist diese nur mit ausdrücklicher Einwilligung des Betroffenen zulässig, was grundätzlich eine schriftliche Erklärung voraussetzt.

2.1.3 Rechte des Betroffenen, Pflichten der datenverarbeitenden Stellen

Jeder Betroffene hat nach Maßgabe des BDSG ein Recht auf Auskunft über die zu seiner Person gespeicherten Daten sowie auf Berichtigung, Sperrung und Löschung seiner Daten. Er ist ferner von der datenverarbeitenden Stelle grundsätzlich zu benachrichtigen, wenn zu seiner Person erstmals Daten gespeichert (3. Abschnitt) oder erstmals übermittelt (4. Abschnitt) werden. Bei Übermittlungen nach dem 4. Abschnitt sind die Gründe für das Vorliegen eines berechtigten Interesses und die Mittel für ihre glaubhafte Darlegung aufzuzeichnen.

Die datenverarbeitenden Stellen haben für ihren Bereich im Wege der Selbstkontrolle die Einhaltung der Vorschriften des BDSG sowie anderer Rechtsvorschriften über den Datenschutz zu gewährleisten. Ab einer gewissen Größenordnung (Beschäftigung von mindestens 5 bzw. 20 Arbeitnehmern) müssen sie intern einen Beauftragten für den Datenschutz bestellen, der die Ausführung des BDSG sowie bereichsspezifischer Datenschutzvorschriften außerhalb des BDSG sicherzustellen hat. Zusätzlich sind die Adressaten des 4. Abschnitts verpflichtet, die Aufnahme ihrer Tätigkeit bei der zuständigen Aufsichtsbehörde anzumelden sowie bestimmte Angaben über Datenverarbeitung und Organisation zu dem bei der Aufsichtsbehörde geführten Register mitzuteilen, hinsichtlich dessen jedermann ein Einsichtsrecht zusteht.

2.1.4 Datensicherung

Die nicht-öffentlichen Stellen haben nach dem BDSG prinzipiell dieselben technischen und organisatorischen Maßnahmen zur Sicherung der Daten gegen unbefugten Zugriff etc. zu treffen wie die öffentlichen Stellen des Bundesbereichs. Im

Vergleich zu den öffentlichen Stellen des Landesbereichs ist festzuhalten, daß für diese hinsichtlich der Datensicherungspflichten das neue Datenschutzgesetz Nordrhein-Westfalen teilweise höhere Anforderungen stellt, etwa bei der Übermittlungskontrolle.

2.1.5 Aufsichtsbehörden

Im Bereich des 3. Abschnitts ist der zuständigen Aufsichtsbehörde lediglich eine "Anlaßaufsicht" zugewiesen (§ 30). Sie kann die Beachtung des Datenschutzes nur im Einzelfall überprüfen, wenn ein Betroffener begründet darlegt, daß er bei der Verarbeitung seiner Daten in seinen Rechten verletzt worden ist. Aufgrund sonstiger Hinweise, wie z.B. Meldungen der Medien, darf die Aufsichtsbehörde hingegen nicht tätig werden, was eine Beratung und sonstige Hinweise aber nicht ausschließt. Bei der geschäftsmäßigen Datenverarbeitung für fremde Zwecke nach dem 4. Abschnitt ist die Aufsichtsbehörde zusätzlich zur Anlaßaufsicht berechtigt und verpflichtet, die rechtmäßige Ausführung der Datenschutzvorschriften von Amts wegen zu überwachen und zu diesem Zweck Kontrollen vorzunehmen (§ 40).

Nach beiden Abschnitten hat die Aufsichtsbehörde den betrieblichen Datenschutzbeauftragten zu unterstützen, wenn er sich an sie wendet. Bei der Ausübung der Kontrollrechte nach dem 3. und 4. Abschnitt sind der Aufsichtsbehörde von den kontrollierten Stellen auf Verlangen grundsätzlich die erforderlichen Auskünfte zu erteilen. Sie ist berechtigt, Grundstücke und Geschäftsräume zu betreten, dort Prüfungen und Besichtigungen vorzunehmen sowie in die geschäftlichen Unterlagen, die gespeicherten personenbezogenen Daten und die Datenverarbeitungsprogramme Einsicht zu nehmen. Die Auskunfspflichtigen haben diese Maßnahmen zu dulden.

Nach dem geltenden Recht besitzt die Aufsichtsbehörde keine Anordnungsbefugnisse. Unberührt bleiben aber Untersagungsmöglichkeiten nach der Gewerbeordnung, wenn sich die Unzuverlässigkeit eines Gewerbetreibenden aus der Nichtbeachtung datenschutzrechtlicher Vorschriften ergibt. Festgestellte Verstöße kann die Aufsichtsbehörde unter Darlegung ihrer Rechtsauffassung nur beanstanden; eine förmliche Beanstandung im Sinne des Datenschutzgesetzes Nordrhein-Westfalen sieht das BDSG allerdings nicht vor. Um so maßgeblicher ist die "Kraft der Argumente".

2.2 Novellierung des BDSG

2.2.1 Sachstand

Nachdem im Jahre 1986 schon einmal ein Regierungsentwurf u.a. zur Änderung des BDSG im Bundestag eingebracht worden war und der Diskontinuität anheimfiel, folgte im Frühjahr 1989 ein zweiter, nämlich der Entwurf eines Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes (Bundestagsdrucksache 11/4306). Die SPD-Fraktion des Deutschen Bundestages hatte im Dezember 1988 im Bundestag den Entwurf eines Gesetzes zum Schutz personenbezogener Informationen (Bundes-Informationsschutzgesetz - BISG -, Bundestagsdrucksache 11/3730) eingebracht; sie war zuvor bereits im Jahre 1984 in ähnlicher Weise initiativ geworden.

Im Rahmen des Gesetzgebungsverfahrens gab der Bundesrat im Februar 1989 zu dem Regierungsentwurf eine Stellungnahme ab. Der Innenausschuß des Bundestages führte im Juni 1989 eine öffentliche Anhörung durch, in der auch Vertreter der obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich (u.a. des Innenministers Nordrhein-

Westfalen) zu Wort kamen. Die Ergebnisse des Gesetzgebungsverfahrens bleiben abzuwarten.

2.2.2 Verfassungsrechtliche Vorgaben für den nicht-öffentlichen Bereich

Die aktuellen Entwürfe sehen auch im nicht-öffentlichen Bereich eine Neufassung des BDSG vor, um Konsequenzen aus dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15.12.1983 (BVerfGE 65, 1) zu ziehen.

Nach dem Grundgesetz sind die Schutzvorschriften zur Sicherung des Rechts auf informationelle Selbstbestimmung mit anderen Grundrechten der am Privatrechtsverkehr Beteiligten zueinander in ein ausgewogenes Verhältnis zu bringen (vgl. u.a. BVerfGE 39, 1, 41; BAG, Urteil vom 22.10.1986, NJW 1987, 2459 - Telefondaten -). In diesem Rahmen gelangen die zum informationellen Selbstbestimmungsrecht entwickelten Grundsätze zur Anwendung, nämlich insbesondere der Grundsatz der Selbstbestimmung (vgl. BAG, Urteil vom 6.6.1984, NJW 1984, 2910 - Personalfragebogen - ; BGH, Urteil vom 20.12.1988, NJW 1989, 902 -Briefkastenwerbung-), der Grundsatz der Verhältnismäßigkeit (vgl. BGH, Urteil vom 17.12.1985, NJW 1986, 2505 - Ein-Mann-GmbH -) und der Grundsatz der Zweckbindung (vgl. BVerfG, Beschluß vom 25.7.1988, NJW 1988, 3009 - Schuldnerverzeichnis -).

2.2.3 Erweiterung des Anwendungsbereichs

Der SPD-Entwurf bezieht im Gegensatz zum Regierungsentwurf die nicht-dateimäßige Datenverarbeitung sowie die Phase der Erhebung ein. Der Bundesrat hatte sich in seiner Stellungnahme dafür eingesetzt, daß im nicht-öffentlichen Bereich auch für personenbezogene Daten, die in Akten enthalten

sind, angemessene Schutzvorschriften geschaffen werden und die Datenerhebung dabei einbezogen wird. Beide Entwürfe regeln nunmehr die Zulässigkeit der "Nutzung" von Daten.

Bereichsspezifische Regelungen finden sich erstmals in beiden Entwürfen zur Datenverarbeitung für wissenschaftliche Zwecke. Zusätzlich zum Regierungsentwurf enthält der SPD-Entwurf ferner spezielle Rechtsvorschriften zu den Bereichen Arbeitnehmerdatenschutz, Fernmessen und Fernwirken sowie Video-Überwachung und -Aufzeichnung. Die Regelungen zur Direktwerbung sind - in Anlehnung an die Europaratsempfehlung Nr. R (85) 20 - wesentlich differenzierter. Zwar will auch der Regierungsentwurf dem Betroffenen ein Recht zum Widerspruch gegen Übermittlungen zu Werbezwecken gewähren, doch verpflichtet der SPD-Entwurf weitergehend die datenverarbeitende Stelle, ihn rechtzeitig zu unterrichten, damit er schon vor der Übermittlung Gelegenheit zur Kenntnisnahme und zum Widerspruch erhält.

2.2.4 Erlaubnisnormen auch künftig Generalklauseln

Als Mangel im Sinne der Normenklarheit mag erscheinen, daß die generalklauselartige Fassung der die Datenverarbeitung ermöglichenden Erlaubnisnormen gegenüber dem geltenden Recht nicht wesentlich präzisiert wurde. Überzeugende Alternativen können wohl nur bereichsspezifisch in Ansehung konkret genannter Verwendungszwecke gefunden werden. Solange und soweit ein bereichsspezifischer Datenschutz im nicht-öffentlichen Bereich nicht zur Verfügung steht, sind allgemein formulierte Befugnisse nicht zu entbehren.

2.2.5 Erweiterung der Rechte des Betroffenen

Besonders hervorzuheben ist die Erweiterung des Auskunftsrechts in beiden Entwürfen. Es soll sich nunmehr auch auf den Zweck der Speicherung sowie auf Herkunft und Empfänger der Daten erstrecken, wobei im Detail teilweise Unterschiede bestehen. Der Regierungsentwurf normiert im Bereich der Datenverarbeitung für eigene Zwecke eine Löschungspflicht bei Wegfall der Erforderlichkeit der Datenverarbeitung, während nach dem SPD-Entwurf in Beibehaltung der derzeitigen Rechtslage die Löschung nur auf Antrag des Betroffenen erfolgen muß. Beide Entwürfe führen eine Gefährdungshaftung hinsichtlich der automatisierten Datenverarbeitung ein. Nach dem Regierungsentwurf soll diese nicht eingreifen, wenn die speichernde Stelle die fehlende Ursächlichkeit der automatisierten Datenverarbeitung oder des Versagens automatisierter Sicherungseinrichtungen nachweist.

2.2.6 Erweiterung der Befugnisse der Aufsichtsbehörden

Die Befugnisse der Aufsichtsbehörden sollen gestärkt werden. Übereinstimmend ist beabsichtigt, die Anlaßaufsicht bei der Datenverarbeitung für eigene Zwecke über Beschwerden Betroffener hinaus auch dann zu ermöglichen, wenn die Aufsichtsbehörden auf sonstige Weise - etwa durch die Medien oder aufgrund von Hinweisen Dritter - Anhaltspunkte für das Vorliegen von Datenschutzverstößen gewinnen. Im Bereich der Datensicherung sollen den Aufsichtsbehörden nunmehr in gewissem Umfang Anordnungs- und Untersagungsbefugnisse zugestanden werden, nach den Vorstellungen des SPD-Entwurfs auch im Blick auf die Einhaltung der materiellen Datenschutzvorschriften.

3. Zuständigkeiten, Organisation und personelle Ausstattung der Datenschutzaufsicht bei den Aufsichtsbehörden

Neben ihrer zentralen Zuständigkeit als Aufsichtsbehörden nach §§ 30,40 BDSG ist den Regierungspräsidenten Arnsberg und Köln die Zuständigkeit für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach § 42 BDSG übertragen (Verordnung über Zuständigkeiten nach dem Bundesdatenschutzgesetz vom 10. Januar 1978 - GV.NW.S.16 -).

Darüber hinaus sind sie zuständige Behörden für Maßnahmen nach Artikel 12 des Bildschirmtext-Staatsvertrages (Verordnung über die Zuständigkeiten nach dem Bildschirmtext-Staatsvertrag vom 5. Juli 1983 - GV.NW.S.1049-). Nach dem Bildschirmtext-Staatsvertrag haben sie die Befugnis, auch ohne Beschwerden Betroffener mittels Bildschirmtext begangene Datenschutzverstöße festzustellen und in letzter Konsequenz das Anbieten von Informationen und anderen Diensten zu untersagen, wenn dies aus Gründen des Gemeinwohls geboten ist, der Zweck der Untersagung nicht in anderer Weise erreicht werden kann und die Maßnahme nicht außer Verhältnis zur Bedeutung des Angebots für den Anbieter und die Allgemeinheit steht. Der Bildschirmtext-Staatsvertrag betrifft den nicht-öffentlichen wie den öffentlichen Bereich.

Schließlich haben die Regierungspräsidenten Arnsberg und Köln die Aufgabe, im öffentlichen Bereich gegen Ordnungswidrigkeiten nach § 34 des Datenschutzgesetzes Nordrhein-Westfalen vorzugehen (§ 34 Abs. 3 DSG NW).

Organisatorisch werden die vorgenannten Zuständigkeiten jeweils vom Dezernat 21 wahrgenommen, dem schwerpunktmäßig

Aufgaben des allgemeinen Ordnungsrechts und des Ausländerrechts sowie Einbürgerungsangelegenheiten zugewiesen sind.

Die Aufgaben der Datenschutzaufsicht werden personell wie folgt wahrgenommen (in Klammern: Besoldungs-/Vergütungsgruppe):

	RP Arnsberg	RP Köln
Juristen	1 (A 15)	1 (A 14)
Verwaltungssachbearbeiter	1 (A 11)	1 (A 11)
technische Prüfer	1 (BAT II a, z.Zt. IV a)	2 (BAT II a)

Die Juristen sind gleichzeitig Hauptdezernent des Dezernats 21. Der Anteil ihrer datenschutzrechtlichen Tätigkeit an der Gesamttätigkeit beträgt etwa 25 % (Arnsberg) bzw. rd. 20 % (Köln). Die Verwaltungssachbearbeiter sind mit ca. 90 % (Arnsberg) bzw. ca. 75 % (Köln) mit Angelegenheiten der Datenschutzaufsicht befaßt. Die technischen Prüfer, bei denen es sich um Programmierer und Informatiker handelt, die teilweise bei Unternehmen der Wirtschaft tätig waren, sind ausschließlich im Bereich der Datenschutzaufsicht tätig und prüfen vornehmlich Fragen der Datensicherung.

Wenn nach der Novellierung des BDSG (2.2) der Umfang der Aufsichtstätigkeit insbesondere durch Erweiterung der Aufsichtsbefugnisse deutlich zunehmen wird, muß die Frage der personellen Ausstattung neu geprüft werden, zumal bereits derzeit eine volle Auslastung gegeben ist und immer wieder Engpässe auftreten.

4. Meldungen zum Register der Aufsichtsbehörden

Die privaten Stellen, die geschäftsmäßig personenbezogene Daten für fremde Zwecke verarbeiten und damit den Vorschriften des 4. Abschnitts des BDSG unterliegen, haben nach § 39 BDSG der Aufsichtsbehörde folgende Angaben zu dem bei ihr geführten Register mitzuteilen:

1. Name oder Firma der Stelle,
2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzlich oder verfassungsmäßig berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
3. Anschrift
4. Geschäftszwecke oder Ziele der Stelle und der Datenverarbeitung,
5. Art der eingesetzten automatisierten Datenverarbeitungsanlagen,
6. Name des Beauftragten für den Datenschutz,
7. Art der von der meldenden Stelle oder in ihrem Auftrag gespeicherten personenbezogenen Daten,
8. bei regelmäßiger Übermittlung personenbezogener Daten Empfänger und Art der übermittelten Daten.

Nach den bisherigen Erfahrungen wird das der Öffentlichkeit zugängliche Register nur in seltenen Fällen eingesehen. Als Hilfsmittel der Aufsichtsbehörden für ein schwerpunkt- und planmäßiges Tätigwerden hat es sich jedoch hervorragend bewährt.

Mit Stand 31.12.1988 waren zum Register der Aufsichtsbehörden folgende Stellen gemeldet:

a) Stellen, die geschäftsmäßig personenbezogene Daten zum Zwecke der Übermittlung speichern und übermitteln (§ 31 Absatz 1 Satz 1 Nr. 1 BDSG)

	RP Arnsberg	RP Köln
Adreßhandel, Direktmarketing	9	15
Auskunfteien, Warndienste	43	57
gesamt:	52	72

b) Stellen, die geschäftsmäßig personenbezogene Daten zum Zweck der Veränderung speichern, anonymisieren und anonymisiert übermitteln (§ 31 Abs. 1 Satz 1 Nr. 2 i.V.m. § 36 BDSG)

	RP Arnsberg	RP Köln
Markt- und Meinungsforschungsinstitute	5	17

c) Stellen, soweit sie geschäftsmäßig personenbezogene Daten im Auftrag als Dienstleistungsunternehmen verarbeiten (§ 31 Abs. 1 Satz 1 Nr. 3 i.V.m. § 37 BDSG)

RP Arnsberg	RP Köln
295	381

In diesen Zahlen sind u.a. erfaßt Service-Rechenzentren, Datenerfassungsbüros, Buchführungshelfer, Lettershops und Datenlöschungsunternehmen.

d) Gemeldete Unternehmen nach a) bis c) insgesamt

RP Arnsberg	RP Köln
352	470

MMV10/2589

Es kann vermutet werden, daß die meldepflichtigen Stellen ihrer Meldepflicht ganz überwiegend nachgekommen sind. Die genaue Zahl aller Meldepflichtigen und meldepflichtigen Tätigkeiten läßt sich praktisch nicht ermitteln, da die Firmenbezeichnungen in Branchenverzeichnissen, Handelsregistern, Gewerberegistern etc. die Zugehörigkeit zu einer der in § 39 Abs. 1 BDSG genannten drei Gruppen häufig nicht erkennen lassen. Soweit aber Anhaltspunkte für das Bestehen einer Meldepflicht vorliegen, gehen die Aufsichtsbehörden ihnen nach.

5. Übersicht über die Kontrolltätigkeit der Aufsichtsbehörden

Hervorgehoben sei zunächst, daß die Datenschutzaufsicht der Regierungspräsidenten in enger Abstimmung mit dem Innenminister als oberster Aufsichtsbehörde erfolgt, etwa durch Berichte und Erlasse zu Grundsatzfragen und gemeinsame Dienstbesprechungen. Der Innenminister seinerseits berät sich regelmäßig mit den Vertretern der anderen obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich ("Düsseldorfer Kreis", s. unten 9.).

Die nachfolgenden Übersichten beziehen sich auf die Kontrolltätigkeit im Rahmen des BDSG. Hinsichtlich des Bildschirmtext-Staatsvertrages sind den Aufsichtsbehörden Datenschutzverstöße nicht bekanntgeworden, wohl aber andere Verstöße, etwa gegen die Bestimmungen über Entgelt, Werbung und Angebotszuordnung. Die Regierungspräsidenten Arnsberg und Köln verfügen zur Wahrnehmung ihrer Aufsichtsaufgaben über Btx-Anschlüsse.

5.1 Beschwerden, Anfragen und Beratungsersuchen

In den Jahren 1987 und 1988 sind gegen datenverarbeitende Stellen, die dem 3. Abschnitt des BDSG unterliegen und für die lediglich eine "Anlaßaufsicht" besteht (vgl. 2.1.5), beim Regierungspräsidenten Arnsberg insgesamt 102 Beschwerden und beim Regierungspräsidenten Köln 256 Beschwerden eingegangen. Gegen private Stellen, die geschäftsmäßig personenbezogene Daten für fremde Zwecke verarbeiten (4. Abschnitt), wurden in dem genannten Zeitraum bei dem Regierungspräsidenten Arnsberg insgesamt 99 Beschwerden und beim Regierungspräsidenten Köln 96 Beschwerden vorgebracht. In diesen Zahlen sind sowohl Betroffenenbeschwerden als auch Beschwerden anderer über allgemeine datenschutzrechtliche Mißstände und Rechtsverstöße bei den privaten Stellen enthalten. Die angegebenen Zahlen verteilen sich wie folgt:

	RP Arnsberg	RP Köln
3. Abschnitt		
Handel, Handwerk	10	65
Industrie, Großunternehmen	9	19
Krankenhäuser, Ärzte, privatärztliche Verrechnungsstellen	7	12
Kreditinstitute	14	28
Versicherungen	16	51

Vereine, Verbände	21	44
Sonstige	25	37
gesamt:	102	256
4. Abschnitt		
Adreßhandel, Direktmarketing	20	6
Auskunfteien, Warndienste	68	84
Markt- und Meinungsforschungsinstitute	6	1
Auftragsdatenverarbeitung	5	5
gesamt:	99	96

Darüber hinaus erhielten die Aufsichtsbehörden zahlreiche schriftliche Anfragen und Beratungsersuchen. Im 3. Abschnitt waren dies beim Regierungspräsidenten Arnsberg 42 und beim Regierungspräsidenten Köln 77, im 4. Abschnitt 14 (Arnsberg) und 25 (Köln). Es ergibt sich folgende Aufschlüsselung:

	RP Arnsberg		RP Köln	
	3.Abschn.	4.Abschn.	3.Abschn.	4.Abschn.
betriebliche Datenschutzbeauftragte	2	2	19	10
Geschäftsleitungen	10	5	4	7

Betriebsräte	4	-	5	1
Einzelpersonen	26	7	49	7
gesamt:	42	14	77	25

Schließlich erreicht die Aufsichtsbehörden täglich eine Reihe telefonischer Anfragen, die in ihrer Gesamtzahl mindestens derjenigen der schriftlichen Eingaben und Anfragen entspricht.

Inhaltlich richteten sich im 3. Abschnitt viele Beschwerden dagegen, daß überhaupt personenbezogene Daten gespeichert wurden. Auch wandten sich immer wieder Bürger dagegen, daß bei Abschluß von Verträgen (z.B. Kauf-, Arbeits- oder Versicherungsverträge) zu viele bzw. nicht erforderliche Daten erfragt wurden. Sehr oft haben sich Beschwerdeführer durch unerwünschte Werbezusendungen belästigt gefühlt; hierbei stellt der Beschwerdeführer zumeist die Frage, wie die werbenden Unternehmen an seine Anschrift gekommen sind. Im Bereich der Versicherungen wurde häufig angefragt, ob eine Verpflichtung zur Unterzeichnung der sog. Schweigepflichtentbindungsklausel sowie der Datenschutzklausel besteht (vgl. 9.2.4). Weitere Beschwerden richteten sich gegen die Übermittlung personenbezogener Daten an zentrale Dateien der Versicherungsverbände oder Rückfragen bei Vorversicherern.

Der Schwerpunkt der Beschwerden im Bereich des 4. Abschnitts betraf die Handelsauskunfteien sowie die SCHUFA. Die häufigsten Fragen waren:

- Dürfen Auskunfteien Daten ohne Einwilligung speichern?
- Welche Daten dürfen gespeichert werden?
- An wen hat die Auskunftei meine Daten übermittelt?
- Hat ein berechtigtes Interesse an der Kenntnis meiner Daten bestanden?
- Welche Abwehrmöglichkeiten bestehen bei Personenverwechslungen sowie der Speicherung und Übermittlung unrichtiger Daten?
- Darf für die Erteilung einer Auskunft an den Betroffenen über seine personenbezogenen Daten ein Entgelt verlangt werden?
- Hat die SCHUFA bei der sog. Selbstauskunft an den Betroffenen Auskunft über alle zu seiner Person gespeicherten Daten erteilt? (In diesem Zusammenhang wird vielfach - unzutreffend - vermutet, daß Daten über Eigentum, Höhe des Einkommens sowie Guthaben auf Giro- und Sparkonten seitens der SCHUFA gespeichert werden.)

Auch Nachbarschaftsbefragungen (vgl. 9.2.6) sind immer wieder Gegenstand von Beschwerden.

Wenn aufgrund von Beschwerden Datenschutzverstöße festgestellt wurden, so waren die datenverarbeitenden Stellen in der ganz überwiegenden Zahl der Fälle zum Einlenken bereit. Dies ist u.a. darauf zurückzuführen, daß Imageverluste bei längeren Auseinandersetzungen mit der Aufsichtsbehörde befürchtet werden. Der Anteil der Verstöße, bei denen es nicht zu einer Einigung mit der Aufsichtsbehörde kam, lag im Bereich von wenigen Prozentpunkten.

Bei allgemeinen Anfragen wurde zumeist um Mitteilung gebeten, inwieweit die Speicherung einzelner Daten oder die Übermittlung zulässig ist (z.B., ob eine Mitgliederliste an Dritte herausgegeben werden darf).

Vielfach werden die Aufsichtsbehörden nicht im Wege der Kontrolle, sondern der Beratung tätig, die vor allem von datenverarbeitenden Stellen (einschließlich betrieblicher Datenschutzbeauftragter und Betriebsräte) oft ausdrücklich gewünscht wird. Die Beratungsersuchen beziehen sich häufig auf die ordnungsgemäße Bestellung des Datenschutzbeauftragten, so z.B.:

- Welche persönlichen Voraussetzungen muß der Beauftragte erfüllen?
- Wann muß ein Datenschutzbeauftragter bestellt werden?
- Besteht Interessenkollision, wenn etwa der Leiter der EDV oder der Personalleiter zum Datenschutzbeauftragten bestellt wird?

Insbesondere sind aber auch Datensicherungsmaßnahmen (z.B. beim Neubau eines Rechenzentrums) Gegenstand von Beratungsgesprächen, die z.T. vor Ort in dem betreffenden Unternehmen stattfinden.

5.2 Überprüfungen vor Ort

Der folgenden Übersicht sind die Zahlen der Überprüfungen vor Ort in den Jahren 1987 und 1988 zu entnehmen. Diese Überprüfungen haben entweder im Rahmen der regelmäßigen Überwachung nach § 40 BDSG bei Stellen des 4. Abschnitts oder aus konkretem Anlaß stattgefunden, d.h. aufgrund von Beschwerden und sonstiger Hinweise.

a) regelmäßige Überwachung (4. Abschnitt)

RP Arnsberg	RP Köln
74	167

b) konkrete Anlässe

	RP Arnsberg	RP Köln
3. Abschnitt	4	48
4. Abschnitt	9	19
gesamt:	13	67

c) Summe von a) und b)

RP Arnsberg	RP Köln
87	234

Zu der Anzahl der Überprüfungen beim Regierungspräsidenten Arnsberg muß angemerkt werden, daß im 1. Halbjahr 1987 infolge Ausscheidens des bisherigen Stelleninhabers ein technischer Prüfer nicht zur Verfügung stand und die Überprüfungen vor Ort auch in der Einarbeitungszeit des neuen Prüfers auf ein Minimum reduziert werden mußten. Von den 87 Überprüfungen des Regierungspräsidenten Arnsberg entfielen 59 allein auf das Jahr 1988. Wenn selbst angesichts dieser Bereinigung die Zahl der Überprüfungen beim Regierungspräsidenten Köln ungleich höher ist, so muß u.a. bedacht werden, daß dieser Aufsichtsbehörde zwei technische Prüfer zur Verfügung stehen.

Bei den regelmäßigen Überprüfungen der Stellen des 4. Abschnitts nahmen Fragen der Datensicherung (§ 6 BDSG und Anlage zu § 6) und der Beachtung organisatorischer Schutzvorschriften den breitesten Raum ein. Hier wurden sehr häufig Mängel angetroffen, die aber oft kleinerer Art waren und meist auf Anregung der Aufsichtsbehörden schon im eigenen Interesse abgestellt wurden. Die Skala dieser Mängel reicht von fehlerhaften Bestellungen des betrieblichen Datenschutzbeauftragten, unterbliebenen Änderungsmeldungen zum Register, unvollständigen Übersichten und mangelndem

Paßwortschutz bis hin zu ungenügender Auftragskontrolle und lückenhafter Aufgabenschreibung für die in der Datenverarbeitung tätigen Personen (vgl. auch 8.1).

5.3 Bußgeldverfahren

Ordnungswidrig handelt nach § 42 BDSG u.a., wer den Betroffenen nicht über die erstmalige Speicherung bzw. erstmalige Übermittlung seiner Daten benachrichtigt, nicht oder nicht rechtzeitig einen betrieblichen Datenschutzbeauftragten bestellt, gegen die Pflicht der Meldung zum Register verstößt oder der Aufsichtsbehörde bei Überprüfungen ihr zustehende Rechte verwehrt. Ordnungswidrigkeiten können mit einer Geldbuße bis zu fünfzigtausend Deutsche Mark geahndet werden.

In den ersten Jahren nach Inkrafttreten des BDSG wurden zahlreiche Ordnungwidrigkeitenverfahren eingeleitet. Den Schwerpunkt der Verstöße bildete die nicht oder verspätet erfolgte Meldung der Stellen des 4. Abschnitts zum Register der Aufsichtsbehörde. Im Laufe der Zeit nahmen die Verstöße bezüglich der Meldepflicht jedoch zunehmend ab, nicht zuletzt aufgrund publizierter Informationen der Aufsichtsbehörden.

In den Jahren 1987 und 1988 leiteten die Aufsichtsbehörden folgende Bußgeldverfahren ein:

	RP Arnsberg	RP Köln
3. Abschnitt	-	2
4. Abschnitt	4	1

Die vier Verfahren des Regierungspräsidenten Arnsberg betrafen Verstöße gegen die Meldepflicht. Zwei Verfahren wur-

den mit Festsetzung einer Geldbuße bestandskräftig abgeschlossen, zwei Verfahren waren Ende 1988 noch anhängig. Die zwei Verfahren des Regierungspräsidenten Köln im Bereich des 3. Abschnitts bezogen sich auf Auskunftsverweigerungen der datenverarbeitenden Stellen gegenüber der Aufsichtsbehörde. Die Auskünfte wurden nach Androhung eines Bußgelds unverzüglich erteilt, die Bußgeldverfahren daraufhin eingestellt. Gegenstand des vom Regierungspräsidenten Köln im Bereich des 4. Abschnitts durchgeführten Bußgeldverfahrens war die nicht erfolgte Meldung eines Adreßhändlers zum Register; das Verfahren endete mit der Festsetzung einer Geldbuße.

Bei weiteren Verstößen gegen die Meldepflicht von nicht gravierender Art wurde aus Opportunitätsgründen von Ordnungswidrigkeitenverfahren abgesehen und lediglich darauf hingewiesen, daß im Wiederholungsfall mit der Festsetzung einer empfindlichen Geldbuße zu rechnen sei. Auch im Bereich der Datensicherungsmaßnahmen erscheint Zurückhaltung sinnvoll. Die Unternehmen des 4. Abschnitts sind dann wesentlich mehr zur Zusammenarbeit mit der Aufsichtsbehörde bereit und realisieren die von ihr gewünschten Maßnahmen.

5.4 Zusammenfassung

Die Konzentration der Datenschutzaufsicht bei zwei Regierungspräsidenten (Arnsberg für Westfalen, Köln für das Rheinland) hat sich bewährt. Auf diese Weise konnte sich spezieller Sachverstand entwickeln, welcher der Qualität der Aufsicht zugute kommt. Für den Bürger allerdings ist diese Zuständigkeitsverteilung zuweilen überraschend; doch hat er ohnehin oft nicht die Kenntnis, daß die Datenschutzkontrolle in Nordrhein-Westfalen bei der staatlichen Mittelinstanz liegt und nicht - wie häufig vermutet - dem Landesbeauftragten für den Datenschutz oder dem Bundesbeauftragten für

den Datenschutz zugewiesen ist. Im übrigen wird der Kontakt zur Aufsichtsbehörde zumeist schriftlich oder telefonisch hergestellt, selten aber durch persönliches Erscheinen, so daß auch von daher eine Zuständigkeitserweiterung auf alle fünf Regierungspräsidenten nicht geboten ist.

Die Kontrolltätigkeit der Aufsichtsbehörden bei der Wirtschaft hat positive Ergebnisse erbracht. Dies ist nicht zuletzt auf die Kooperationsbereitschaft der Unternehmen zurückzuführen, denen vorgekommene Verstöße gegen den Datenschutz zunächst oft nicht bewußt gewesen waren. Zu einem nicht geringen Teil besteht die Tätigkeit der Aufsichtsbehörden in Beratung, die durchaus auch von datenverarbeitenden Stellen selbst gesucht wird. Die Wirtschaft läßt sich erfreulicherweise auf Beratungen selbst in Fällen ein, in denen der Aufsichtsbehörde die Zuständigkeit fehlt, etwa bei Geltendmachung von Rechtsverletzungen Nichtbetroffener oder in Fällen nicht-dateimäßiger Datenverarbeitung.

Ungeachtet der relativ geringen Zahl von Fällen, in denen es nicht zu einer Einigung kommt, wäre jedoch eine Erweiterung der Aufsichtsbefugnisse wünschenswert, dahin zum Beispiel, daß die Aufsichtsbehörde dem Verdacht von Datenschutzverstößen auch ohne Betroffenenbeschwerden nachgehen kann (etwa aufgrund von Hinweisen in den Medien) oder daß ihr Anordnungsbefugnisse zur Beseitigung von Verstößen zugestanden werden (vgl. auch 2.2.6). Wiederholt haben betroffene Bürger der Aufsichtsbehörde erklärt, ihnen fehle das Verständnis dafür, daß im Weigerungsfall der staatlichen Aufsicht die Hände gebunden sind und der Betroffene auf den Rechtsweg verwiesen wird. Der mit Risiken in rechtlicher, zeitlicher und finanzieller Hinsicht behaftete Gang zu den Gerichten "lohnt" sich für viele nicht, wie das Faktum verhältnismäßig weniger Entscheidungen höherer Instanzen zum Datenschutz im nicht-öffentlichen Bereich zeigt. Zuweilen werden Prozesse

offenbar erst durch fremde Hilfe möglich. So haben Verbraucherverbände das Grundsatzurteil des Bundesgerichtshofs zum SCHUFA-Verfahren vom 19.9.1985 (NJW 1986, 46) und das BGH-Urteil vom 8.6.1989 (Betriebs-Berater 1989, 1777) erstritten, in welchem Telefonwerbung ohne Einverständnis des Betroffenen als Verletzung des Persönlichkeitsrechts gewertet wurde.

6. Nichteinbeziehung der Akten-Datenverarbeitung in das BDSG: Bedeutung für die Aufsichtspraxis

Das BDSG schützt nur solche personenbezogene Daten, die in Dateien gespeichert, verändert, gelöscht oder aus Dateien übermittelt werden. Akten und Aktensammlungen fallen unter den Dateibegriff nur, wenn sie durch automatisierte Verfahren umgeordnet und ausgewertet werden können (§ 2 Abs. 3 Nr. 3 BDSG). Grundsätzlich ist damit die nicht-dateimäßige Datenverarbeitung, üblicherweise bezeichnet als Datenverarbeitung in "Akten", von dem Anwendungsbereich des Gesetzes ausgenommen.

Nach der höchstrichterlichen Rechtsprechung gilt das allgemeine Persönlichkeitsrecht im nicht-öffentlichen Bereich auch außerhalb von Dateien. Dies ist beispielsweise ständige Spruchpraxis des Bundesarbeitsgerichts für die Führung von Personalakten (vgl. NJW 1988, 791 m.w.N.). Bei entgegenstehenden Interessen muß eine Güter- und Interessenabwägung vorgenommen werden, die sich am Verhältnismäßigkeitsgrundsatz orientiert (vgl. BGH NJW 1986, 46 - SCHUFA-Klausel - und NJW 1986, 2505 -Ein-Mann-GmbH-).

Eine Reihe von Beschwerdefällen und Anfragen bei den Aufsichtsbehörden betrifft die Datenverarbeitung in Akten, wie u.a. einige der unter 7. angeführten Beispielsfälle zeigen. In diesen Fällen sind ganz überwiegend Daten

schutzverstöße festgestellt worden, darunter auch solche, die tief in die Privatsphäre der Betroffenen eingriffen, z.B. Fragen einer Wohnungsbaugesellschaft an Mietbewerber über Verlobung, Trennung und Scheidung in mehrseitigen Fragebogen (7.6.1), Befragung eines früheren Arbeitgebers über Lohnpfändungen bei einem Stellenbewerber (7.6.2) sowie die Bekanntgabe des Nettoeinkommens einer Versicherungsnehmerin an den behandelnden Arzt auf dem Formblatt einer Krankentagegeldversicherung (7.11). Weitere Fälle nicht-dateimäßiger Datenverarbeitung finden sich unter 7.6.1 (Fragebogen für Stellenbewerber), 7.6.3 (geheime Auswahl für Stipendien), 7.8 (Ladendiebstahl im Verbrauchermarkt) und 7.11 (Mitteilung der Grundpfandgläubiger von Wohnungseigentümern an Verwalter). Ferner ist allgemein zu bemerken, daß in der Versicherungswirtschaft mit Hilfe zentraler Warndateien in großer Zahl z.T. sehr sensitive Daten aus Akten unter den Versicherungen ausgetauscht werden (7.2).

Insbesondere bei telefonischen Anfragen verfolgt der Betroffene seine Angelegenheit häufig nicht weiter, wenn er von der Aufsichtsbehörde erfährt, daß seine Daten nicht nach dem BDSG geschützt sind und insoweit keine Zuständigkeit der Aufsichtsbehörde gegeben ist. Andererseits verschließen sich die Aufsichtsbehörden dem Bürger nicht, wenn er gleichwohl ihre Hilfe wünscht. In derartigen Fällen nimmt die Aufsichtsbehörde Kontakt mit der datenverarbeitenden Stelle auf und ist im Wege der Beratung bemüht, daß nicht gerechtfertigte Beeinträchtigungen des Persönlichkeitsrechts abgestellt werden, was in den meisten Fällen erfreulicherweise auch gelingt.

Es kann jedoch nicht befriedigen, daß die Aufsichtsbehörden hinsichtlich der Akten-Datenverarbeitung weder eine Kontrollbefugnis besitzen, um in Weigerungsfällen ihrer Auffassung größeres Gewicht zu verleihen, noch daß ihnen klare

MMV10/2589

gesetzliche Vorgaben für die Zulässigkeit der Datenverarbeitung in Akten fehlen. Die Datenverarbeitung in Akten wird auch weiterhin die Aufsichtsbehörden beschäftigen, angesichts der Sensibilisierung durch das die Akten im öffentlichen Bereich erfassende Datenschutzgesetz Nordrhein-Westfalen eher in zunehmendem Maße.

7. Einzelprobleme, Beispielsfälle aus der Kontrolltätigkeit

In diesem Abschnitt werden wesentliche Bereiche privater Datenverarbeitung mit ihrer datenschutzrechtlichen Problematik vorgestellt und durch Beispiele aus der Praxis der Aufsichtsbehörden veranschaulicht. Mit Rücksicht darauf, daß in diesem Tätigkeitsbericht die Datenverarbeitung im nichtöffentlichen Bereich erstmals behandelt wird, muß die Darstellung - bei allem Bemühen um Straffung - teilweise ausführlicher ausfallen.

7.1 Kreditinformationssystem der SCHUFA

7.1.1 Organisation, Aufgabe, Verfahren

Die SCHUFA (Schutzgemeinschaft für allgemeine Kreditsicherung) ist eine Gemeinschaftseinrichtung der kreditgebenden Wirtschaft. Sie wird repräsentiert durch die BUNDES-SCHUFA, Vereinigung der deutschen Schutzgemeinschaften für allgemeine Kreditsicherung e.V., und 12 regionale SCHUFA-Gesellschaften in der Rechtsform der GmbH (davon 4 mit 11 Geschäftsstellen in Nordrhein-Westfalen).

Die SCHUFA betreibt ein Kreditinformationssystem, das vor Verlusten im Kreditgeschäft schützen und gleichzeitig die Möglichkeit eröffnen soll, die Kreditnehmer durch Beratung vor einer übermäßigen Verschuldung zu bewahren. Vertrags-

partner der SCHUFA können nur Unternehmen sein, die gewerbsmäßig Geld oder Warenkredite an Konsumenten geben oder gewerbsmäßig Forderungen einziehen. Hierbei handelt es sich in erster Linie um Kreditinstitute, aber auch u.a. um Versandhandelsunternehmen, Warenhäuser, Kreditkartenunternehmen, Inkassounternehmen sowie Versicherungen und Bausparkassen, soweit sie Konsumenten grundpfandrechtlich gesicherte Kredite geben. Inkassounternehmen erhalten nur Angaben, die der Adressenermittlung von Schuldnern dienen. Derzeit hat die SCHUFA etwa 20.000 Vertragspartner.

Die SCHUFA arbeitet nach dem Prinzip der Gegenseitigkeit. Auskunft erhält lediglich, wer der SCHUFA selbst Informationen gibt. Die Auskünfte beruhen auf Informationen anderer Vertragspartner oder auf Angaben aus öffentlichen Verzeichnissen (z.B. Schuldnerverzeichnis).

Die Kreditinstitute übermitteln personenbezogene Daten (bei Konsumentenkrediten Meldepflicht bis zu einem Betrag von 100.000,-- DM) nur, wenn ihre Kunden bei Kreditanträgen, Kontoeröffnungsanträgen und Bürgschaftserklärungen diesbezügliche "SCHUFA-Klauseln" unterschrieben haben. Darin erklären sie ihre Einwilligung in die Übermittlung sog. Positivdaten, d.h. Daten über vertragliche Vereinbarungen und die vereinbarungsgemäße Vertragsabwicklung (z.B. Kreditbetrag, Laufzeit, Ratenbeginn). Ferner wird in den Klauseln darauf hingewiesen, daß aufgrund gesetzlicher Erlaubnis nach dem BDSG sog. Negativdaten wegen nicht vertragsgemäßen Verhaltens der SCHUFA gemeldet werden (z.B. beantragter Mahnbescheid bei unbestrittener Forderung und Zwangsvollstreckungsmaßnahmen). Sowohl hinsichtlich der Übermittlung von Positiv- als auch von Negativdaten erklärt der Kunde zugleich die Befreiung vom Bankgeheimnis. Darüber hinaus wird u.a. mitgeteilt, daß subjektive Werturteile sowie persönliche Einkommens- und Vermögensverhältnisse in

SCHUFA-Auskünften nicht enthalten sind. Nach einem Hinweis über das Auskunftsrecht des Kunden gegenüber der SCHUFA erfolgt abschließend ein Hinweis auf ein ausführliches Merkblatt mit Einzelheiten zum SCHUFA-Verfahren, das lt. Klauseltext auf Wunsch zur Verfügung gestellt wird, jedoch bei den meisten Kreditinstituten auf der Rückseite des Klausel-Formulars abgedruckt ist.

Die SCHUFA-Klausel wird nicht verwendet von Einzelhandels- und Versandhandelsunternehmen, Waren- und Kaufhäusern sowie sonstigen Unternehmen, die Warenkredite an Privatpersonen vergeben, weil sie nur Negativdaten ohne Einwilligung aufgrund gesetzlicher Erlaubnis (BDSG) an die SCHUFA übermitteln und von dieser erhalten können. Bei Warenkrediten erhält der Kunde kein Geld, sondern Vorteile hinsichtlich der Zahlungsweise (z.B. Lieferung gegen Rechnung, Einräumung von Zahlungszielen).

7.1.2 Zulässigkeit des SCHUPA-Verfahrens

Das vorstehend skizzierte SCHUFA-Verfahren in der mit den obersten Aufsichtsbehörden für den Datenschutz vereinbarten Form (vgl. näher 9.2.3) entspricht bei einer Gesamtbetrachtung im wesentlichen den gesetzlichen Anforderungen, wie sie durch das Grundsatzurteil des Bundesgerichtshofs vom 19.9.1985 (NJW 1986, 46) präzisiert worden sind. In einigen Einzelfragen konnte allerdings bisher ein Konsens nicht gefunden werden.

Die Übermittlung von Negativdaten ist danach bei der aufgrund der §§ 24, 32 BDSG im Einzelfall vorzunehmenden Interessenabwägung grundsätzlich zulässig, weil das Ziel, potentiellen Kreditgebern die Beurteilung der Kreditwürdigkeit zu erleichtern und eine Kreditvergabe an Kreditun

würdige zu verhindern, im berechtigten Interesse der Kreditwirtschaft liegt. Das Kreditinformationssystem muß dabei so organisiert sein, daß die gespeicherten Daten insgesamt ein möglichst vollständiges, aussagekräftiges und aktuelles Bild der Kreditwürdigkeit bieten (BGH, a.a.O.).

Im Rahmen der Interessenabwägung ist zu unterscheiden zwischen "harten" und "weichen" Negativmerkmalen. Die Übermittlung harter Negativmerkmale (z.B. Zahlungsurteile, Zwangsvollstreckungsmaßnahmen) ist wegen ihrer objektiven Aussagekraft und ihres Gewichts in der Regel gerechtfertigt (vgl. näher BGH, Urteil vom 7.7.1983, NJW 1984, 436). Bei den weichen Merkmalen (z.B. beantragter Mahnbescheid bei unbestrittener Forderung, Kündigung eines Girokontos wegen mißbräuchlicher Nutzung) handelt es sich dagegen um einseitige Maßnahmen der datenverarbeitenden Stelle, bei denen genauer zu prüfen ist, ob schutzwürdige Belange des Betroffenen beeinträchtigt werden. Aus diesem Grunde unterrichten die Kreditinstitute aufgrund interner Richtlinien für ihre Mitarbeiter in solchen Fällen den Kunden über eine beabsichtigte Meldung an die SCHUFA, damit dieser seine Belange im Blick auf die endgültige Interessenabwägung rechtzeitig geltend machen kann; so wird ein etwaiger Widerspruch des Betroffenen gegen einen Mahnbescheid der SCHUFA sofort nachgemeldet.

7.1.3 Mehrfache Verwechselung eines "Unschuldigen" mit Folgen

In einem Informationssystem von der Größe des Datenbestandes der SCHUFA lassen sich Personenverwechselungen offenbar nicht ganz ausschließen, wie immer wieder in der Praxis festgestellt wird. In einem Fall waren der erste Vorname,

der Nachname und das Geburtsdatum des Beschwerdeführers (A) identisch mit den Daten eines anderen (B); Abweichungen bestanden bei dem zweiten Vornamen und bei der Adresse: A wohnte in Dortmund, B früher in Berlin, derzeitiger Aufenthalt unbekannt. Aus ungeklärten Gründen erhielten Kreditinstitute in Norddeutschland, die der SCHUFA Daten über B gemeldet hatten, von der SCHUFA die Nachricht, B habe jetzt die Anschrift des A; der zweite Vorname war dabei nicht angegeben. Der Beschwerdeführer wurde deshalb anstelle des B auf Betreiben eines der Kreditinstitute zur Abgabe einer eidesstattlichen Versicherung in einer Zwangsvollstreckungssache geladen und drei Monate später von einem anderen Kreditinstitut zur Erfüllung einer Forderung aufgefordert.

Nach einer Beanstandung durch den Rechtsanwalt des Beschwerdeführers teilte die SCHUFA mit, sie führe in ihrem Datenbestand zur Person des Beschwerdeführers den Hinweis, daß er mit B nicht identisch sei. Gleichwohl wurde etwa ein halbes Jahr später infolge einer Meldung eines norddeutschen Kreditinstituts (Gläubigerin des B) zum Datensatz des Beschwerdeführers eine uneinbringliche Forderung von ca. 49.000 DM gespeichert, was dem Beschwerdeführer eine Aufforderung seines Kreditinstituts in Dortmund zu einer Rücksprache eintrug. Nachdem der Beschwerdeführer durch seinen Anwalt erneut bei der SCHUFA vorstellig geworden war, erhielt er die Auskunft, der zwischenzeitliche Hinweis zur Identität sei leider aus dem Datensatz des Beschwerdeführers gelöscht, inzwischen jedoch erneut eingespeichert worden; außerdem sei eine Löschung hinsichtlich der uneinbringlichen Forderung von ca. 49.000 DM erfolgt, nachdem die Gläubigerbank, welche anscheinend ebenfalls die eingangs genannte Meldung über eine Anschriftenänderung erhalten hatte, die SCHUFA von dem Ergebnis ihrer Identitätsprüfung unterrichtet hatte.

Damit nicht genug, wurde der Beschwerdeführer ein Jahr später von einem Gerichtsvollzieher in einer Zwangsvollstrekkungssache angemahnt, nachdem die Gläubigerbank in Norddeutschland seine Adresse von der SCHUFA erfahren hatte. Hierzu gab die SCHUFA gegenüber der Aufsichtsbehörde an, bei der Datenverwechslung habe es sich um einen "Bedienerfehler" gehandelt, was grundsätzlich bei fast 30 Mio Auskünften im Jahr nicht auszuschließen sei. Die SCHUFA übersandte der Aufsichtsbehörde einen Datenausdruck bezüglich des Beschwerdeführers, in welchem nunmehr - im gesamten Schriftverkehr nach mehreren Datenausdrucken erstmalig - der Hinweis enthalten war, daß der Beschwerdeführer nicht identisch sei mit B, der auch mit seinem zweiten Vornamen angegeben wurde.

Der bewußt ausführlich geschilderte Fall spricht eine deutliche Sprache. Zwar ist einzuräumen, daß die Daten von A und B in ungewöhnlicher Weise gleich in mehreren Punkten übereinstimmten. Aufgrund nicht nachvollziehbarer Nachlässigkeiten mußte der Beschwerdeführer jedoch mehr als zwei Jahre, trotz mehrfacher Hinweise auf die Verwechselung, Unannehmlichkeiten über sich ergehen lassen und um sein Recht streiten. Der Rechtsanspruch des Beschwerdeführers auf Berichtigung und Löschung stand allerdings nie in Frage. Vielmehr ging es primär um "Pannen" bei der Führung des Datenbestandes und der Auskunftserteilung, möglicherweise auch (zu Beginn der Vorfälle) um eine von der SCHUFA nicht zu vertretende fehlerhafte Meldung eines angeschlossenen Kreditinstituts. Um so entschlossener sollte daran gearbeitet werden, daß derartige Mängel im System nach Möglichkeit nicht mehr auftreten.

MMV 10/2589

7.1.4 Datenschutz durch Meldung des Geburtsdatums

Eine Beschwerdeführerin beklagte sich darüber, daß sie nach einer Bestellung bei einem Modehaus schriftlich aufgefordert worden sei, ihr Geburtsdatum anzugeben, damit die gewünschte Ware geliefert werden könne. Auf telefonische Nachfrage sei ihr mitgeteilt worden, das Geburtsdatum sei zur Erkennung minderjähriger Kunden erforderlich. Bei dem Modehaus handelte es sich um ein Unternehmen des Versandhandels, das den Kunden Warenkredite einräumt.

Nach den Teilnahmebedingungen der SCHUFA ist bei Anfragen eines Vertragspartners u.a. das Geburtsdatum des Betroffenen mitzuteilen. Dies dient der nach dem BDSG erforderlichen glaubhaften Darlegung eines berechtigten Interesses des anfragenden Unternehmens für eine Auskunft der SCHUFA. Das Unternehmen kann ein berechtigtes Interesse nur hinsichtlich von ihm so konkret benannter Personen verlangen, daß eine Verwechselung ausgeschlossen ist. Damit werden zugleich unbeteiligte Dritte gegen ungerechtfertigte Preisgabe ihrer Daten geschützt. Hiervon profitiert auch der Betroffene selbst, wenn Anfragen zu anderen Personen ergehen, mit denen er ohne Angabe des Geburtsdatums möglicherweise verwechselt werden könnte. In der Praxis gelingt es den Aufsichtsbehörden, den Betroffenen verständlich zu machen, daß hier nicht etwa eine Beeinträchtigung schutzwürdiger Belange vorliegt, sondern daß es im Gegenteil um eine Verbesserung des Datenschutzes geht.

Im vorliegenden Fall hat das Versandhandelsunternehmen allerdings der Beschwerdeführerin verschleiert, daß es die

Angabe des Geburtsdatums für eine SCHUFA-Anfrage benötigte und nicht etwa zur Erkennung einer etwaigen Minderjährigkeit bei Anbahnung des Vertragsverhältnisses. Gleichwohl war die Anfrage bei der SCHUFA als solche rechtlich nicht zu beanstanden. -

In diesem Zusammenhang sei darauf hingewiesen, daß es bei der SCHUFA wiederholt zu Personenverwechselungen deshalb kommt, weil sie bei den Datenbeständen aus dem Schuldnerverzeichnis (§ 915 ZPO) über das Geburtsdatum der Betroffenen keine Erkenntnisse hat, denn in einer Reihe von Fällen enthält das Schuldnerverzeichnis die Geburtsdaten nicht. Um ihrer Verpflichtung, nur richtige Daten zu speichern, nachzukommen, sollte die SCHUFA nach Ansicht der obersten Aufsichtsbehörden für den Datenschutz ihre Vertragspartner in allen derartigen Fällen zur Überprüfung der Identität des Betroffenen und zur Rückmeldung des Prüfungsergebnisses an die SCHUFA verpflichten. Bisher verlangt die SCHUFA von den Vertragspartnern eine Rückmeldung nur, wenn der Auskunftsempfänger die Identität des Betroffenen nicht eindeutig feststellen kann; bei positiver Übereinstimmung wird eine Benachrichtigung der SCHUFA nicht gefordert. Die obersten Aufsichtsbehörden stehen insoweit mit der SCHUFA noch in Verhandlungen. Das Problem könnte weitgehend gelöst werden, wenn bei der vorgesehenen Novellierung der Vorschriften über das Schuldnerverzeichnis festgelegt würde, daß auch das Geburtsdatum in das Schuldnerverzeichnis aufzunehmen ist, wie es u.a. vom Landesbeauftragten für den Datenschutz angeregt wurde (9. Tätigkeitsbericht, S. 28).

7.1.5 Waffengleichheit: Meldung des Widerspruchs gegen Mahnbescheid

Ein Kreditinstitut hatte einen Mahnbescheid gegen einen Beschwerdeführer erwirkt und der SCHUFA gemeldet. Der Beschwerdeführer erhob Widerspruch gegen den Mahnbescheid und teilte dem Kreditinstitut mit, er habe die Forderung nie bestritten; außerdem sei jeden Tag mit eine Steuerrückerstattung zu rechnen, so daß die Forderung beglichen werden könne. Das Kreditinstitut sah von einer Meldung des Widerspruchs an die SCHUFA ab und berief sich im Beschwerdeverfahren darauf, der Beschwerdeführer habe die dem Mahnbescheid zugrundeliegende Forderung ausdrücklich anerkannt. Nachdem der Beschwerdeführer vier Wochen nach Einlegung des Widerspruchs die Forderung durch Zahlung erfüllt hatte, erstattete das Kreditinstitut eine Erledigtmeldung an die SCHUFA.

Nach den Teilnahmebedingungen der SCHUFA ist ein Mahnbescheid zu melden, wenn die geltend gemachte Forderung bis dahin unstreitig ist und die Nichtzahlung auf Zahlungsunfähigkeit bzw. Zahlungsunwilligkeit des Kunden beruht. Zwar wird grundsätzlich erst mit rechtskräftigem Abschluß des Verfahrens verbindlich über die Forderung entschieden, doch läßt sich nach Auffassung des Bundesgerichtshofs (Urteil vom 15.12.1983 - III ZR 207/82 -, NJW 1984, 1889) der Unterrichtung über ein eingeleitetes gerichtliches Verfahren ein Informationswert für die Teilnehmer am Kreditinformationssystem der SCHUFA grundsätzlich nicht absprechen. Ist damit von einem berechtigten Interesse im Sinne des BDSG für die Übermittlung an die SCHUFA auszugehen, so ist die Gefahr einer unberechtigten Beeinträchtigung der Belange des Schuldners deutlich herabgesetzt, wenn sein Widerspruch

gegen den Mahnbescheid ebenfalls im Datenbestand der SCHUFA vermerkt wird, und zwar ebenso deutlich und ebenso schnell, wie das bei den g e g e n den Schuldner gerichteten Vorgängen geschieht (BGH, a.a.O.). Demgemäß sehen auch die Teilnahmebedingungen der SCHUFA eine unverzügliche Meldung des Widerspruchs vor.

Der Meldung des Widerspruchs bedarf es auch dann, wenn der Kunde gegenüber seinem Kreditinstitut erklärt, er bestreite die Forderung nicht. Mit dem bei Gericht eingelegten Widerspruch erscheint es nämlich nicht ausgeschlossen, daß der Schuldner sich trotz seines Nichtbestreitens gegen die Forderung in irgendeinem Punkt zur Wehr setzen will. Von einem eindeutigen Bestehen der Forderung kann somit zu Lasten des Schuldners nicht ausgegangen werden.

7.2 Weitere Hinweis- und Warnsysteme

7.2.1 "Schwarzfahrer"-Dateien

Auch im Berichtszeitraum haben sich immer wieder Bürger an die Aufsichtsbehörde gewandt und beklagt, daß Verkehrsbetriebe ihre Daten in sog. Schwarzfahrer-Dateien speichern. Derartige Dateien dienen zum einen der Überwachung, ob das bei Fahren ohne gültigen Fahrausweis verwirkte erhöhte Beförderungsentgelt entrichtet worden ist, zum anderen für die Entscheidung, ob Strafantrag wegen vorsätzlicher Beförderungserschleichung gestellt werden soll, wenn jemand innerhalb einer bestimmten Frist (i.d.R. zwei Jahre) wiederholt ohne gültigen Fahrausweis angetroffen wurde.

Die datenschutzrechtliche Zulässigkeit dieser Dateien beur-

teilt sich nach dem 3. Abschnitt des BDSG. Die Speicherung der Daten bis zur Einziehung des erhöhten Beförderungsentgelts ist im Rahmen der Zweckbestimmung des Vertragsverhältnisses, nämlich des Beförderungsvertrages, zulässig. Die Speicherung zur Beurteilung von Wiederholungsfällen findet ihre Rechtfertigung in der Wahrung berechtigter Interessen des Verkehrsbetriebes. Eine Beeinträchtigung schutzwürdiger Belange der Betroffenen liegt nicht vor, weil die Betroffenen bei einem strafrechtlich relevanten Verhalten den Verzicht auf eine Strafanzeige billigerweise nicht beanspruchen können.

Wenn ein Fahrgast erstmalig ohne gültigen Fahrausweis angetroffen wird, sehen Verkehrsbetriebe des öfteren von der Erhebung eines erhöhten Beförderungsgelts aus Kulanzgründen ab. Auch diese Kulanzfälle werden gespeichert, um insbesondere spätere Fälle bewerten zu können. Die Speicherung von Kulanzfällen wird als statthaft anzusehen sein, wenn sie zur Vermeidung der Beeinträchtigung schutzwürdiger Belange in Abgrenzung von den anderen Fällen mit einem Unterscheidungsmerkmal erfaßt werden. Denn in diesen Fällen ist die Berechtigung zur Erhebung eines erhöhten Beförderungsentgelts nicht eindeutig festgestellt worden.

In einem Fall hatte der Verkehrsbetrieb nicht das volle Beförderungsentgelt von seinerzeit 40,-- DM verlangt, sondern einen reduzierten Betrag von 20,-- DM gefordert und erhalten. Der Fahrgast hatte bei einer Fahrkartenkontrolle zwar gültige Fahrkarten für sich und einen begleitenden Familienangehörigen vorgewiesen, die jedoch nicht zur Fahrt auf der konkreten Strecke berechtigten. Zur Begründung berief er

sich darauf, in einer U-Bahnstation aus Versehen falsche Fahrausweise aus einem Fahrkartenautomaten gezogen zu haben. Der Verkehrsbetrieb weigerte sich, den Fall in der Datei besonders zu kennzeichnen, weil es sich nach seiner Ansicht nicht um einen Kulanzfall handelte. Die Aufsichtsbehörde vertrat gleichwohl gegenüber dem Unternehmen die Auffassung, es gehe um einen Kulanzfall, was schon in der Reduzierung des erhöhten Beförderungsentgelts zum Ausdruck komme. Sie forderte eine entsprechende Kenntlichmachung, um eindeutig eine Beeinträchigung schutzwürdiger Belange auszuschließen.

Ohne daß es hier eine Vertiefung bedarf, ist darauf hinzuweisen, daß die Daten von Kindern unter 14 Jahren nicht zum Zwecke etwaiger Strafanzeigen in einer Schwarzfahrer-Datei gespeichert werden dürfen, da diese Personen nach § 19 StGB schuldunfähig sind und nicht nach § 265a StGB wegen vorsätzlicher Beförderungserschleichung bestraft werden können. Allerdings ist die Speicherung insoweit zulässig, als nachgehalten werden soll, ob ein erhöhtes Beförderungsentgelt nach Genehmigung des Beförderungsvertrages durch den gesetzlichen Vertreter entrichtet worden ist. Unterbleibt die Genehmigung oder wird sie versagt, sind die Daten wegen Unzulässigkeit der Speicherung zu löschen (§ 27 Abs. 3 Satz 2 BDSG).

7.2.2 Datei über Mietinteressenten

Erhebliche Resonanz durch Presseveröffentlichungen hat die Gründung einer zentralen Datei über Mietinteressenten gefunden, mit der Vermieter vor Verlusten im Vermietungs- und Verpachtungsgeschäft geschützt und die "schwarzen Schafe" unter den Mietern rechtzeitig erkannt werden sollen.

Nach Angaben des Betreibers waren im November 1988 rd. 1.700 Datensätze von Mietern gespeichert; bis auf ca. 30 Datensätze von Vermietern hatte der Betreiber alle Datensätze aus Schuldnerverzeichnissen der Vollstreckungsgerichte (§ 915 ZPO) bezogen. Aufgrund einer Abstimmung der obersten Aufsichtsbehörden im "Düsseldorfer Kreis" (vgl. 9.) und mehrfacher Intervention der Aufsichtsbehörde sollen die Vermieter auf Veranlassung des Betreibers nur noch unanfechtbare Vollstreckungsbescheide und rechtskräftige Urteile im Zusammenhang mit Mietverhältnissen (u.a. Mietschulden, Nebenkostenschulden, Kautionsschulden) melden, ferner eidesstattliche Versicherungen wegen Mietschulden, Haftbefehle zur Abgabe der eidesstattlichen Versicherung wegen Mietschulden, Wohnungsklagen aufgrund unanfechtbarer Vollstreckungsbescheide und rechtskräftiger Urteile, fruchtlose Pfändungen aus Mietschulden sowie Kündigungen wegen unanfechtbarer Vollstreckungsbescheide oder rechtskräftiger Urteile.

Bei dem Betrieb der Datei handelt es sich um eine Auskunfei, die nach dem 4. Abschnitt des BDSG zu beurteilen ist, weil geschäftsmäßig geschützte personenbezogene Daten zum Zweck der Übermittlung gespeichert und übermittelt werden. Nach § 32 Abs. 1 und 2 BDSG ist die Speicherung und Übermittlung von Mieterdaten nur zulässig, wenn schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden und die Empfänger ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft darlegen. Zwar wird prinzipiell das Interesse der als Systemnutzer vorgesehenen potentiellen Vermieter/ Verpächter, Informationen zu erhalten, die geeignet sind, vor finanziellen Verlusten im Vermietungs- und Verpachtungsgeschäft zu schützen, als ein berechtigtes Interesse anzuerkennen sein. Sofern Vermieter nur die vorgenannten Negativmerkmale insbesondere aus unanfechtbaren und

rechtskräftigen Entscheidungen in die Datei einmelden, ist eine Beeinträchtigung schutzwürdiger Belange nicht festzustellen, da es sich um sog. "harte" Merkmale mit objektivem Aussagegehalt und von erheblichem Gewicht handelt, die speziell Mietverhältnisse betreffen. Allerdings verbleiben gewisse Zweifel, weil die als Vertragspartner in Betracht kommenden Vermieter regelmäßig keiner Datenschutzkontrolle unterliegen.

Bei den Angaben aus dem Schuldnerverzeichnis handelt es sich zwar auch um "harte" Daten. Jedoch ist eine Selektion hinsichtlich nur mietrelevanter Angaben zumeist nicht möglich, auch nicht danach, ob es sich bei den Betroffenen um Mieter oder Vermieter handelt. Allerdings können sich die Anfragen von Vermietern bei der Datei immer nur auf Miet- und Pachtinteressenten beziehen, so daß auf diese Weise ein spezieller Bezug hergestellt wird. Unter Zurückstellung von Bedenken kann auch nicht eindeutig in Abrede gestellt werden, daß die Angaben aus dem Schuldnerverzeichnis für die Beurteilung des Mietrisikos auch dann von Bedeutung sein können, wenn sie nicht mietrechtliche Schuldverhältnisse betreffen. Soweit im Schuldnerverzeichnis die Angabe des Geburtsdatums fehlt, ergeben sich im Hinblick auf die Identitätsprüfung im Grundsatz die gleichen Probleme wie bei der SCHUFA (s. 7.1.4).

Insgesamt stellt sich die Frage, ob der Betreiber der Warndatei sein Ziel erreicht, da bislang nur sehr wenige Vermieter als Anschlußpartner gewonnen werden konnten und andererseits für anfragende Vermieter sehr bald erkennbar werden dürfte, daß der Großteil der Daten aus dem Schuldnerverzeichnis stammt und nur eine verhältnismäßig pauschale Bewertung ermöglicht. Dies ist allerdings weniger ein

Problem des Datenschutzes. Die Aufsichtsbehörde wird das Unternehmen weiterhin laufend überwachen. Zu beobachten ist vor allem, ob die Daten aus den Schuldnerverzeichnissen entsprechend § 915 Abs. 4 ZPO nach drei Jahre gelöscht werden.

7.2.3 Frauenärzte-Datei

In einer Großstadt hat ein von Frauen gegründeter eingetragener Verein in Zusammenarbeit mit ärztlichen Berufsverbänden, Ärztekammern und der städtischen Frauengleichstellungsstelle eine Frauenärzte-Kartei errichtet, deren Ziel es ist, die persönlichen Erfahrungen von Patientinnen bei Frauenärzten und -ärztinnen interessierten Frauen verfügbar zu machen. Für die Kartei werden von Patientinnen ausgefüllte Fragebogen ausgewertet, die u.a. Fragen enthalten zu Wartezeiten, Unterschieden zwischen Kassen- und Privatpatientinnen, Verhalten der Praxismitarbeiter und -mitarbeiterinnen, Wahrung der Intimsphäre bei der Untersuchung sowie Bereitschaft des Arztes oder der Ärztin zur Beantwortung von Fragen. Auch die betroffenen Ärzte und Ärztinnen können Einblick in die als Datei anzusehende Kartei nehmen.

Bei der nach dem 4. Abschnitt des BDSG vorzunehmenden Interessenabwägung sind die berechtigten Interessen künftiger Patientinnen von erheblichem Gewicht, weil Frauen gerade an Frauenärzte und -ärztinnen wegen der u.U. tiefgreifenden Offenlegung ihrer Privat- und Intimsphäre besondere Vertrauensanforderungen stellen. Demgegenüber besteht nicht die Gefahr, daß ein ganzer Berufsstand in Mißkredit gebracht wird. Die mitgeteilten Erfahrungen können durchaus auch positiver Natur sein. Außerdem sind die Fragen insgesamt verhältnismäßig neutral und objektiv formuliert; Negativ-

einschätzungen werden den Frauen, die ihre Erfahrungen wiedergeben, nicht nahegelegt. Zwar werden auch Werturteile erbeten, jedoch hat die Aufsichtsbehörde empfohlen, insoweit im Fragebogen die Möglichkeit zu begründenden Angaben zu eröffnen. Mit Rücksicht auf die besondere Sensitivität der Datenverarbeitung für die betroffenen Frauenärzte und -ärztinnen hat die Aufsichtsbehörde gefordert, daß die Betroffenen vor Aufnahme in die Datei Gelegenheit zur Stellungnahme und zu einem gewünschten Gespräch mit der Patientin erhalten, die den Fragebogen ausgefüllt hat, sofern sie einem Gespräch zustimmt. Auf die Sperrung vom Arzt oder von der Ärztin bestrittener Daten kann verzichtet werden, wenn eine von ihm oder ihr verfaßte Gegendarstellung in die Datei aufgenommen und zur Einsichtnahme breitgehalten wird.

Sofern die auskunftgebenden Frauen nicht ausdrücklich schriftlich einwilligen, dürfen ihre Namen und Anschriften nicht in die Datei aufgenommen werden; diese sind aber getrennt zu speichern, um Gespräche mit den betroffenen Ärzten und -ärztinnen zu ermöglichen. Im übrigen muß sichergestellt sein, daß Frauenärzte -und -ärztinnen Einblick nur in die sie betreffenden Daten nehmen können.

7.2.4 EPOS - Datei zum Schutz gefährdeter Führungskräfte -

Ein bundesweit tätiges privates Sicherheitsunternehmen richtete an die Datenschutzaufsicht die Anfrage, ob ein von ihr geplantes Konzept für einen EDV-gestützten Personen- und Objekt-Schutz ("EPOS") datenschutzrechtlich unbedenklich sei. Mit EPOS sollen Ausspähungs- und Tatvorbereitungshandlungen hinsichtlich etwaiger Anschläge auf Führungskräfte der Wirtschaft erfaßt und bei verdichtetem Verdacht an die Auftraggeber und/oder die Polizei gemeldet werden.

M 10/2589

Im regelmäßigen Aufenthaltsbereich von Schutzpersonen werden beobachtete sicherheitsrelevante Zustände von Mitarbeitern des Unternehmens in einen tragbaren Computer eingegeben und in einen Zentralrechner bei der betreffenden Regionalgesellschaft des Unternehmens fernübertragen. Die Beobachtungen werden dezentral und zentral abgeglichen mit früher eingespeicherten Feststellungen. Bei "Treffern", d.h. bei wiederholtem Auftreten von sicherheitsrelevanten Zuständen, werden die Informationen bewertet und ggf. weitergeleitet. Folgende Daten beobachteter Personen finden Aufnahme in die Datei: äußere Beschreibung, Art des auffälligen Verhaltens, benutzte Fahrzeuge mit Beschreibung sowie Kfz-Kennzeichen. Die Ein- und Ausgabemasken sehen das Einfügen von Personalien nicht vor. Identifizierungsmaßnahmen einschließlich Halterabfragen sowie weitere Ermittlungshandlungen sollen ausschließlich der Polizei und der Staatsanwaltschaft vorbehalten sein.

Obwohl ein Personenbezug in der Datei selbst ohne Zusatzwissen regelmäßig nicht gegeben ist, findet das BDSG dennoch Anwendung, weil der Zweck der Datenerfassung darin besteht, im Trefferfalle erfaßte Personen nach Datenübermittlung an die Polizei durch diese bestimmbar zu machen (vgl. § 2 Abs. 1 BDSG). Überdies sind Kfz-Kennzeichen schon nach gesetzlicher Definition (§ 45 Satz 2 StVG) personenbezogene Informationen. Nach vorläufiger Einschätzung gilt für EPOS der 3. Abschnitt, weil Hauptzweck der Datei der Personenschutz ist und für diesen eigenen Zweck die Datei nur ein "Hilfsmittel" darstellt. Soweit im Rahmen von Aufträgen Daten aus anderen Aufträgen in Form von Treffermeldungen an andere Auftraggeber übermittelt werden und dies in nicht unerheblichem Umfang "geschäftsmäßig" geschieht, liegt zugleich Datenverarbeitung für fremde Zwecke im Sinne des 4. Abschnitts vor.

Bei der nach beiden Abschnitten vorzunehmenden Interessenabwägung ist einerseits zu bedenken, daß Personen, die sich auffällig im Sinne möglicher Ausspähungs- und Tatvorbereitungshandlungen verhalten (z.B. Beobachten und Fotografieren einer Industriellenvilla aus einem parkenden PKW mit auswärtigem Kennzeichen), mit Mitteln der elektronischen Datenverarbeitung systematisch erfaßt werden, ohne daß sie davon Kenntnis haben und obwohl sich die Vermutungen später als tatsächlich unbegründet erweisen können. Andererseits geht es um die Verhütung schwerer Straftaten gegen Führungskräfte, denen nicht das Recht abgesprochen werden kann, zunächst ohne Hilfe der Polizei Maßnahmen zu ihrem Schutz zu ergreifen. Da auch die Datei größtenteils faktisch "anonym" ist, darin lediglich grundsätzlich nachprüfbare Beobachtungen festgehalten werden und der Polizei bleibt, was der Polizei gebührt, sind bei einer ersten Würdigung durchgreifende Bedenken gegen das Konzept EPOS nicht geltend zu machen. Entscheidend wird es auf die Realisierung in der Praxis ankommen.

Bei der regelmäßigen Überwachung wird sich die Datenschutzaufsicht auch der Erkenntnisse und Bewertungen eingeschalteter Polizeibehörden bedienen. Neben der Prüfung, ob wirklich nur eindeutig auffällige Verhaltungsweisen gespeichert werden, wird insbesondere zu prüfen sein, ob äußerst kurze Löschungsfristen eingehalten werden (in der Regel nicht länger als 6 Monate) und schon vor deren Ablauf die Löschung erfolgt, wenn - etwa aufgrund von Rückmeldungen der Polizei - "Entwarnung" gegeben werden kann oder bei Speicherung des Verdachts strafbarer Handlungen die Richtigkeit der Daten von der speichernden Stelle nicht bewiesen werden kann (§§ 27 Abs. 3 Satz 3, 35 Abs. 3 Satz 3 BDSG).

MMV 10/2589

Selbstverständlich bedarf es auch eines besonders hohen Standards von Datensicherungsmaßnahmen, um einen Zugriff Unbefugter auszuschließen.

7.2.5 Sachschadendatei SAVIS (Sachschadenversicherung-Informationssystem)

Verdächtigtendaten sind es auch, die - neben anderen Daten - aufgenommen werden in die Datenbank, die beim Verband der Sachversicherer in Köln errichtet worden ist. Die Datenbank hat die Funktion einer "Sammel- und Verteilstation" für Warnmeldungen der Sachschadenversicherer jeweils an andere Mitglieds-Versicherungsunternehmen des Verbandes. Die Daten natürlicher Personen werden vor der Absendung an den Verband mit Hilfe eines Match-Codes verschlüsselt. Der Verband faßt die Meldungen auf Datenträgern zusammen und leitet diese monatlich an die Mitglieder weiter. Diese gleichen die gesammelten Daten unter Verwendung desselben Match-Codes mit dem eigenen Datenbestand ab und filtern die Daten heraus, bei denen sich eine Übereinstimmung mit bei ihnen bereits vorhandenen Daten ergibt. Gemeldet wird bei Schäden aus allen Sparten der Sachversicherung ab einem Schadensaufwand von 10.000,-- DM, bei denen die betreffende Versicherung aufgrund eines Verdachts des Versicherungsmißbrauchs eine Kündigung ausgesprochen hat; ferner sind alle Brandstiftungsfälle ab 10.000,-- DM meldepflichtig. Das wesentliche Ziel des Verfahrens besteht darin, Risiken bei Vertragsabschlüssen zu erkennen, Schäden aufzuklären und weiteren Mißbrauch zu verhindern. Die zentrale Datei dient dabei als Hilfsmittel, um im Trefferfalle einen Datenaustausch aus den Schadensakten der dem Verband angeschlossenen Versicherungsunternehmen zu ermöglichen.

Soweit es um SAVIS geht, verarbeitet der Verband der Sachversicherer als Dienstleistungsunternehmen geschäftsmäßig geschützte personenbezogene Daten im Auftrag und unterliegt damit dem 4. Abschnitt des BDSG (§ 31 Abs. 1 Satz 1 Nr. 3 i.V.m. § 37 BDSG). "Personenbezogene" Daten verarbeitet er schon deshalb, weil der bislang verwendete Match-Code, der u.a. den Nachnamen des Betroffenen mit den ersten sechs Buchstaben, die Postleitzahl mit vier Stellen sowie Straße und Hausnummer mit je einer Stelle erfaßt, Reidentifizierungen ermöglicht, und zwar auch durch den Verband. Selbst bei vollständiger Anonymisierung wird der Verband in der Phase der Übermittlung personenbezogener Daten tätig, denn die Daten sind für die Versicherungsunternehmen als Übermittlungsempfänger im Trefferfalle eindeutig und gewollt hinsichtlich natürlicher Personen "bestimmbar" (vgl. Definition des § 2 Abs. 1 BDSG). Keineswegs ginge es an, diese Daten in der Phase des Sammelns und Weiterleitens durch den Verband gewissermaßen aus dem BDSG auszublenden und vom Datenschutz freizustellen, während sie anschließend beim Übermittlungsempfänger unzweifelhaft wieder gesetzlich geschützt sind. Überdies sei angemerkt, daß bei der Versicherungswirtschaft ein phonetischer Strukturcode in Vorbereitung ist, der eine völlige Anonymisierung der "Nichttreffer"-Daten bewirken soll, an denen die einzelnen Versicherungen im konkreten Abgleichfall kein eigenes - berechtigtes - Interesse haben können.

Die Datenverarbeitung im Auftrag ist nur im Rahmen der Weisungen des Auftraggebers gestattet (§ 37 BDSG). Als Auftragnehmer ist der Verband nicht den Speicherungs- und Übermittlungsvorschriften des § 32 BDSG unterworfen; auch treffen ihn nicht die Benachrichtigungs- und Auskunfts-

pflichten nach § 34 BDSG. Verantwortlich für die Datenverarbeitung, in deren Rahmen der Verband kein selbständiges Interesse hat, sondern sich lediglich als Mittler zur Verfügung stellt, sind allein die meldenden und empfangenden Mitglieds-Versicherungsunternehmen, und zwar nach dem 3. Abschnitt. Somit liegt die Systemverantwortlichkeit in den Händen vieler und bedingt deshalb größere Risiken als in den Fällen, in denen nur eine Stelle den Datenschutz gewährleisten muß. Allerdings hat auch der Verband für die erforderliche Datensicherung Sorge zu tragen (§ 6 BDSG).

Ohne daß hier auf alle Einzelheiten eingegangen werden kann, ist festzustellen, daß das Meldeverfahren SAVIS grundsätzlich berechtigten Interessen der angeschlossenen Versicherungsunternehmen dient, zumal es sich um Fälle erheblicher Größenordnung handelt. Die Tatsache der Vertragsaufhebung stellt auch prinzipiell ein objektiv aussagefähiges Kriterium dar. Problematisch muß es aber erscheinen, wenn bezüglich bestimmter Personen der Verdacht, in betrügerische Handlungen verwickelt zu sein, anderen Versicherungen zugetragen wird, ohne daß dieser Verdacht zumindest zur Einleitung eines strafrechtlichen Ermittlungsverfahrens geführt hat und bisher weder durch die Strafverfolgungsorgane noch durch die Organe der Rechtspflege bestätigt wurde. Es müssen jedenfalls nachprüfbare, objektive Anhaltspunkte vorliegen, um ein berechtigtes Interesse der Versicherungsunternehmen im Sinne des § 24 Abs. 1 Satz 1 3. Alt. BDSG bejahen zu können. Vielfach wird es sich aber um mehr subjektive Einschätzungen handeln.

Um eine Beeinträchtigung schutzwürdiger Belange der Betroffenen durch Übermittlung von staatlich nicht geprüften Verdachtsmomenten auszuschließen, sollten die Betroffenen Gelegenheit zu ihrer Verteidigung erhalten und ggf. gericht-

MMV10/2589

liche Schritte einleiten können. Eine Arbeitsgruppe des "Düsseldorfer Kreises" (vgl. 9.) verhandelt bereits seit längerem mit der Versicherungswirtschaft, um u.a. die Frage einer angemessenen Benachrichtigung der Betroffenen zu klären, die nicht als Versicherungsnehmer durch das der Aufklärung dienende Merkblatt (dazu näher unten 9.2.4) als informiert gelten können.

7.2.6 Weitere Systeme, Zusammenfassung

Außer dem System SAVIS gibt es in der Versicherungswirtschaft noch zahlreiche andere zentrale Hinweissysteme, so hinsichtlich der Haftpflichtversicherer, Unfallversicherer, Autoversicherer und Rechtsschutzversicherer beim HUK-Verband in Hamburg, ferner beim Verband der Lebensversicherungsunternehmen, beim Deutschen Transport-Versicherungsverband sowie beim Verband der Privaten Krankenversicherung. Auch zu einer nicht geringen Zahl dieser Hinweissysteme führen die obersten Aufsichtsbehörden der Länder seit geraumer Zeit Verhandlungen mit der Versicherungswirtschaft. Eine Beschleunigung dieser Verhandlungen erscheint wünschenswert. Insoweit sind Zweifel nicht ausgeräumt, solange schon grundsätzliche Fragen wie die der Anwendbarkeit des 3. oder 4. Abschnitts oder (im Hinblick auf die Verschlüsselung durch Match-Codes) die Frage der Anwendbarkeit des BDSG überhaupt kontrovers diskutiert werden. Vorrangig sollte es darum gehen, Kriterien zu finden, was gemeldet werden darf, und darum, die Transparenz der Datenflüsse für die Betroffenen sicherzustellen.

Die Reihe zentraler Warndateien ist auch mit der vorstehenden Ergänzung noch nicht abgeschlossen. Vor allem die Möglichkeiten der EDV üben einen Anreiz auf die Errichtung im-

mer neuer Warndateien aus. Jüngstes Beispiel ist das Videotheken-Gewerbe (Schutz gegen den Verlust von Kassetten). Ferner werden auch im Bereich des Beherbergungsgewerbes Überlegungen in Richtung auf eine Warndatei angestellt, um über negative Erfahrungen mit Gästen Kunde zu geben. Im Wege des Warnverbundes werden seit langem die Spielbanken tätig, die sich gegenseitig über Hausverbote nach der Spielordnung unterrichten; eine externe Zentraldatei wird insoweit nicht geführt.

Permanent und wirksam überprüft werden können derartige Hinweissysteme von der Aufsichtsbehörde nur, wenn sie in den 4. Abschnitt des BDSG fallen und - anders als bei bloßer Datenverarbeitung im Auftrag (Sachschadendatei, 7.2.5) - eine eigenständige Verarbeitung personenbezogener Daten vornehmen. Bei Dateien, auf die der 3. Abschnitt anzuwenden ist, wie etwa "Schwarzfahrer"-Dateien (7.2.1) oder auch hauseigene Dateien über Ladendiebstähle und die Sperrdateien der Spielbanken , ist die Aufsichtsbehörde bis zur Neufassung des BDSG auf konkrete Beschwerden Betroffener im Einzelfall angewiesen (§ 30 Abs. 1 BDSG). Unabhängig von der Anwendbarkeit des 3. und 4. Abschnitts sollten bereichsspezifische Rechtsvorschriften ins Auge gefaßt werden, soweit es nicht zu tragfähigen Verhandlungsergebnissen mit den Spitzenverbänden der Wirtschaft in absehbarer Zeit kommt. Es wäre dann Sache des Gesetzgebers, klipp und klar über die Zulässigkeit ansonsten "dubioser" Warnsysteme zu befinden. So kann es nicht befriedigen, wenn etwa bei EPOS (7.2.4) mangels eindeutiger Gesetzesregelungen von einem Fernsehreporter problematisiert wurde, ob die Privatwirtschaft mehr "darf" als der Staat.

7.3 Wirtschafts- und Handelsauskunfteien

Zu den großen Wirtschaftszweigen, die Auskunft über Bestehen und Nichtbestehen wirtschaftlicher Risiken erteilen, gehören neben der SCHUFA die Wirtschafts- und Handelsauskunfteien. Nach dem Bericht eines Wochenmagazins vom Mai 1989 setzt diese Branche inzwischen 450 Mio. DM im Jahr um; die drei größten Gesellschaften (in alphabetischer Reihenfolge: Bürgel, Creditreform, Schimmelpfeng) haben etwa 100.000 Unternehmen als Stammkunden. Zunehmend werden die Auskünfte über On-line-Anschluß abgewickelt.

Zum großen Teil beziehen die Auskunfteien ihre Informationen aus allgemein zugänglichen Quellen wie Telefonbüchern und öffentlichen Registern. Aber auch Informationen der Kunden (z. B. über das Zahlungsverhalten von Vertragsfirmen), Selbstauskünfte Betroffener sowie Befragungen sowohl Betroffener als auch in deren Umfeld durch fest angestellte oder freie Rechercheure gehen in die Datenbestände ein. Gespeichert werden u. a. Angaben wie berufliche Tätigkeit, Arbeitgeber, Verdienst, Vermögen, Haus- und Grundeigentum, Belastung, Anzahl der Kinder, Zahlungsmoral.

Die Zulässigkeit von Speicherung und Übermittlung der Daten richtet sich bei den personenbezogenen Informationen (dem kleineren Teil der Datenbänke) nach § 32 Abs. 1 und 2 BDSG (4. Abschnitt). Voraussetzung ist zunächst, daß die Daten richtig, aktuell und hinsichtlich eines berechtigten Bonitätsinteresses aussagekräftig sind. Diese Punkte bedürfen schon im Blick auf Datenmenge und Datenvielfalt kritischer Betrachtung. Da es sich zum Teil um sehr sensitive Daten aus dem finanziellen, familiären und beruflichen Bereich handelt, sind an die glaubhafte Darlegung eines - überwiegenden - berechtigten Interesses im einzelnen Übermittlungsfall insoweit besondere Anforderungen zu stellen. Bedenken begegnet von daher die weitverbreitete Praxis, nach welcher der Anfragende

lediglich eine bestimmte Fallgruppe anzukreuzen braucht (z. B. "Anbahnung von Geschäftsbeziehungen"). Die obersten Aufsichtsbehörden haben dies nur hingenommen, weil eine stichprobenartige Kontrolle und Überprüfung durch die Auskunfteien zugesagt wurde. Jedenfalls bei besonders sensitiven Daten ist aber eine genauere Einzelfallprüfung vor Übermittlung unentbehrlich; so dürfen einem künftigen Arbeitgeber nur arbeitsplatzrelevante Informationen mitgeteilt werden, nicht aber darüber hinausgehende Daten. Die - auch lediglich stichprobenweise - Überprüfung bedingt die sorgfältige Beachtung der gesetzlichen Aufzeichnungspflicht, nicht zuletzt auch im On-line-Verkehr.

Der Betroffene kann seine Rechte wahren, da er nach § 34 Abs. 1 bei erstmaliger Übermittlung von der Speicherung im Datenbestand der Auskunftei zu benachrichtigen ist. Über sein Auskunftsrecht kann er jedoch weder Informationen über die Herkunft noch über die Empfänger der Daten beanspruchen, ein Umstand, der immer wieder zu Beschwerden geführt hat. Zum Schutze des Betroffenen sind die Daten am Ende des fünften Kalenderjahres nach ihrer Einspeicherung zu sperren und dürfen dann grundsätzlich nicht mehr übermittelt oder sonst genutzt werden (§§ 35 Abs. 2 Satz 2 i. V. m. 14 Abs. 2 Satz 3 BDSG).-

Ein Unternehmen in Nordrhein-Westfalen bietet einen Informationsdienst über mehr als 20.000 bundesdeutsche Firmen an, um im Geschäftsverkehr einen einfachen Zugriff auf Firmendaten zu ermöglichen. Gegenstand dieser "Firmenprofile" sind auch Namen von Entscheidungs- und Funktionsträgern, wie Aufsichtsräte, Vorstände und Gesellschafter. Die Daten werden nicht nur allgemein zugänglichen Quellen entnommen, sondern auch durch eine sog. Firmenselbstbefragung erhoben. Der jeweiligen Firma werden die vorhandenen Kerndaten mit der Bitte um Aktualisierung und Ergänzung zugesandt. Bei den Rückantworten werden auch Daten von Entscheidungsträgern genannt, ohne daß diese stets davon wissen.

Aufgrund zahlreicher Eingaben wurde der Firmeninformationsdienst einer eingehenden Prüfung unterzogen. Im Ergebnis konnte Einvernehmen darüber erzielt werden, daß Entscheidungsträger-Daten, die von der eigenen Firma übermittelt worden sind, bei Widerspruch des Betroffenen gelöscht werden. Dies gilt nicht für natürliche Personen, die der registergerichtlichen Pubizität und damit einer allgemeinen Öffentlichkeit unterliegen (z. B. Daten von Gesellschaftern). Die Widerspruchslösung ist ein taugliches Mittel, um der Gefahr einer fortdauernden Beeinträchtigung schutzwürdiger Belange entgegenzuwirken.

Die im Zusammenhang der Auskunfteien auch zu nennenden Detekteien, die u. a. im häuslichen Umfeld eingehende Recherchen anstellen, führen in der Regel keine personenbezogenen Dateien über ihre Erhebungen und werden insoweit nicht vom BDSG erfaßt.

Abschließend sei noch bemerkt, daß Auskunfteien vielfach Inkassodaten in ihren Bestand aufnehmen und hierüber Auskunft erteilen. Datenlieferanten können dabei sowohl rechtlich selbständige Inkassounternehmen als auch unselbständige Inkassoabteilungen der Auskunfteien sein. Auch im letzteren Fall ist eine Einzelfallprüfung im Hinblick auf die Auskunfteizwecke erforderlich (§ 32 BDSG). Ein berechtigtes Interesse hinsichtlich der Übermittlung wird regelmäßig nur bei "harten" Daten wie etwa titulierten Forderungen angenommen werden können. Nach dem Gesetz ist es geboten (§§ 26 Abs. 1, 34 Abs. 1), daß bei interner "Zweigleisigkeit" von Inkasso- und Auskunfteidienst ebenso wie bei jeweils rechtlicher Selbständigkeit der Betroffene über die erstmalige Speicherung seiner Daten einerseits im Inkassobereich und andererseits im Bereich der Auskunftei - unter Hinweis auf die Speicherung auch zu Auskunfteizwecken - informiert wird.

7.4 Adressenhandel und Direktwerbung

Eine Quelle ständigen Ärgernisses stellt für viele Bürger die unverlangte Zusendung von Werbematerial dar. Fast 30 % des gesamten Briefverkehrs soll adressierte Direktwerbung sein, mit der etwa 25 Mio. Verbraucher erreicht werden (Frankfurter Rundschau, 01.04.1989).

Die Adressen stammen auch hier zunächst aus allgemein zugänglichen Quellen wie Telefonbüchern, Adreßbüchern, Branchenverzeichnissen, Jahrbüchern, Mitgliederverzeichnissen, Standesamtsnachrichten, Zeitungsannoncen und nicht zuletzt aus den Schuldnerverzeichnissen. Darüber hinaus werden u. a. Teilnehmerlisten, Vorlesungsverzeichnisse und Rückläufe aus Preisausschreiben, Verlosungen und Gutscheinen ausgewertet. Schließlich werden auch Kundendateien von Versandhäusern, Buchclubs etc. gewinnbringend nicht-konkurrierenden Unternehmen zur Werbung überlassen. Als besonders wertvoll werden Adressen sogenannter "opinion leaders" (insbesondere Lehrer, Akademiker) angepriesen.

Häufig werden zu Zwecken der Direktwerbung Adressenmakler (Listbroker) und Lettershops eingeschaltet. Lettershops führen Adressen- und Werbematerial zusammen und übernehmen den Postversand. Die obersten Aufsichtsbehörden für den Datenschutz haben stets den Standpunkt vertreten, daß der Adressenhändler personenbezogene Daten an das werbende Unternehmen übermittelt, wenn der Umworbene sich bei diesem meldet, etwa durch Bestellung von Waren. Der Umworbene ist gewissermaßen ein unfreiwilliges Werkzeug des Adressenhändlers, da er dem werbenden Unternehmen unbewußt bekannt gibt, daß bei der Sortierung des Adressenmaterials festgelegte Auswahlkriterien von ihm erfüllt werden. Jedenfalls wegen der Art, wie die Übermittlung zustande kommt (Benutzung des Betroffenen als "willenloses" Werkzeug), wird eine Beeinträchtigung schutzwürdiger Belange anzunehmen sein. Es bedarf daher nach

Ansicht der obersten Aufsichtsbehörden für den Datenschutz einer Mitteilung der Auswahlkriterien an den Betroffenen.

Die Verwendung personenbezogener Daten zu Werbezwecken ist weder grundsätzlich zulässig noch grundsätzlich unzulässig. Das BDSG verlangt auch insoweit eine Interessenabwägung, wobei für sog. Listendaten wie Name und Anschrift erleichterte Voraussetzungen gelten (§§ 24 Abs. 2, 32 Abs. 3 BDSG). Zu berücksichtigen ist, daß Werbung zwar ein berechtigtes wirtschaftliches Interesse sein kann, diesem Interesse aber im Regelfall kein besonderes Gewicht zukommt. Schwerpunktmäßig ist daher zu prüfen, ob schutzwürdige Belange der Betroffenen beeinträchtigt werden. Dies liegt bei der Überlassung von Daten an Dritte (z. B. Kundendaten, Arbeitnehmerdaten) näher als in den Fällen, in denen das werbende Unternehmen bereits vertragliche Beziehungen zu dem Umworbenen unterhält. Werbung ist schon dann unzulässig, wenn wegen Art, Gegenstand oder Zusammenhang der Werbung eine Beeinträchtigung schutzwürdiger Belange nicht auszuschließen ist.

Eindeutig wird die Schwelle zwischen "harmloser" Belästigung und unzulässiger Beeinträchtigung durch einen Widerspruch des Betroffenen im Falle der Briefkastenwerbung überschritten. Das folgt aus dem Selbstbestimmungsrecht des Betroffenen, das sich gegenüber dem Interesse des Unternehmens an der Werbung durchsetzt (so BGH-Urteil vom 20.12.1988 - NJW 1989, 902 - bezüglich des Einwurfs nicht adressierter Werbung von Supermärkten in Briefkästen). Angesichts des erreichten Ausmaßes der Briefkastenwerbung stellt diese ein rechtswidriges Eindringen in den häuslichen Eigenbereich in den Fällen dar, in denen der Betroffene unmißverständlich seinen entgegenstehenden Willen geäußert hat (BGH, a.a.O.). Der Widerspruch allein bewirkt allerdings keine "absolute Bindungswirkung"; ob das allgemeine Persönlichkeitsrecht verletzt ist, hängt von dem Ergebnis einer Güter- und Interessenabwägung im Einzelfall ab (BVerwG, Urteil vom 21.04.1989, NJW 1989, 2409 - Beifügung von Werbung zu Kontoauszügen des Postgiroamts dreimal im Monat dem

MMV 10/2589

Grad nach keine unzumutbare Belästigung, zumal Zahl der Briefe unverändert). Für die Zulässigkeit der Telefonwerbung bei Privatpersonen verlangt der Bundesgerichtshof im vorhinein eine ausdrückliche Einwilligung des Betroffenen, selbst wenn bereits geschäftliche Kontakte mit ihm bestehen (Urteil vom 08.06.1989, Betriebs-Berater 1989, 1777). Bei der Vielfältigkeit der Werbemethoden erfordern es die berechtigten Interessen der gewerblichen Wirtschaft nicht, mit der Werbung auch in den privaten Bereich des Verbrauchers einzudringen (BGH, a.a.O.).

U. a. in folgenden Beispielsfällen aus dem Berichtszeitraum sind die Aufsichtsbehörden davon ausgegangen, daß eine Beeinträchtigung schutzwürdiger Belange Betroffener nicht auszuschließen war:

In einem Fall beabsichtigte ein Verkäufer von Hunde- und Katzenfutter, 5.000 Kundendaten von Hundehaltern gewinnbringend verschiedenen Versicherungen zu Werbezwecken zu überlassen. Die Aufsichtsbehörde sah in einer derartigen Zweckentfremdung vertraglich gewonnener Kundendaten ohne Zustimmung der Betroffenen eine Beeinträchtigung schutzwürdiger Belange. Auf entsprechende Abmahnung versprach der Händler, von seinem Vorhaben abzulassen.

In einem weiteren Fall versandte eine Apotheke Geburtstagsgrußkarten an eigene Kunden, deren Anschriften sie zuvor Rezeptblättern entnommen hatte. Die Speicherung und Verwendung von Daten aus ärztlicher Behandlung zu Werbezwecken erscheint schon im Blick auf das besondere Vertrauen der Betroffenen, daß diese im sensitiven Zusammenhang gewonnenen Daten grundsätzlich nur für Behandlungszwecke verwendet werden, bedenklich. Unzulässig ist die Verwendung zu Werbezwecken aber auch deshalb, weil nicht wenige der Glückwunschempfänger es eher für eine zweifelhafte Ehre halten dürften, als "Stammkunden" einer Apotheke betrachtet bzw. nach Möglichkeit gewonnen zu werden.

Um unerwünschte Reklameflut zu verhindern, kann man sich in die sog. Robinson-Liste beim Verband der Adressenverleger und Direktwerbeunternehmer (Schiersteiner Str. 29, 6200 Wiesbaden) eintragen lassen. Soweit Daten des Petenten von Mitgliedsunternehmen gespeichert werden, erfolgt daraufhin die Löschung. Die Werbewirtschaft ist jedoch längst nicht überwiegend in dem Verband vertreten; auch wird die Robinson-Liste jährlich nur zweimal aktualisiert. Ferner besteht die Möglichkeit, gegenüber dem Kraftfahrtbundesamt in Flensburg und der Deutschen Postreklame GmbH in Frankfurt die Einwilligung zur Verwendung von Daten, die beim Erwerb von Kraftfahrzeugen und bei der Beantragung von Telefonanschlüssen angegeben wurden, für Werbezwecke zu verweigern. Schließlich hat jedermann ein Widerspruchsrecht bezüglich der Weitergabe von Meldedaten an Adreßbuchverlage durch die Meldebehörden.

Hinsichtlich der Forderungen der obersten Aufsichtsbehörden für den Datenschutz, dem Bürger bereits vor Verwendung seiner Adresse für Werbezwecke eine Widerspruchsmöglichkeit einzuräumen sowie Herkunft der Anschriften und Auswahlkriterien zu benennen, wird auf die Ausführungen zu 9.2.6 verwiesen.

7.5 Markt- und Meinungsforschung

Nicht eben selten werden von privaten Markt- und Meinungsforschungsinstituten Umfragen durchgeführt, z. B. Haushaltsbefragungen im Interesse von Warenhäusern, Befragungen über den Service von KfZ-Vertragswerkstätten und -Händlern im Auftrag von Herstellerwerken oder Befragungen nach umweltfreundlichem Verbrauchsverhalten im Auftrag einer von Wirtschaftsunternehmen geförderten Aktionsgemeinschaft.

Markt- und Meinungsforschungsinstitute unterliegen dem 4. Abschnitt des BDSG, soweit sie geschäftsmäßig geschützte personenbezogene Daten zum Zweck der Veränderung speichern,

MMV.10/2589

anonymisieren und in anonymisierter Form übermitteln (§ 31 Abs. 1 Satz 1 Nr. 2 BDSG). Nach § 36 BDSG dürfen personenbezogene Merkmale mit den anonymisierten Daten nicht mehr zusammengeführt werden, es sei denn (u. a.), daß die dadurch ermöglichte Nutzung der Daten noch für die Erfüllung des Speicherungszwecks erforderlich ist. Dies kommt vor allem in Betracht für Untersuchungen, bei denen dieselben Personen wiederholt befragt werden, um Trendveränderungen feststellen zu können. Eine Deanonymisierung ist hier notwendig, um herauszufinden, welche Aussagen eine bestimmte Person zu früheren Zeitpunkten gemacht hat.

Ein Hauptproblem bei den Befragungen stellt die Frage dar, ob und in welcher Form eine Einwilligung der Befragten zu der anfangs noch personenbezogenen Datenspeicherung erforderlich ist. Die Befragung selbst als Form der Datenerhebung wird vom BDSG nicht erfaßt. Die obersten Aufsichtsbehörden haben bereits im Jahre 1979 mit den Verbänden der Markt- und Sozialforscher folgendes Einvernehmen erzielt:

a) Bei Einfachbefragungen werden die Daten nur in manuell geführten internen Dateien gespeichert, so daß nach § 1 Abs. 2 Satz 2 BDSG nur die Vorschrift des § 6 BDSG über die Datensicherung Anwendung findet, ein Einwilligungserfordernis also nicht gegeben ist. Vorausgesetzt wird dabei, daß eine Zusammenführung von Adreß- und Fragenteil nur zum Zweck der Interviewer-Kontrolle erfolgt. Nach Abschluß dieser Kontrollen, spätestens bei Beginn der automatisierten Verarbeitung der Fragenteile, d. h. der Erfassung der Daten, sind die Adreßteile zu vernichten.

   Vorausgesetzt wird ferner, daß die Angaben im Fragenteil keine Herstellung eines Personenbezugs ermöglichen, etwa mit Hilfe von Zusatzwissen.

b) Bei Mehrfachbefragungen mit Vergleich der Befragungsergebnisse halten die Aufsichtsbehörden in allen Fällen eine Einwilligung für erforderlich, während nach Auffassung der Vertreter der Markt- und Meinungsforschungsinstitute eine analoge Anwendung des gesetzlichen Tatbestandes (§ 32 Abs. 1 BDSG) möglich ist. Die Aufsichtsbehörden haben aber anerkannt, daß im Hinblick auf ein bei den einzelnen Bevölkerungsgruppen zu besorgendes unterschiedliches Anschwellen der Verweigerungsrate und die damit verbundenen Verfälschungen der Ergebnisse auf die Schriftform der Einwilligung verzichtet werden kann. Unter Wahrung der beiderseitigen Rechtsstandpunkte haben sich die Markt- und Meinungsforschungsinstitute bereiterklärt, eine mündliche Einwilligungserklärung herbeizuführen, der eine Belehrung über die Freiwilligkeit, eine Unterrichtung über den allgemeinen Zweck der Befragung und die Aushändigung eines Merkblatts vorangehen muß, aus dem sich u. a. ergibt, was mit den Angaben geschieht. Werden dem Betroffenen Fragebogen vorgelegt oder zugesandt, so müssen diese einen ausdrücklichen Hinweis auf die Freiwilligkeit der Angaben enthalten.

Nach diesen Grundsätzen ist bei den häufig stattfindenden Telefonbefragungen eine Einwilligung nicht erforderlich, wenn personenbezogene Daten lediglich in manuellen internen Dateien erfaßt werden; bei Telefonbefragungen handelt es sich regelmäßig um Einmalbefragungen. An diesem Beispiel zeigt sich, daß die Ausklammerung der internen manuellen Dateien aus dem Anwendungsbereich des BDSG auch im privaten Bereich nicht unproblematisch erscheint, jedenfalls im Blick auf sensitive Datenkategorien.

Wenn aber bei Telefoninterviews personenbezogene Daten automatisiert gespeichert werden, ist das BDSG anzuwenden. Von der Schriftform der Einwilligung kann nur abgesehen wer-

MMV 10/2589

den, soweit im Einzelfall "wegen besonderer Umstände eine andere Form angemessen ist" (§ 3 Satz 2 BDSG). Hat der Interviewer, wie oft der Fall, lediglich nach dem Zufallsprinzip ausgewählte Telefondaten ohne Namen und Anschriften zur Hand, kommt es darauf an, ob ein Personenbezug mit Zusatzwissen herstellbar ist, etwa dadurch, daß der Angerufene sich mit seinem Namen meldet.

7.6 Arbeitnehmerdaten

7.6.1 Fragebogen für Stellenbewerber

Im Rahmen von Bewerbungen um einen Arbeitsplatz verlangen die Arbeitgeber nach den Erfahrungen der Aufsichtsbehörden in der Regel vom Bewerber die Ausfüllung umfangreicher Fragebogen. Diese Fragebogen werden teilweise nicht in Dateien aufbewahrt, so im Fall des BAG-Urteils vom 06.06.1984 (NJW 1984, 2910). Es kommt aber auch vor, daß die Fragebogen mehrerer Bewerber in Ordnern abgelegt werden, womit der Dateibegriff erfüllt ist. In beiden Fällen finden die Zulässigkeitsvorschriften des BDSG keine Anwendung, entweder, weil es sich um Akten handelt, oder weil die Daten der manuellen Datei nicht zur Übermittlung an Dritte bestimmt sind (§ 1 Abs. 2 Satz 2 BDSG). Das BDSG greift auch dann nicht, wenn die Fragebogen nach Einstellung von Bewerbern in Personalakten abgeheftet werden, die nicht als Datei im Sinne des BDSG angesehen werden können.

Nur wenn die Bewerberdaten automatisiert erfaßt werden, ist stets das BDSG zu beachten. Die Befragung als solche fällt allerdings nicht unter das BDSG, weil das BDSG die Phase der Erhebung nicht einbezieht. Jedoch dürfen (etwa wegen Verstoßes gegen das Persönlichkeitsrecht, d. h. das Grundrecht auf Datenschutz) unzulässig erhobene Daten nicht gespeichert

werden (BAG-Urteil vom 22.10.1986, NJW 1987, 2459). Im übrigen kommt es darauf an, ob die Speicherung der Bewerberdaten vor Entscheidung über die Einstellung im Rahmen der Zweckbestimmung eines vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen erforderlich ist (§ 23 Satz 1, 2.Alt. BDSG).

Nach der Rechtsprechung des BAG läßt der Schutz des Persönlichkeitsrechts nur solche Fragen des Arbeitgebers zu, an denen er zur Beurteilung der Eignung und Befähigung des Arbeitnehmers ein objektiv gerechtfertigtes Interesse hat. In die Privatsphäre des Arbeitnehmers darf nicht tiefer eingedrungen werden, als es der Zweck des Arbeitsverhältnisses unbedingt erfordert, wobei allerdings Unverzichtbarkeit nicht zu verlangen ist. Was der Arbeitgeber im Anbahnungsverhältnis über die Eignung des Bewerbers wissen muß, braucht sich nicht mit den Kenntnissen zu decken, die er nach Einstellung für den Arbeitseinsatz benötigt.

Prinzipiell dürfen Fragen über Ausbildung und beruflichen Werdegang, soweit arbeitsplatzrelevant, gestellt werden. Nach Auffassung des BAG sind gegen die Frage nach dem Familienstand schon im Anbahnungsverhältnis ebenfalls keine Einwendungen zu erheben, denn hiervon könne die Versetzungsmöglichkeit oder die Auswahl des Beschäftigungsortes mit den Folgeproblemen (z. B. Wohnraumbedarf, Schulprobleme usw.) abhängen. In dieser pauschalen Form ist dies nicht unbedenklich. Die Angaben "geschieden" oder "verwitwet" berühren nicht die Eignung für den Arbeitsplatz. Kinderlos Verheiratete können ebenso mobil sein wie Ledige, wenn der Ehegatte des Bewerbers nicht berufstätig ist.

Fragen nach dem Gesundheitszustand und nach früheren oder anhängigen Strafverfahren dürfen speziell nur gestellt werden, soweit sie streng arbeitsplatzbezogen sind. Gleiches gilt für Fragen nach vorhandenen Schulden. Zudem muß stets der Grundsatz der Verhältnismäßigkeit beachtet werden.

MMV10/2589

Unzulässig sind etwa Fragen nach einer Gewerkschaftszugehörigkeit. Für die Entscheidung über die Bewerbung interessieren auch weder Fragen nach Name, Geburtsdatum und Beruf von Ehegatten und Kindern noch beispielsweise nach der Zugehörigkeit zu einer bestimmten Krankenkasse.

7.6.2 Befragung des früheren Arbeitgebers

Eine Aufsichtsbehörde hatte aufgrund der Eingabe einer politischen Partei zu beurteilen, inwieweit ein Arbeitgeber über einen Stellenbewerber Auskünfte bei dessen früherem Arbeitgeber einholen darf. In dem konkreten Fall hatte der Bewerber offenbar kein Arbeitszeugnis seines früheren Arbeitgebers vorgelegt. Der Betrieb, bei dem er sich beworben hatte, übersandte deshalb dem früheren Arbeitgeber einen Fragebogen, in dem u. a. gefragt wurde nach Beschäftigungsdauer, Art der ausgeübten Tätigkeiten, Zuverlässigkeit und Gewissenhaftigkeit, Lohnpfändungen und Lohnabtretungen, häufiger Arbeitsunfähigkeit und unentschuldigtem Fehlen, Beanstandungen z. B. hinsichtlich Ehrlichkeit und Pünktlichkeit, Kündigungsgrund und danach, wer das Arbeitsverhältnis gelöst hatte.

Es kann davon ausgegangen werden, daß der überwiegende Teil der Fragen nur aus der Personalakte und sonstigem Wissen der Vorgesetzten beantwortet werden konnte. Teilweise werden aber die benötigten Informationen automatisiert gespeichert gewesen sein (z. B. Lohnabtretungen, Fehlzeiten). Da die Erhebung durch den prospektiven neuen Arbeitgeber im BDSG nicht geregelt ist, stellt sich nach dem BDSG nur die Frage, ob bei automatisierter Speicherung eine Übermittlung nach § 24 BDSG zulässig sein konnte. Die Aufsichtsbehörde hat den Fall mangels Vorliegens einer Beschwerde eines Betroffenen nicht konkret geprüft (§ 30 Abs. 1 BDSG), sondern lediglich der Petentin eine allgemeine Rechtsauskunft gegeben.

Soweit § 24 herangezogen werden kann, ist zu prüfen, ob die Übermittlung im Rahmen der Zweckbestimmung eines vertragsähnlichen Vertrauensverhältnisses, das hier nach Beendigung des Arbeitsvertrages ggf. fortbestanden hat, erfolgen konnte. Nach dem Urteil des BAG vom 18.09.1984 (JZ 1985, 1062) ist der Arbeitgeber aus dem Gesichtspunkt der nachwirkenden Fürsorgepflicht gehalten, "über die Erteilung des Zeugnisses hinaus im Interesse des ausgeschiedenen Arbeitnehmers Auskünfte über diesen an solche Personen zu erteilen, mit denen der Arbeitnehmer in Verhandlungen über den Abschluß eines Arbeitsvertrages steht." Ferner heißt es dort:" Der Arbeitgeber darf solche Auskünfte auch gegen den Willen des ausgeschiedenen Arbeitnehmers erteilen. Er kann grundsätzlich nicht gehindert werden, andere Arbeitgeber bei der Wahrung ihrer Belange zu unterstützen..... Die Auskünfte, zu denen der Arbeitgeber berechtigt ist, betreffen nur Leistung und Verhalten des Arbeitnehmers während des Arbeitsverhältnisses.".

Diese Entscheidung ist in Rechtsprechung und Literatur auf Kritik gestoßen. Es fragt sich, warum der neue Arbeitgeber entgegen der sonstigen Rechtsprechung des BAG zum Fragerecht auch solche Informationen erhalten dürfen soll, die nicht für den neuen Arbeitsplatz relevant sind, sondern sich lediglich auf den früheren Arbeitsplatz beziehen. Derartige "redundante" Daten werden zwar auch in Arbeitszeugnissen mitgeteilt; deren Vorlage durch Bewerber geschieht aber auf freiwilliger Basis. Im übrigen erscheint es weder im Rahmen des Vertrauensverhältnisses zu dem früheren Arbeitgeber noch zur Wahrung berechtigter Interessen des neuen Arbeitgebers (§ 24 Abs. 1 Satz 1, 3.Alt. BDSG) erforderlich, gegen den Willen des Bewerbers Auskünfte beim früheren Arbeitgeber einzuholen. Wenn der neue Arbeitgeber diese Auskünfte zur Entscheidung

über die Einstellung benötigt, kann er sie sich auch mit Einwilligung des Bewerbers verschaffen, dem es im Rahmen seines Selbstbestimmungsrechts vorbehalten ist, sich einmal überhaupt zu bewerben, und zum anderen, die dafür notwendigen Informationen bereitzustellen bzw. beschaffen zu lassen. Konsequent ist im öffentlichen Bereich nach dem Datenschutzgesetz Nordrhein-Westfalen die Datenübermittlung an einen künftigen Dienstherrn oder Arbeitgeber nur mit Einwilligung des Betroffenen zulässig (§ 29 Abs. 1 Satz 1 Satz 3 DSG NW). Zumindest aber muß der Bewerber Gelegenheit haben, sich zu den Auskünften seines früheren Arbeitgebers zu äußern.

Was die im vorliegenden Fall in dem Fragebogen gestellten Fragen betrifft, sind Fragen nach Lohnpfändungen und -abtretungen nur zulässig, wenn sie für den neuen Arbeitsplatz objektiv Bedeutung haben (ggf. bei Buchhaltern und Kassierern). Zu Unrecht erhobene Fragen darf der neue Arbeitgeber nicht speichern, weder nach dem BDSG noch unter arbeitsrechtlichen Gesichtspunkten (vgl. BAG-Urteil vom 22.10.1986, NJW 1987, 2459).

Der Arbeitgeber darf die ihm im Rahmen seines Fragerechts auferlegten Einschränkungen nicht dadurch umgehen, daß er Auskunfteien mit der Ermittlung beauftragt (s. auch 7.3).

Schließlich ist im Hinblick auf die Aufbewahrung von Fragebogen nach Ablehnung von Bewerbern festzuhalten, daß ein schutzwürdiges Interesse hieran grundsätzlich nur im Blick auf zu erwartende Rechtsstreitigkeiten und für deren Dauer bestehen kann, nicht aber, um den Bewerber zu einem späteren Zeitpunkt erneut anzusprechen (BAG-Urteil vom 06.06.1984, NJW 1984, 2910). Will sich der Arbeitgeber bei definitiver Ablehnung gegen die Verwaltungs- und Vorstellungskosten erneuter - aussichtsloser - Bewerbungen schützen, genügt die Speicherung von Name, Anschrift und Geburtsdatum als Identifizierungsdaten; die eigentlichen Bewerbungsunterlagen sind zu vernichten (BAG, a.a.O.).

MMV10/2589

7.6.3 Geheime Auswahl für Stipendium

In einem Fall aktenmäßiger Datenverarbeitung hatte ein Großbetrieb der EDV-Branche von seiner rechtlich selbständigen Tochterfirma, die Ausbildungs- und Umschulungsmaßnahmen im EDV-Bereich durchführt, sämtliche Unterlagen der teilnehmenden Schüler mit der Bitte um Prüfung erhalten, in welchen Fällen die Personalabteilung ein Stipendium gewähren könne. Kenntnis davon erhielten die Teilnehmer erst durch den Umstand, daß einige von ihnen zu Vorstellungsgesprächen eingeladen wurden.

Sicherlich hatte die Tochterfirma in bester Absicht gehandelt. Andererseits fand hinsichtlich der Nichtauserwählten eine geheime Negativauslese statt, so daß jedenfalls deren Selbstbestimmungsrecht beeinträchtigt wurde. Nachdem die Aufsichtsbehörde die Tochterfirma um Stellungnahme gebeten hatte, versprach diese von sich aus, in Zukunft die Teilnehmer vorher zu befragen und deren schriftliches Einverständnis einzuholen.

7.6.4 Telefondatenerfassung

Die lange Zeit umstrittene Frage, inwieweit private Arbeitgeber Daten über Telefongespräche der Arbeitnehmer erfassen dürfen, kann durch den Beschluß des BAG vom 27.05.1986 (NJW 1987, 674; Vorinstanz: LAG Düsseldorf) weitgehend als geklärt angesehen werden, soweit es um die Daten der anrufenden Arbeitnehmer geht, nicht jedoch im Blick auf die Daten der Angerufenen. Danach darf der Arbeitgeber zu Kontrollzwecken auch Zeitpunkt und Dauer von Privatgesprächen in automatisierter Form festhalten. Rechtsgrundlage im konkreten Fall war zwar eine Betriebsvereinbarung (mit ergänzendem Einigungsspruch), welche die Speicherung als "andere Rechtsvorschrift" im Sinne des § 3 Satz 1 Nr. 1 BDSG er-

laubte. Man wird jedoch die Feststellungen des BAG heranziehen können, um bei Fehlen einer Betriebsvereinbarung die Zulässigkeit der Speicherung nach § 23 BDSG (Zweckbestimmung des Vertragsverhältnisses) zu bejahen.

Nach zutreffender Ansicht des BAG bedarf auch die Verarbeitung personenbezogener Daten der Angerufenen als Anschlußinhaber oder Gesprächsteilnehmer datenschutzrechtlich eines Erlaubnistatbestandes. Hierüber war jedoch in dem zu entscheidenden Fall nicht zu befinden. Man wird jedoch die Speicherung der vollständigen Zielnummer nicht als zu Kontrollzwecken erforderlich im Rahmen der Zweckbestimmung des Vertragsverhältnisses bzw. zur Wahrung berechtigter Interessen des Arbeitgebers ansehen können. Die Kontrolle, etwa zu dem Zweck, ein extensives Gebrauchmachen von privaten Telefongesprächen zu verhindern, erscheint auch möglich, wenn die beiden letzten Ziffern der Telefonnummer weggelassen werden, wie in Nordrhein-Westfalen in den Dienstanschlußvorschriften des Finanzministers für automatische Gesprächsdatenerfassungsanlagen vorgesehen. Auch hat der Arbeitgeber bei Privatgesprächen den Angerufenen gegenüber kein Kontrollrecht. Jedenfalls dürfte bei vollständiger Erfassung der Zielnummer eine Beeinträchtigung schutzwürdiger Belange der Angerufenen anzunehmen sein, wobei auch die Drittwirkung des Fernmeldegeheimnisses (Art. 10 GG) zu berücksichtigen ist (vgl. BAG, a.a.O.).

Am Rande sei noch auf das BAG-Urteil vom 13.01.1987 (DB 1987, 1153) hingewiesen, nach der Arbeitgeber die (vollständigen) Zielnummern solcher Gespräche nicht erfassen dürfen, die Berufspsychologen im Rahmen ihrer Geheimhaltungspflicht (§ 203 Abs. 1 Nr. 2 StGB) mit Privatpersonen führen.

7.6.5 Personalinformationssysteme

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentli-

chen Bereich haben keinen genauen Überblick über den Einsatz komplexer Personalinformationssysteme in der Wirtschaft (vgl. für den öffentlichen Bereich 9. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz, S. 77). Da hierfür der 3. Abschnitt des BDSG maßgebend ist, können sich die Aufsichtsbehörden systematische Erkenntnisse hierüber auch nicht verschaffen. Im übrigen sind im Berichtszeitraum entsprechende Beschwerden nicht vorgebracht worden.

Schwerpunkt der Rechtsdiskussion war insoweit in der jüngeren Vergangenheit nicht der individuelle Datenschutz, sondern der durch Mitbestimmungs- und Unterrichtungsrechte des Betriebsrates charakterisierte kollektive Datenschutz (vgl. u. a. BAG-Beschluß vom 23.04.1985, NZA 1985, 669, und BAG-Beschluß vom 17.03.1987, RDV 1987, 189).

7.7 Mieterdaten

Nicht nur bei der Anbahnung von Arbeitsverhältnissen (vgl. 7.6.1), sondern auch bei der Anbahnung von Mietverhältnissen ist die Verwendung von Fragebogen weitverbreitete Übung.

Fragebogen von Vermietern werden, wie die Praxis der Aufsichtsbehörden zeigt, oft nur aktenmäßig aufbewahrt und sind darüber hinaus vielfach nicht zur Übermittlung an Dritte, sondern nur zur Verwendung durch den Vermieter bestimmt. Obwohl das Bundesdatenschutzgesetz in solchen Fällen grundsätzlich nicht anwendbar ist, wirken die Aufsichtsbehörden, wenn sie mit derartigen Fragebogen befaßt werden, auf eine

M ... 10/2589

datenschutzgerechte Gestaltung hin, wie sie bei Verarbeitung in automatisierten Verfahren zu erfolgen hätte.

Nach § 23 BDSG ist die Speicherung der von Mietern erfragten Daten zulässig im Rahmen der Zweckbestimmung des vertragsähnlichen Vertrauensverhältnisses zwischen Mieter und Vermieter oder soweit es zur Wahrung berechtigter Interessen des Vermieters erforderlich ist und kein Grund zur Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden. Im Kern dürfen danach nur solche Angaben erfragt werden, die zur Abschätzung des Mietrisikos erforderlich sind. Auf Bedenken stoßen grundsätzlich Fragen nach Verlobung, Trennung und Scheidung. Nicht relevant sind in der Regel auch Angaben zum getrennt lebenden Ehegatten sowie zum Einkommen von Angehörigen.

Dagegen dürften Fragen nach dem Arbeitgeber und dem aktuellen Einkommen des Mietbewerbers im Prinzip zulässig sein, da ihre Beantwortung wesentliche Anhaltspunkte für die Einschätzung der wirtschaftlichen Leistungsfähigkeit und der Zuverlässigkeit des Mietbewerbers zu liefern vermag und der Vermieter bei einer Fehleinschätzung mit erheblichen Nachteilen zu rechnen hätte. Angaben über die Staatsangehörigkeit von Bewerbern können in solchen Fällen gespeichert werden, in denen es sich um große Wohnanlagen handelt und Nachteilen, wie etwa Gettoisierung oder Streitigkeiten zwischen verschiedenen Nationalitäten, vorgebeugt werden soll.

Auskunfteien dürfen Vermietern auf Anfrage Auskünfte über den Mietbewerber geben, soweit sie Grundlage der Beurteilung des wirtschaftlichen Risikos sein können. Eine andere Beurteilung ergibt sich allerdings für die SCHUFA, die als

geschlossenes Kreditinformationssystem lediglich an ihre Anschlußpartner und nur zu dem Zweck der Minderung eines Kreditrisikos Auskunft erteilen darf. Auskünfte im Hinblick auf die Vermietung von Wohnraum sind danach unzulässig (so auch Teilnahmebedingungen der SCHUFA). In einem konkreten Fall hatte jedoch ein Vermieter, der zugleich Inhaber einer Einzelhandelsfirma war, diese Einschränkung umgangen, indem er bei der SCHUFA offenbar vorgab, die Auskunft bezüglich der Vergabe eines Warenkredits begehren zu wollen. Auf Veranlassung der eingeschalteten Datenschutzaufsichtsbehörde wurde der Vermieter von der SCHUFA entsprechend abgemahnt.

Im Rahmen bestehender Mietverhältnisse ergeben sich u. a. datenschutzrechtliche Probleme bei der Bekanntgabe von Verbrauchsdaten an die Bewohner von Mehrfamilienwohnhäusern. So wurde in einem konkreten Beschwerdefall gefragt, ob die Bekanntgabe der Verbrauchsdaten einzelner Mieter gegenüber allen Mietern datenschutzrechtlich zulässig ist. Aus dem Mietvertrag selbst kann eine solche Berechtigung generell nicht abgeleitet werden. Auch ist ein berechtigtes Interesse, ohne weitere Voraussetzungen sämtliche Verbrauchsdaten aller Mieter einer Wohnanlage zu erhalten, nicht anzuerkennen. Vielmehr wird ein solches Interesse erst dann zu bejahen sein, wenn sich Anhaltspunkte für eine fehlerhafte Berechnung der Abrechnungsdaten ergeben. Das Interesse der Mieter, deren Daten für die Überprüfung erforderlich sind, muß dann zurückstehen. Es ist jedoch ein Verfahren zu wählen, bei dem die Offenbahrung personenbezogener Daten auf das unbedingt notwendige Maß beschränkt wird.

Des öfteren stellt sich in der Praxis auch die Frage, inwieweit die Bekanntgabe personenbezogener Daten bei der Angabe von Vergleichswohnungen im Rahmen von Mieterhöhungsverlangen statthaft ist. Bei einer Aufsichtsbehörde führte

ein Mieter Beschwerde darüber, daß ihm von seinem Vermieter bei einem Mieterhöhungsverlangen außer den Verleichswohnungen sowohl die Eigentümer bzw. Vermieter dieser Vergleichswohnungen mit voller Anschrift als auch die Mieter mit Anschrift und Höhe der Miete benannt worden seien.

Das Gesetz zur Regelung der Miethöhe, welches die Benennung von drei Vergleichswohnungen als eine Möglichkeit einräumt, den Anspruch des Vermieters auf Mieterhöhung zu begründen, enthält zu der Frage, inwieweit personenbezogene Daten bekanntgegeben werden dürfen, keine Regelung. Maßgeblich ist daher bei dateimäßiger Verarbeitung § 24 BDSG. Im Rahmen der danach vorzunehmenden Interessenabwägung müßte die Offenbarung personenbezogener Daten bei der Benennung von Vergleichswohnungen zunächst zur Wahrung berechtigter Interessen des Mieters erforderlich sein.

Nach dem Beschluß des Bundesgerichtshofs vom 20.9.1982 (NJW 1982, 2867) braucht der Vermieter lediglich Hinweise zu Art, Größe, Ausstattung, Beschaffenheit und Lage von Wohnungen anderer Vermieter zu geben. Die Benennung der jeweiligen Mietvertragsparteien oder einer von ihnen sei dagegen nicht erforderlich; wer der Vermieter der Vergleichswohnung sei oder wer sie als Mieter nutze, sei für die Bemessung des Mietzinses ohne Bedeutung. Dagegen hat das Bundesverfassungsgericht keine Bedenken gegen die Bekanntgabe des Namens des Wohnungsinhabers und von dessen Adresse erhoben (vgl. Beschluß vom 8.11.1988, NJW 1989, 969). In keiner der beiden Entscheidungen werden allerdings Aspekte des BDSG behandelt.

Die Erforderlichkeit der Offenbarung durch den Vermieter kann nicht damit begründet werden, daß durch spätere Erkundigungen des Mieters oder im Falle eines Rechtsstreits

über das Mieterhöhungsverlangen die Namen möglicherweise ohnehin aufgedeckt werden (vgl. BGH, a.a.O.). Es ist nämlich durchaus möglich, daß der Mieter dem mit der Angabe von Vergleichswohnungen begründeten Mieterhöhungsverlangen ohne weiteres zustimmt, so daß die Anonymität der Vertragspartner dieser Wohnungen gewahrt bleibt. Im übrigen scheinen Befragte häufig Wert darauf zu legen, in Mieterhöhungsverlangen nicht namentlich benannt zu werden, um nach Möglichkeit nicht behelligt zu werden (BGH, a.a.O). Um eine Beeinträchtigung schutzwürdiger Belange der Betroffenen auszuschließen, erscheint es geboten, die Betroffenen vor der Weitergabe ihrer Daten zumindest zu informieren und ihnen die Möglichkeit zum Widerspruch zu geben.

7.8 Kundendaten

Eine Vielzahl von Fällen betrifft den Bürger in seiner Eigenschaft als Kunde und Verbraucher. Die Skala reicht dabei bis hin zu Fällen, in denen der Kunde "zu seinem Glück gezwungen wird", und Fällen, in denen der Datenschutz zu Unrecht als Grund einer Auskunftsverweigerung angegeben wird. Einige Beispiele sollen dies verdeutlichen.

Ein Betroffener beschwerte sich darüber, daß ihm ein Reisebüro unter Hinweis auf den Datenschutz die Benennung der Telefonnummer eines ihm bekannten Hotels, in dem, wie er wußte, seine Eltern in der Türkei in Urlaub weilten, verweigert habe, obwohl er einige wichtige Fragen an seine Eltern hatte. Ein Versuch des Betroffenen bei der Auslandsauskunft war zuvor gescheitert. Eine Beeinträchtigung schutzwürdiger Belange der Eltern durch die Bekanntgabe der Telefonnummer des Hotels wäre nicht eingetreten, da der Sohn ein nahestehender Angehöriger war und sicherlich nicht ohne triftigen

Grund die kostspielige Mühe auf sich nehmen wollte, eine Verbindung zu seinen Eltern in einem weit entfernten Land herzustellen. Falls trotz des offenbarten Wissens des Sohnes Zweifel an seiner Identität nicht ausgeschlossen gewesen sein sollten, hätte das Reisebüro die Vorlage seines Personalausweises erbitten können. Wenn auch der Datenschutz die Auskunftsverweigerung nicht rechtfertigte, so ist nicht zu verkennen, daß der Datenschutz hier nicht als Vorwand diente; vielmehr dürfte die "Angst" vor einem etwaigen Datenschutzverstoß die treibende Kraft gewesen sein.

In einem anderen Fall nahm eine Firma den Kauf einer Autotelefonanlage zum Anlaß, für den Kunden ohne sein Wissen die Mitgliedschaft bei einem Automobilclub zu beantragen und für ihn im voraus einen Jahresbeitrag zu entrichten. Eine Beeinträchtigung der schutzwürdigen Belange des betroffenen Kunden durch diese unverhoffte "Vergünstigung" war nicht auszuschließen, weil der Bürger in der Regel selbst entscheiden will, ob und wo er Mitglied wird, und weil eine von ihm gewollte Trennung mit dem damit verbundenen Schriftverkehr eine unzumutbare Belästigung darstellen kann. Zudem scheint es durchaus denkbar, daß der Betroffene bereits Mitglied in einem anderen Automobilclub war. Auf Intervention der Aufsichtsbehörde erklärte sich die Firma bereit, in Zukunft die Clubmitgliedschaft für ihre Kunden nur noch mit deren ausdrücklicher schriftlicher Einwilligung zu beantragen.

Um einen u. U. "faulen Kunden", der ohne Berechtigung für sich Datenschutz in Anspruch nehmen wollte, ging es in folgendem Fall. Ein Verbrauchermarkt hatte gegen den Betroffenen Strafanzeige wegen Diebstahls geringwertiger Sachen erstattet. Die Staatsanwaltschaft stellte das Strafverfahren

gegen Zahlung eines Geldbetrages von DM 150.-- ein. Der Betroffene wollte nun über die Aufsichtsbehörde die Vernichtung seiner Unterlagen erreichen, die bei dem Verbrauchermarkt zusammen mit anderen Diebstahlsvorgängen in einem Geschäftsordner abgelegt worden waren. Das BDSG konnte keine Anwendung finden, da keine dateimäßige Datenverarbeitung vorlag. Auch im übrigen sah die Aufsichtsbehörde keine Veranlassung, auf eine Löschung der Daten hinzuwirken, da der Vorfall bei einem weiteren Auffälligwerden des Betroffenen hätte Bedeutung erlangen können, obwohl es zu einer rechtskräftigen Entscheidung über den Diebstahlsverdacht nicht gekommen war.

Kann im Zusammenhang mit dem SCHUFA-Verfahren die Angabe des Geburtsdatums dem Schutz des Betroffenen dienen (vgl. 7.1.4), so trifft dies nicht auf den im Rahmen einer Beschwerde bekanntgewordenen Fall zu, daß ein Kreditinstitut in seinen Kontonummern die Geburtsdaten der Bankkunden ausweist, und zwar sechsstellig mit Tag, Monat und Jahr.

Bereits die Zulässigkeit der Speicherung des Geburtsdatums als Bestandteil der Kontonummer durch das Kreditinstitut ist zweifelhaft, weil sie weder zur Zweckerfüllung des Vertrages mit dem Bankkunden noch zur Wahrung eines berechtigten Interesses des Kreditinstituts erforderlich ist. Auf erhebliche Bedenken stößt das Verfahren jedenfalls deshalb, weil der Kontoinhaber beim bargeldlosen Zahlungsverkehr (z. B. bei Überweisungen oder Scheckausstellungen) regelmäßig dem Adressaten der Bankleistungen gegenüber seine Kontonummer preisgeben muß. Wenn dieser den Aufbau der Kontonummer kennt, könnte er hieraus ohne Schwierigkeiten das Geburtsdatum des Kontoinhabers entnehmen und dieses unberechtigterweise nutzen. Eine Beeinträchtigung der schutzwürdigen Belange des Kontoinhabers ist daher nicht auszuschließen. Nach

Auffassung der im "Düsseldorfer Kreis" (s. 9.) vertretenen obersten Aufsichtsbehörden der Länder kann auch die Angabe des Geburtsdatums gegenüber der Bank nicht als Einwilligung im Sinne des § 3 BDSG in diese Form der Kontoführung gewertet werden.

Das vom "Düsseldorfer Kreis" eingeschaltete Bundesaufsichtsamt für das Kreditwesen hat das Kreditinstitut gebeten, zukünftig den Kunden bereits im formularmäßig abgefaßten Kontoeröffnungsantrag darüber aufzuklären, wie sich die von dem Institut vergebene Kontonummer zusammensetzt. Unterschreibt der Kunde den Antrag, so bringt er damit auch zum Ausdruck, daß er mit der Einbeziehung seines Geburtsdatums in die Kontonummer einverstanden ist. Gegen dieses Verfahren hat der "Düsseldorfer Kreis" keine Bedenken erhoben. Die Wirksamkeit einer solchen Einwilligung dürfte allerdings im Blick auf die Freiwilligkeit fraglich sein, wenn die Verwendung des Geburtsdatums als Teil der Kontonummer von sämtlichen Kreditinstituten praktiziert würde. Dies ist jedoch nicht der Fall.

7.9 Patientendaten

Wiederholt haben Bürger um Miteilung gebeten, ob die Weitergabe ihrer Daten durch ihren Arzt zur Honorarabrechnung an eine privatärztliche Verrechnungsstelle oder ein freies Rechenzentrum zulässig ist.

Im "Düsseldorfer Kreis" (s. 9.) haben die obersten Aufsichtsbehörden mehrheitlich die Auffassung vertreten, daß derartige Übermittlungen von Patientendaten nur auf der Grundlage einer ausdrücklichen Einwilligung der Patienten rechtlich unangreifbar sind. Über die Frage, ob

eine Datenweitergabe ohne Einwilligung geltendem Recht zuwiderläuft, wurde keine abschließende Klärung erzielt. Sie ist auch im Schrifttum umstritten (vgl. OLG Stuttgart, NJW 1987, 1490). Überlegenswert wäre möglicherweise (hier nicht zu entscheiden), die Delegierung der Honorarabrechnung als im Rahmen der Zweckbestimmung des Behandlungsvertrages liegend (§ 24 Abs. 1 Satz 1, 1.Alt., BDSG) anzusehen, weil eine eigene Abrechnung durch den Arzt wegen des damit verbundenen Aufwandes auch aus Patientensicht kaum noch erwartet werden kann. Ein solches weitgehend übliches und sozialadäquates Verhalten könnte u. U. auch nach § 203 StGB von der Schweigepflicht befreien, wenn in dessen Rahmen die Sozialäquanz zur Offenbarung des Arztgeheimnisses berechtigen würde.

Die Übermittlung gegen den erklärten Willen des Patienten würde jedoch einen Verstoß gegen das strafrechtliche Verbot des Geheimnisverrats in § 203 StGB und eine Verletzung schutzwürdiger Belange im Sinne des § 24 Absatz 1 BDSG darstellen. Um aber überhaupt die Möglichkeit zu einem rechtzeitigen Widerspruch zu eröffnen, sollte der Arzt die Patienten - etwa durch einen Aushang im Wartezimmer - über das bei ihm übliche Abrechnungsverfahren informieren. Damit könnte der Patient auf einer Liquidation ohne Einschaltung dritter Stellen bestehen. Im übrigen unterliegen immerhin auch die Angehörigen einer privatärztlichen Verrechnungsstelle der strafrechtlich gesicherten Schweigepflicht (§ 203 Absatz 1 Nr. 6 StGB). Denkbar wäre schließlich, nach Maßgabe einer besonderen Rechtsvorschrift die Honorarabrechnung durch bestimmte dritte Stellen ausdrücklich zu legitimieren.

Ein nicht befriedigend gelöstes "Dauerproblem" stellt auch die Frage dar, inwieweit bei dem Verkauf von Arztpraxen ganze Patientenkarteien ohne Einwilligung der Patienten an

MMW 10/2589

den Praxisnachfolger übergeben werden dürfen. Aufgrund einer in Baden-Württemberg von politischer Seite neu entfachten Diskussion und eines von der Presse aufgegriffenen aktuellen Rechtgsgutachtens hat sich auch der "Düsseldorfer Kreis" mit der Thematik beschäftigt.

In der Realität erfolgt die Übergabe von Patienkarteien regelmäßig ohne Einwilligung der Patienten. Gestützt wird dies auf ein Urteil des Bundesgerichtshofs vom 7.11.1973 (NJW 1974, 602). Der BGH berief sich auf einen Beschluß des Bundesverfassungsgerichts vom 8.3.1972 (NJW 1972, 1123), das hierüber aber weder zu entscheiden hatte noch entschieden hat. Die Entscheidung des Bundesgerichtshofs ist, wenn nicht schon mit Inkrafttreten des BDSG, so doch spätestens mit der Ausprägung des Rechts der Bürger auf informationelle Selbstbestimmung durch das Volkszählungsurteil überprüfungsbedürftig geworden.

Nach § 3 BDSG bedarf es der ausdrücklichen, grundsätzlich schriftlich zu erklärenden Einwilligung der Betroffenen zur Weitergabe ihrer Daten ohne gesetzliche Grundlage. Es kann nicht ohne weiteres davon ausgegangen werden, daß ein Patient, zumal in Gebieten mit hoher Arztdichte, vom Praxisnachfolger weiterhin betreut werden möchte. So kommt es durchaus vor, daß bereits Praxisvertreter von Patienten nicht akzeptiert werden.

Eine gesetzliche Befugnis zur Übergabe ganzer Patientenkarteien ohne (strafrechtlich auch schon mutmaßliche) Einwilligung dürfte der Bestimmung des § 203 Absatz 1 Nr. 1 StGB, die gerade zum Schutze der Patienten die Verletzung der ärztlichen Schweigepflicht mit Strafe bedroht, kaum normenklar zu entnehmen sein, ebensowenig den standesrechtlichen Berufsordnungen für die Ärzte. Auch die

allgemeine Übermittlungsregelung des § 24 Abs. 1 Satz 1,3. Alt. BDSG wird schwerlich als Rechtfertigung dienen können. Mag ein berechtigtes Interesse jedenfalls des Praxisveräußerers gegeben sein, so spricht einiges dafür, daß bei der vorzunehmenden Interessenabwägung die schutzwürdigen Belange zumindest der Patienten überwiegen, die sich nicht vom Praxisnachfolger behandeln lassen wollen, selbst angesichts dessen, daß auch der Nachfolger an die ärztliche Schweigepflicht gebunden ist. Das Vertrauensverhältnis des Patienten zu dem Arzt seiner Wahl (bisheriger Praxisinhaber) ist durch § 203 StGB in besonderer Weise geschützt. Bei Patientendaten handelt es sich prinzipiell um besonders sensitive Informationen, für deren Verwendung ohne Willen des Betroffenen nach dem im Rahmen des informationellen Selbstbestimmungsrechts zu beachtenden Verhältnismäßigkeitsgrundsatz strenge Anforderungen gelten. Danach bestehen erhebliche Bedenken, dem - anzuerkennnenden - wirtschaftlichen Interesse an der "Veräußerung des Patientenstammes" den Vorrang einzuräumen. Überdies verlangt § 24 BDSG eine Einzelfallabwägung hinsichtlich jedes einzelnen Patienten.

Der "Düsseldorfer Kreis" hat angesichts der ärztlicherseits befürchteten praktischen Schwierigkeiten der Einwilligungslösung (u.a. ungenügender Rücklauf) die Möglichkeit einer (künftigen) gesetzlichen Widerspruchslösung erörtert, nach welcher der Übergabe der Patientenkarteien nichts im Wege stünde, wenn die zuvor in geeigneter Weise informierten Patienten kein "Veto" einlegten. Darüber hinaus wäre zu prüfen, ob andere gesetzliche Lösungen in Betracht kommen.

7.10 Mitgliederdaten

Für Mitglieder von Vereinen stellt sich immer wieder die Frage, unter welchen Voraussetzungen die Übermittlung ihrer

MMV 10/2589

Daten - sei es an andere Vereinsmitglieder, sei es an außenstehende Dritte - statthaft ist.

Besonders häufig werden die Aufsichtsbehörden mit der Frage befaßt, ob im Rahmen von Gruppenversicherungsverträgen Daten von Vereinsmitgliedern an das Versicherungsunternehmnen weitergegeben werden dürfen, damit dieses die Mitglieder zwecks Abschlusses von Einzelversicherungen, bei denen in Ansehung der Gruppenversicherung günstigere Konditionen als sonst üblich gewährt werden, umwerben kann. Der "Düsseldorfer Kreis" (vgl. 9.) hatte im Jahre 1979 dem Lösungsvorschlag des Bundesaufsichtsamtes für das Versicherungswesen zugestimmt, daß der Verein unter Verzicht auf Datenübermittlungen die Werbung für den Abschluß von Einzelversicherungen selbst übernimmt oder die Daten nur mit schriftlicher Einwilligung der Mitglieder weitergibt. Im Jahre 1984 kam der "Düsseldorfer Kreis" mit Mehrheit zusätzlich zu dem Ergebnis, daß es bei Alt-Mitgliedern ausreichend erscheint, ihnen aufgrund entsprechender Information eine Widerspruchsmöglichkeit bezüglich der Datenübermittlung einzuräumen.

Dementsprechend konnte der Hamburger Datenschutzbeauftragte auch mit einem großen Hamburger Versicherungsunternehmen Einigung dahin erzielen, daß Datenübermittlungen bei Neumitgliedern nur mit schriftlicher Einwilligung, bei Alt-Mitgliedern nur im Rahmen der Widerspruchslösung erfolgen sollten. Einige Vereine sind aber bisher offenbar nicht zu einer vollständigen Übernahme dieses Konzepts bereit gewesen. Andererseits liegen den Aufsichtsbehörden aber auch Fälle vor, in denen die Vereine das Verhandlungsergebnis anscheinend nicht einmal kannten. Im übrigen ist klarzustellen, daß sich die Absprachen nur auf Name und Anschrift,

nicht aber auf die Übermittlung auch des Geburtsdatums bezogen.

Weit verbreitet ist das Bestreben von Vereinen, für ihre Mitglieder Mitgliederverzeichnisse herauszugeben. So erhielt eine Aufsichtsbehörde hinsichtlich der Zulässigkeit eines solchen Verzeichnisses eine Anfrage von einem Verein, der sich nach seiner Satzung mit Problemen medizinischer Kunstfehler auf der Basis persönlicher Betroffenheit auseinandersetzt und sich im wesentlichen als Selbsthilfeorganisation Betroffener versteht. Wesentlicher Vereinszweck ist demgemäß ein entsprechender Erfahrungsaustausch.

Die Aufsichtsbehörde vertrat die Auffassung, daß insoweit grundsätzlich eine durch Vereinsbeschluß herbeigeführte Widerspruchslösung ausreicht. In diesem besonderen Fall wäre es aber auch vertretbar gewesen, die in der Ausgabe des Mitgliederverzeichnisses an die Mitglieder liegende Datenweitergabe ohne die Bedingung der Widerspruchsmöglichkeit für zulässig zu erachten, da sie sich im Rahmen des vertragsähnlichen Vertrauensverhältnises, nämlich der Vereinsmitgliedschaft, hielt und kein Grund zu der Annahme bestand, daß dadurch schutzwürdige Belange der Betroffenen beeinträchtigt wurden. Bei einem in solch intensiver Weise auf Kontakt und Austausch der Mitglieder ausgelegten Vereinszweck wie im vorliegenden Fall wird man die gegenseitige Kenntnis der Adreßdaten als von den Vereinsmitgliedern gewollt ansehen können.-

Zu Zwecken der Mitgliederwerbung verschickte eine Vereinigung von Hochschullehrern ein Rundschreiben an Nichtmitglie-

der in der Professoren- und Dozentenschaft. Gleichzeitig wurden die Mitglieder gebeten, Nichtmitglieder persönlich zu werben; hierzu erhielten sie einen Computerausdruck mit den Namen der Nichtmitglieder sowie früherer Mitglieder mit einem Vermerk über deren Austritt.

Bei der hier erfolgten Bekanntgabe der Daten von Nichtmitgliedern an Mitglieder der Vereinigung war eine Beeinträchtigung schutzwürdiger Belange im Einzelfall nicht auszuschließen. Durch persönliche Werbegespräche von Kollegen konnten sich Umworbene u. U. in ihrer Entscheidungsfreiheit eingeengt oder gar in ihrer engeren Privatsphäre bedrängt fühlen. Dies gilt in besonderen Maße für Angesprochene, die aus der Vereinigung ausgetreten waren. Überdies schien bereits die Erforderlichkeit dieser Werbemethode zweifelhaft, da ein Rundschreiben-Verfahren möglich war und praktiziert wurde. Der Inhalt des Werberundschreibens hielt sich im Rahmen des Angemessenen. Widersprüche von Betroffenen gegen etwaige künftige Werbeschreiben hätten wegen offenkundiger Aussichtslosigkeit auch deren Erforderlichkeit in Frage gestellt.

In einem anderen Fall ging es um die Weitergabe der Daten von Vereinsmitgliedern an Außenstehende. Eine Tageszeitung hatte eine Reportage über einen Turnverein veröffentlicht. Aus den Reihen der Vereinsmitglieder kam die Anregung, den Beitrag auch den Mitgliedern zugänglich zu machen, die nicht Abonnenten der Zeitung waren. Der Verein gab die automatisiert geführten Adreßdaten aller Mitglieder an die Zeitung weiter, damit diese entsprechend tätig werden konnte. Ein Vereinsmitglied beschwerte sich bei der Aufsichtsbehörde über dieses Vorgehen, da es darauf vertraut hatte, daß seine Daten nicht an Dritte weitergegeben würden.

Die Aufsichtsbehörde sah zutreffend keine gesetzliche Vorschrift, welche die Übermittlung erlaubt hätte. Bei der Weitergabe aller Daten an die Tageszeitung war nicht auszuschließen, daß schutzwürdige Belange Betroffener beeinträchtigt wurden. Dies gilt vor allem für die Abonnenten der Zeitung, die den Beitrag bereits aufgrund ihres Abonnements zur Kenntnis erhalten hatten, so daß hier die Bekanntgabe der Vereinsmitgliedschaft an die Zeitung nicht zu rechtfertigen war. Auch hinsichtlich der Nichtabonnenten kann vielfach unterstellt werden, daß ihnen die Preisgabe ihrer Mitgliedschaft gerade gegenüber einer örtlichen Tageszeitung aus mancherlei Gründen unangenehm gewesen wäre. Auch sollte ja nicht eigentlich dem Interesse der Tageszeitung, sondern gezielt demjenigen der Vereinsmitglieder gedient werden. Es war aber weder ein berechtigtes Interesse des Vereins noch der Tageszeitung, die Nichtabonnenten zu ihrem eigenen Besten zu "bevormunden".

Generelle Aussagen für alle Arten von Vereinen lassen sich jedoch nicht treffen. So dürfte es nicht von vornherein allen Mitgliedern eines großen Automobilclubs recht sein, wenn ihre Daten in einem mehrere Millionen erfassenden, bundesweiten Mitgliederverzeichnis des Clubs gewissermaßen "veröffentlicht" werden, zumal bei dieser Größenordnung die Gefahr der Weitergabe an außenstehende Dritte kaum auszuschließen sein wird.

7.11 Versichertendaten

Bezüglich der Daten von Versicherungsnehmern wird zunächst auf die Ausführungen zu allgemeinen Datenschutzproblemen unter 9.2.4 (Klauseln der Versicherungswirtschaft) und 7.2.5/7.2.6 (zentrale Warndateien) verwiesen; genannt sei

auch die aus der Sicht der Mitgliedschaft in Vereinen behandelte Thematik der Gruppenversicherungsverträge (7.10). Zusätzlich sollen hinsichtlich der von den Aufsichtsbehörden bearbeiteten Einzelfälle zwei Beispiele genannt werden, in denen es um eine aktenmäßige Datenverarbeitung von Versichertendaten ging, auf die das BDSG nicht anwendbar ist.

Der Verwalter einer Wohnungseigentümergemeinschaft kündigte gegenüber einem Sachversicherungsunternehmen eine Glasversicherung. Daraufhin sandte ihm die Versicherung nach Auswertung ihrer Akten eine Aufstellung über die Grundpfandgläubiger der Wohnungseigentümer mit dem Bemerken, es bedürfe der Einverständniserklärung der Wohnungseigentümer, weil der Verwalter zur Kündigung für diese nicht befugt sei. Die Übermittlung der genannten Daten war jedoch nicht erforderlich. Vielmehr hätte ein allgemeiner Hinweis genügt, damit der Verwalter die Wohnungseigentümer von sich aus zur Abgabe ihres Einverständnisses und Beibringung der Zustimmungserklärung der Grundpfandgläubiger nach § 106 des Versicherungsvertragsgesetzes auffordern konnte. Die Aufsichtsbehörde teilte dem beschwerdeführenden Wohnungseigentümer mit, aufgrund der aktenmäßigen Datenverarbeitung sei ihr ein Einschreiten nicht möglich, sie habe aber der Versicherung mitgeteilt, daß das praktizierte Verfahren mit Grundgedanken des Datenschutzrechts nicht vereinbar sei.

In dem zweiten Fall war eine Beschwerdeführerin von ihrer Krankenversicherung aufgefordert worden, auf einem Formblatt, das zur Weiterleitung an den behandelnden Arzt bestimmt war, Angaben zu ihrem Netto-Gehalt zu machen. Es handelte sich um einen Antrag auf Auszahlung des Krankentagegeldes, auf dessen Vorderseite der Versicherungsnehmer u. a. Angaben zum Netto-Einkommen machen sollte, während auf

der Rückseite des Formulars die Bescheinigung der Arbeitsunfähigkeit durch den behandelnden Arzt vorgesehen war. Die Krankentagegeldversicherung ist eine Verdienstausfallversicherung, die sich an dem Netto-Einkommen orientiert. Auf die Kenntnis entsprechender Angaben ist jedoch nur die Versicherung, nicht aber der Arzt angewiesen. Auf den Vorschlag der Aufsichtsbehörde sagte die Versicherung zu, künftig statt eines vor- und rückseitig bedruckten Fragebogens zwei getrennte Formulare zu verwenden.

Beide geschilderten Fälle hatten eine sensitive Datenverarbeitung zum Gegenstand (Mitteilung der Grundpfandläubiger bzw. des Einkommens). Zumindest in dem zuletzt angeführten Fall lag ein objektiv erheblicher Datenschutzverstoß gegen das Grundrecht auf informationelle Selbstbestimmung vor, wenn auch auf seiten der datenverarbeitenden Stelle keine Absicht vermutet werden soll.

8. Datensicherung

8.1 Allgemeine Erfahrungen

Da regelmäßige Kontrollen nur im Bereich des 4. Abschnitts gesetzlich zugelassen sind, verwundert es nicht, daß sich die Prüfung der Aufsichtsbehörden hinsichtlich der erforderlichen Datensicherungsmaßnahmen hauptsächlich auf die Betriebe erstreckt, die geschäftsmäßig Daten verarbeiten. Bei den Kontrollbesuchen der Stellen des 4. Abschnitts nahmen die Fragen der Datensicherung im Vergleich zu materiell-rechtlichen Datenschutzproblemen den breitesten Raum ein. Im 3. Abschnitt (Datenverarbeitung für eigene Zwecke) können die Aufsichtsbehörden nur auf Veranlassung betroffener Bürger tätig werden. Diesen fehlt aber vor allem im Hinblick auf EDV-Anlagen oft die erforderliche Kenntnis, um sie benachteiligende Verstöße gegen die Gebote der Datensicherung geltend zu machen und begründet darzulegen.

MMV 10/2589

Die Erfahrungen der Aufsichtsbehörden zeigen, daß im privaten Bereich im wesentlichen gleichartige Probleme in der Praxis auftreten wie im öffentlichen Bereich (so etwa beim Einsatz von PC's und der Verwendung von Paßwörtern). Dies liegt in der Natur der Sache. Nicht von ungefähr waren die Datensicherungsvorschriften im öffentlichen und privaten Bereich lange Zeit identisch und stimmen auch dort, wo inzwischen teilweise abweichende Regelungen getroffen wurden (vgl. § 10 Abs. 2 des neuen DSG NW mit der Anlage zu § 6 Abs. 1 Satz 1 BDSG), weitgehend überein. Es kann daher zur Vertiefung der sich bei der Datensicherung stellenden Probleme auf die Tätigkeitsberichte des Landesbeauftragten für den Datenschutz und die hierzu dem Landtag vorgelegten Stellungnahmen der Landesregierung verwiesen werden. Im übrigen sei angemerkt, daß die im "Düsseldorfer Kreis" von den obersten Aufsichtsbehörden der Länder erarbeiteten vorläufigen Richtlinien zur Durchführung des BDSG (s. 9.2.1) den Fragen der Datensicherung breiten Raum widmen.

Hinsichtlich der Tätigkeit der Aufsichtsbehörden im privaten Bereich ist hervorzuheben, daß Datensicherungsmängel im besonderen bei kleineren und mittleren Betrieben festgestellt wurden. So fehlte es häufig bezüglich der innerbetrieblichen Organisation an notwendigen Funktionstrennungen und schriftlichen Festlegungen der jeweiligen Befugnisse. Zur Datenverarbeitung im Auftrag (§ 37 BDSG) ist zu bemerken, daß die Erteilung schriftlicher Weisungen durch den Auftraggeber bei kleineren Betrieben nicht "branchenüblich" zu sein scheint, während bei größeren Auftraggebern meist schriftliche Regelungen mit Kontrolle ihrer Einhaltung angetroffen wurden. Es soll aber eingeräumt werden, daß der Gesetzgeber die Schriftform der Auftragserteilung bislang nicht vorgesehen hat, obwohl sie für eine wirksame Auftragskontrolle mehr als wünschenswert wäre, um eine dem Auftrag genau entsprechende Datenverarbeitung im Sinne des Gesetzes zu "gewährleisten".

8.2 Gespendete Disketten mit Fehlern

Eine gemeinnützige nicht-öffentliche Stelle informierte die Aufsichtsbehörde darüber, sie habe festgestellt, daß ca. 200 ihr von einem Unternehmen gespendete Disketten noch personenbezogene Daten enthielten. Da das spendende Unternehmen den Regelungen des 4. Abschnitts des BDSG unterliegt, nahm die Aufsichtsbehörde dort eine Überprüfung vor. Dabei kam folgendes zutage:

Das Unternehmen hatte vor der Schenkung die auf den Disketten gespeicherten personenbezogenen Daten durchaus löschen wollen und insoweit einen Fachmann eingeschaltet. Dieser hatte empfohlen, die Disketten zu "initialisieren", d. h. das programmierte "Inhaltsverzeichnis" zu löschen, um damit nach seiner Ansicht die Daten unleserlich zu machen. Das Unternehmen hatte diesen Rat befolgt.

Nach § 6 BDSG in Verbindung mit der zugehörigen Anlage hat die datenverarbeitende Stelle die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um u. a. die unbefugte Kenntnisnahme gespeicherter personenbezogener Daten zu verhindern. Die Stelle, die im Wege der Spende in den "Genuß" der Disketten kommen sollte, war selbstverständlich nicht befugt, die für Zwecke des spendenden Unternehmens gespeicherten Daten für ihre ganz anderen Zwecke zu benutzen. Eine derartige Zweckentfremdung lag ihr auch völlig fern, wie ihr "Hilferuf" bei der Aufsichtsbehörde beweist.

Die Daten waren daher zu löschen. "Löschen" ist nach dem Gesetz das Unkenntlichmachen gespeicherter Daten. Unkenntlich gemacht sind Daten nur dann, wenn die Kenntnisnahme wie auch die Rekonstruierbarkeit ihres Informationsgehalts unmöglich

10/2589

geworden sind. Die Aufsichtsbehörde hat das Unternehmen darauf hingewiesen, daß die Daten durch Initialisierung zwar nicht mehr logisch gezielt aufgerufen werden konnten, jedoch physisch auf dem Datenträger weiter vorhanden und durch sequentielles Ablesen einer Kenntnisnahme zugänglich waren. So hatte im vorliegenden Fall die Spendenempfängerin auf den Disketten gespeicherte Daten in der Tat ablesen können, was sie gerade zur Anrufung der Aufsichtsbehörde veranlaßte.

Die Aufsichtsbehörde hat sichergestellt, daß die personenbezogenen Daten auf den Disketten eindeutig gelöscht wurden, so daß die beschenkte Stelle die Disketten von nun an auch wirklich gemeinnützig verwenden konnte.

8.3 Postversand an Nichtadressaten

Im Berichtszeitraum und auch in den Vorjahren wurde eine Aufsichtsbehörde wiederholt darauf aufmerksam gemacht, daß Bürger Schriftstücke zugesandt erhalten hatten, die nicht sie, sondern Dritte betrafen. In den meisten Fällen erhielt der Bürger die fremde Post (vorwiegend Kontoauszüge) zusammen mit an ihn adressierten Schreiben.

Soweit Unternehmen des 3. Abschnitts Absender der fehlgeleiteten Schreiben waren, hatte die Aufsichtsbehörde keine Eingriffsmöglichkeiten, da Beschwerden der eigentlichen Adressaten nicht vorlagen und die "Fürsprache" Dritter, nämlich hier der tatsächlichen Empfänger, eine Anlaßaufsicht nicht auslösen kann. Dennoch bittet die Aufsichtsbehörde die Unternehmen regelmäßig um Stellungnahme, wie es zu dem Postversand an unbeteiligte Dritte kommen konnte. Zumeist ist individuelle Unachtsamkeit die Ursache. Soweit darüber hinausgehende technische und organisatorische Mängel zugrunde lagen, wurden die Unternehmen entsprechend beraten.

MMV10/2589

8.4 Daten in der Tonne: Aufsicht auf Spurensuche

Auch im privaten Bereich gibt es in wiederkehrenden Abständen Fälle, in denen es infolge Nachlässigkeit oder gar Leichtsinn zu unliebsamen "Pannen" bei der Datenträgervernichtung gekommen ist. So werden EDV-Belege, Rezepte usw. in offenen Containern auf der Straße "zwischengelagert". Die Aufsichtsbehörde erfährt von solchen Vorfällen zumeist aus der Presse oder von unbeteiligten Dritten, so daß sie nicht im Wege der Anlaßaufsicht einschreiten kann. Am Beispiel eines Falles soll geschildert werden, wie sehr die Aufsichtsbehörde in Anspruch genommen werden kann, wenn sich dennoch einmal ein Betroffener bei ihr meldet.

Eine Bürgerin hatte sich an die Aufsichtsbehörde gewandt und dargelegt, ihr sei ein Computerausdruck mit u. a. sie betreffenden personenbezogenen Daten zugesandt worden von einem ihr unbekannten Herrn, der auf diese Weise selbst einen persönlichen Bezug herstellen wollte. Der Computerausdruck enthielt zu mehreren Personen Name, Anschrift und eine Zuordnungsnummer, die jedoch keinen Schluß auf die Herkunft des Computerausdrucks zuließ. Der Bundesbeauftragte für den Datenschutz, den die Betroffene zunächst angerufen hatte, hatte die Eingabe an die Aufsichtsbehörde weitergeleitet.

Der Absender hatte sich der Betroffenen nicht ohne Umschweife gänzlich offenbaren wollen und nur sein Postfach angegeben. Nachdem die Aufsichtsbehörde ihn ausfindig gemacht hatte, teilte er mit, daß er den Computerausdruck in einer Mülltonne vor einem Kindergarten gefunden hatte, die voller EDV-Listen gewesen sei. Es stand zu vermuten, daß diese Listen dem Kindergarten zum Bemalen der Rückseite zur Verfügung gestellt worden waren, eine Vernichtung der Datenträger also allenfalls über den Umweg des Papierkorbes in der Absicht der datenverarbeitenden Stelle gelegen hat. Die Befragung weiterer

Betroffener, deren Daten aus dem Computerausdruck hervorgingen, ergab keine konkreten Hinweise auf die Herkunft, sondern nur die Erkenntnis, daß alle von ihnen in den letzten Jahren gebaut hatten. Nunmehr nahm die Aufsichtsbehörde unter dem Suchbegriff "Bauen" eine systematische Durchsicht des Telefon- und Branchenfernsprechbuches vor. Bei einer von mehreren daraufhin angerufenen Stellen wurde die Aufsichtsbehörde schließlich fündig. Da es sich um eine öffentliche Stelle handelte, gab sie die Beschwerde zur weiteren Bearbeitung an den Bundesbeauftragten für den Datenschutz zurück.

Die Klärung der Zuständigkeitsfrage durch die nicht nur tätige, sondern überaus tatkräftige Aufsichtsbehörde war ein notwendiger Schritt. Trotz des für sie negativen Ergebnisses hatte sie dem Datenschutz gleichwohl einen Dienst erwiesen, indem sie den zunächst vermeintlich unzuständigen Bundesbeauftragten für den Datenschutz nach Abschluß ihrer geradezu detektivischen Ermittlungen auf die richtige Spur führte.

9. Zusammenarbeit der obersten Aufsichtsbehörden im "Düsseldorfer Kreis"

9.1 Entstehung, Funktion, Arbeitsweise

Im Hinblick auf eine möglichst einheitliche Auslegung und Anwendung des Bundesdatenschutzgesetzes vom 27. Januar 1977 kamen die Länder bereits im Jahre 1977 überein, sich bezüglich auftretender Zweifelsfragen untereinander abzustimmen und ihre Erfahrungen auszutauschen. Aus einer im November 1976 zusammengetretenen Gesprächsrunde entstand eine ständige Arbeitsgemeinschaft der Vertreter der obersten Aufsichtsbehörden der Länder für den Datenschutz im nicht-öffentlichen Bereich (Innenministerien der Länder Baden-Württemberg, Bayern,

Hessen, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz und Schleswig-Holstein, Senator für Inneres Berlin, Datenschutzbeauftragte der Länder Bremen, Hamburg und Saarland). Nordrhein-Westfalen erklärte sich zur Federführung bereit. Vorsitz und Geschäftsführung liegen seitdem beim Innenminister Nordrhein-Westfalen, der die zweimal jährlich stattfindenden Plenarsitzungen regelmäßig in Düsseldorf ausrichtet. Dies führte zu der Kurzbezeichnung "Düsseldorfer Kreis".

Um dem Ziel einer effektiven Umsetzung des BDSG in der Praxis möglichst nahezukommen, suchte der "Düsseldorfer Kreis" von Anfang an den Kontakt zu den Spitzenorganisationen der Wirtschaft, insbesondere vor dem Hintergrund der überregionalen und länderübergreifenden Datenverarbeitung großer Wirtschafts- und Dienstleistungsunternehmen. Mit den alsbald aufgenommenen Verhandlungen sollte eine freiwillige Selbstbindung der den Dachverbänden angeschlossenen Unternehmen im Sinne einer möglichst datenschutzfreundlichen Handhabung des neuen Gesetzes erreicht werden.

Der "Düsseldorfer Kreis" bildet zur rationelleren Bewältigung seiner Aufgaben Arbeitsgruppen, die nach Bedarf einberufen werden. Beispielhaft genannt seien die Arbeitsgruppen "SCHUFA", "Versicherungswirtschaft", "Handelsauskunfteien", "Versandhandel" und "Adreßhandel" sowie seit 1989 im Hinblick vor allem auf den EG-Binnenmarkt 1992 die Arbeitsgruppe "Internationaler Datenverkehr". Der Vorsitz der Arbeitsgruppen ist in der Regel nach dem Sitz der Spitzenverbände oder der schwerpunktmäßigen Vertretung der jeweiligen Gesprächspartner aus der Wirtschaft auf die Bundesländer verteilt. Die Ergebnisse der Arbeitsgruppen werden im Gesamtgremium beraten.

Die Beratungsergebnisse des "Düsseldorfer Kreises" haben zwar als Interpretationen und Empfehlungen für die Mitglieder keine Verbindlichkeit im rechtlichen Sinne. In vielen Fällen werden jedoch tragbare Kompromisse gefunden. Darüber hinaus liefert der Meinungsaustausch wichtige Orientierungspunkte für die Datenschutzaufsicht in den Ländern, die in Bayern, Niedersachsen, Nordrhein-Westfalen und Rheinland-Pfalz den Regierungspräsidenten übertragen ist und in den anderen Ländern unmittelbar von den Innenressorts oder von den eingangs genannten Landesdatenschutzbeauftragten wahrgenommen wird.

Der "Düsseldorfer Kreis" hält auch Kontakt mit den für den öffentlichen Bereich zuständigen Datenschutzbeauftragten des Bundes und der Länder, soweit diese nicht bereits Mitglieder des "Düsseldorfer Kreises" sind, sowie mit dem auf Bundesebene für die Datenschutzgesetzgebung zuständigen Bundesminister des Innern. So nehmen an den Sitzungen regelmäßig Vertreter und des Bundesministers des Innern und des Bundesbeauftragten für den Datenschutz teil. Bei wesentlichen Berührungspunkten mit dem Datenschutz im öffentlichen Bereich waren Mitarbeiter der Datenschutzbeauftragten der Länder in Arbeitsgruppen des "Düsseldorfer Kreises" vertreten und hat eine enge sachliche Abstimmung mit der Konferenz der Datenschutzbeauftragten des Bundes und der Länder stattgefunden. Dies gilt insbesondere im Hinblick auf Kreditinformationssysteme und die Versicherungswirtschaft.

Schließlich ist auf die Mitwirkung des "Düsseldorfer Kreises" in der alljährlich stattfindenden Internationalen Konferenz der Datenschutzbeauftragten hinzuweisen.

9.2 Wesentliche Ergebnisse

9.2.1 Vorläufige Verwaltungsvorschriften zum BDSG

Schon bald nach Inkrafttreten des Gesetzes erarbeitete die "Münchener Runde", eine Arbeitsgruppe des "Düsseldorfer Kreises", mit dem Ziel einer einheitlichen Handhabung der Aufsichtspraxis einen Vorschlag für vorläufige Verwaltungsvorschriften zum BDSG. Diese wurden in den Ländern, in denen die Datenschutzaufsicht im nicht-öffentlichen Bereich von der Mittelinstanz wahrgenommen wird, als verbindliche Richtlinien umgesetzt (in Nordrhein-Westfalen durch Runderlaß des Innenministers vom 21. Februar 1979). Eine Länderinitiative schien geboten, weil nicht damit zu rechnen war, daß der Bund von seiner Kompetenz zum Erlaß von Verwaltungsvorschriften Gebrauch machen würde; dies hat er bis heute auch nicht getan.

So wertvoll die vorläufigen Verwaltungsvorschriften waren, so wollten und konnten sie nicht auf alle nur denkbaren Auslegungs- und Anwendungsfragen Antwort geben. Vielmehr traten zunehmend Absprachen des "Düsseldorfer Kreises" in den Vordergrund, um in der Aufsichtspraxis flexibel auf ständig neu sich stellende Einzelprobleme reagieren zu können.

9.2.2 Bankauskunftsverfahren

Im Jahre 1984 erzielte der "Düsseldorfer Kreis" mit der Kreditwirtschaft nach intensiven Verhandlungen Einigung über die Neugestaltung des Bankauskunftsverfahrens. Eine Änderung der Allgemeinen Geschäftsbedingungen der Kreditinstitute hatte zu einem offenkundigen Vertrauensverlust bei der Öffentlichkeit geführt, deren Datenschutzbewußtsein durch das soeben ergangene Volkszählungsurteil erheblich sensibilisiert worden war.

Bankauskünfte sind allgemein gehaltene Feststellungen und Bemerkungen über die wirtschaftlichen Verhältnisse des Kunden, seine Kreditwürdigkeit und Zahlungsfähigkeit; betragsmäßige Angaben über Kontostände, Sparguthaben, Depot- oder sonstige dem Kreditinstitut anvertraute Vermögenswerte sowie Kreditinanspruchnahmen werden nicht gemacht. Bankauskünfte erhalten nur eigene Kunden sowie andere Kreditinstitute für deren eigene Zwecke und die ihrer Kunden, nicht aber beispielsweise Auskunfteien. Im Hinblick auf das die vertraglichen Beziehungen zwischen den Kreditinstituten und ihren Kunden prägende sog. Bankgeheimnis wurde vereinbart, Bankauskünfte über Privatkunden nur noch mit ausdrücklicher Einwilligung des Betroffenen im Einzelfall zu erteilen. Bankauskünfte über Geschäftskunden (juristische Personen sowie im Handelsregister eingetragene Kaufleute) dürfen gegeben werden, sofern keine anderslautende Weisung des betroffenen Kunden vorliegt. Die Auskunftsverweigerung wegen fehlender Einwilligung ist so zu formulieren, daß sie nicht als nachteilige Auskunft verstanden werden kann. Auf Verlangen des Betroffenen hat das Kreditinstitut diesem den Inhalt einer erteilten Auskunft mitzuteilen. Auch in Ansehung anderer, hier im Überblick nicht darstellbarer Einzelheiten konnte auf diesem Gebiet ein wegweisender Erfolg für den Datenschutz erzielt werden.

9.2.3 SCHUFA-Verfahren

Bereits während der Verhandlungen über das Bankauskunftsverfahren bestand zwischen dem "Düsseldorfer Kreis" und der Kreditwirtschaft Einvernehmen, daß auch das SCHUFA-Informationssystem, in welchem zentral von der SCHUFA (Schutzgemeinschaft für allgemeine Kreditsicherung) zur Beurteilung der Kreditwürdigkeit Auskünfte im Rahmen von Kreditgewährungen, Kontoeröffnungen und Bürgschaftsübernahmen erteilt

MMV10/2589

werden, unter datenschutzrechtlichen Aspekten durchleuchtet werden müsse (vgl. zu SCHUFA und SCHUFA-Verfahren auch 7.1). Zu einem Durchbruch bei den Verhandlungen kam es jedoch erst nach dem Urteil des Bundesgerichtshofs vom 19. September 1985 (NJW 1986, 46) zu der damals in den AGB verwendeten SCHUFA-Klausel. Der Bundesgerichtshof erblickte in dieser pauschalen Klausel einen Verstoß gegen die für Einwilligungserklärungen nach dem BDSG vorgeschriebene besondere Hinweispflicht sowie eine unangemessene Benachteiligung des Kreditnehmers nach § 9 AGB-Gesetz; ferner ermächtige sie entgegen dem BDSG zu pauschalen Datenübermittlungen ohne Interessenabwägung im Einzelfall.

Gemeinsam mit dem Zentralen Kreditausschuß und der BUNDES-SCHUFA wurden neue SCHUFA-Klauseln entwickelt, die seit dem 01.07.1986 u. a. für Kontoeröffnung, Kreditaufnahme und Bürgschaftserklärung Verwendung finden und zusammen mit einem Merkblatt für den Kunden die Transparenz der Datenverarbeitung wesentlich erhöhen. Im Hinblick darauf, daß das SCHUFA-Informationssystem seine Legitimation ausschließlich aus der Beurteilung der Kreditwürdigkeit bezieht, wurde der Kreis der Systemnutzer grundsätzlich auf Kreditinstitute und solche Wirtschaftsunternehmen, die Konsumenten Geld oder Warenkredite zur Verfügung stellen, beschränkt. Ausgeschlossen wurden danach u. a. Immobilienvermieter, Getränkegroßhändler sowie bestimmte Dienstleistungsunternehmen wie Lesezirkel, Fernschulen und Möbelspeditionen; Versicherungsunternehmen dürfen am SCHUFA-Verfahren nur insoweit teilnehmen, als sie Darlehen (zur Wohnungsbaufinanzierung) gewähren.

9.2.4 Klauseln der Versicherungswirtschaft

Das Volkszählungsurteil und das BGH-Urteil zur SCHUFA-Klausel

A 1 / 10 / 2589

sowie ein weiteres Urteil des Bundesgerichtshofs vom 17. Dezember 1985 (NJW 1986, 2505 - Ein-Mann-GmbH -) hatten neue Maßstäbe gesetzt , die eine Überprüfung der von den Datenschutzaufsichtsbehörden Ende der siebziger Jahre akzeptierten Versicherungsklauseln auf ihre datenschutzrechtliche Tragfähigkeit erforderlich machten.

Es handelte sich hierbei zum einen um die Schweigepflichtentbindungsklauseln, die bei Abschluß einer privaten Kranken-, Unfall- oder Lebensversicherung zu unterzeichnen sind und für die Versicherungsunternehmen die Grundlage zur Erhebung von Gesundheitsdaten bei Ärzten, anderen Personenversicherern und sonstigen Stellen zur Einschätzung des Risikos eines Vertragsabschlusses mit dem Antragsteller sowie für die Beurteilung der Leistungspflicht im jeweiligen Leistungsfalle bilden sollen. Der zweite Problemkreis betraf die nahezu in allen Zweigen der Versicherungswirtschaft seit langem übliche, bislang unter der fragwürdigen Überschrift "Datenschutzklausel" oder "Datenschutzermächtigungsklausel" firmierende Datenverarbeitungsklausel, mit deren Anerkennung die Versicherungsunternehmen zu einer Datenübermittlung an andere Versicherer, Rückversicherer, Verbände und sonstige Stellen ermächtigt sein sollen. Insbesondere geht es hierbei um die Übermittlung personenbezogener Daten an in der Versicherungswirtschaft besonders zahlreiche zentrale Warndateien zur Beurteilung besonderer Risiken und anderer Auffälligkeiten (vgl. dazu näher 7.2). Die Rechtswirksamkeit der genannten Einwilligungsklauseln war nach Auffassung der Datenschutzaufsichtsbehörden im Lichte der erwähnten Rechtsprechung zweifelhaft geworden, da sie in ihrer Tragweite von den Versicherungsnehmern nicht überblickt werden konnten; auch lag jedenfalls im Blick auf die Schweigepflichtentbindungsklauseln die Annahme einer unangemessenen Benachteiligung im Sinne des AGB-Gesetzes nahe.

Nach langwierigen Verhandlungen der obersten Aufsichtsbehörden für den Datenschutz mit der Versicherungswirtschaft, an denen auch das Bundesaufsichtsamt für das Versicherungswesen beteiligt war, konnten im Jahre 1989 neu gefaßte Schweigepflichtentbindungsklauseln in den Bereichen Kranken-, Unfall- und Lebensversicherung abschließend vereinbart werden. Zugleich wurden hinsichtlich der Zulässigkeit der Datenverarbeitung eine neue Einwilligungsklausel sowie ein diesbezügliches Merkblatt mit einer Übersicht über die Datenverarbeitungsprozesse in der Versicherungswirtschaft formuliert. Beide Klauseln (Schweigepflichtentbindung, Einwilligung) bedürfen der Genehmigung des Bundesaufsichtsamtes für das Versicherungswesen, die wegen wiederholter redaktioneller Änderungswünsche bezüglich des Merkblatts bedauerlicherweise bisher nicht erteilt werden konnte.

In den neugefaßten Schweigepflichtentbindungsklauseln wird die Befreiung von der ärztlichen Schweigepflicht nunmehr zeitlich begrenzt auf die letzten 10 Jahre vor und 5 Jahre nach Antragstellung; bei der Lebensversicherung ist nur eine Befristung auf die Zeit nach der Antragsannahme vorgesehen (3 Jahre). Ferner wird nunmehr ausdrücklich die Frage der Schweigepflichtentbindung in sog. Leistungsfällen, d. h. den Fällen konkreter Inanspruchnahme der Versicherung, geregelt. Danach hat (erst) die Geltendmachung eines Leistungsanspruchs durch Vorlage von Abrechnungsunterlagen die Bedeutung einer Schweigepflichtentbindung im jeweiligen Einzelfall; von der Schweigepflicht befreit werden lediglich die Angehörigen von Heilberufen oder Krankenanstalten, die in den vorgelegten Unterlagen genannt sind oder an der Heilbehandlung beteiligt waren.

Die neue Einwilligungsklausel bedeutet einen datenschutz-

rechtlichen Fortschritt vor allem deshalb, weil in einem umfänglichen Merkblatt für den Versicherungsnehmer beschrieben wird, an wen seine Daten übermittelt werden und zu welchen Zwecken dies geschieht. Nach der Einwilligungsklausel gilt die Einwilligung nur, wenn der Versicherungsnehmer die Möglichkeit hatte, in zumutbarer Weise vom Inhalt des Merkblatts zur Datenverarbeitung Kenntnis zu nehmen. In dem Merkblatt wird ausdrücklich festgehalten, daß die Einwilligungserklärung unabhängig von der nach den Erlaubnistatbeständen des BDSG im Einzelfall vorzunehmenden Interessenabwägung abgegeben wird. Die Einwilligung wird danach vor allem in Grenzfällen der Zulässigkeit der Datenverarbeitung nach den Abwägungskriterien des BDSG bedeutsam.

Können die zu den Versicherungsklauseln erzielten Ergebnisse insgesamt als Erfolg gewertet werden, so vermögen sie gleichwohl aus der Sicht des Datenschutzes nicht gänzlich zu befriedigen. Den Versicherungsnehmern bleibt faktisch nur die Wahl, die Klauseln zu unterzeichnen oder auf Versicherungsschutz zu verzichten. Die Transparenz der Datenverarbeitung wurde zwar wesentlich verbessert, doch erscheint zweifelhaft, ob das ausführliche Merkblatt immer gelesen wird. Einfluß auf die Datenverarbeitung, vor allem auf die Betreibung zentraler Warndateien, hat der Kunde nicht. Auch eröffnet der Gesetzgeber in den Generalklauseln des BDSG relativ weite Verarbeitungsräume und setzt der Verwendung personenbezogener Daten aufgrund von Einwilligungserklärungen keine umschriebenen Grenzen. Die Bedenken des Landesbeauftragten für den Datenschutz in seinem neunten Tätigkeitsbericht (S. 30/31) gehen in die gleiche Richtung. Wünschenswert wären daher klare gesetzgeberische Entscheidungen, die geeignet sind, einen gerechten Interessenausgleich im Hinblick auf die sensitiven Daten der Versicherungsnehmer herbeizuführen.

MMV 10/2589

9.2.5 Novellierung des BDSG

Seit dem ersten Referentenentwurf zur Novellierung des BDSG aus dem Jahre 1983 hat sich der "Düsseldorfer Kreis" mehrfach mit den Novellierungsbestrebungen des Bundes zu diesem Gesetz beschäftigt. Bei der Vorbereitung der Stellungnahme des Bundesrates vom Februar 1989 zu dem aktuellen Regierungsentwurf (s. 2.2.1) hat der weitgehende Konsens der obersten Aufsichtsbehörden einen erheblichen Beitrag gleistet.

9.2.6 Sonstiges

Von den Verhandlungen und Aktivitäten des "Düsseldorfer Kreises", über die vorstehend nicht gesondert berichtet wurde, seien zunächst ferner hervorgehoben die Gespräche mit den Handelsauskunfteien. Mit diesen konnte schon im Jahre 1980 eine Einigung hinsichtlich der in der Öffentlichkeit kritisierten sog. Nachbarschaftsbefragungen erzielt werden. Nach Ansicht der obersten Aufsichtsbehörden besteht bei derartigen Befragungen die Gefahr, daß die Nachbarn zu nachteiligen Spekulationen über den Betroffenen veranlaßt werden können, was insbesondere in Bagatellfällen in keinem angemessenem Verhältnis zu dem berechtigten Interesse des Kunden der Auskunftei steht. Die Vertreter der Wirtschaftsauskunfteien erklärten dazu, daß zwar Grundlage einer seriösen Recherche die Befragung des Betroffenen selbst sei, jedoch die von ihm gemachten Angaben einer weiteren Überprüfung bedürften. Sie erklärten sich aber bereit, die Fälle der Nachbarschaftsbefragung auf ein Minimum zu reduzieren und in erkennbaren Bagatellfällen auf die Nachbarschaftsbefragung ganz zu verzichten. Dennoch erfolgende Nachbarschaftsbefragungen sollen auf folgende Angaben beschränkt werden: Wohnort, Aufenthaltsdauer, Einkommen, Arbeitgeber und wirt-

MMV 10/2589

schaftliche Verhältnisse. Ferner sollen absprachegemäß Fragen nach einer persönlichen Beurteilung des Betroffenen durch die Nachbarn unterblieben.

Erwähnt seien auch die langjährigen Verhandlungen mit der Deutschen Krankenhausgesellschaft, die auf deren ausdrücklichen Wunsch im Jahre 1978 aufgenommen wurden und zu einem fruchtbaren Meinungsaustausch führten. Die dabei erzielten Ergebnisse hinsichtlich des Datenschutzes im Krankenhaus flossen in die Krankenhausgesetzgebung der Länder ein, ebenso eine Entschließung vom März 1986 der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, welcher der "Düsseldorfer Kreis" eine umfängliche Problemanalyse zur Verfügung gestellt hatte.

Weniger erfolgreich verliefen die Verhandlungen in den Sektoren Adreßhandel und Direktwerbung. Hier war die betreffende Arbeitsgruppe des "Düsseldorfer Kreises" vor allem bemüht, eine Unterrichtung der Betroffenen über die Quellen, aus denen deren Anschriften bezogen werden, sowie über die Auswahlkriterien zu erreichen. Auch sollte den Betroffenen die Möglichkeit eröffnet werden, bereits beim ersten Kontakt mit einem werbenden Unternehmen (z. B. durch Ankreuzen auf dem Erstbestellschein) der Weitergabe seiner Anschrift zu Werbezwecken an Dritte zu widersprechen. Während die Vertreter der Werbewirtschaft diese Vorschläge jedenfalls als diskussionswürdig ansahen, steht ihnen der Spitzenverband des Versandhandels, ohne den eine Einigung nicht herbeigeführt werden kann, bislang ablehnend gegenüber, weil dafür nach seiner Ansicht das BDSG keine Grundlage bietet und der erforderliche Aufwand unverhältnismäßig ist. Die obersten Aufsichtsbehörden haben inzwischen ihre Vorstellungen in das Gesetzgebungsverfahren zur Novellierung des BDSG eingebracht.

9.3 Zusammenfassung

Die Zusammenarbeit der obersten Aufsichtsbehörden im "Düsseldorfer Kreis" hat sich nicht nur als nützlich, sondern als unentbehrlich erwiesen. Ohne seine Bemühungen wären für weiteste Bevölkerungskreise so wichtige Ergebnisse wie in den Bereichen SCHUFA und Versicherungswirtschaft für den Datenschutz nicht erzielbar gewesen. Allerdings muß festgehalten werden, daß in einigen Problembereichen und Detailfragen eine Annäherung der Standpunkte bislang nicht möglich war.

Der "Düsseldorfer Kreis" wird auch nach der Neufassung des Bundesdatenschutzgesetzes als Mittler zwischen Bürger und Wirtschaft gebraucht werden. Der "Stein der Weisen" zur Präzisierung der Generalklauseln des BDSG ist noch immer nicht gefunden, so daß angesichts des Erfindungsreichtums der Wirtschaft stets von neuem der Interessenausgleich mit den schutzwürdigen Belangen der Betroffenen gesucht werden muß.

10. Grenzüberschreitender Datenverkehr

Im Zeichen der bevorstehenden Vollendung des EG-Binnenmarkts widmet sich der "Düsseldorfer Kreis" den Fragen des grenzüberschreitenden Datenverkehrs in verstärktem Maße. Schon heute lassen sich im Bank- und Kreditkartenbereich, in der Touristik-Branche, bei Wirtschaftsauskunfteien und im Arbeitnehmerbereich grenzüberschreitende Datenströme erheblichen Umfangs feststellen. Mit dem weiteren Zusammenwachsen der nationalen Märkte werden andere Bereiche folgen; vorstellbar sind insbesondere gesteigerte Aktivitäten und Zentralisierungsbestrebungen bei Kreditinformationssystemen, der Versicherungswirtschaft, dem Versandhandel, dem Adressenhandel und Direktmarketing sowie Telekommunikationsdiensten.

M 10/2589

Das BDSG erlaubt im nicht-öffentlichen Bereich den Transfer personenbezogener Daten in andere Staaten grundsätzlich nur im Rahmen der Zweckbestimmung von Vertragsverhältnissen und vertragsähnlichen Vertrauensverhältnissen oder soweit es zur Wahrung berechtigter Interessen erforderlich ist und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. Diese Übermittlungsvoraussetzungen gelten auch für die Datenverarbeitung im Auftrag (vor allem Service-Rechenzentren).

Jedoch darf der Datenverkehr zwischen Staaten, die die Datenschutzkonvention des Europarates vom 28. Januar 1981 (BGBl. II 1985, S. 538) ratifiziert haben, allein zum Zweck des Schutzes des Persönlichkeitsbereichs nicht verboten oder von einer besonderen Genehmigung abhängig gemacht werden, weil die Konvention voraussetzt, daß die Vertragsparteien die Datenschutzgrundsätze der Konvention in ihrem innerstaatlichen Recht verwirklicht haben. Hat allerdings ein Vertragsstaat für bestimmte Arten von personenbezogenen Daten oder automatisierten Dateien/Datensammlungen mit personenbezogenen Daten wegen der Beschaffenheit dieser Arten besondere Vorschriften erlassen, ist er berechtigt, den Datentransfer in einen anderen Vertragsstaat zu verbieten, wenn dessen Vorschriften keinen gleichwertigen Schutz vorsehen.

Bisher sind der Konvention nur 8 von 23 Mitgliedstaaten des Europarates wirksam beigetreten, nämlich innerhalb der EG die Bundesrepublik Deutschland, Frankreich, Großbritannien, Luxemburg und Spanien sowie außerhalb der EG Norwegen, Österreich und Schweden. Entgegen der Konvention verfügt Spanien noch nicht über eine nationale Datenschutzgesetzgebung. Im Falle von Spanien und der zuvor nicht genannten Staaten muß das Vorliegen eines dem BDSG oder jedenfalls der Europa-

ratskonvention vergleichbaren Datenschutzstandards geprüft werden. Von dessen Vorhandensein ist grundsätzlich nicht auszugehen bei Staaten, die bislang keine Vorschriften über den Datenschutz haben; in der EG sind dies (außer Spanien) die Länder Belgien, Italien, Griechenland und Portugal.

Vorrangig kommt es darauf an, daß die Länder ohne Datenschutzgesetzgebung alsbald für einen gleichwertigen Datenschutz in ihrem Recht sorgen. Das eigentliche Hindernis für einen - auch im Sinne der Wirtschaft - unproblematischen internationalen Datenverkehr sind nicht die Staaten mit angeblich "strengen" Datenschutzgesetzen, sondern diejenigen, in denen es an nationalen Datenschutzgesetzen überhaupt mangelt. Die EG könnte, wie von der Internationalen Konferenz der Datenschutzbeauftragten im August 1989 in Berlin vorgeschlagen, einen der Europaratskonvention entsprechenden Datenschutz durch Rechtsakte sowohl im Hinblick auf Mitgliedstaaten als auch auf ihre eigenen Institutionen fördern und eine unabhängige Datenschutzkontrollinstanz einrichten, die u. a. mit den nationalen Datenschutzorganen zusammenarbeitet. In Betracht kämen auch bereichsspezifische Richtlinien zum Datenschutz, etwa nach dem Vorbild von Empfehlungen des Europarates, wie sie z. B. für die Bereiche Direktmarketing und Arbeitnehmerdatenschutz verabschiedet worden sind.

Da der Harmonisierungsprozeß noch geraume Zeit in Anspruch nehmen wird und auch danach viele Zweifelsfragen bestehen werden, wäre die Wirtschaft gut beraten, von sich aus in Zusammenarbeit mit den öffentlichen Datenschutzkontrollinstanzen vertragliche Lösungskonzepte zu entwickeln, die zumindest den Datenschutzgrundsätzen der Europaratskonvention entsprechen. Dazu gehört auch die Gewährleistung von Auskunfts-, Berichtigungs- und Löschungsrechten hinsichtlich der Verarbeitung übermittelter Daten im Ausland sowie eine

MMV 10/2589

Benachrichtigung über den Datenexport. Es sollte seitens der Wirtschaft alles getan werden, um fehlende gesetzliche Datenschutzregelungen durch vertragliche Verpflichtungen soweit wie möglich zu kompensieren. Eine Verletzung des informationellen Selbstbestimmungsrechts Betroffener in Deutschland durch ausländische Stellen könnte nicht hingenommen werden.

Kurzsichtig wäre es, zur Vermeidung datenschutzrechtlicher Reglementierungen Firmensitze in Länder ohne Datenschutz zu verlagern, zumal ungewiß ist, wie lange diese "Datenoasen" bleiben; außerdem wären die von dort exportierten Daten in Länder mit Datenschutz dem dortigen Recht unterworfen. Wie im Umweltschutz wird sich hoffentlich auf längere Sicht auch im Datenschutz die Erkenntnis durchsetzen, daß effizienter Datenschutz vom Verbraucher honoriert wird und der Wirtschaft - national wie international - Risiken bei der Vermarktung ihrer Produkte eher vermeiden hilft.

MMV 10/2589

Stichwortverzeichnis

	Seite
A	
Adressenhandel	19, 55ff., 99.
Akten	1, 27 ff.
Ärzte	18, 43 f., 75 ff.
Arbeitnehmerdaten	
- Befragung des früheren Arbeitgebers	63 ff.
- Fragebogen	61 ff.
- Personalinformationssysteme	67 f.
- Stipendium	66
- Telefondaten	66 f.
Aufsichtsbehörden	
- Akten	27 ff.
- Beispielsfälle	29 ff.
- Bußgeldverfahren	24 f.
- Datensicherung	22, 23, 84 ff.
- Kontrolltätigkeit	17 ff.
- Organisation	13 f.
- personelle Ausstattung	14
- Register	15 ff.
- Zuständigkeit	3, 13
Auftragsdatenverarbeitung	19, 48 f., 85
Auskunfteien	16, 18, 19f., 40, 52 ff., 65, 69 98 f.,
- Firmenprofile	53
- Nachbarschaftsbefragungen	21, 98 f.
B	
Bankauskunftsverfahren	92 f.
Bundesdatenschutzgesetz	
- Novellierung	9 ff., 98

IM M y 10/2589

	Seite
- Regelungskonzept	4 ff.
- Verwaltungsvorschriften	85, 92
D	
Datensicherung	
- allgemeine Erfahrungen	2, 84 f.
- Datenträger (Mülltonne)	87 ff.
- Kontrollbesuche	22 f.
- Löschung (Disketten)	86 f.
- Paßwörter	85
- persönliche Computer (PC's)	2, 85
- Postversand	87
Detekteien	54
Direktwerbung (s. auch Werbung)	11, 16, 19, 20 55 ff., 99
"Düsseldorfer Kreis"	2, 89 ff.
G	
grenzüberschreitender Datenverkehr	2, 100 ff.
H	
Handel	18
Handwerk	18
I	
Industrie	18
Inkasso	30, 54

MMV 10/2589

	Seite
K	
Krankenhäuser	18, 99
Kreditinstitute	17
- Kontonummern	74 f.
- SCHUFA (s. SCHUFA)	29 ff., 93 f.
Kundendaten	
- Autotelefonanlage	73
- Kontonummern	74 f.
- Reisebüro	72 f.
- Verbrauchermarkt (Diebstahl)	73 f.
M	
Markt- und Meinungsforschung	16, 19, 58 ff.
Mieterdaten	
- Auskunfteien	69
- Fragebogen	68 f.
- Verbrauchsdaten	70
- Vergleichswohnungen	70 f.
- Warndatei	40 ff.
Mitgliederdaten	
- Automobilclub	82
- Gruppenversicherungen	79
- Mitgliederwerbung	80 f.
- Mitgliederverzeichnisse	80
- Weitergabe (Tageszeitung)	81 f.
P	
Patientendaten	
- Arztpraxen (Verkauf)	76 ff.
- Honorarabrechnung	75 f.

10/2589

Seite

R

Robinson-Liste 58

S

SCHUFA
- Aufgabe 29 f.
- Aufsicht 20 f.
- Geburtsdatum 35 f.
- Mahnbescheid 37 f.
- Organisation 29 f.
- Personenverwechselung 32 ff.
- Verfahren 30 f., 31 f., 93 f.
- Vermieter-Anfragen 69 f.

Schuldnerverzeichnis 36, 42 f., 55

V

Vereine (s. auch Mitgliederdaten) 19
Versichertendaten
- Glasversicherung (Wohnungseigentümer) 82
- Krankenversicherung (Einkommen) 83 f.

Versicherungswirtschaft
- allgemein 18
- Gruppenversicherungen 79
- Klauseln 94 ff.
- Warndateien 47 ff., 50

W

Warndateien (-dienste)
- Beherbergungsgewerbe 51

M M 10/2589

	Seite
- EPOS (Führungskräfte)	44 ff., 51
- Frauenärzte	43 f.
- Ladendiebstähle	51
- Mietinteressenten	40 ff.
- Sachschadenversicherung (SAVIS)	47 ff.
- "Schwarzfahrer"	38 ff., 51
- Spielbanken	51
- Versicherungswirtschaft (außer SAVIS)	50
- Videotheken	51
Werbung (s. auch Direktwerbung)	2, 56 f.
- Apotheke	57
- Hundehalter	57
- Vereinsmitglieder	80 f.

MMV10/2589

Diese Druckschrift wird im Rahmen der Öffentlichkeitsarbeit der Landesregierung Nordrhein-Westfalen herausgegeben. Sie darf weder von Parteien noch von Wahlbewerbern oder Wahlhelfern während eines Wahlkampfes zum Zwecke der Wahlwerbung verwendet werden.
Dies gilt für Landtags-, Bundestags- und Kommunalwahlen sowie auch für die Wahl der Mitglieder des Europäischen Parlaments.
Mißbräuchlich ist insbesondere die Verteilung auf Wahlveranstaltungen, an Informationsständen der Parteien sowie das Einlegen, Aufdrucken oder Aufkleben parteipolitischer Informationen oder Werbemittel. Untersagt ist gleichfalls die Weitergabe an Dritte zum Zwecke der Wahlwerbung.
Eine Verwendung dieser Druckschrift durch Parteien oder sie unterstützende Organisationen ausschließlich zur Unterrichtung ihrer eigenen Mitglieder bleibt hiervon unberührt. Unabhängig davon, wann, auf welchem Wege und in welcher Anzahl diese Schrift dem Empfänger zugegangen ist, darf sie auch ohne zeitlichen Bezug zu einer bevorstehenden Wahl nicht in einer Weise verwendet werden, die als Parteinahme der Landesregierung zugunsten einzelner politischer Gruppen verstanden werden könnte.