Datenschutz
im nicht-öffentlichen Bereich

Fünfter Bericht

der Landesregierung Nordrhein-Westfalen

über die Tätigkeit der für den

Datenschutz im nicht-öffentlichen Bereich

zuständigen Aufsichtsbehörden

an den Landtag

Nordrhein-Westfalen

Berichtszeitraum:
1. Januar 1995 bis 31. Dezember 1996

LANDTAG
NORDRHEIN-WESTFALEN
12. WAHLPERIODE
VORLAGE
12/2040
Alle Abg.

GLIEDERUNG

		Seite
Überblick		5
1.	**Übersicht über die Kontrolltätigkeit in Zahlen**	7
1.1	Meldungen zum Register	7
1.2	Beschwerden	9
1.3	Anfragen und Beratungsersuchen	12
1.4	Überprüfungen vor Ort	13
1.5	Bußgeldverfahren/Verwaltungsverfahren nach § 38 Abs. 5 BDSG	15
2.	**Entwicklungen in einzelnen Bereichen**	16
2.1	Tele- und Mediendienste	16
2.2	Scoring-Verfahren bei der SCHUFA	18
2.3	Handels- und Wirtschaftsauskunfteien	20
2.3.1	Verfahren bei der Erteilung telefonischer Auskünfte	20
2.3.2	Auskünfte über Ehegatten	20
2.3.3	Auskünfte aus dem Schuldnerverzeichnis	21
2.4	Versicherungswirtschaft	22
2.4.1	Versicherungen im Internet	22
2.4.2	Hinweissystem im Bereich der privaten Krankenversicherung	23
2.4.3	Private Krankenversicherungskarte	23
2.5	Kreditwirtschaft	25
2.5.1	Allfinanz-Konzept	25
2.5.2	Datenerhebung nach dem Wertpapierhandelsgesetz	26
2.5.3	Unbefugtes Abfragen von Kontoständen	27
2.5.4	Elektronische Geldbörse	27
2.6	Videoüberwachung	29

2.7	Herausgabe von Telefonverzeichnissen auf elektronischen Datenträgern (CD-ROM)	30
2.8	Chipkarten im Gesundheitswesen	31
3.	**Einzelfälle aus der aufsichtsbehördlichen Praxis**	32
3.1	Werbeflut wird immer größer	32
3.2	Weitergabe von Patientendaten durch Angestellte einer Arztpraxis	33
3.3	Warndatei über Ärzte	34
3.4	Übermittlung sensibler Daten mittels Telefax	35
3.5	Personaldatenerfassung durch Fragebögen	36
3.6	Verkauf einer nicht gelöschten Festplatte	38
3.7	Fernwartung durch Servicetechniker	39
4.	**EU-Datenschutzrichtlinie und Novellierung in Bund und Land**	40

Überblick

Der 5. Tätigkeitsbericht für den nicht-öffentlichen Bereich erstreckt sich auf die Jahre 1995 und 1996 und fällt in eine Zeit der Veränderung:

Das Fortschreiten der Informations- und Kommunikationstechnik eröffnet nahezu täglich neue Betätigungsfelder, wobei sich gerade im nicht-öffentlichen Bereich in immer vielfältigerer Weise Fragen des Datenschutzes ergeben; einerlei, ob es um elektronische Speichermedien mit umfangreichen Suchfunktionen in bezug auf personenbezogene Daten aus veröffentlichten Verzeichnissen geht, um Chipkarten zur Ausweitung des bargeldlosen Zahlungsverkehrs oder als Träger für jederzeit verfügbare Daten (z.B. von Gesundheitsdaten) des Karteninhabers oder um völlig neue Dienste.

Zugleich bedeutet die bis Oktober 1998 durchzuführende Umsetzung der Datenschutzrichtlinie der Europäischen Union in jeweils nationales Recht für Bund und Länder eine große Herausforderung, aber auch die Chance - z.B. in der Privatwirtschaft -, einen der Bedeutung des "Grund"-Rechts auf informationelle Selbstbestimmung angemessenen Datenschutzstandard zu erreichen, etwa durch die Stärkung der betrieblichen Selbstkontrolle oder der verstärkten Kontrolle durch die zuständigen Aufsichtsbehörden, die künftig nicht mehr nur "anlaßbezogen" erfolgt.

Die Bedrohung seiner Persönlichkeitsrechte empfindet der einzelne Bürger heutzutage weniger durch staatliche Institutionen als durch die wachsende Technisierung seiner Umwelt in alltäglichen Bereichen. Mediendienste, Telebanking, On-line-Zugriffe von Banken und Versicherungen und Adreßhändler sind nur einige Beispiele für die rasante Zunahme der Verbreitung, Nutzung und Vernetzung von Informations- und Kommunikationstechnik. Die Gefahr eines möglichen Mißbrauchs und der Zusammenführung von Daten zu vollständigen Persönlichkeitsprofilen nimmt angesichts dieser Entwicklung ständig zu. Die Vielfalt, in der Daten heute bereitgehalten werden können, läßt erahnen, welche Wege und Chancen der Medien- und Informationsgesellschaft von morgen eröffnet werden und welche Vorkehrungen zum Datenschutz und zur Datensicherheit zu treffen sind.

Die im Berichtszeitraum gewonnenen Erkenntnisse zeigen auch, daß nicht nur im Bereich neuer Entwicklungen Belange des Datenschutzes mit Nachdruck weiter zu verfolgen sind. Die auffallend starke Zunahme der Beschwerden betroffener Bürger - eine Tendenz, die auch für

das Jahr 1997 festzustellen ist - sowie die unverändert hohe Zahl der bei Überprüfungen vor Ort festgestellten Mängel im Bereich Datensicherheit und der sonstigen organisatorischen Schutzvorkehrungen deuten darauf hin, daß in vielen Unternehmen längst nicht alle Möglichkeiten zur Verbesserung des Datenschutzes ausgeschöpft sind. Gleichwohl ist der gute Wille erkennbar, den Datenschutz als gemeinsames Anliegen zu verstehen.

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich werden daher im Rahmen ihrer Möglichkeiten noch stärker als bisher ihrem Beratungsauftrag nachkommen müssen, damit es auch in Zukunft den "gläsernen" Kunden nicht gibt. Auf seiten der Wirtschaft besteht durchaus die Bereitschaft zum Dialog. Der "Düsseldorfer Kreis" wird hierzu - wie schon in den vergangenen Jahren - ebenfalls seinen Beitrag leisten. Den Verantwortlichen in den Unternehmen kann und soll aber die Verantwortung für eine datenschutzgerechte Verarbeitung nicht abgenommen werden.

Auch im Rahmen der bevorstehenden Umsetzung der Europäischen Datenschutzrichtlinie im Bundesdatenschutzgesetz, zu der der "Düsseldorfer Kreis" im Berichtszeitraum Vorschläge erarbeitet hat, wird daher zu prüfen sein, inwieweit das Element der betrieblichen Selbstkontrolle effizienter ausgestaltet werden kann.

In zahlreichen Verhandlungen des "Düsseldorfer Kreises" mit Spitzenverbänden der Wirtschaft konnten im Berichtszeitraum weitere Ergebnisse und Fortschritte erzielt werden.

1. Übersicht über die Kontrolltätigkeit in Zahlen[1]

Die Datenschutzaufsicht im nicht-öffentlichen Bereich liegt bei der Bezirksregierung Arnsberg für die Regierungsbezirke Arnsberg, Detmold und Münster sowie bei der Bezirksregierung Köln für die Regierungsbezirke Düsseldorf und Köln.

1.1 Meldungen zum Register

Mit Stand 31.12.1996 waren zum Register der Aufsichtsbehörden folgende Stellen gemeldet:

a) Stellen, die geschäftsmäßig personenbezogene Daten zum Zwecke der Übermittlung speichern (§ 32 Abs. 1 Nr. 1 BDSG)

	Arnsberg	Köln
- Adreßhandel, Direktmarketing	19 (18)	24 (24)
- Auskunfteien, Warndienste	42 (45)	56 (59)
Gesamt:	61 (63)	80 (83)

b) Stellen, die geschäftsmäßig personenbezogene Daten zum Zwecke der anonymisierten Übermittlung speichern (§ 32 Abs. 1 Nr. 2 BDSG)

	Arnsberg	Köln
- Markt- und Meinungsforschungsinstitute	15 (7)	19 (15)

[1]Zahlen in Klammern sind Vergleichszahlen aus dem 4. Tätigkeitsbericht.

c) Stellen, die geschäftsmäßig personenbezogene Daten im Auftrag als Dienstleistungsunternehmen verarbeiten oder nutzen (§ 32 Abs. 1 Nr. 3 BDSG)

Arnsberg	Köln
403 (340)	546 (422)

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

d) Gemeldete Unternehmen nach a) bis c) insgesamt

Arnsberg	Köln
479 (410)	645 (520)

Die Zahlen lassen eine deutliche Zunahme erkennen. Der Anstieg der gemeldeten Stellen kann im wesentlichen auf die Ausgliederung der datenverarbeitenden Unternehmen zurückgeführt werden (Outsourcing), die dann als "Auftragsdatenverarbeiter" nach § 32 Abs. 1 Nr. 3 BDSG meldepflichtig werden.

1.2 Beschwerden

In den Jahren 1995 und 1996 sind gegen datenverarbeitende Stellen, die Datenverarbeitung für **eigene** Zwecke (§ 28 BDSG) durchführten und für die eine Anlaßaufsicht nach § 38 Abs. 1 BDSG bestand, bei der Bezirksregierung Arnsberg insgesamt 178 (126) Beschwerden und bei der Bezirksregierung Köln 370 (219) Beschwerden eingegangen.

Gegen Stellen, die geschäftsmäßig personenbezogene Daten für **fremde** Zwecke verarbeiteten (§ 32 Abs. 1 Nr. 1 bis 3 BDSG), wurden im vorgenannten Zeitraum bei der Bezirksregierung Arnsberg insgesamt 94 (71) Beschwerden und bei der Bezirksregierung Köln 98 (72) Beschwerden vorgebracht.

In diesen Zahlen sind - wie in den Vorjahren - sowohl Beschwerden von Betroffenen als auch Beschwerden von anderen Personen enthalten.

Die angegebenen Zahlen verteilen sich wie folgt:

Beschwerden gegen Stellen, die Datenverarbeitung für **eigene** Zwecke durchführen

	Arnsberg	Köln
- Handel/Handwerk	39 (23)	53 (27)
- Industrie/Großunternehmen	11 (11)	38 (41)
- Krankenhäuser, Ärzte, privatärztliche Verrechnungsstellen	20 (14)	18 (22)
- Kreditinstitute/ -vermittler	16 (17)	85 (19)
- Versicherungen	17 (19)	83 (53)
- Vereine, Verbände	26 (13)	27 (25)
- Sonstige	49 (29)	66 (32)
Gesamt	178 (126)	370 (219)

Beschwerden gegen Stellen, die geschäftsmäßig personenbezogene Daten für **fremde** Zwecke verarbeiten

	Arnsberg	Köln
- Adreßhandel, Direktmarketing	24 (10)	34 (10)
- Auskunfteien, Warndienste	51 (49)	46 (56)
- Konzerndatenverarbeiter	9 (2)	- (-)
- Markt- und Meinungsforschungsinstitute	5 (3)	3 (4)
- Rechenzentren (Auftragsdatenverarbeiter)	5 (4)	15 (2)
- Sonstige	- (3)	- (-)
Gesamt	94 (71)	98 (72)

Zu denken gibt die auffallende Zunahme der Beschwerden insgesamt von 488 in den Jahren 1993 und 1994 auf 740 im Berichtszeitraum. Auffällig, besonders im Aufsichtsbereich der Bezirksregierung Köln, ist der Schwerpunkt der Zunahme im Bereich der Datenverarbeitung für **eigene** Zwecke und hierbei insbesondere in bezug auf Handel/Handwerk, Kreditinstitute, Versicherungsunternehmen. Im Bereich der Datenverarbeitung für **fremde** Zwecke läßt sich ebenfalls eine Zunahme feststellen; zu erwähnen sind die Bereiche Adreßhandel/Direktmarketing, Auftragsdatenverarbeitung.

Bei der Datenverarbeitung für **eigene** Zwecke scheint eine stärkere Kontrolle der Tätigkeiten von Kreditinstituten und Versicherungsunternehmen aufgrund der allgemein feststellbaren Sensibilisierung der Bevölkerung in Sachen Datenschutz stattzufinden, die sich in einer großen Anzahl von Anfragen und insbesondere von Beschwerden niederschlägt.

Ein Teil der Zunahme der Beschwerden bei Versicherungsunternehmen kann auf in der Vergangenheit neu gestaltete und von den Kunden in vielen Fällen nicht immer verstandene Datenschutz- und Schweigepflichtentbindungserklärungen und Datenschutz-Merkblätter zurückgeführt werden.

Ebenso stand im Vordergrund vieler Beschwerden nach wie vor die Verarbeitung personenbezogener Daten zu Werbezwecken.

Beschwerden zu Datenverarbeitungen für **fremde** Zwecke betrafen schwerpunktmäßig unverändert die Tätigkeit von Auskunfteien (z.B. zur Zulässigkeit und Dauer der Speicherung von "Negativ"-Merkmalen). Die geschäftsmäßige Verarbeitung personenbezogener Daten zu Werbezwecken hat insbesondere aus Anlaß der unerwünschten Zusendung von Werbematerial zu Beschwerden z.B. zur Herkunft, Verarbeitung und Auswertung des Adressenmaterials und sonstiger Daten - wie bereits dargestellt in verstärktem Maße - geführt.

Bei den insgesamt 740 (488) Beschwerden kam es in immerhin 187 (115) Fällen zu Beanstandungen oder Empfehlungen der Aufsichtsbehörden, denen **sämtlich** entsprochen wurde; in den übrigen Fällen ergab sich kein Grund zu Beanstandungen bzw. wurden in einzelnen Fällen die Beschwerden aus verschiedenen Gründen (z.B. wegen Einstellung der Geschäftstätigkeit) nicht weiter verfolgt

Die Entwicklung der Zahl der Beschwerden gibt zu denken, zumal - wie bereits im letzten Tätigkeitsbericht ausgeführt werden mußte - Möglichkeiten zur Rückführung der Zahl von vielen Unternehmen offenbar nicht ausgeschöpft worden sind. Es kann hier auch nicht beruhigen, daß im Berichtszeitraum, nicht anders als in den Vorjahren, die Mehrzahl der Beschwerden sich als unbegründet erwies. Ebensowenig kann der absoluten Zahl der Beschwerden entnommen werden, es handele sich hierbei um eine lediglich überschaubare Größenordnung.

Beschwerden vermitteln den Aufsichtsbehörden einen Einblick zunächst nur in den durch die Beschwerden bekannt gewordenen Fällen. Soweit Beschwerden nicht erhoben werden oder nicht vorliegen, kann nicht etwa angenommen werden, in diesen Bereichen ergäbe sich auch kein Grund zu Beanstandungen oder Empfehlungen; ließe sich, die vorhandenen Zahlen auch der Vorjahre zugrundelegend, flächendeckend von einer "Beanstandungs-/Empfehlungs"-Quote von durchschnittlich etwa 20 bis 25 % ausgehen, müßte bei der Gesamtzahl der stattfindenden Datenverarbeitungen eine sich auch in absoluten Zahlen darstellende eindrucksvolle Größenordnung kritischer oder zu verbessernder Fälle angenommen werden.

1.3 Anfragen und Beratungsersuchen

Die Aufsichtsbehörden erhielten wieder zahlreiche schriftliche Anfragen und Beratungsersuchen. Es ergibt sich folgende Aufschlüsselung:

	Arnsberg		Köln	
	§ 28[1]	§ 32 Abs. 1[2]	§ 28[1]	§ 32 Abs. 1[2]
Anfragen von				
- betriebl. Datenschutzbeauftragten	16 (11)	11 (9)	29 (25)	16 (14)
- Geschäftsleitungen	23 (18)	9 (6)	51 (50)	48 (21)
- Betriebsräten	9 (8)	4 (5)	8 (10)	3 (-)
- Einzelpersonen, Vereinen, Verbänden	44 (32)	6 (5)	57 (81)	49 (27)
Gesamt	92 (69)	30 (25)	145 (166)	116 (62)

In einer Vielzahl von Fällen kam es zu Anfragen über die Meldepflicht oder über die Bestellung eines betrieblichen Datenschutzbeauftragten.

Die Unternehmen gehen - der Trend aus den Vorjahren setzt sich fort - verstärkt dazu über, bereits im Vorfeld von geplanten Datenverarbeitungsmaßnahmen die datenschutzrechtlichen Aspekte mit den Aufsichtsbehörden zu erörtern. Außerdem ist - wie bereits oben unter Ziffer 1.2 ausgeführt - von einer hohen Sensibilität der Bürger beim Umgang mit personenbezogenen Daten auszugehen.

---

[1] § 28 BDSG: Anfragen zu Stellen mit Datenverarbeitung für eigene Zwecke

[2] § 32 Abs.1 BDSG: Anfragen zu Stellen mit Datenverarbeitung für fremde Zwecke

1.4 Überprüfungen vor Ort

Der Übersicht sind die Zahlen der Überprüfungen vor Ort zu entnehmen. Diese Überprüfungen haben entweder im Rahmen der regelmäßigen Überwachung nach § 38 Abs. 2 BDSG bei Stellen mit Datenverarbeitung für fremde Zwecke (§ 32 Abs. 1 BDSG) oder aus konkretem Anlaß, d.h. aufgrund von Beschwerden und sonstigen Hinweise gem. § 38 Abs. 1 BDSG, stattgefunden.

		Arnsberg	Köln
a)	regelmäßige Überwachung (nach § 38 Abs. 2 BDSG)	92 (85)	152 (125)
b)	konkrete Anlässe bei Stellen mit Datenverarbeitung		
	für **eigene** Zwecke	1 (3)	86 (53)
	für **fremde Zwecke**	2 (2)	20 (7)
	Gesamt:	3 (5)	106 (60)
	Gesamt a) und b)	95 (90)	258 (185)

Bei den insgesamt 244 (210) regelmäßigen Überprüfungen, die wieder überwiegend z.B. bei Rechenzentren, Buchführungshelfern, Datenerfassungsbüros, Aktenvernichtungsunternehmen und Adreßhandel-/Direktmarketingunternehmen stattfanden, kam es in 94 (88) Fällen zu Beanstandungen und in 71 (79) Fällen zu Empfehlungen, denen die Unternehmen ebenso in **sämtlichen** Fällen gefolgt sind.

Auch im Rahmen der regelmäßigen Kontrolle bei Unternehmen, die geschäftsmäßig personenbezogene Daten für fremde Zwecke verarbeiten, wurden den technischen Prüfern immer wieder allgemeine Fragen zu datenschutzrechtlichen Problemen vorgetragen, die nicht in unmittelbarem Zusammenhang mit der Routineüberprüfung standen. Diese nicht gesondert erfaßten Anfragen sind in den o.g. Zahlen nicht enthalten.

Wie in den Vorjahren handelt es sich um Mängel, die technische Fragen der Datensicherheit und organisatorische Schutzvorkehrungen betreffen (hierzu im einzelnen zuletzt 4. Tätigkeitsbericht, Ziff. 1.4, S. 15).

Die bereits im letzten Berichtszeitraum festgestellte hohe Quote von Mängeln hat sich abermals gezeigt; dies gibt ebenfalls zu denken. Zu den Zahlen gilt Entsprechendes für das unter Ziffer 1.2 Gesagte. Bemühungen um die Datensicherheit und die organisatorischen Schutzvorkehrungen sind - wie bereits im letzten Tätigkeitsbericht aufgeführt - nachhaltig zu verstärken, und zwar aus eigenem Antrieb, ohne daß es eines Anstoßes von außen bedarf.

1.5 Bußgeldverfahren/Verwaltungsverfahren nach § 38 Abs. 5 BDSG

Ebenso wie in den Vorjahren führten die Aufsichtsbehörden in den Jahren 1995 und 1996 keine Bußgeldverfahren durch. Festgestellte Mängel konnten wie in den Vorjahren im Wege der Beanstandung oder Empfehlung behoben werden. Die Notwendigkeit zur Durchführung von Bußgeldverfahren hat sich nicht ergeben.

Fälle für eine Anwendung der den Aufsichtsbehörden nach § 38 Abs. 5 BDSG eingeräumten Eingriffsbefugnisse (zur Datensicherheit und zum betrieblichen Beauftragten für den Datenschutz) lagen im Berichtszeitraum ebenso wie in den Vorjahren nicht vor.

2. Entwicklungen in einzelnen Bereichen

2.1 Tele- und Mediendienste

Die Bedingungen des Informationsaustausches haben sich in den vergangenen Jahren in allen Lebensbereichen entscheidend verändert. Unter dem Begriff "Multimedia" sind technische Verfahren entwickelt worden, Computer- und Telekommunikationstechnik sowie Techniken zum Einsatz von Bild und Ton miteinander zu verbinden. Diese Entwicklung setzt sich dynamisch fort.

Die allgemeinen Gesetze haben sich als Rechtsgrundlage für den Einsatz der Multimedia-Angebote als nicht ausreichend gezeigt. Deshalb wurden im Berichtszeitraum sowohl von den Ländern als auch vom Bund Initiativen ergriffen, als Ergänzung der allgemeinen Gesetze einen speziellen Rechtsrahmen für die "neuen Dienste" zu schaffen. Im Jahr 1996 wurde vom Bundesgesetzgeber das Telekommunikationsgesetz (TKG) vom 25.07.1996 erlassen. Bereits kurz vorher war, noch auf Grund alten Rechts, die Telekommunikationsdienstunternehmen-Datenschutzverordnung (TDSV) erlassen worden, die nunmehr der Anpassung an das neue Recht bedarf. Zwei weitere Regelwerke wurden 1996 in Angriff genommen: der Mediendienste-Staatsvertrag der Länder und das Informations- und Kommunikationsdienste-Gesetz des Bundes, das als Artikelgesetz u. a. in ein Teledienstegesetz, ein Teledienstedatenschutzgesetz und ein Signaturgesetz gegliedert wurde.

(Die beiden letztgenannten Regelwerke sind am 1. August 1997 in Kraft getreten. Während der Staatsvertrag die rechtlichen Bedingungen der an die Allgemeinheit gerichteten Dienste (Mediendienste) regelt, befaßt sich das Bundesgesetz mit Diensten, die für eine individuelle Nutzung bestimmt sind (Teledienste).

Die Aufsicht für den Bereich des Datenschutzes ist einheitlich den bestehenden Aufsichtsbehörden für den nicht-öffentlichen Bereich übertragen worden, in Nordrhein-Westfalen also den Bezirksregierungen Arnsberg und Köln. Die damit verbundenen neuen Aufgaben werden dadurch erschwert, daß das Bundesgesetz unter großem Zeitdruck beraten und verabschiedet worden ist. Die Mängel des Gesetzgebungswerks zeigen sich besonders in begrifflichen Abgrenzungsproblemen zwischen Tele- und Mediendiensten; sie zeigen sich auch in Fragen der Abgrenzung zu den Regelungsbereichen des Telekommunikationsgesetzes, des Rundfunk-Staatsvertrages und des Bundesdatenschutzgesetzes mit Auswirkung auf die Zuständigkeits-

verteilung zwischen den Kontrollstellen der Länder und dem Bundesbeauftragten für den Datenschutz. Ein neues Verständnis der Aufsicht wird dadurch gefordert, daß die neuen Regelungen bereits im Vorgriff auf die Umsetzung der Europäischen Datenschutzrichtlinie den Schritt von der Kontrolle aus gegebenem Anlaß nach dem Bundesdatenschutzgesetz zur ständigen, anlaßunabhängigen Kontrolle vollzogen haben. Um diesem Auftrag gerecht zu werden, gilt es, neue Prüfstrategien der Aufsichtsbehörden zu entwickeln.

Als Forum für den Erfahrungsaustausch der Länder und zur Entwicklung von Problemlösungen hat der "Düsseldorf Kreis" im Berichtszeitraum eine Arbeitsgruppe unter dem Vorsitz von Nordrhein-Westfalen eingesetzt. In engem Zusammenhang damit stehen Gespräche der übrigen Arbeitsgruppen des "Düsseldorfer Kreises" mit Vertretern der Versicherungswirtschaft und der Kreditwirtschaft über die Abwicklung von Geschäften im Internet.

2.2 Scoring-Verfahren bei der SCHUFA

Bereits der zweite Tätigkeitsbericht der Landesregierung für den Berichtszeitraum 1989/1990 enthielt Ausführungen über ein mathematisch-statistisches Verfahren, mit dessen Hilfe einem Unternehmen Aufschluß darüber verschafft werden soll, ob ein Kunde kreditwürdig ist (Scoring). Es wurden damals grundsätzliche Befürchtungen insofern geäußert, als die betroffenen Einzelpersonen aufgrund nicht nachprüfbarer Bewertungen bestimmten Gruppen zugerechnet und damit - sei es in positiver oder negativer Hinsicht - gewissermaßen "kategorisiert" werden könnten (Ziffer 1.2.1, S. 16).

Die SCHUFA hat das Verfahren inzwischen eingeführt und seit dem 01.11.1996 bei ausgewählten Pilot-Anwendern eingesetzt. Es wurden bereits SCHUFA-Scorewerte in einer Vielzahl von Auskunftsfällen errechnet und an die angeschlossenen Firmen weitergegeben. Demnächst können auch die übrigen SCHUFA-Vertragspartner das Scoring-Verfahren in Anspruch nehmen. Der "Düsseldorfer Kreis" ist über die Einzelheiten des Verfahrens unterrichtet worden.

Scoring ist ein Punktbewertungsverfahren, das auf mathematisch-statistischen Analysen der zugrunde liegenden Daten beruht (Score = Punktzahl). Der Einsatz von Scoring-Systemen in der Bonitätsprüfung bedeutet den Übergang von qualitativen, durch Erfahrung gestützten Aussagen zu quantifizierbaren, d.h. meßbaren Risikoeinschätzungen auf der Basis der vorliegenden Kundendaten. Der "Düsseldorfer Kreis" betrachtet die vorstehend skizzierten Bedenken als ausgeräumt, weil der Scorewert eines Kunden aufgrund vorliegender Fakten individuell und zeitnah errechnet wird.

Einige Einzelfragen bedürfen jedoch noch der Prüfung. Die SCHUFA vertritt z.B. die Rechtsauffassung, daß sie nach dem Wortlaut des Gesetzes nicht verpflichtet sei, dem Betroffenen seinen Scorewert auf Anfrage mitzuteilen, weil der für einen bestimmten Zeitpunkt errechnete und dem SCHUFA-Vertragspartner übermittelte Scorewert nicht im Datensatz des Betroffenen gespeichert werde. Nach Auffassung der Aufsichtsbehörden kann es dem Betroffenen jedoch kaum vermittelt werden, daß der SCHUFA-Vertragspartner jederzeit einen Scorewert erhält, der Betroffene aber diese Information, bei der es sich um ein personenbezogenes Datum handelt, von der SCHUFA nicht erfahren kann.

Wegen fehlender praktischer Erfahrungen ist eine endgültige Aussage über alle Einzelfragen

des Scoring-Verfahrens noch nicht möglich. Es wird erforderlich sein, diesen Fragen in der aufsichtsbehördlichen Praxis besondere Aufmerksamkeit zu widmen und dabei auch bei den in Frage kommenden SCHUFA-Vertragspartnern bei sich bietendem Anlaß gezielt nachzufragen.

2.3 Handels- und Wirtschaftsauskunfteien

2.3.1 Verfahren bei der Erteilung telefonischer Auskünfte

In dem 4. Tätigkeitsbericht der Landesregierung (Ziff. 2.2.2, S. 18) wurden Maßnahmen zur Datensicherheit bei der Erteilung telefonischer Auskünfte durch Handelsauskunfteien gefordert. Gespräche des "Düsseldorfer Kreises" mit dem Verband der Handelsauskunfteien haben ergeben, daß mit den einzelnen Kunden der Handelsauskunfteien Paßwörter vereinbart werden, die bei telefonischen Anfragen als Voraussetzung für die Erteilung einer Auskunft angegeben werden. Die einzelnen telefonischen Anfragen werden ebenso wie die erteilten Auskünfte schriftlich dokumentiert. Die Auskunfteien weisen darauf hin, daß diese Maßnahmen unabhängig von den datenschutzrechtlichen Erfordernissen schon deshalb notwendig seien, um die Erbringung der Leistung zum Zweck der Abrechnung nachzuweisen.

Damit scheinen die datenschutzrechtlichen Bedenken ausgeräumt. Die Aufsichtsbehörden halten es allerdings in diesem Zusammenhang für notwendig, bei den Stichprobenkontrollen, die zur Überprüfung des berechtigten Interesses an den Auskünften vorgenommen werden, auch telefonische Auskünfte zu berücksichtigen.

2.3.2 Auskünfte über Ehegatten

Der 4. Tätigkeitsbericht der Landesregierung befaßte sich unter Ziff. 2.2.3 (S. 19) ebenfalls mit der Frage, in welchen Fällen eine Auskunftei Daten auch über den Ehegatten der angefragten Person übermitteln darf, ohne daß sich die Anfrage unter Darlegung des berechtigten Interesses ausdrücklich auf den Ehegatten erstreckt. In Gesprächen des "Düsseldorfer Kreises" mit dem Verband der Handelsauskunfteien wurde Einigkeit erzielt, daß eine Auskunft über den Ehegatten nicht gleichsam "automatisch" erteilt werden darf. Das schutzwürdige Interesse des Ehegatten am Ausschluß einer Übermittlung seiner Daten verbietet ein derart schematisches Vorgehen. Eine Befugnis oder gar eine vertragliche Verpflichtung der Auskunftei zur Übermittlung von Ehegattendaten besteht nur dann, wenn etwa Erkenntnisse der Art vorliegen, daß die angefragte Person eine leitende Funktion in ihrem Unternehmen nur als "Strohmann" des Ehegatten ausübt.

In den Verhandlungen mit dem Verband konnte weitgehend, wenn auch nicht in allen Punkten,

Einigkeit erzielt werden. Der Verband wies jedoch darauf hin, daß bei den Auskunfteien noch zahlreiche Datensätze mit Ehegattendaten bestehen, die der Bereinigung bedürfen. Es besteht daher Veranlassung, der Frage der Ehegattenauskünfte in der aufsichtsbehördlichen Praxis weiterhin besondere Aufmerksamkeit zu widmen.

2.3.3 Auskünfte aus dem Schuldnerverzeichnis

In der Vergangenheit wurde festgestellt, daß bei der Erlangung von Auskünften aus dem Schuldnerverzeichnis die gesetzlichen Vorschriften nicht immer eingehalten wurden.

Nach den Vorschriften der Zivilprozeßordnung können die Auskunfteien aus den bei den Gerichten geführten Schuldnerverzeichnissen unter bestimmten Voraussetzungen Auskünfte erhalten und an ihre Kunden weitergeben. Zu diesem Zweck können sie direkt bei den Amtsgerichten Abdrucke aus den Schuldnerverzeichnissen beziehen oder über die Berufsverbände Listen mit Schuldnerverzeichnisdaten erhalten. Während Daten aus den Abdrucken aufgrund gesetzlicher Erlaubnis im automatisierten Verfahren abgerufen werden können, ist dies bei Listen nicht gestattet.

In der aufsichtsbehördlichen Praxis wurde wiederholt festgestellt, daß Handelsauskunfteien Auskünfte nicht nur aus Abdrucken, sondern auch aus Listen im automatisierten Verfahren erteilen. Beanstandungen der Aufsichtsbehörden wurde entgegengehalten, daß kein sachlicher Grund für die unterschiedliche Regelung ersichtlich sei. Die Aufsichtsbehörden sahen einstweilen von Maßnahmen gegen solche Verstöße ab, weil Bestrebungen bekannt wurden, im Wege der Gesetzgebung Auskünfte durch automatisierten Abruf aus Listen bei Antragstellern zuzulassen, die auch Abdrucke beziehen dürfen. Inzwischen hat sich herausgestellt, daß der Bundesgesetzgeber die Bestrebungen nicht aufgreift und eine entsprechende Änderung der Zivilprozeßordnung auf absehbare Zeit nicht erfolgt. Die Aufsichtsbehörden werden deshalb dem Verbot der Erteilung von Auskünften aus Listen im automatsierten Abrufverfahren künftig besondere Aufmerksamkeit widmen müssen.

2.4 Versicherungswirtschaft

2.4.1 Versicherungen im Internet

Die vielfältigen und ständig wachsenden Möglichkeiten des Datenaustausches im Internet werden auch von der Versicherungswirtschaft in zunehmendem Maße genutzt. Eine Untersuchung im Berichtszeitraum ergab, daß etwa 200 Anbieter weltweit ihre Angebote über Internet on-line anboten. Erhebungen des Gesamtverbandes der deutschen Versicherungswirtschaft haben speziell zu den deutschen Verhältnissen ergeben, daß im Berichtszeitraum rund 50 % der Unternehmen einen Internetzugang hatten, ihn überwiegend aber nur nutzten, um über das Unternehmen und seine Produkte zu informieren. Angebote zum Abschluß eines Vertrages bieten zur Zeit noch wenige Versicherer. Immerhin fiel z.B. das Angebot eines Versicherungsmaklers im Internet auf, mit dem von den potentiellen Kunden zur Erstellung eines Angebots sensible Daten erfragt wurden. Ein Versicherungsunternehmen stellt über Internet ein Formular zur Verfügung, mit dem ein Antrag auf Abgabe eines Angebots gestellt werden kann. Ein weiteres Unternehmen bietet die Möglichkeit, einen Autoschutzbrief über T-Online zu erwerben, in diesem Fall kommt der Vertrag über die Kommunikation im Internet direkt zustande.

Die Tendenz der Entwicklung läßt mit Sicherheit erwarten, daß sich künftig immer mehr Versicherungsunternehmen verstärkt des Internet bedienen werden, um nicht nur in allgemeiner Form für ihre Produkte zu werben, sondern auch konkrete Angebote zu unterbreiten und Geschäftsbeziehungen bis hin zum Vertragsabschluß über das Internet abzuwickeln. Dabei kann nicht ausgeschlossen werden, daß Sicherheitsprobleme übersehen oder falsch beurteilt werden. Der faktisch unbegrenzte Zugang zu Informationen im Internet zwingt bei der Übermittlung personenbezogener Daten zu besonderen Sicherheitsvorkehrungen. Darüber hinaus bedarf es der Klärung, in welcher Weise z.B. die Einwilligungserklärung nach dem Bundesdatenschutzgesetz auf diesem Wege wirksam werden kann.

Der "Düsseldorfer Kreis" hat beschlossen, dieses komplexe Thema schwerpunktmäßig zu behandeln. Die Aufsichtsbehörden werden die Entwicklung in der Praxis aufmerksam beobachten.

2.4.2 Hinweissystem im Bereich der privaten Krankenversicherung

Fragen des Datenschutzes im Zusammenhang mit Hinweissystemen der Versicherungswirtschaft beschäftigen die Aufsichtsbehörden in verschiedenen Versicherungsbereichen. Im Berichtszeitraum befaßte sich der "Düsseldorfer Kreis" besonders mit Fragen im Zusammenhang mit einem Hinweissystem der privaten Krankenversicherung, das bereits im 4. Tätigkeitsbericht der Landesregierung (Ziff. 2.3.2, S. 21) erwähnt worden war. Ermittlungen der zuständigen Bezirksregierung bei dem in Köln ansässigen Verband der Privaten Krankenversicherung ergaben, daß die privaten Krankenversicherer bei Verdacht auf Versicherungsmißbrauch Einmeldungen bei dem Verband vornehmen, der die Meldungen an andere ihm angeschlossene Krankenversicherer weitergibt.

Die Überprüfung aus datenschutzrechtlicher Sicht führte zu Empfehlungen an den Verband zur Begrenzung der Anlässe für Einmeldungen und der zur Übermittlung gelangenden Daten. Es wurde erreicht, daß Einmeldungen und eine dadurch ausgelöste Weitergabe von Daten nur bei Vorhandensein konkreter Verdachtsumstände und auch nur in gravierenden Fällen vorgenommen werden. Als gravierender Anlaß wird der Verdacht auf verschwiegene anderweitige Versicherungen oder sonst anzeigepflichtige Umstände angesehen. Meldungen dürfen nur von besonders vertrauenswürdigen, entsprechend verpflichteten Mitarbeitern nach Rückfrage bei ihren Vorgesetzten veranlaßt werden. Die übermittelten Daten werden strikt auf das für den angestrebten Zweck notwendige Maß beschränkt.

Ein automatisiert betriebenes Hinweissystem besteht im Bereich der privaten Krankenversicherung zur Zeit nicht und ist aus Sicht der Aufsichtsbehörden auch nicht anzustreben.

2.4.3 Private Krankenversicherungskarte

Die im Berichtszeitraum bekannt gewordenen Absichten, im Bereich der privaten Krankenversicherung eine ähnliche Versichertenkarte einzuführen, wie sie im Bereich der gesetzlichen Krankenversicherung verwendet wird, gab Anlaß, bei einer im Aufsichtsbereich des Landes ansässigen privaten Krankenversicherung um Auskunft zu bitten. Die Informationen wurden mit dem Ergebnis aufsichtsbehördlich überprüft und im "Düsseldorfer Kreis" erörtert, daß gegen das Vorhaben keine Bedenken erhoben werden. Für diese Beurteilung ist maßgebend, daß der Inhalt der Karte nach dem Beispiel der Karte für die gesetzliche Krankenversicherung

strikt auf "Verwaltungsdaten" beschränkt wird und dem auch die Speicherkapazität entspricht. Medizinische Daten werden nicht gespeichert. Überdies ist dem Patienten freigestellt, ob und in welchem Maße er die Karte benutzt. Die Karte kann beispielsweise bei der Aufnahme in ein Krankenhaus zum Nachweis des Versicherungsschutzes und zur Vermeidung von Vorauszahlungen auf die Pflegekosten verwendet werden.

Die Versichertenkarte ist im Bereich der privaten Krankenversicherung am 01.04.1996 allgemein eingeführt worden.

2.5 Kreditwirtschaft

2.5.1 Allfinanz-Konzept

Nachdem die Verhandlungen der obersten Aufsichtsbehörden der Länder mit der Versicherungswirtschaft über sogenannte "Allfinanz-Konzepte" - wie im 4 Tätigkeitsbericht dargelegt (Ziff. 2.3.1) - abgeschlossen werden konnten, fanden im Berichtszeitraum auch im Bereich der Kreditwirtschaft intensive Verhandlungen zwischen der unter dem Vorsitz des Landes tagenden Arbeitsgruppe "Kreditwirtschaft" des "Düsseldorfer Kreises" und dem Zentralen Kreditausschuß über sogenannte "Allfinanzklauseln" statt. Dabei geht es um Einwilligungsklauseln für die Datenweitergabe für Kundenberatung und -werbung im Rahmen von "Allfinanz-Konzepten". Mit entsprechender Einwilligung des Bankkunden soll eine Übermittlung einzelner Daten an mit einem Kreditinstitut als Verbundpartner kooperiende Unternehmen, z.B. an Bausparkassen, ermöglicht werden, damit jene den Bankkunden gezielt und umfassend beraten und ihm alle Dienstleistungen der Unternehmen des gleichen "Allfinanz-Verbundes" anbieten können, ohne im Einzelfall die Zustimmung für die Beiziehung der Daten aus bestehenden Verträgen erbitten zu müssen. Da in diesem Zusammenhang auch besonders schützenswerte Daten, wie z.B. Kontostände, übermittelt werden, kommt der Transparenz und der Freiwilligkeit in den entsprechenden Einwilligungserklärungen besonderes Gewicht zu. Daher bedurfte die konkrete Ausgestaltung der Einwilligungsklauseln besonderer Beratung durch die Arbeitsgruppe "Kreditwirtschaft".

(Die Verhandlungen konnten im Mai 1997 abgeschlossen werden. Die kombinierte Hinweis- und Einwilligungsklausel für die Datenübermittlung zu vermittelten Verträgen lautet nunmehr:

"Ich bin damit einverstanden, daß der Vermittler die Daten darüber hinaus für die Beratung und Betreuung auch in sonstigen Finanzdienstleistungen nutzen darf. Soweit hiernach eine Datenübermittlung erfolgen kann, entbinde ich/entbinden wir die (Name der Bausparkasse/Name des Kreditinstituts) vom Bankgeheimnis."

Die Einwilligungserklärung wird drucktechnisch hervorgehoben und mit dem Hinweis verbunden, daß die Erklärung ohne Folgen für den Vertrag gestrichen oder jederzeit für die Zukunft widerrufen werden kann.

Auch wenn weitere Präzisierungen wünschenswert gewesen wären, kann das Ergebnis der

Verhandlungen mit dem Zentralen Kreditausschuß insgesamt aus datenschutzrechtlicher Sicht als Erfolg gewertet werden.)

2.5.2 Datenerhebung nach dem Wertpapierhandelsgesetz

Das Wertpapierhandelsgesetz verpflichtet Banken und andere Wertpapierdienstleistungsunternehmen, von ihren Kunden Angaben über deren Erfahrungen oder Kenntnisse in Geschäften, die Gegenstand von Wertpapierdienstleistungen sein sollen, über ihre mit den Geschäften verfolgten Ziele und über ihre finanziellen Verhältnisse zu verlangen. Nach dem Inkrafttreten des Gesetzes am 01 01.1995 kam es zu Beschwerden, daß einige Banken die genannte Vorschrift zum Anlaß nahmen, mit Hilfe von Fragebögen umfangreiche Daten über ihre Kunden zu erheben und in Dateien zu verarbeiten. Der "Düsseldorfer Kreis" hat diese Beschwerden zum Anlaß genommen, Grundsätze über die datenschutzgerechte Ausgestaltung der Befragungspflicht für die aufsichtsbehördliche Praxis zu entwickeln. Entsprechende Empfehlungen wurden von dem vorsitzenden Innenministerium des Landes Nordrhein-Westfalen auch dem Bundesaufsichtsamt für den Wertpapierhandel mitgeteilt. Im einzelnen wird festgestellt:

Die Befragung dient dem Interesse der Kunden an einer sachgerechten und individuellen Beratung. Die Kreditinstitute müssen aber beachten, daß für den Kunden keine gesetzliche Auskunftspflicht besteht. Der Kunde muß selbst entscheiden können, ob und welche Angaben er zu machen bereit ist. Die Beratung erfolgt auf der Grundlage der freiwillig mitgeteilten Kundenangaben. Für eine etwaige Haftung der Bank im Regreßfall wird es im wesentlichen nur darauf ankommen, ob das Kreditunternehmen seiner Pflicht nachgekommen ist, vom Kunden "Angaben zu verlangen".

Das Kreditunternehmen darf beim Kunden weder bei Verwendung von Fragebögen noch im Beratungsgespräch die irrige Auffassung erzeugen oder unterstützen, er sei zu Auskünften verpflichtet. Das Unternehmen muß ihn daher auf die Freiwilligkeit seiner Angaben - bei entsprechender Aufklärung auch über etwaige haftungsrechtliche Folgen - hinweisen.

Wegen der Schutzbedürftigkeit der im Rahmen einer Befragung anfallenden - häufig sensiblen - Angaben erscheint ein Hinweis auf die ausschließliche Zweckbindung für die Werpapierberatung angeraten. Eine Nutzung der Daten zu anderen, etwa zu Marketingzwecken ist nicht zulässig.

Aufzeichnungs- und Aufbewahrungspflichten bestehen nach § 34 Abs. 1 des Gesetzes nur in engen gesetzlichen Grenzen, die strikt einzuhalten sind.

2.5.3 Unbefugtes Abfragen von Kontoständen

Durch Presseveröffentlichungen erhielten die Aufsichtsbehörden für den Datenschutz davon Kenntnis, daß bei verschiedenen Geldinstituten die Möglichkeit bestand, mittels manipulierter Magnetkarten an Kontoauszugdruckern unbefugt die Kontostände Dritter abzufragen. In diesen Fällen benötigte man lediglich die Kontonummer des Kunden, die Bankleitzahl des Instituts und einen Magnetkartenrohling, um mit geeigneter Hard- und Software eine Magnetkartenfälschung herzustellen.

Nach den aufsichtsbehördlichen Feststellungen wurde das Verfahren der in dem Presseartikel namentlich genannten Banken zum Ausdruck von Kontoauszügen geändert, wobei zusätzliche Sicherheitshürden installiert wurden. Da aber davon auszugehen war, daß auch bei derzeit nicht bekannten Geldinstituten noch Sicherungslücken bei der Nutzung von Kontoauszugdruckern bestehen könnten, wurden die Spitzenverbände der Banken und Kreditinstitute aufgefordert, ihre Mitglieder auf mögliche Schwachstellen dieser Systeme hinzuweisen und eine Verbesserung der Kartensicherheit zu empfehlen.

Auf längere Sicht sollte angestrebt werden, die bisher verwendeten Magnetkarten durch Chipkarten zu ersetzen, die einen höheren Sicherheitsstandard gewährleisten.

2.5.4 Elektronische Geldbörse

In den letzten Jahren hat beim Zahlungsverkehr die elektronische Geldbörse zunehmend das Bargeld ersetzt. Hierdurch sind völlig neue Datenschutzprobleme entstanden, da beim elektronischen Bezahlen notwendigerweise immer Datenspuren gelegt werden, ohne daß der Betroffene dies im einzelnen erkennt.

Grundlage der elektronischen Geldbörse ist die Euroscheckkarte. Mit einem Multifunktionschip ausgerüstet, können nach der Aufladung bei den Banken und Sparkassen (bis zu 400,-- DM) bei Unternehmen, die über entsprechende Automaten verfügen, durch elektronische

Abbuchung Verbindlichkeiten beglichen werden. Hierbei wird im Händlerterminal ein Datensatz gespeichert, der Kaufdatum und Betrag enthält sowie weitere Daten, aus denen sich die Kartennummer der Käuferkarte und die Nummer der Händlerkarte ergeben. Zur Abwicklung des Zahlungsverkehrs werden die einzelnen Transaktionssätze von den Händlern gesammelt und an die jeweilige Evidenzstelle weitergeleitet. Diese kontrolliert und aggregiert die entgegengenommenen Beträge und leitet sie über Verrechnungsbanken an die zuständigen Kunden- und Händlerbanken weiter. Die von den Evidenzstellen verarbeiteten anonymisierten Daten können nur bei Zusammenwirken der Evidenzstellen, Verrechnungsbanken und Kundenbanken bestimmten natürlichen Personen zugeordnet werden, wie dies z.B. auch für Reklamations- und Verlustfälle vorgesehen ist.

Dieses Verfahren ist datenschutzrechtlich als nicht unproblematisch anzusehen, da die Zahlungsabwicklung insgesamt nicht anonym erfolgt. Bei den Evidenzstellen werden personenbezogene Daten in "Schattenkonten" gespeichert, die - auf die Transaktionen bezogen - Auskünfte über sämtliche Umsätze ermöglichen. Damit ist die Gefahr von umfangreichen Datensammlungen über den Verkauf von Konsumgütern gegeben, die zu Kunden- und Bewegungsprofilen verdichtet werden können und für die werbende Wirtschaft von Interesse sind.

Aus datenschutzrechtlicher Sicht sollten daher nach Möglichkeit zumindest alternativ Zahlungsverfahren ohne personenbezogene Daten und daher datenschutzfreundlicher zur Anwendung kommen. Hier kommen sogenannte "White Cards" in Betracht, kontenunabhängige Chipkarten, bei denen das Zahlungsverfahren anonym abgewickelt wird.

Die für den Datenschutz zuständigen Aufsichtsbehörden werden die Entwicklung weiterverfolgen.

2.6 Videoüberwachung

Der Einsatz von Videotechniken, um u.a. Geschäftsräume, Verkehrseinrichtungen oder Geldautomaten zu überwachen, hat in den letzten Jahren immer größere Bedeutung gewonnen. Kunden werden nicht nur in Warenhäusern und Kreditinstituten elektronisch beobachtet, sondern geraten zunehmend auch in Bahnhöfen, Parkhäusern, Taxis oder auf öffentlichen Wegen in das Blickfeld von Videokameras.

Wie eine solche Videoüberwachung rechtlich zu bewerten ist, unterscheidet sich danach, ob es sich um eine reine Augenblicksüberwachung ohne Aufzeichnung handelt, oder ob gleichzeitig eine Aufzeichnung der von der Videokamera erfaßten Geschehnisse erfolgt. Wenn die Technik sichtbar ist oder ausdrücklich darauf hingewiesen wird, kann eine solche Überwachung - wenn sie ohne Aufzeichnung erfolgt - hingenommen werden. Demgegenüber stellt die Aufzeichnung einen erheblichen Eingriff in die Persönlichkeitsrechte des Betroffenen dar. Die Videoüberwachung kann durchaus ein geeignetes Mittel sein, um Gefahren zu begegnen, Straftaten zu verhindern oder möglicherweise deren Aufklärung zu erleichtern. An den Umgang mit dem gespeicherten Datenmaterial sind allerdings hohe Anforderungen hinsichtlich der Zweckbindung zu stellen. So sind die Videoaufnahmen kurzfristig daraufhin zu überprüfen, ob sie zur Gefahrenabwehr oder Strafverfolgung weiter benötigt werden; andernfalls sind die Aufzeichnungen zu löschen, eine Weitergabe an andere Stellen ist auszuschließen.

In Beratungsgesprächen - u.a. mit dem Zentralen Kreditausschuß - wurde im Berichtszeitraum daher auch immer wieder darauf hingewiesen, daß private Stellen grundsätzlich die Bürger oder Kunden nur klar erkennbar und nicht mit heimlichen Videoaufnahmen durch versteckte Kameras überwachen dürfen. Dabei haben sie jeweils deutlich auf die Videoüberwachung z.B. durch Aufkleber aufmerksam zu machen, die den Hinweis enthalten, daß aus Sicherheitsgründen o.ä. Bildaufnahmen erstellt und aufgezeichnet werden.

Es wäre zu begrüßen, wenn das Bundesdatenschutzgesetz um eine entsprechende Regelung ergänzt würde.

2.7 Herausgabe von Telefonverzeichnissen auf elektronischen Datenträgern (CD-ROM)

In zunehmendem Maße ist festzustellen, daß Firmen - zum Teil auch aus dem Ausland - CD ROM (compact disc - read only memory) als "elektronisches Telefonbuch" auf den deutschen Markt bringen. Bei entsprechenden technischen Vorkehrungen (Tele-Finder) eröffnen sich zusätzlich zu der einfachen Telefonnummernsuche aufgrund der neben der Anschlußnummer im Telefonverzeichnis angegebenen weiteren Daten (Name, Beruf, Anschrift u.ä.) weitere Selektions- und Suchmöglichkeiten (Rückwärtssuche). Hier sind insbesondere folgende Möglichkeiten zu nennen:

- Selektion nach Namen (vollständig oder unvollständig), Namenszusätzen, Berufsangaben, Regionen, Postleitzahlen, Orten, Straßen, Hausnummern, Vorwahl und Telefonnummern,
- sog. Invertsuche, die es ermöglicht, über die Telefonnummer den Teilnehmer zu identifizieren,
- logische Verknüpfung von Stichwörtern bei der Suche,
- Auswertung in Form von Straßenlisten nach Hausnummern oder Teilnehmernamen sortiert,
- Anzeige aller Teilnehmer mit demselben oder ähnlichen Namen und
- Exportfunktion in andere Datenverarbeitungsprogramme.

Die Speicherplatte kann - anders als die Festplatte des PC - in ihrem Dateninhalt nicht überschrieben werden. Auch die fehlenden Löschungsmöglichkeiten (außer durch Zerstörung) begründen datenschutzrechtliche Bedenken.

Darüber hinaus ist die Identifikation von Teilnehmern nach der Rufnummer als Verletzung schutzwürdiger Persönlichkeitsrechte insgesamt als datenschutzrechtlich bedenklich anzusehen.

Seit dem Inkrafttreten der Telekommunikationsdienstunternehmen-Datenschutzverordnung (TDSV) im Juli 1996 hat der Telefonkunde nunmehr ein abgestuftes Widerspruchsrecht und kann selbst entscheiden, ob er überhaupt - und in welcher Form - in ein Verzeichnis eingetragen werden möchte, und ob dies nur in gedruckte oder auch in elektronische Verzeichnisse - wie bei der CD-ROM - geschehen soll.

2.8 Chipkarten im Gesundheitswesen

Im 4. Tätigkeitsbericht der Landesregierung (Ziff. 2.5, S. 27) wurden Überlegungen angesprochen, eine kartengestützte Patientendatenverarbeitung in verschiedenen Bereichen einzuführen. Im Berichtszeitraum hat ein Unternehmen in Nordrhein-Westfalen geplant, eine "Patientenkarte" in Form einer multifunktionalen Chipkarte mit einem leistungsfähigen optischen Speicher einzuführen, auf der durch die am Projekt beteiligten Ärzte eine Vielzahl von medizinischen Daten des Inhabers gespeichert werden sollte. Die zuständige Aufsichtsbehörde hat das Unternehmen von Anfang an intensiv beraten, um eine datenschutzgerechte Praxis bei der Verwendung der Karte zu gewährleisten. Vor allem wurde Wert darauf gelegt, folgende Rechte der Karteninhaber sicherzustellen:

- umfassende Unterrichtung über die Einsatzmöglichkeiten der Karte und das vorgesehene Verfahren,
- vollständige Entscheidungsfreiheit über die Verwendung der Karte und die darin zu speichernden Daten,
- Angebot einer technischen Möglichkeit, die Eintragungen auf der Karte jederzeit selbst zu lesen,
- das Recht und die technische Möglichkeit, bei einem Arztbesuch zu entscheiden, ob durch Eingabe einer persönlichen Indentitätsnummer (PIN) alle in der Karte enthaltenen Daten oder nur die Daten bestimmter medizinischer Fachgebiete zur Einsicht durch den Arzt freigegeben werden; freie Einsicht des Arztes nur für medizinische Notfalldaten.

Das Projekt wurde von dem Unternehmen so weit entwickelt, daß bereits die Durchführung eines Pilotversuchs beabsichtigt war. Das gesamte Vorhaben wurde dann aber wegen anderer Prioritäten der Unternehmenspolitik aufgegeben.

Da derzeit bundesweit eine Vielzahl anderer Chipkartenprojekte im Gesundheitswesen bekannt ist, muß die Entwicklung insgesamt weiter beobachtet werden.

3. Einzelfälle aus der aufsichtsbehördlichen Praxis

3.1 Werbeflut wird immer größer

Die Zahl der Datenschutzeingaben wegen unverlangter Werbesendungen ist gegenüber den Vorjahren weiter angestiegen. Neben allgemeinen Werbesendungen betrafen Beschwerden u.a. Aktivitäten extremistischer Gruppen, die neue Mitglieder werben wollten. In diesem Zusammenhang ergaben sich Schwierigkeiten der Betroffenen, in den Werbekarteien gelöscht zu werden. Auch die datenschutzrechtlich vorgesehene Möglichkeit des Widerspruchs gegen die Nutzung personenbezogener Daten für Werbezwecke führte oft nicht zum gewünschten Ergebnis. Auch wenn die speichernde Stelle bereit war, die Daten des Betroffenen zu sperren oder auch zu löschen, erreichten Betroffene nach einiger Zeit von anderen Stellen erneut Werbebriefe. Hinsichtlich der Herkunft der Daten gab dann diese speichernde Stelle an, daß man die Daten von einem anderen Interessenten erhalten habe. Darüber hinaus war oft eine weitere Aufklärung nicht möglich.

In einem anderen Beschwerdefall wegen unverlangter Werbung fühlte sich ein Betroffener durch die Datennutzung eines Kreditinstitutes in seinem Recht auf informationelle Selbstbestimmung empfindlich gestört. Das Institut hatte die Daten seiner Bankkunden nach dem Merkmal "Fahrzeughalter" selektiert, darüber hinaus in Erfahrung gebracht, bei welchem Versicherer die Fahrzeuge versichert waren, die Prämienzahlungen des Versicherers mit denen des Verbundpartners verglichen und anschließend den Fahrzeughaltern in einem Werbeschreiben mitgeteilt, daß man mit dem Verbundpartner ein günstigeres Angebot als das des bisherigen Versicherers machen könne. Der Beschwerdeführer war über diese Form der Werbung derart verärgert, daß er sofort die Vertragsbeziehung mit dem Kreditinstitut kündigte und sich an die Aufsichtsbehörde wandte. Diese beanstandete die vorgenommene Datenverarbeitung, worauf das Kreditinstitut von weiteren Werbeaktionen dieser Art Abstand nahm.

3.2 Weitergabe von Patientendaten durch Angestellte einer Arztpraxis

Wie einer Aufsichtsbehörde bekannt wurde, übermittelten Bedienstete einer Arztpraxis in mehreren Fällen personenbezogene Daten an einen Mietwagenunternehmer.

Der Mietwagenunternehmer wurde ohne Kenntnis der Patienten darüber informiert, daß der jeweilige Patient in Zukunft Bestrahlungstermine in der Praxis wahrnehmen müßte, wobei er für die Heimfahrt ein Taxi benötige. Der Unternehmer setzte sich daraufhin mit den Patienten in Verbindung.

Eine Übermittlung der Patientendaten in der oben genannten Form war weder datenschutzrechtlich noch nach anderen Rechtsvorschriften zulässig, da diese sich konkludent auf gesundheitliche Verhältnisse des jeweiligen Betroffenen bezog und somit ein schutzwürdiges Interesse des Betroffenen an dem Ausschluß der Übermittlung bestand.

Die Aufsichtsbehörde beanstandete das Verfahren und verdeutlichte in diesem Zusammenhang, daß in solchen Fällen nur der Betroffene selbst entscheiden könne, ob ein Dritter Kenntnis davon erhält, daß er sich in einer Strahlenbehandlung befindet.

Das Verfahren wurde von der Arztpraxis daraufhin in der Weise geändert, daß nur noch auf ausdrücklichen Wunsch der Betroffenen Taxis angefordert werden.

3.3 Warndatei über Ärzte

Eine Aufsichtsbehörde hatte erfahren, daß eine Arbeitsgemeinschaft von Unternehmen gegen solche Ärzte vorgehen wollte, die auffallend oft Arbeitnehmer krank schrieben. Die 130 Unternehmer der Arbeitsgemeinschaft sollten aufgefordert werden, für das Jahr 1995 mitzuteilen, welche Ärzte wie oft und für welchen Zeitraum Arbeitsunfähigkeit bescheinigt hatten. Die Einzelangaben sollten für jeden Arzt zusammengefaßt und ausgewertet werden.

Durch die Weiterleitung der Namen der Ärzte, die überdurchschnittlich oft krankschrieben, an die kassenärztliche Vereinigung sollte ein psychologischer Druck auf die betroffenen Ärzte ausgeübt werden.

Nachdem die Aufsichtsbehörde sich eingeschaltet und datenschutzrechtliche Bedenken vorgetragen hatte, nahm die Arbeitsgemeinschaft Abstand von ihrem ursprünglichen Vorhaben

3.4 Übermittlung sensibler Daten mittels Telefax

Auch im vergangenen Berichtszeitraum mußten sich die Aufsichtsbehörden wieder mit der Problematik der Übermittlung von sensiblen Daten durch den Einsatz von Telefaxgeräten beschäftigen.

Eine Aufsichtsbehörde erhielt davon Kenntnis, daß ein Inkasso-Unternehmen Schriftstücke, die sensible personenbezogene Daten beinhalteten, wie z.B. Darlehensverträge oder Abtretungserklärungen, mittels Telefax an den Arbeitgeber der Betroffenen übersandt hatte. Das Empfangsgerät befand sich an einem Ort, an dem sich auch für unbeteiligte Dritte eine Zugriffsmöglichkeit bot. Das Inkasso-Unternehmen ging von einer zulässigen Vorgehensweise aus, da es nach seiner Ansicht Sache des Empfängers ist, das Empfangsgerät an einer Stelle zu plazieren, wo nur für einen legitimierten Personenkreis die Zugriffsmöglichkeit gegeben ist.

Dieser Auffassung konnte sich die Aufsichtsbehörde nicht anschließen. Normadressat der datenschutzrechtlich geforderten Verarbeitungsschranken und Sicherungsvorkehrungen ist zunächst der "Herr der Daten", der somit Gewähr für eine ausreichende Transportkontrolle leisten muß. Diese war im vorliegenden Fall nicht gegeben, da die personenbezogenen Daten auch von unbefugten Personen gelesen werden konnten.

Die Aufsichtsbehörde empfahl dem Unternehmen, in Zukunft nur dann Fax-Zustellungen an Arbeitgeber durchzuführen, wenn sichergestellt ist, daß die Daten dort tatsächlich direkt an die zuständige Stelle gelangen, bzw. wenn diese Art der Korrespondenz vom Betroffenen (z.B. durch Angabe der Fax-Nr.) ausdrücklich gewünscht wird. Das Inkasso-Unternehmen sicherte dies zu.

3.5 Personaldatenerfassung durch Fragebögen

Im Berichtszeitraum wurde immer wieder die Frage der Erforderlichkeit der Erhebung und Speicherung bestimmter personenbezogener Daten durch interessierte Arbeitgeber bei der Anbahnung von Arbeitsverhältnissen an die Aufsichtsbehörde herangetragen. Die erhöhte Nachfrage nach Beschäftigung führt in vielen solcher Fälle durch die Verwendung von Fragebögen zu einer Erhebung und anschließenden dateimäßigen Speicherung von Daten in erheblichem Umfang.

Hierzu ist festzustellen, daß datenschutzrechtlich nur Fragen zulässig sind, die einen unmittelbaren Bezug zum künftigen oder bereits bestehenden Arbeitsverhältnis haben. Die Frage der Erforderlichkeit kann jedoch nicht katalogartig für alle Einzelfälle entschieden werden. Als unzulässig anzusehen sind u.a. Fragen nach einer Schwangerschaft und wohl auch nach der Ableistung des Wehr- oder Zivildienstes männlicher Bewerber. Bei letzterem ist z.B. bei der Frage nach dem zuletzt bekleideten Dienstgrad in der Regel kein Bezug zu dem angestrebten Arbeitsverhältnis zu sehen. Fragen, wie z.B. nach Kindern, Krankheiten, ärztlicher Behandlung, Gewerkschaften sowie Vorstrafen, sind je nach dem angestrebten Arbeitsverhältnis bzw. Arbeitsplatz zu bewerten. Voraussetzung für die Zulässigkeit dieser Fragen ist immer ein unmittelbarer Bezug zu dem Arbeitsverhältnis. Das Interesse des Arbeitgebers an den persönlichen Verhältnissen des Bewerbers muß gegenüber dessen schutzwürdigen Interessen als vorrangig anzusehen sein. Dabei muß dem Arbeitgeber ein entsprechender Spielraum bei der Bewertung der Frage, ob ein unmittelbarer Bezug zum künftigen oder bereits bestehenden Arbeitsverhältnis besteht, zugestanden werden. Soweit aber dieser Bezug zum Arbeitsverhältnis nicht erkennbar ist, ist im Rahmen der Möglichkeit des Bundesdatenschutzgesetzes auf eine Reduzierung der Datenerhebung und -verarbeitung auf ein erforderliches verträgliches Maß hinzuwirken.

Entscheidend ist dabei, daß verhindert werden soll, daß Arbeitnehmer zu Erklärungen veranlaßt werden, die nicht durch das konkrete Arbeitsverhältnis bedingt und mit dem Persönlichkeitsrecht vereinbar sind. Zur Verarbeitung derartiger nicht rechtmäßig erhobener Daten besteht keine gesetzliche Erlaubnis. Diese kann auch nicht generell durch eine Einwilligung der betroffenen Person ersetzt werden. Ein arbeitsrechtlich eindeutiger Verbotstatbestand kann durch eine Einwilligung nicht umgangen werden. Dagegen sollte in zweifelhaften Fällen auch im Interesse der Rechtssicherheit eine Einwilligung als Voraussetzung für die Erhebung und

Verarbeitung personenbezogener Daten akzeptiert werden. Von Bedeutung sind hierbei immer die Umstände des Einzelfalles.

3.6 Verkauf einer nicht gelöschten Festplatte

Ein Unternehmen aus der Computerbranche verkaufte einen PC, auf dessen gebrauchter Festplatte sich noch Daten eines Unternehmens (vorheriger Eigentümer) befanden. Außer handelsüblichen Programmen konnten der Festplatte u.a. sensible Daten über Beschäftigte des Unternehmens (Gehälter, Beurteilungen) sowie private Aufzeichnungen entnommen werden.

Bei der Überprüfung des Sachverhaltes bei dem Unternehmen durch die Aufsichtsbehörde war es in diesem konkreten Fall nicht mehr möglich, die näheren Umstände für den Einbau einer gebrauchten, nicht-gelöschten Festplatte nachzuvollziehen.

Auf Empfehlung der Aufsichtsbehörde wurde die bisherige Verfahrensweise geändert, so daß eine Übermittlung von Daten, die sich auf gebrauchten Festplatten befinden, in Zukunft ausgeschlossen ist. Die gebrauchten Festplatten werden nun vor einem Wiederverkauf einer sogenannnten Vorkonfiguration unterzogen. Dabei werden die gespeicherten Altdaten unwiederbringlich gelöscht.

3.7 Fernwartung durch Servicetechniker

Mehrere fernmündliche und schriftliche Anfragen wurden von nicht-öffentlichen Stellen zur datenschutzrechtlichen Bewertung der Fernwartung durch Servicetechniker eines beauftragten Unternehmens vorgetragen. Die datenschutzrechtliche Unsicherheit seitens der anfragenden Stellen bestand deshalb, weil bei der Fernwartung eines Datenverarbeitungssystems der Servicetechniker in die Lage versetzt wird, u.U. personenbezogene Datenbestände einzusehen bzw. einsehen zu müssen.

Hierzu vertreten die Aufsichtsbehörden der Länder für den Datenschutz im nicht-öffentlichen Bereich die Auffassung, daß bei der Wartung und Fernwartung die dabei als Nebenfolge sich ergebende Möglichkeit der Kenntnisnahme personenbezogener Daten keine Datenübermittlung im Rechtssinne darstellt, da es nicht zum Zweck der Wartung bzw. Fernwartung gehört, die Daten mit ihrem Informationsgehalt der Wartungsfirma zur Nutzung und weiteren Verarbeitung zu überlassen. Ferner besteht unter den Aufsichtsbehörden Einigkeit darüber, daß unbeschadet der rechtlichen Einordnung und unabhängig von - etwa im Hinblick auf besonders geschützte Daten - gesondert zu treffenden Vorkehrungen sowohl von der datenverarbeitenden Stelle als auch von der mit der Wartung beauftragten Stelle Sicherheitsmaßnahmen zu treffen sind, die einen Mißbrauch ausschließen.

So kann z.B. die beauftragte Wartungsfirma verpflichtet werden, im Falle einer erforderlichen Fernwartung nur einen eng begrenzten Mitarbeiterkreis, der dem Auftraggeber namentlich bekanntzugeben ist, einzusetzen. Ferner sollen diese Servicetechniker schriftlich auf das Datengeheimnis nach § 5 Bundesdatenschutzgesetz verpflichtet werden. Weiterhin besteht die Möglichkeit, die für die Fernwartung vorgesehene Datenleitung physikalisch zu trennen. Nur im Störungsfall sollte nach telefonischer Absprache mit der beauftragten Wartungsfirma ein direkter Zugriff auf die ADV-Anlage möglich sein.

4. EU-Datenschutzrichtlinie und Novellierung in Bund und Land

Wie bereits im 4. Tätigkeitsbericht (vgl. Ziff. 3, S. 28) ausgeführt, sind die Datenschutzgesetze des Bundes und der Länder an die Europäische Datenschutzrichtlinie vom 24. Oktober 1995 anzupassen. Die Richtlinie ist innerhalb von drei Jahren in nationales Recht umzusetzen. Sie erweitert die Informationsrechte des Bürgers und verpflichtet alle Mitgliedstaaten der EU zur Einrichtung staatlicher Kontrollstellen, die die Einhaltung der nationalen Vorschriften überwachen.

Das Fortschreiten der europäischen Einigung wird künftig zu einer spürbaren Zunahme der grenzüberschreitenden Ströme personenbezogener Daten zwischen allen am wirtschaftlichen und sozialen Leben der Mitgliedstaaten Beteiligten im öffentlichen und im privaten Bereich führen. Auch der Austausch personenbezogener Daten zwischen Unternehmen in den verschiedenen Mitgliedstaaten wird zunehmen. Die verstärkte Zusammenarbeit auf dem Gebiet der Informations- und Telekommunikationstechnik in der Europäischen Union erleichtert den grenzüberschreitenden Austausch personenbezogener Daten. Daher ist es aus hiesiger Sicht zu begrüßen, daß das zum Teil unterschiedliche Niveau des Schutzes personenbezogener Daten in den Mitgliedstaaten nunmehr harmonisiert wird. Künftig ist der innergemeinschaftliche Datenverkehr dem inländischen gleichzustellen. Das bedeutet, kein Mitgliedstaat darf wegen des gleichwertigen Schutzes, der sich aus der Anpassung der nationalen Datenschutzvorschriften ergibt, den Austausch personenbezogener Daten aus Gründen hindern, die den Schutz der Rechte und Freiheiten natürlicher Personen und insbesondere das Recht auf die Privatsphäre betreffen.

Die Mitgliedstaaten besitzen einen Spielraum, innerhalb dessen sie unter Beachtung des Gemeinschaftsrechts durchaus unterschiedliche nationale Regelungen treffen können. Angesichts des bereits vorhandenen hohen Datenschutzstandards sowie des Systems und der Verfahren der Datenschutzkontrolle in der Bundesrepublik Deutschland können die hiesigen Datenschutzbestimmungen im wesentlichen beibehalten und Weiterentwicklungen fortgeführt werden. Eine Absenkung des Datenschutzstandards ist nicht vorgegeben.

Allerdings sollte die Gelegenheit genutzt werden, über den sich aus der Richtlinie ergebenden zwingenden Änderungsbedarf hinaus Klarstellungen in den Gesetzen vorzunehmen, insbesondere neue technische Entwicklungen in die Novellierungen einzubeziehen, z.B. Chipkarten oder Videokameraüberwachung (vgl. 4. Tätigkeitsbericht, Ziff. 3, S. 29). Der "Düsseldorfer

Kreis" hat daher in seiner Sitzung am 07./08. März 1996 zur Novellierung des Bundesdatenschutzgesetzes (nicht-öffentlicher Bereich) aus Anlaß der Umsetzung der EU-Datenschutzrichtlinie entsprechende Vorschläge erarbeitet.

In Nordrhein-Westfalen hat das Datenschutzgesetz bereits einen so hohen Standard, daß im Rahmen der Anpassung an die EU-Datenschutzrichtlinie nur wenige Änderungen oder Ergänzungen erfolgen müssen. Es ist beabsichtigt, die Umsetzung der EU-Richtlinie in nordrhein-westfälisches Datenschutzrecht fristgemäß durchzuführen.