LANDTAG NORDRHEIN-WESTFALEN
12. Wahlperiode

22.12.1995

Vorlage

an den Ausschuß für Innere Verwaltung

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

Schreiben des Innenministers vom 21. Dezember 1995

Die Landesregierung hat in der Kabinettsitzung am 19. Dezember 1995 den 4. 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 vor.

LANDTAG
NORDRHEIN-WESTFALEN
12. WAHLPERIODE

VORLAGE
12/ 290
alle Abg.

Datum des Originals: 22.12.1995/Ausgegeben: 27.12.1995

Die Veröffentlichungen des Landtags sind fortlaufend oder auch einzeln gegen eine Schutzgebühr beim Archiv des Landtags Nordrhein-Westfalen, 40002 Düsseldorf, Postfach 10 11 43, Telefon (02 11) 8 84-24 39, zu beziehen.

Vierter Bericht

der Landesregierung Nordrhein-Westfalen

über die Tätigkeit der für den

Datenschutz im nicht-öffentlichen Bereich

zuständigen Aufsichtsbehörden

G L I E D E R U N G

		Seite
Überblick		4
1.	**Übersicht über die Kontrolltätigkeit in Zahlen mit Erläuterungen**	6
1.1	Meldungen zum Register	6
1.2	Beschwerden	8
1.3	Anfragen und Beratungsersuchen	12
1.4	Überprüfungen vor Ort	14
1.5	Bußgeldverfahren/Verwaltungsverfahren nach § 38 Abs. 5 BDSG	16
2.	**Einzelprobleme, Entwicklungen in einzelnen Bereichen**	17
2.1	Schufa - Stichproben zur Überprüfung des "berechtigten Interesses" bei erteilten Auskünften	17
2.2	Handels- und Wirtschaftsauskunfteien	17
2.2.1	Datensicherheit bei automatisierten Abrufverfahren	17
2.2.2	Datensicherheit bei telefonischen Auskünften	18
2.2.3	Auskünfte über Ehegatten	19

2.3	Versicherungswirtschaft	20
2.3.1	Allfinanz-Konzept	20
2.3.2	Hinweissystem im Bereich der privaten Krankenversicherung	21
2.3.3	Sonstige Hinweissysteme	22
2.3.4	Weitergabe von Gesundheitsdaten an Außendienstmitarbeiter	22
2.4	Kreditwirtschaft	25
2.4.1	Allfinanz-Konzept	25
2.4.2	Multifunktionaler Chip auf EC-Karten	25
2.4.3	Verarbeitung von Kundendaten	26
2.5	Weitere Entwicklungen - Kartengestützte Verarbeitung von Patientendaten	27
3.	**EG-Datenschutzrichtlinie**	28

Überblick

Die im Berichtszeitraum 1993 und 1994 zum Stand und zu den Perspektiven des Datenschutzes im nicht-öffentlichen Bereich gewonnen Erkenntnisse deuten darauf hin, daß die Belange des Datenschutzes beharrlich weiterzuverfolgen sind und insbesondere in vielen Unternehmen Bemühungen um eine Optimierung des Datenschutzes nachhaltig verstärkt werden sollten.

Unbefriedigend ist nach wie vor die relativ hohe Zahl der bei Überprüfungen vor Ort festgestellten Mängel im Bereich der Datensicherheit und der sonstigen organisatorischen Schutzvorkehrungen. Wenn die Mehrzahl von Beschwerden betroffener Bürger sich auch als unbegründet erweist, ist dennoch ferner zu fragen, ob die Unternehmen Möglichkeiten zu einer Rückführung der Beschwerden, deren Zahl sich gegenüber 1991 und 1992 nicht erhöht hat, ausgeschöpft haben.

Zwar ist es den Aufsichtsbehörden wiederum gelungen, in **allen** durch Überprüfungen und Beschwerden ihnen bekannt gewordenen Fällen, auch dank der Kooperationsbereitschaft der datenverarbeitenden Stellen, auf Lösungen hinzuwirken, die zu einer Verbesserung des Datenschutzes beitragen; es sollte aber nicht übersehen werden, daß das Bundesdatenschutzgesetz die datenschutzrechtliche Verantwortung den datenverarbeitenden Stellen zuweist. Ihnen obliegt es, und zwar aus eigenem Antrieb und ohne daß es eines Anstoßes von außen bedarf, auf datenschutzgerechte Lösungen hinzuwirken.

Erfreulich ist die Zunahme von Anfragen und Beratungsersuchen besonders im Vorfeld geplanter Datenverarbeitungsmaßnahmen. Unverändert bleibt die **Beratung** der datenverarbeitenden Stellen bedeutender Schwerpunkt der Aufsichtstätigkeit. In Zeiten nicht vermehrbarer Personalstellen stößt die Wahrnehmung dieser wichtigen Aufgabe allerdings auf Dauer wegen des damit verbundenen vielfach hohen Verwaltungsaufwandes auf Kapazitätsgrenzen bei den Aufsichtsbehörden, wenn es in den zuvor angesprochenen Bereichen den Verantwortlichen in der Wirtschaft nicht gelingt, für Verbesserungen zu sorgen und angesichts des zunehmenden öffentlichen Interesses an Fragen des Datenschutzes auch eigene Möglichkeiten zur Aufklärung der Öffentlichkeit auszuschöpfen.

Weitere Fortschritte konnten in Verhandlungen mit Verbänden der Wirtschaft erzielt werden, die die obersten Aufsichtsbehörden der Länder gemeinsam im Rahmen des unter dem Vorsitz des Landes tagenden "Düsseldorfer Kreises" führten.

Einen bedeutenden Schritt in Richtung Harmonisierung des Datenschutzes in Europa hat die Europäische Union nach langen und, insbesondere während des Berichtszeitraumes, schwierigen Verhandlungen mit der zwischenzeitlich (1995) erfolgten Annahme der Datenschutzrichtlinie durch den Rat vollzogen.

1. Übersicht über die Kontrolltätigkeit in Zahlen[1]

1.1 Meldungen zum Register

Mit Stand 31.12.1994 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	18 (16)	24 (16)
- Auskunfteien, Warndienste	45 (43)	59 (58)
Gesamt:	63 (59)	83 (74)

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

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

---

[1] Zahlen in Klammern sind Vergleichszahlen aus dem 3. Tätigkeitsbericht

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

Arnsberg	Köln
340 (323)	422 (417)

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

d) Gemeldete Unternehmen nach a) bis c) insgesamt

Arnsberg	Köln
410 (389)	520 (506)

1.2 Beschwerden

In den Jahren 1993 und 1994 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 126 (116) Beschwerden und bei der Bezirksregierung Köln 219 (226) 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 71 (75) Beschwerden und bei der Bezirksregierung Köln 72 (71) 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	23 (17)	27 (33)
- Industrie/Großunternehmen	11 (10)	41 (48)
- Krankenhäuser, Ärzte, privatärztliche Verrechnungsstellen	14 (13)	22 (13)
- Kreditinstitute/ -vermittler	17 (18)	19 (21)
- Versicherungen	19 (12)	53 (50)
- Vereine, Verbände	13 (12)	25 (27)
- Sonstige	29 (34)	32 (34)
Gesamt	126 (116)	219 (226)

Beschwerden gegen Stellen, die geschäftsmäßig personenbezogene Daten für fremde Zwecke verarbeiten	Arnsberg	Köln
- Adreßhandel, Direktmarketing	10 (9)	10 (5)
- Auskunfteien, Warndienste	49 (54)	56 (64)
- Konzerndatenverarbeiter	2 (2)	- (-)
- Markt- und Meinungsforschungsinstitute	3 (4)	4 (1)
- Rechenzentren (Auftragsdatenverarbeiter)	4 (1)	2 (1)
- Sonstige	3 (5)	- (-)
Gesamt	71 (75)	72 (71)

Der Schwerpunkt der Überprüfungsersuchen hat sich gegenüber den Vorjahren kaum geändert.

Unverändert betraf ein großer Teil der Beschwerden gegen Unternehmen, die Datenverarbeitung für eigene Zwecke durchführten, die unerwünschte Zusendung von Werbesendungen und insbesondere die Frage der Herkunft des Adressenmaterials. Von den Betroffenen wird ferner immer wieder die Zulässigkeit der Datenverarbeitung z.B. bei der Verwendung von Bewerber- und Personalfragebögen, Mieterfragebögen oder bei der Verwaltung von Mitgliederdaten in Vereinen und Verbänden angesprochen. Viele Beschwerden betrafen die Datenverarbeitung durch Versicherungsunternehmen; diese bezogen sich im wesentlichen auf Datenübermittlungen z.B. an andere Versicherer und an die zentralen Hinweissysteme der Fachverbände.

Im Bereich der Datenverarbeitung für fremde Zwecke standen wieder die Datenverarbeitung der Handelsauskunfteien sowie

der SCHUFA im Vordergrund. Vielfach ging es um Fragen zur Zulässigkeit und Dauer der Speicherung von Negativ-Merkmalen. Wiederholt wurden die Speicherung falscher Angaben im Datensatz der Betroffenen oder auch Personenverwechselungen (Name, Wohnort und/oder Geburtsdatum des Betroffenen identisch mit den entsprechenden Daten einer anderen Person) beanstandet.

Bei den insgesamt 488 (488) Beschwerden kam es in 115 (105) Fällen zu Beanstandungen oder Empfehlungen der Aufsichtsbehörden.

Die datenverarbeitenden Stellen haben diese Beanstandungen oder Empfehlungen, deren Zahl leicht zugenommen hat, **ausnahmslos** befolgt.

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.

Auch wenn im Berichtszeitraum im Vergleich zu den Jahren 1991 und 1992 eine Zunahme der Beschwerden nicht zu verzeichnen ist, bleibt aber dennoch zu bedenken, daß die Zahl der Beschwerden zurückgeführt werden könnte. Zunächst kommt es, wie bereits oben ausgeführt, bei 488 Beschwerden immerhin in 115 Fällen zu Beanstandungen oder Empfehlungen. Davon abgesehen mußte bereits im vorhergehenden Berichtszeitraum festgestellt werden, daß es in einer Reihe von Fällen gar nicht zu Beschwerden käme, wenn die Unternehmen frühzeitig für Transparenz sorgen würden. Mindestens in den Bereichen, in denen in verstärktem Maße mit Fragen zum Datenschutz zu rechnen ist (dazu zählt insbesondere die Verarbeitung von Kundendaten für Werbezwecke), sollten die Unternehmen im vorhinein umfassend über die beabsichtigte Verarbeitung von personenbezogenen Daten aufklären. Zur

Transparenz würde es beitragen, wenn die Unternehmen die Betroffenen auch über die Möglichkeit nach dem BDSG aufklären würden, der Nutzung oder Übermittlung von eigenen Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung widersprechen zu können (vgl. hierzu bereits 3. Tätigkeitsbericht, Ziff. 1.2, S. 7).

Oftmals ließe sich gerade in Fällen unbegründeter Beschwerden der später bei den Aufsichtsbehörden entstehende, häufig recht hohe Verwaltungsaufwand durch rechtzeitige Aufklärung oder auch durch eingehende Bearbeitung der von Betroffenen zunächst an die Unternehmen gerichteten Anfragen oder Beschwerden dort vermeiden oder verringern. Wenn die Unternehmen für die notwendige Offenheit sorgen, müssen Beschwerdeführer um so weniger behördliche Hilfe in Anspruch nehmen.

1.3 Anfragen und Beratungsersuchen

Die Aufsichtsbehörden erhielten unverändert 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	11 (14)	9 (7)	25 (19)	14 (3)
- Geschäftsleitungen	18 (17)	6 (8)	50 (47)	21 (6)
- Betriebsräten	8 (6)	5 (3)	10 (7)	- (-)
- Einzelpersonen, Vereinen, Verbänden	32 (35)	5 (2)	81 (55)	27 (11)
Gesamt:	69 (72)	25 (20)	166 (128)	62 (20)

---

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

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

Daneben kam es wiederum in einer Vielzahl von Fällen zu Anfragen über die Meldepflicht.

Hervorzuheben ist eine deutliche Zunahme der Anfragen und Beratungsersuchen im Aufsichtsbereich der Bezirksregierung Köln.

Bei den datenverarbeitenden Stellen ist ein Teil dieser Zunahme nach wie vor auf die Novellierung des Bundesdatenschutzgesetzes zurückzuführen, da sich einige Fragen im Zusammenhang mit der Novellierung erst im Laufe der Zeit ergeben haben (vgl. hierzu 3. Tätigkeitsbericht, Ziff. 2, S. 13 ff.). Die Unternehmen gehen außerdem verstärkt dazu über, bereits im Vorfeld von geplanten Datenverarbeitungsmaßnahmen die datenschutzrechtlichen Aspekte mit den Aufsichtsbehörden zu erörtern.

Der Anstieg von allgemeinen Anfragen durch Privatpersonen im Aufsichtsbereich der Bezirksregierung Köln kann auf eine erhöhte Sensibilität der Bürger beim Umgang mit personenbezogenen Daten zurückgeführt werden. Hier ist ebenso wie bei den Beschwerden zu fragen, ob bereits die Unternehmen Möglichkeiten zu einer Aufklärung über ihre Datenverarbeitung ausgeschöpft haben.

Auch im Rahmen der regelmäßigen Kontrolle bei Unternehmen, die geschäftsmäßig personenbezogene Daten für fremde Zwecke verarbeiten (hierzu nachfolgend Ziff. 1.4), 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.

Unverändert bleibt die **Beratung** der datenverarbeitenden Stellen im Rahmen des Bundesdatenschutzgesetzes bedeutender Schwerpunkt der Aufsichtstätigkeit.

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 sonstiger Hinweise gem. § 38 Abs. 1 BDSG, stattgefunden.

a) regelmäßige Überwachung (nach § 38 Abs. 2 BDSG)

	Arnsberg	Köln
	85 (81)	125 (123)

b) konkrete Anlässe bei	Arnsberg	Köln
Stellen mit Datenverarbeitung für eigene Zwecke	3 (5)	53 (46)
für fremde Zwecke	2 (3)	7 (10)
Gesamt:	5 (8)	60 (56)
Gesamt a) und b)	90 (89)	185 (179)

Bei den insgesamt 210 (204) regelmäßigen Überprüfungen, die wieder überwiegend z. B. bei Rechenzentren, Buchführungshelfern, Datenerfassungsbüros, Aktenvernichtungsunternehmen und Adreßhandel-/Direktmarketingunternehmen stattfanden, kam es in 88 (100) Fällen zu Beanstandungen und in 79 (67) Fällen zu Empfehlungen.

Unverändert gilt, daß Überprüfungen vor Ort, insbesondere bei kleineren oder mittleren Unternehmen - mit zunehmender Betriebsgröße nehmen die Mängel ab -, eine relativ hohe Zahl an Mängeln zutage treten lassen. Wie in den Vorjahren handelt es sich um Mängel, die technische Fragen der Datensicherheit und organisatorische Schutzvorkehrungen be

treffen. Im wesentlichen werden nach wie vor folgende Mängel festgestellt:

- Fehlende bzw. mangelnde Absicherung des Gebäudeäußeren und des Gebäudeinneren z.B. durch Alarmanlagen,
- fehlende Zugangskontrolle zum Maschinenraum/kein closed-shop Betrieb,
- keine ausreichende Funktionstrennung bei den Mitarbeitern der Datenverarbeitung, insbesondere bei kleineren Betrieben,
- kein ausreichender Paßwort-Schutz (z.B. kein Paßwort, ein zu kurzes Paßwort, keine Paßwort-Änderung),
- keine geordnete Datenträgerverwaltung und -aufbewahrung/Mängel bei der Auslagerung der Magnetbänder,
- unzureichende Programm- und Verfahrensdokumentation,
- fehlende schriftliche Weisungen der Auftraggeber,
- fehlerhafte Eingabekontrolle,
- Lücken und Fehler bei der Dateienübersicht nach § 37 Abs. 2 BDSG,
- nicht mehr aktuelle Registermeldungen,
- Probleme bei der Bestellung und Tätigkeit des betrieblichen Datenschutzbeauftragten.

Die geprüften Stellen waren - die Tendenz aus den Vorjahren hat sich auch hier fortgesetzt - **ausnahmslos** bereit, für entsprechende Änderungen zu sorgen.

Wenn einerseits die in den genannten Bereichen erkennbare Kooperationsbereitschaft der Wirtschaft als erfreulich zu bezeichnen ist, kann andererseits aber nicht übersehen werden, daß Bemühungen um die Datensicherheit und die organisatorischen Schutzvorkehrungen nachhaltig zu verstärken sind. Insbesondere gilt es, aus eigenem Antrieb für Verbesserungen zu sorgen, ohne daß es eines Anstoßes von außen bedarf.

1.5 Bußgeldverfahren/Verwaltungsverfahren nach § 38 Abs. 5 BDSG

In den Jahren 1993 und 1994 führten die Aufsichtsbehörden 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 ebenfalls nicht vor.

2. Einzelprobleme, Entwicklungen in einzelnen Bereichen

2.1 Schufa

Nach weiteren Erörterungen mit der Schufa hat diese gegenüber der zuständigen Arbeitsgruppe des "Düsseldorfer Kreises" nunmehr ihre Bereitschaft erklärt, zur auch nachträglichen Überprüfung des vom Gesetz für Anfragen geforderten berechtigten Interesses die Zahl der **Stichprobenkontrollen** zu erhöhen (hierzu 3. Tätigkeitsbericht, Ziff. 3.1, S. 18 und 19).

2.2 Handels- und Wirtschaftsauskunfteien

2.2.1 Auch im Berichtszeitraum waren die Aufsichtsbehörden mit Anforderungen befaßt, die sich aus dem Betrieb **automatisierter Abrufverfahren** ergeben. Aufmerksamkeit galt hier wieder Maßnahmen, die dazu dienen, unbefugte Zugriffe so weit wie möglich auszuschließen.

In einem Fall, bei dem es nach den von einer Handels- und Wirtschaftsauskunftei getroffenen Feststellungen zu einer auffallenden Häufung von unbefugten Abrufen auch personenbezogener Daten aus deren Datenbestand gekommen war, die von der Auskunftei auf die mißbräuchliche Nutzung eines Paßwortes zurückgeführt wurde, schaltete sich die zuständige Aufsichtsbehörde in die Überprüfung ein. Trotz getroffener Vorkehrungen zur Datensicherheit - Anhaltspunkte für einen Zugriff etwa durch Hacker, wie ein Wochenmagazin zu dem Fall gemeldet hatte, waren nicht gegeben - zeigte die Überprüfung, daß weitere

Bemühungen immer wieder aufs neue gefordert sind. Einer Forderung der Aufsichtsbehörde, die Online-Nutzervereinbarung mit den abrufenden Stellen zu präzisieren und in ihr nähere Regelungen über die Paßwortvergabe für Datennutzer innerhalb der abrufenden Stelle vorzusehen, ist die Auskunftei gefolgt. Zugleich wurden weitere Empfehlungen gegeben.

Die Entwicklung in der Praxis werden die Aufsichtsbehörden aufmerksam daraufhin beobachten, welche weiteren Maßnahmen zu fordern sind. Ohnehin bleibt es - wie bereits im Überblick (S. 4 oben) zum Ausdruck gebracht - Sache der Unternehmen, von sich aus die gebotenen Datensicherungsmaßnahmen zu ergreifen. Im übrigen ist die am 1. Januar 1995 in Kraft getretene Schuldnerverzeichnisverordnung (SchuVVO) vom 15. Dezember 1994 - BGBl. I S. 3822 - zu beachten, die eigens für die Verarbeitung von Daten aus dem Schuldnerverzeichnis und von mit diesen Daten verknüpften weiteren Daten im automatisierten Abrufverfahren Vorkehrungen vorsieht.

2.2.2 Auch bei **telefonischen Auskunftsverfahren** halten die Aufsichtsbehörden weitere Maßnahmen zur Datensicherheit für unerläßlich, um mißbräuchliche Anfragen soweit wie möglich zu unterbinden.
So sind insbesondere zusätzliche Vorkehrungen hinsichtlich der Überprüfbarkeit einzelner Anfragen aus den auskunfteinholenden Unternehmen zu verlangen. Für die Aufsichtsbehörden steht weiterhin fest, daß auf telefonischer Grundlage erfolgende Auskünfte zudem in besonderer Weise in Stichprobenkontrollen einzubeziehen sind (vgl. hierzu 3. Tätigkeitsbericht, Ziff. 3.2.1, S. 20). Im übrigen gilt hier ebenfalls, daß die Unternehmen von sich aus weitere Möglich-

keiten zur Erhöhung der Datensicherheit ständig ausschöpfen müssen. Im Berichtszeitraum konnten die Gespräche der Arbeitsgruppe "Handelsauskunfteien" (Arbeitsgruppe des "Düsseldorfer Kreises" - im Berichtszeitraum - unter dem Vorsitz des Landes) mit dem Verband der Handelsauskunfteien zu den seinerzeit erhobenen Forderungen der obersten Aufsichtsbehörden noch nicht abgeschlossen werden.

2.2.3 Mit dem Verband der Handelsauskunfteien konnte im Berichtszeitraum auch noch nicht einvernehmlich die Frage geklärt werden, in welchen einzelnen Fallgruppen eine Auskunftei Daten auch über den Ehegatten des Betroffenen übermitteln darf.

Entscheidend ist, ob sich das berechtigte Interesse des Anfragenden an einer Auskunft auch auf den Ehegatten bezieht und kein Grund zu der Annahme besteht, daß der Ehegatte ein einer Übermittlung seiner Daten entgegenstehendes schutzwürdiges Interesse besitzt. Gleichsam "automatisch" darf danach eine Auskunft über den Ehegatten nicht erteilt werden. Auch wenn in einzelnen Fallgruppen ein eine Übermittlung rechtfertigendes Interesse angenommen werden kann, gehen die Aufsichtsbehörden bei der Beurteilung nach wie vor nach strengen Maßstäben vor; eine restriktive Bewertung ergibt sich insbesondere in Fällen, in denen Negativmerkmale über den Ehegatten überhaupt nicht vorhanden sind.

Es bleibt weiteren Gesprächen mit dem Verband vorbehalten, eine datenschutzgerechte Lösung zu diesem schwierigen Fragenkomplex zu finden.

2.3 Versicherungswirtschaft

2.3.1 Im Berichtszeitraum konnten die Verhandlungen der obersten Aufsichtsbehörden der Länder mit der Versicherungswirtschaft über sog. "**Allfinanz-Konzepte**" abgeschlossen werden.

Danach sollen, wie bereits im 3. Tätigkeitsbericht (Ziff. 3.4.3, S. 32) dargelegt, auf der Grundlage einer entsprechenden Einwilligung des Versicherungskunden Vermittlern von Versicherungsverträgen, z.B. Kreditinstituten oder Bausparkassen, die im Rahmen der branchenübergreifenden Zusammenarbeit mit einzelnen Versicherungen diesen Versicherungsverträge vermitteln, einzelne Daten aus den jeweils vermittelten Verträgen zum Zwecke der Beratung und Betreuung auch in Bezug auf sonstige (eigene) Produkte (Finanzdienstleistungen) zur Verfügung stehen.

Die dahingehende mit der Versicherungswirtschaft vereinbarte Einwilligungserklärung lautet:

> "Ohne Einfluß auf den Vertrag und jederzeit widerrufbar willige ich weiter ein, daß der/die Vermittler meine allgemeinen Antrags-, Vertrags- und Leistungsdaten darüber hinaus für die Beratung und Betreuung auch in sonstigen Finanzdienstleistungen nutzen darf/dürfen.
>
> Diese Einwilligung gilt nur, wenn ich bei Antragstellung vom Inhalt des Merkblatts zur Datenverarbeitung Kenntnis nehmen konnte, das mir vor Vertragsabschluß (mit weiteren Verbraucherinformationen), auf Wunsch auch sofort, überlassen wird."

Die Erklärung zielt darauf ab, zum einen durch die vorgesehene Möglichkeit, sich das Merkblatt zur Datenverarbeitung schon bei Antragstellung aushändigen

zu lassen, wofür sich die Aufsichtsbehörden mit Nachdruck eingesetzt haben, die **Transparenz** für den Versicherungskunden zu erhöhen und zum anderen die **Freiwilligkeit** einer Einwilligung in die weitere Nutzung der Daten zu betonen.

2.3.2 Der Präzisierung bedürfen, wie sich im Berichtszeitraum gezeigt hat, die Voraussetzungen, unter denen Krankenversicherer bei Verdacht auf Versicherungsmißbrauch Einmeldungen beim im Aufsichtsbereich des Landes gelegenen Verband der Privaten Krankenversicherung e.V. vornehmen, der die Meldungen an andere ihm angeschlossene Krankenversicherer weitergibt. Derzeit wird eine automatisierte zentrale **Hinweisdatei** wie bei anderen Versicherungsverbänden nicht betrieben; Meldungen werden vom Verband lediglich weiterversandt.

Aus datenschutzrechtlicher Sicht können Übermittlungen nur in konkret begründeten Verdachtsfällen und auch nur in signifikanten, für die Einschätzung des Wagnisses und der Leistungsgewährung wichtigen Fällen in Betracht gezogen werden. Der Verband, der diese Auffassung teilt, hat zugesagt, entsprechende Begrenzungen ausdrücklich sicherzustellen.

Einer Eingrenzung bedürfen ebenfalls die zur Übermittlung gelangenden Daten; für die Übermittlung z.B. von Gesundheitsdaten ist schon deshalb kein Raum, weil das Verfahren lediglich auf die Identifizierbarkeit von Mißbrauchsfällen für andere Krankenversicherer abzielt, die Kenntnis weiterer als der Identifizierung dienender Daten bei der Übermittlung daher nicht erforderlich ist. Auch hierüber konnte Einvernehmen erzielt werden; Vorschläge hierzu und

zu anderen Fragen sind angekündigt worden.

2.3.3 Anläßlich einer Prüfung erhielt eine Aufsichtsbehörde des Landes davon Kenntnis, daß bundesweit ca. 40 Arbeitskreise von Versicherern bestehen, in denen jeweils auf regionaler Ebene zwischen den beteiligten Versicherungsunternehmen Fälle in Form von sog. "**Rundsprüchen**" geklärt werden, bei denen ein Anfangsverdacht auf Versicherungsmißbrauch - soweit bekannt im Kfz-Bereich - besteht. Jeweils ein Versicherungsunternehmen hat den Vorsitz in einem solchen Arbeitskreis, wobei Anfragen zu einem Verdachtsfall an dieses Unternehmen gehen, welches lediglich als Postverteilungsstelle diese Anfragen an die beteiligten Unternehmen des Arbeitskreises weiterleitet. Falls einem Versicherungsunternehmen Erkenntnisse vorliegen, setzt es sich mit dem anfragenden Versicherungsunternehmen unmittelbar in Verbindung.

Aus Sicht der Aufsichtsbehörden war insbesondere das Verhältnis dieser Art des Datenaustauschs zu den **zentralen** Hinweissystemen der Versicherungswirtschaft (vgl. hierzu 3. Tätigkeitsbericht, Ziff. 3.4.1, S. 31) aufklärungsbedürftig. Zu prüfen war, ob und inwieweit es zu einer Aufdeckung von Mißbrauchsfällen nicht erforderlichen, weil mehrfachen Verarbeitung personenbezogener Daten kommt (zwischenzeitlich haben Vertreter der Versicherungswirtschaft der zuständigen Arbeitsgruppe des "Düsseldorfer Kreises" mitgeteilt, daß das Rundspruchverfahren eingestellt werden soll).

2.3.4 Ein Unternehmen der privaten Krankenversicherung erteilte - wie einer Aufsichtsbehörde bekannt wurde - in Fällen, in denen Versicherungsnehmer den Versicherungsvertrag gekündigt hatten, dem jeweils zu-

ständigen Außendienstmitarbeiter einen sog. **Kunden rückgewinnungsauftrag** mit der Bitte, den Kunden nochmals aufzusuchen, um ihm die Auswirkungen seiner Kündigung zu erläutern und ggf. alternative Angebote zu unterbreiten. Zu diesem Zweck wurden den Außendienstmitarbeitern Gesundheitsdaten der Versicherungsnehmer zur Verfügung gestellt, die auf Risikozuschläge oder Leistungsausschüsse Einfluß haben können.

Die Versicherung stützte diese Verfahrensweise auf die Einwilligung der Kunden bzw. auf § 28 Abs. 1 Satz 1 Nr. 1 BDSG; nach ihrer Ansicht lag die Verfahrensweise im Interesse der Kunden, da diese über etwaige Nachteile (z.B. Maßgeblichkeit des Eintrittsalters, Risikozuschlag bei beitragserheblichen Krankheiten, Leistungsausschluß u.ä.) eines Versicherungswechsels informiert würden und ihnen auch alternative Angebote unterbreitet werden könnten.

Die von der Versicherung praktizierte Weitergabe von Gesundheitsdaten wird datenschutzrechtlich nicht aufrechtzuerhalten sein. Zwar erklärt sich ein Versicherungsnehmer in den von den Versicherungsunternehmen verwandten Einwilligungsklauseln u.a. damit einverstanden, daß Gesundheitsdaten an Vermittler - gemeint sind hiermit auch Außendienstmitarbeiter weitergegeben werden, "soweit es zur Vertragsgestaltung erforderlich ist". Ziffer 6 des von den Versicherungsunternehmen ausgegebenen Merkblattes mit Angaben zur Datenverarbeitung stellt klar, daß an den Vermittler neben den Antrags-, Vertrags- und Leistungsdaten des Kunden ausschließlich zum Zwecke von Vertragsanpassungen in der Personenversicherung auch Gesundheitsdaten übermittelt werden dürfen.

Eine Vertragsnachbearbeitung in der oben dargestellten Art und Weise ist allerdings hiervon ("Vertragsgestaltung") nicht erfaßt. Auch wenn ein Interesse des Versicherungskunden an einer Beratung über mit dem Versicherungswechsel verbundene Folgen nicht zu leugnen ist, wird aber zu diesem Zweck die Kenntnis der konkreten risikoerheblichen Krankheiten des Versicherungsnehmers nicht erforderlich sein. Vielmehr werden allgemeine Hinweise des Vertreters auf Risikozuschläge bzw. Leistungsausschlüsse ausreichen. Sollte die konkrete Beratungssituation es erfordern, steht es dem Kunden frei, seine risikoerheblichen Krankheiten selbst zu offenbaren. Hierüber konnte zwischenzeitlich in der zuständigen Arbeitsgruppe des "Düsseldorfer Kreises" Einvernehmen auch mit dem Gesamtverband der Deutschen Versicherungswirtschaft (GDV) erzielt werden.

2.4 Kreditwirtschaft

2.4.1 Auch aus dem Bereich der Kreditwirtschaft (seitens des Zentralen Kreditausschusses) sind an die unter dem Vorsitz des Landes tagende Arbeitgruppe "Kreditwirtschaft" des "Düsseldorfer Kreises" Überlegungen zu sog. **"Allfinanz-Konzepten"** herangetragen worden.

Gedacht wird beispielsweise an die Übermittlung einzelner Daten eines Bankkunden, sofern dessen Einwilligung vorliegt, an mit dem Kreditinstitut als Verbundpartner kooperierende Unternehmen, z.B. an Bausparkassen, damit jene den Bankkunden auch in eigenen Finanzdienstleistungen gezielt beraten können.

Hier zeichnet sich ebenso ab, daß den Gesichtspunkten der Transparenz und der Freiwilligkeit in den entsprechenden Einwilligungserklärungen großes Gewicht zukommt.

2.4.2 Im Berichtszeitraum lagen endgültige Entscheidungen des Zentralen Kreditausschusses zur Einführung und Ausgestaltung **von multifunktionalen Chips auf EC-Karten** noch nicht vor.

Im Unterschied zum "electronic-cash-Verfahren" (3. Tätigkeitsbericht, Ziff. 3.3.2, S. 29) kann bei einem derartigen System auf eine Online-Autorisierung verzichtet werden, solange sich der Zahlungsvorgang in dem Betragsrahmen bewegt, den der Kartenausgeber festgelegt hat. Möglich sind auch aufgrund spezieller, vorher aufladbarer Guthaben auf dem Chip Anwendungen als Telefonkarte oder als Börse für Kleinbeträge in sonstigen Bereichen. Hier sind Lösungen, die eine anonyme Zahlung ermöglichen, als

datenschutzfreundlich einzustufen. Die Aufsichtsbehörden werden die weitere Entwicklung verfolgen.

2.4.3 Anläßlich der Überprüfung bei einem Kreditinstitut war der Frage nachzugehen, welche Daten im Rahmen der **Verarbeitung von Kundendaten**, die für die Führung eines Kreditkontos von Bedeutung sind, gespeichert werden können.

Gegen eine für eigene Zwecke des Kreditinstitutes erfolgende Verarbeitung von Kundendaten bestehen regelmäßig keine Bedenken, sofern die Daten nachweisbare, konkrete und aussagekräftige Tatsachen im Hinblick auf die Zahlungsfähigkeit eines Kunden widerspiegeln (z.B. Verstöße gegen einschlägige vertragliche Verpflichtungen). Insoweit kann im Rahmen der Kontoführung die Verarbeitung von Daten über das - konkrete - Zahlungsverhalten als vom Vertragszweck umfaßt angesehen werden, § 28 Abs. 1 Nr. 1 BDSG.

Etwas anderes gilt - auch nach einhelliger Auffassung des "Düsseldorfer Kreises" - für sonstige Informationen über bestimmte Eigenschaften von Kunden, auch wenn diese auf das Finanzgebahren des Kunden Einfluß haben mögen; ein Speichervermerk mit Daten insbesondere über gesundheitliche Verhältnisse des Kunden (z.B. "Kreditlimit wegen Suchterkrankung") wird schon mangels Erforderlichkeit nicht in Betracht kommen können, zumal solche Daten ohnehin zu löschen wären, falls die datenverarbeitende Stelle ihre Richtigkeit nicht beweisen kann, § 35 Abs. 2 Nr. 2 BDSG.

Kommt es im Hinblick z.B. auf die gesundheitlichen

Verhältnisse eines Kunden überhaupt zu einer Vertragsänderung (ggf. zu einem neuen Zahlungsmodus), reicht für einen innerhalb des Unternehmens verfügbaren Hinweis auf die Zahlungsfähigkeit des Kunden die Speicherung einer Angabe wie "Kreditlimit" ggf. mit erläuterndem, die Tatsache der Vertragsänderung angebendem Zusatz aus, ohne daß Gesundheitsdaten des Betroffenen offenbart werden müßten.

2.5 Weitere Entwicklungen

- Kartengestützte Verarbeitung von Patientendaten

Neben der in der gesetzlichen Krankenversicherung eingeführten Krankenversichertenkarte bestehen im privaten Bereich Überlegungen, eine kartengestützte Patientendatenverarbeitung in verschiedenen Bereichen einzuführen, wobei die Inanspruchnahme solcher Karten auf freiwilliger Grundlage erfolgen soll. Die Überlegungen reichen von Krankenversichertenkarten ohne Gesundheitsdaten bis hin zu Karten mit medizinischen Daten oder Angaben über Medikationen. Einerseits sollen Verwaltungsabläufe vereinfacht werden. Andererseits wird auch an eine nicht nur auf Ärzte beschränkte Verwendung von Karten gedacht; beispielsweise wird überlegt, Karten mit bestimmten Daten über Medikationen auch im Bereich der Apotheken zur Beratung des Kunden über Arzneimittel einzusetzen.

Wegen einzelner Projekte haben sich Unternehmen im Hinblick auf die datenschutzrechtliche Problematik an eine Aufsichtsbehörde des Landes gewandt. Wegen der mit derartigen Karten verbundenen Gefahren für

das informationelle Selbstbestimmungsrecht wird sich die Aufmerksamkeit neben den technischen Sicherheitsanforderungen besonders auf die Gesichtspunkte der Transparenz und der Freiwilligkeit richten.

3. EG-Datenschutzrichtlinie

Mit der Richtlinie, die im Berichtszeitraum unter Beteiligung der Länder (NRW und Bayern) intensiv beraten worden ist, ist die aus datenschutzrechtlicher Sicht wünschenswerte Harmonisierung des Datenschutzes in der Europäische Union vorangebracht worden. Es galt, trotz der in den Mitgliedstaaten zum Teil völlig unterschiedlichen Ausgangslage eine gemeinsame Lösung zu finden. Aus deutscher Sicht kann nach dem gefundenen Ergebnis davon ausgegangen werden, daß der im Inland bereits gewährte Datenschutzstandard sowie das praktizierte Verfahren der Datenschutzkontrolle im wesentlichen unverändert beibehalten und darüber hinaus Weiterentwicklungen des Datenschutzes fortgeführt werden können.

Auch die im Bundesdatenschutzgesetz vorgesehene Selbstkontrolle der datenverarbeitenden Stellen greift die Richtlinie durch Regelungen über interne (im privaten Bereich betriebliche) Datenschutzbeauftragte auf.

Datentransfers in Drittländer dürfen grundsätzlich nur stattfinden, wenn dort ein angemessenes Schutzniveau herrscht. Für den Transfer in Länder, die kein angemessenes Schutzniveau gewährleisten, sieht die Richtlinie nähere Regelungen zur Gewährleistung des Datenschutzes vor.

Um wenigstens einstweilen bis zum Inkrafttreten verbindlicher Regelungen für den Datenexport Lösungskonzepte zu entwickeln, die bei einem Datenexport in Länder mit schwächerem oder gar fehlendem Datenschutz, soweit ein solcher überhaupt in Erwägung gezogen werden kann, der Gefährdung schutzwürdiger Belange der Betroffenen soweit wie möglich entgegenwirken sollen, haben die im "Düsseldorfer Kreis" vertretenen obersten Aufsichtsbehörden bisher schon Empfehlungen für Schutzvorkehrungen auf vertraglicher Basis an die Unternehmen gerichtet (vgl. 3. Tätigkeitsbericht, Ziff. 3.2.3, S. 25). Eine zuletzt von den Aufsichtsbehörden erarbeitete "Checkliste" mit Anhaltspunkten für eine eigenverantwortliche, der jeweiligen Situation angepaßte Beurteilung der Zulässigkeit von Datentransfers durch die Wirtschaft hat große Beachtung gefunden; es müssen noch Erfahrungen abgewartet werden, inwieweit die einzelnen Punkte zur Ausfüllung der Richtlinie herangezogen werden können.

Für die Umsetzung der Richtlinie in nationales Recht stehen seit Annahme durch den Rat (im Juli 1995) drei Jahre zur Verfügung.