53 Seiten!

Zweiter 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

Überblick

Der vorliegende Bericht betrifft die Jahre 1989 und 1990. Mit ihm gibt die Landesregierung, anknüpfend an den ersten, im wesentlichen die Jahre 1987 und 1988 betreffenden Bericht, zum zweiten Mal einen Überblick über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörden in Nordrhein-Westfalen.

Auch im nunmehr darzustellenden Berichtszeitraum waren die Aufsichtsbehörden mit einer Vielzahl von Beschwerden, Anfragen und Beratungsersuchen sowie mit Überpüfungen vor Ort befaßt, wobei die Beratung der datenverarbeitenden Stellen ein bedeutender Schwerpunkt der Aufsichtstätigkeit bleibt.
Im Vergleich zu dem dem 1. Tätigkeitsbericht zugrundeliegenden Zeitraum haben sich keine überraschenden Erkenntnisse ergeben. Die Zahlen weisen zwar in einigen Punkten interessante Veränderungen auf; ob darin der Beginn einer positiven Entwicklung zu sehen ist, muß allerdings offenbleiben.
Nach wie vor gilt es, die erfolgreichen Bemühungen der Aufsichtsbehörden fortzusetzen und auf Verbesserungen bei den datenverarbeitenden Stellen hinzuwirken (hierzu nachfolgend **Ziff. 1**).

Das mit Gesetz vom 20. Dezember 1990 novellierte, mit Ausnahme einer Vorschrift zum automatisierten Abrufverfahren seit dem 1. Juni 1991 geltende Bundesdatenschutzgesetz enthält, wenngleich es in einigen nicht unwesentlichen Punkten hinter den Erwartungen der Aufsichtsbehörden zurückbleibt, weitere Schritte zur Sicherung des Persönlichkeitsrechts. Die Zukunft wird zeigen, welchen Beitrag die Novelle zur Verbesserung des Datenschutzes in der Praxis zu leisten vermag (hierzu nachfolgend **Ziff. 2**).

Beinahe zeitgleich mit dem Abschluß des Gesetzgebungsverfahrens zur Novellierung des Bundesdatenschutzgesetzes legte die EG-Kommission ein Paket von Vorschlägen zum Datenschutz in der EG vor, wobei der "Vorschlag für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten" als gleichsam allgemeine Regelung für den Datenschutz in Europa hervorzuheben ist.
Hier gilt es, die Erfahrungen der Aufsichtsbehörden in die Beratungen einzubringen und auf eine Mitwirkung auf europäischer Ebene hinzuwirken (hierzu nachfolgend **Ziff. 3**).

Nach wie vor fehlen für die Mitgliedstaaten der EG verbindliche Regelungen zum Datenschutz beim grenzüberschreitenden Datenverkehr. Dessen ungeachtet waren und sind die Aufsichtsbehörden angesichts der zunehmenden grenzüberschreitenden Datenflüsse um eine Verbesserung des Datenschutzes bemüht. Erste Schritte konnten mit Hilfe des sogenannten "Vertragsmodells" unternommen werden (hierzu nachfolgend **Ziff. 4**).

1. Erfahrungen der Aufsichtsbehörden im Berichtszeitraum 1)

1.1 Übersicht über die Kontrolltätigkeit in Zahlen 2)

1.1.1 Meldungen zum Register

Mit Stand 31.12.1990 waren zum Register der Aufsichtsbehörden folgende Stellen gemeldet:

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

	RP Arnsberg	RP Köln
- Adreßhandel, Direktmarketing	9 (9)	14 (15)
- Auskunfteien, Warndienste	44 (43)	60 (57)
Gesamt:	53 (52)	74 (72)

---

1) Paragraphenangaben unter Ziff. 1 beziehen sich auf das im Berichtszeitraum in der alten Fassung geltende Bundesdatenschutzgesetz

2) Zahlen in Klammern sind Vergleichszahlen aus dem 1. Tätigkeitsbericht

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

	RP Arnsberg	RP Köln
- Markt- und Meinungsforschungsinstitute	7 (5)	20 (17)

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

RP Arnsberg	RP Köln
309 (295)	413 (381)

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

d) Gemeldete Unternehmen nach a) bis c) insgesamt

RP Arnsberg	RP Köln
369 (352)	507 (470)

Gegenüber dem 1. Tätigkeitsbericht weisen die Zahlen nicht auf bemerkenswerte Veränderungen hin; von einer weiteren Zunahme ist allerdings auszugehen. Nach den bisherigen Erfahrungen der Aufsichtsbehörden ist davon auszugehen, daß eine ganze Reihe von Unternehmen aus Unkenntnis der Meldepflicht nicht nachkommt.

1.1.2. Beschwerden

In den Jahren 1989 und 1990 sind gegen datenverarbeitende Stellen, die Datenverarbeitung für eigene Zwecke (3. Abschnitt des BDSG) durchführten und für die lediglich eine Anlaßaufsicht bestand, beim RP Arnsberg insgesamt 99 (102) Beschwerden und beim RP Köln 225 (256) Beschwerden eingegangen.

Gegen Stellen, die geschäftsmäßig personenbezogene Daten für fremde Zwecke verarbeiteten (4. Abschnitt des BDSG), wurden im vorgenannten Zeitraum beim Regierungspräsidenten Arnsberg insgesamt 57 (99) Beschwerden und beim Regierungspräsidenten Köln 69 (96) Beschwerden vorgebracht.

In diesen Zahlen sind sowohl Beschwerden von Betroffenen als auch Beschwerden von anderen Personen enthalten.
Die angegebenen Zahlen verteilen sich wie folgt:

3. Abschnitt (Beschwerden)	RP Arnsberg	RP Köln
- Handel/Handwerk	13 (10)	48 (65)
- Industrie/Großunternehmen	8 (9)	32 (19)
- Krankenhäuser, Ärzte, privatärztliche Verrechnungsstellen	13 (7)	15 (12)
- Kreditinstitute	14 (14)	21 (28)
- Kreditvermittler	2 (-)	5 (-)
- Versicherungen	8 (16)	47 (51)
- Vereine, Verbände	12 (21)	32 (44)
- Sonstige	29 (25)	25 (37)
Gesamt	99 (102)	225 (256)

4.Abschnitt	RP Arnsberg	RP Köln
- Adreßhandel, Direktmarketing	3 (20)	4 (6)
- Auskunfteien, Warndienste	49 (68)	61 (84)
- Konzerndatenverarbeiter	2	-
- Markt- und Meinungsforschungsinstitute	1 (6)	2 (1)
- Rechenzentren (Auftragsdatenverarbeiter)	- (5)	2 (5)
- Sonstige	2	-
Gesamt	57 (99)	69 (96)

Der Schwerpunkt der Überprüfungsersuchen hat sich gegenüber dem Berichtszeitraum des 1. Tätigkeitsberichts kaum geändert:

- Im Bereich des 3.Abschnitts des BDSG spielten Fragen zur Zulässigkeit der Datenspeicherung in den verschiedenen Bereichen (z.B. in Versicherungsverträgen, Bewerber-/Personalfragebögen, Mieterfragebögen, Mitgliederverwaltung in Vereinen und Verbänden) eine wesentliche Rolle. Gerade in Vereinen bestand häufig Unsicherheit, welche personenbezogenen Daten gespeichert und unter welchen Voraussetzungen sie übermittelt werden dürfen. Weiterhin gingen Fragen zu unerwünschten Werbezusendungen/Herkunft von Adreßmaterial etc. ein.

- Im Bereich des 4.Abschnitts des BDSG bildeten nach wie vor Fragen zur Tätigkeit von Handelsauskunfteien sowie der SCHUFA einen Schwerpunkt. Die Fragestellungen haben sich gegenüber den Vorjahren nicht geändert.

Bei den insgesamt 450 Beschwerden kam es in 80 Fällen zu Beanstandungen oder Empfehlungen der Aufsichtsbehörden. Bis auf eine Ausnahme haben die datenverarbeitenden Stellen die Beanstandungen oder Empfehlungen befolgt. In den übrigen Fällen ergab sich kein Grund zu Beanstandungen bzw. wurden in einzelnen Fällen die Beschwerden aus verschiedenen Gründen (z.B. auf Wunsch des Beschwerdeführers oder wegen Einstellung der Geschäftstätigkeit) nicht weiter verfolgt.

Auffallend ist der Rückgang der Zahl der Beschwerden von 553 (s. 1. Tätigkeitsbericht) auf 450 sowie auch die nicht allzu hohe Zahl der begründeten Beschwerden. Ob bereits hierin der Beginn einer Entwicklung hin zu einer tatsächlichen und dauerhaften Verbesserung des Datenschutzes erblickt werden kann, wird die Zukunft zeigen.

Zu begrüßen ist die Bereitschaft der datenverarbeitenden Stellen, den Beanstandungen bzw. Empfehlungen der Aufsichtsbehörden zu folgen. Insoweit hat sich die schon in den Vorjahren erkennbar gewordene Bereitschaft zur Kooperation erfreulicherweise fortgesetzt.

1.1.3 **Anfragen und Beratungsersuchen**

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

	RP Arnsberg		RP Köln	
	3.Abschn.	4.Abschn.	3.Abschn.	4.Abschn.
Anfragen von				
- betriebl. Datenschutzbeauftragten	3 (2)	- (2)	7 (19)	5 (10)
- Geschäftsleitungen	12 (10)	4 (5)	47 (4)	8 (7)
- Betriebsräten	1 (4)	-	5 (5)	- (1)
- Einzelpersonen, Vereinen, Verbänden	29 (26)	8 (7)	60 (49)	14 (7)
Gesamt:	45 (42)	12 (14)	119 (77)	27 (25)

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

Bemerkenswert erscheint die Zunahme der Beratungsersuchen im Aufsichtsbereich des Regierungspräsidenten Köln, wobei die Zunahme der Beratungsersuchen von Geschäftsleitungen von Unternehmen des 3.Abschnitts des BDSG besonders auffällt.

Es wäre zu begrüßen, wenn hier eine Entwicklung eingesetzt hätte, nach der schon aus der Sicht der Unternehmen dem Datenschutz als Unternehmensaufgabe zunehmend Bedeutung einzuräumen ist, ohne daß es eines Anstoßes von außen bedarf.

Die eigentlichen Beratungsersuchen sowie die aus Anlaß von Beschwerden (s.o. Ziff. 1.1.2) und Überprüfungen vor Ort (nachfolgend Ziff. 1.1.4) gegebenen Empfehlungen der Aufsichtsbehörden weisen darauf hin, daß die **Beratung** einen bedeutenden Schwerpunkt der behördlichen Tätigkeit darstellt und angesichts der Kooperationsbereitschaft der Wirtschaft noch mehr Gewicht als bisher erhalten dürfte und sollte.

1.1.4 Überprüfungen vor Ort

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

a) regelmäßige Überwachung (4.Abschnitt)

	RP Arnsberg	RP Köln
	105 (74)	154 (167)

b) konkrete Anlässe	RP Arnsberg	RP Köln
3.Abschnitt	2 (4)	44 (48)
4.Abschnitt	5 (9)	11 (19)
Gesamt:	7 (13)	55 (67)
Gesamt a) und b)	112 (87)	209 (234)

Der Schwerpunkt der **regelmäßigen** Überprüfungen lag z.B. bei Aktenvernichtungsunternehmen, Buchführungshelfern sowie insbesondere bei Rechenzentren.

Bei diesen insgesamt 259 regelmäßigen Überprüfungen kam es in 110 Fällen zu Beanstandungen und in 91 Fällen zu Empfehlungen.

Hier wird deutlich, daß Überprüfungen vor Ort doch eine relativ hohe Zahl an Mängeln zutage treten lassen.

Insbesondere folgende - nicht erst im Berichtszeitraum bekanntgewordene - wesentliche Mängel wurden bei den geprüften Stellen festgestellt (s.a. unten Ziff. 1.3):

- 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 (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 § 29 BDSG,
- nicht mehr aktuelle Registermeldungen,
- Probleme bei der Bestellung und Tätigkeit des betrieblichen Datenschutzbeauftragten.

Eine deutliche Mehrzahl der geprüften Stellen war auch hier freiwillig bereit, für eine entsprechende Änderung zu sorgen. Nur in wenigen Fällen waren die überprüften Stellen erst aufgrund mehrfachen Schriftwechsels bereit, die erbetenen Änderungen umzusetzen.

1.1.5 **Bußgeldverfahren**

In den Jahren 1989 und 1990 leiteten die Aufsichtsbehörden folgende Bußgeldverfahren ein:

	RP Arnsberg	RP Köln
3.Abschnitt	- (-)	- (2)
4.Abschnitt	1 (4)	2 (1)
Gesamt:	1 (4)	2 (3)

Zwei im Berichtszeitraum noch nicht rechtskräftig abgeschlossene Verfahren betrafen die Meldepflicht zum Register nach § 39 BDSG. Ein Verfahren bezog sich auf den Fall einer Auskunftsverweigerung.

Die nach wie vor verschwindend geringe Zahl der Bußgeldverfahren zeigt, daß "repressive" Elemente in der Aufsichtspraxis eine untergeordnete Rolle spielen. Dem Datenschutz dient es mehr, wenn mit den Unternehmen einvernehmliche Lösungen gefunden werden.

1.2 Einzelprobleme, Beispielsfälle aus der Kontrolltätigkeit

1.2.1 SCHUFA, Handels- und Wirtschaftsauskunfteien, Versandhandel

An den unter dem Vorsitz des Landes tagenden "Düsseldorfer Kreis" (Arbeitsgemeinschaft der Länder) wurde die Frage herangetragen, in welchem Umfang von der SCHUFA Auskünfte an **Kreditkartenunternehmen** bei der Ausgabe von Kreditkarten (nicht von sog. Kundenkarten) Übermittelt werden dürfen.
Ursprünglich erhielten jene Unternehmen von der SCHUFA Auskünfte im Rahmen von sogenannten "B-Verträgen". Danach war die Übermittlung von Daten lediglich über sog. "Negativmerkmale" (nicht vertragsgemäße Abwicklung von Geschäftsbeziehungen) vorgesehen. Nunmehr sollen im Rahmen sog. "A-Verträge" auch "Positivdaten" (Daten über Beantragung, Abschluß und Beendigung eines Kreditkartenvertrages) übermittelt bzw. von den Kreditkartenunternehmen an die SCHUFA gemeldet werden können.
Grundsätzliche Bedenken gegen die Umstellung wurden in Übereinstimmung mit der Mehrheit der obersten Aufsichtsbehörden der Länder - soweit sog. Kundenkarten ausgeklammert (s.o.) und über die o.g. Daten hinaus keine zusätzlichen Daten übermittelt werden - nicht geltend gemacht, da die Übermittlung von "Positivdaten" aufgrund einer Einwilligung erfolgen soll und im übrigen ein gewisses kreditorisches Risiko der Kreditkarten-Emittenten - ähnlich wie hinsichtlich der Überziehungskredite bei Girokonten - nicht in Abrede gestellt werden kann (im üblichen Bankauskunftsverfahren läßt sich auch nicht detailliert klären, über welche anderen Kreditkarten ein Kunde verfügt).

Die Aufsichtsbehörden werden die Praxis der Datenverarbeitung und -nutzung in diesem Bereich weiter aufmerksam verfolgen.-

Die Anzahl der **Personenverwechslungen** bei Auskünften im Verhältnis zur Gesamtzahl der erteilten Auskünfte kann als gering eingestuft werden. Dennoch traten auch im Berichtszeitraum mehrere Fälle mit dieser Problematik auf.

In einem Fall kam es aufgrund der Gleichheit des Namens und des Geburtsdatums zu unrichtigen Datenspeicherungen bei der SCHUFA. Der Beschwerdeführer wandte sich zunächst direkt an die SCHUFA als datenspeichernde Stelle. Der Hinweis auf die Unrichtigkeit der Daten führte jedoch zunächst nicht zu der gewünschten Änderung. Die SCHUFA wies darauf hin, daß sie die ihr von den Vertragspartnern übermittelten Daten lediglich treuhänderisch verwalte. Durch das Einschreiten der Aufsichtsbehörde konnte eine weitere Überprüfung und Korrektur der Datenspeicherung sowohl bei der SCHUFA als auch bei ihrem Vertragspartner veranlaßt werden.

Schwierigkeiten beklagte in einem anderen Fall der Inhaber eines Betriebs. Ausgangspunkt war die Namensgleichheit einer im selben Wohnort lebenden Person. Durch fehlende Sorgfalt beim Umgang mit sensiblen Daten kam es zu einer Personenverwechslung, die dazu führte, daß von einer Wirtschaftsauskunftei fälschlicherweise Negativmerkmale zum Beschwerdeführer als Auskunft übermittelt wurden.

Erst nachdem der Beschwerdeführer mehrfach bei der Wirtschaftsauskunftei vorstellig geworden war und sich letztlich auch die Aufsichtsbehörde noch einschaltete, konnten die Daten korrigiert werden.

Die datenverarbeitenden Stellen sollten wegen der nicht zu übersehenden Nachteile, die das Opfer einer Verwechslung zu befürchten hat, ihre Bemühungen um Verbesserungen fortsetzen und auf eine vollständige Behebung der Fehlerquellen hinwirken. -

Bonitätsüberprüfungen, sei es, daß sie durch Handels- und Wirtschaftsauskunfteien oder durch Unternehmen des Versandhandels vorgenommen werden, werfen immer wieder aufs neue datenschutzrechtliche Fragen auf:

Mehrere Beschwerdeführer wandten sich an eine Aufsichtsbehörde, weil sie mit der Speicherung und Nutzung von Daten durch ein Unternehmen des Versandhandels nicht einverstanden waren. Sie hatten Waren per Rechnung bestellt und waren kurz darauf über die Ablehnung der Belieferung benachrichtigt worden. Bei allen Beschwerdeführern wurde gleichermaßen festgestellt, daß beim Versandhandelsunternehmen selbst keine negativen personenbezogenen Daten über sie vorlagen.

Das Unternehmen gab in jedem Beschwerdefall an, daß im Rahmen eines Bonitätsprüfungsverfahrens hohe Forderungsausfälle auf die Bestellanschrift festgestellt worden seien. Dies war z.B. dann gegeben, wenn der Vormieter einer Wohnung die bestellte Ware nicht bezahlt hatte.

Auch wenn in Fällen dieser Art ein gewisses Unbehagen darüber, daß Betroffene aufgrund von nicht in ihrer Person liegenden Umständen eine bestimmte Wertung erfahren, nicht auszuräumen ist, kann es einem Unternehmen nicht verwehrt werden, erforderliche und angemessene Vorkehrungen zu treffen, um sich auf der Grundlage von zutreffenden Erfahrungstatsachen dem jeweiligen Risiko entsprechend absichern zu können.

Im "Düsseldorfer Kreis" wurde die datenschutzrechtliche Bewertung von **mathematisch-statistischen** Verfahren erörtert, mit deren Hilfe einem Unternehmen Aufschluß darüber verschafft werden soll, ob ein Kunde kreditwürdig ist. Es handelt sich hierbei um Verfahren mit recht unterschiedlicher Ausgestaltung, denen gemeinsam das Prinzip zugrundeliegt, daß auf der Grundlage von zu Einzelangaben erstellten Punktebewertungen eine Gesamtbewertung erfolgt.

Ob schutzwürdige Belange beeinträchtigt werden, kann letztlich nur im Einzelfall geklärt werden.

Grundsätzliche Bedenken erheben sich insofern, als die betroffenen Einzelpersonen aufgrund der Bewertung bestimmten Gruppen zugerechnet und damit - sei es in positiver oder in negativer Hinsicht - gewissermaßen "kategorisiert" werden können.

Vorbehaltlich der Umstände im Einzelfall ist für derartige Verfahren daher mindestens zu fordern, daß sie z.B. auf wahren, nachprüfbaren Tatsachenangaben beruhen, das Bewertungssystem in sich schlüssig, nachvollziehbar und vertretbar ist und das Verfahren zu einer verläßlicheren Einschätzung der Bonität eines Kunden führt.

Um hier dem Einzelnen Gelegenheit zu einer Überprüfung seiner Belange zu geben, kommt seiner umfassenden Benachrichtigung oder Unterrichtung bzw. einer entsprechenden Auskunft an ihn besondere Bedeutung zu.

Die Aufsichtsbehörden werden die Praxis weiter aufmerksam verfolgen.

1.2.2 Zentrale Datensammlungen

Im Interesse der Rechtssicherheit wären klare gesetzliche Regelungen zu der Frage, ob und in welchem Rahmen zentrale Datenbanken mit aus öffentlichen (amtlichen) Registern (z.B. aus dem Handelsregister oder aus dem Schuldnerverzeichnis) entnommenen Daten für kommerzielle Zwecke errichtet werden dürfen, wünschenswert.

Die in der Praxis bestehenden Datensammlungen sind unterschiedlich ausgestaltet; sie können unterschiedlichen Zwecken dienen. Auf der Grundlage amtlicher Bekanntmachungen werden z.B. auch private Veröffentlichungen (z.B. mit Daten über Konkurse oder Zwangsversteigerungen) herausgegeben.

Eine Beurteilung anhand der Generalklauseln des Bundesdatenschutzgesetzes insbesondere wegen der Frage der Verletzung "schutzwürdiger Belange" erfordert eine auf den jeweiligen Einzelfall bezogene Prüfung der Zulässigkeitsvoraussetzungen. Auch wenn danach Bedenken gegen einzelne Vorhaben zurückgestellt werden mögen, etwa weil bestimmte Maßgaben (z.B. Weglassen von Namen oder Firmenbezeichnungen) beachtet oder weil keine sensitiven "Negativdaten" verarbeitet werden

oder weil man davon ausgeht, daß Auskunft aus Datensammlungen nur bei Glaubhaftmachung eines überwiegenden berechtigten Interesses nach entsprechender Abwägung im Einzelfall erteilt wird, lassen sich z.B. im Hinblick auf die (ursprüngliche) gesetzliche Zweckbestimmung der amtlichen Veröffentlichung, das Erfordernis der Richtigkeit und Aktualität der Daten und wegen der Möglichkeit von Verwechslungen Zweifel an der Vereinbarkeit derartiger Vorhaben mit den schutzwürdigen Belangen einzelner nicht ganz ausschließen (s.a. Beschluß d. BGH vom 12.7.1989 in BB 89, 1635 zur Mikroverfilmung des gesamten Handelsregisters durch eine private Firma).

Der im Gesetzgebungsverfahren befindliche Gesetzentwurf der Bundesregierung für ein "Gesetz zur Änderung von Vorschriften über das **Schuldnerverzeichnis**" bedarf insofern weiterer Beobachtung. Auf Initiative des Landes hat der Bundesrat um eine Prüfung und Klarstellung zu der Frage der Errichtung und Führung zentraler bundesweiter Schuldnerverzeichnisse durch Private im Gesetzgebungsverfahren gebeten (zuletzt Bundesrats-Drucksache 78/91; vgl. in diesem Zusammenhang auch den 10. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Nordrhein-Westfalen unter Ziff. 5.19.2, S. 131).

1.2.3 **Hinweis- und Warnsysteme**

Zu zentralen Hinweis- und Informationssystemen der **Versicherungswirtschaft** sich ergebende Einzelfragen sind schon im 1. Tätigkeitsbericht angesprochen worden (vgl. Ziff. 7.2.5, S. 47 ff). U.a. steht bei einigen Hinweissystemen, die der Risikoprüfung bei Antragstellung und im Schadensfall dienen, die Frage der Benach-

richtigung Dritter im Mittelpunkt des Interesses, d.h. solcher Personen, die nicht auf andere Weise von der Aufnahme ihrer Daten in diese Informationssysteme Kenntnis erhalten. Der Benachrichtigung kommt insofern Bedeutung zu, als eigentlich erst durch eine Benachrichtigung die Betroffenen in die Lage versetzt werden, ihre Belange gegenüber den Versicherungsunternehmen darlegen zu können. Die Verhandlungen der zuständigen Arbeitsgruppe des "Düsseldorfer Kreises" mit der Versicherungswirtschaft vor allem über die Frage des Inhalts dieser Benachrichtigung halten noch an.
Bei diesen zentralen Dateien ist es noch nicht zu der von der Versicherungswirtschaft ins Auge gefaßten Einführung eines "phonetischen Strukturcodeverfahrens" gekommen, mit dessen Hilfe eine Reidentifizierung insbesondere solcher eingemeldeter Personen erschwert werden könnte, an deren Kenntnis die einzelnen Versicherungsunternehmen - wenn ein Abgleich in der Datei Anhaltspunkte für die Risikoprüfung nicht ergibt - kein Interesse haben dürften. Eine unverzügliche und vollständige Umstellung dieser von den verschiedenen Versicherungsverbänden betriebenen Hinweisdateien auf ein dem Datenschutz eher gerecht werdendes Verfahren erscheint daher geboten. In Zukunft wird - auch nach einer Umstellung auf ein neues Verfahren - weiter zu prüfen sein, ob hier weitere Maßnahmen im Interesse des Datenschutzes erforderlich sind. -

Bereits im 1.Tätigkeitsbericht wurde dargelegt, wie die Speicherung personenbezogener Daten seitens der Verkehrsbetriebe in den sogen. "Schwarzfahrer-Dateien" datenschutzrechtlich zu beurteilen ist. In diesem Berichtszeitraum wurde einer Aufsichtsbehörde durch die Beschwerde eines Betroffenen bekannt, daß ein Verkehrsbetrieb eine sog. **Namensmißbrauchs-Datei** führt.

Bei Fahrausweiskontrollen treffen die Kontrolleure der Verkehrsbetriebe auch Fahrgäste ohne gültigen Fahrausweis an, die keinerlei Papiere mit sich führen und falsche Personalien angeben. Dies kann dazu führen, daß jemand eine Mahnung zur Zahlung des erhöhten Beförderungsentgelts erhält, ohne tatsächlich gefahren zu sein.

Nach Überprüfung und Feststellung des Verkehrsbetriebes, daß es sich um einen Fall von Namensmißbrauch handelt, wird der Vorgang mit dem Vermerk "Namensmißbrauch" in der Datei "Fahrgäste ohne gültigen Fahrausweis" besonders gekennzeichnet und in eine besondere Datei übernommen. Aus der Datei "Namensmißbrauch" heraus erhält der Fahrausweisprüfer eine Auflistung der Namen, die mehrfach mißbraucht worden sind, um sofort bei der Aufnahme der Personalien diese überprüfen zu können. Fast 80 % der "Namensmißbräuche" kommen nach Angaben des Verkehrsbetriebes mindestens zwei Mal vor.

Die Speicherung der personenbezogenen Daten in dieser Datei erfordert das Vorliegen eines berechtigten Interesses. Die berechtigten Interessen des Verkehrsbetriebes bestehen darin, derartige Fälle von Namensmißbrauch aufzuklären, um Strafantrag zu stellen. Gleichzeitig liegt die Aufklärung derartiger Fälle im Interesse des Bürgers, dessen Daten fälscherlicherweise angegeben worden sind.

Eine Speicherung der mißbrauchten Daten kann nur eine gewisse Zeit lang erforderlich sein. Eine längerfristige Speicherung erfolgt nur dann, wenn der Betroffene dies wünscht. Wünscht er eine Löschung seiner personenbezogenen Daten, so kommt der Verkehrsbetrieb dem nach.

Dies setzt allerdings voraus, daß der Betroffene in ausreichender Weise über das vom Verkehrsbetrieb praktizierte Verfahren unterrichtet wird. Denn auch nur dann kann er eine evtl. Beeinträchtigung seiner schutzwürdigen Belange geltend machen.

Der Verkehrsbetrieb ist dem Hinweis der Aufsichtsbehörde, die Betroffenen schriftlich über das Verfahren zu unterrichten, nachgekommen.

1.2.4 Nach wie vor ergeben sich datenschutzrechtliche Fragestellungen bei der Begründung oder Abwicklung von **Mietverhältnissen.**

Einem Vermieter ist es nicht zu verwehren, den Mietbewerber nach Umständen zu befragen, die für die Begründung des Mietverhältnisses von Bedeutung sind. Wie im 1. Tätigkeitsbericht (vgl. Ziff. 7 S. 68) ausgeführt, stoßen z.B. Fragen nach Verlobung oder Scheidung auf grundsätzliche Bedenken. Zulässig sind Fragen, die zur Abschätzung des Mietrisikos erforderlich sind. Die Aufsichtsbehörden waren auch im Berichtszeitraum damit befaßt, in nicht immer einfachen Grenzfällen zu beraten und den Umgang mit personenbezogenen Daten auf ein angemessenes Maß zu reduzieren. So nahm im Zuge der Bearbeitung einer Kleinen Anfrage (Ltgs.-Drucksache 11/349 sowie 11/547 - Antwort der Landesregierung -) zur Befragungspraxis einer Wohnungsbaugesellschaft diese eine die Wohnungsvergabe betreffende Dienstanweisung zurück, nachdem ihr entsprechende Bedenken erläutert worden waren. -

Im Berichtszeitraum wurde einer Aufsichtsbehörde bekannt, daß ein Haus- und Grundbesitzerverein ein **Mietkataster** mit Angaben zur Lage, Größe, Ausstattung von Wohnungen und zur Miete erstellen wollte.

Dieses Mietkataster sollte u.a. der Bekanntgabe der Daten von jeweils 3 Vergleichswohnungen an anfragende Vermieter des Haus- und Grundbesitzervereins zum Zwecke der Begründung von Mieterhöhungsverlangen nach § 2 Abs. 2 Satz 4 des Gesetzes zur Regelung der Miethöhe dienen. Die beabsichtigte Übermittlung der Daten an Vermieter wurde datenschutzrechtlich wie folgt beurteilt:

Auch ungeachtet fehlender Angaben über die Namen von Mietern handelt es sich bei den gespeicherten Angaben um personenbezogene Daten, da der Mieter vielfach schon im Hinblick auf Angaben wie Straße, Haus-Nummer, Stockwerk, Stockwerklage und Wohnfläche bestimmbar ist. Eine Übermittlung der Daten durch den Haus- und Grundbesitzerverein an Vermieter zum Zwecke von Mieterhöhungsverlangen ist als Auskunfteitätigkeit nach dem 4.Abschnitt des BDSG zu beurteilen. Ein berechtigtes Interesse der Vermieter an der Übermittlung von Daten über Vergleichswohnungen wird zwar grundsätzlich anzunehmen sein, weil das Gesetz zur Regelung der Miethöhe deren Benennung gegenüber Mietern ausdrücklich als eine von mehreren Möglichkeiten zur Begründung von Mieterhöhungsverlangen zuläßt und es bei unterbleibender Übermittlung den Vermietern erfahrungsgemäß oft Schwierigkeiten bereitet, geeignete Vergleichswohnungen benennen zu können.

Es sind aber im Hinblick auf die hier maßgebliche Vorschrift des § 32 Abs. 2 BDSG nicht nur die Eigentümer - und Vermieterinteressen zu berücksichtigen, sondern auch die Belange der Mieter, für die die eigene Wohnung zum Kernbereich ihrer Privatsphäre gehört.
Das Mietkataster führt für die von der Datenverarbeitung betroffenen Mieter dazu, daß deren Wonungen aufgrund der durch die automatisierte Datenverarbeitung eröffneten schnellen und leichten Verfügbarkeit deutlich häufiger als bisher zur Begründung von Mieterhöhungsverlangen - insbesondere in Fällen vergleichsweise hoher Mieten - herangezogen werden können. Damit besteht eine erhöhte Wahrscheinlichkeit, daß bei Mietern Nachforschungen über ihre Wohnungen angestellt werden. Darüber hinaus wird aufgrund der Datenausdrucke des Computers, in dem das Mietkataster geführt wird, eine Reihe von Einzelangaben über die Wohnverhältnisse der Betroffenen bekannt, was auch Rückschlüsse auf ihre Einkommenslage und sonstige Lebensumstände ermöglicht. Es ist folglich nicht auszuschließen, daß sich die gesteigerte Aufmerksamkeit als unverhältnismäßige Belästigung von Mietern auswirkt, jedenfalls dann, wenn die Mieter dies durch ihren Widerspruch klar zum Ausdruck bringen. Insoweit lassen sich Parallelen zur Rechtsprechung des BGH ziehen, nach der häufige Briefkastenwerbung im Falle des Widerspruchs des Betroffenen als unzumutbares Eindringen in den häuslichen Eigen bereich zu werten ist und daher dessen informationelles Selbstbestimmungsrecht verletzt (BGH, Urteil vom 20.12.1988, NJW 1989, 902).

Dieser Meinung haben sich auch die im "Düsseldorfer Kreis" vertretenen Aufsichtsbehörden für den nichtöffentlichen Bereich mehrheitlich angeschlossen.

Die Übermittlung der mieterbezogenen Daten an die Vermieter ist demnach nur dann zulässig, wenn die betroffenen Mieter vor der Erstübermittlung unter Einräumung einer Widerspruchsmöglichkeit über das praktizierte Verfahren informiert werden und keinen Widerspruch erheben.

Aufgrund der Ausführungen der Aufsichtsbehörde hat der Haus- und Grundbesitzerverein sein ursprünglich beabsichtigtes Verfahren nicht verwirklicht. Die Aufsichtsbehörde wird die weitere Entwicklung aufmerksam verfolgen.

1.2.5 Die Verarbeitung von **Kundendaten**, die aus Anlaß von Vertragsverhältnissen erhoben worden sind, bedarf häufig der Prüfung, ob die Grenzen des Vertragsverhältnisses eingehalten sind. Ein Bürger teilte einer Aufsichtsbehörde mit, daß eine Videothek bei der computerunterstützten Abwicklung des Verleihgeschäftes neben den Daten des Kunden (Name, Adresse, Personalausweis-Nummer) sowie den entliehenen Filmen auch darüber hinausgehende Angaben zu den in der Vergangenheit entliehenen Filmen speichere, um das Ausleihverhalten transparent zu gestalten.

Die Speicherung des Namens, der Anschrift des Kunden sowie der Film-Nummer wirft, soweit diese der Abwicklung des Verleihgeschäftes dient, keine Probleme auf.

Personenbezogene Daten sind jedoch zu sperren, wenn ihre Kenntnis für die Erfüllung des Zweckes der Speicherung nicht mehr erforderlich ist. Die Speicherung der Film-Nummer ist demnach nur bis zur Erledigung des nächsten Verleihgeschäftes (z.B. zur Kontrolle von Sachschäden, die der neue Ausleiher reklamiert) zulässig. Eine weitergehende Speicherung, die die Interessen des Ausleihers ohne sein Wissen offenbart, begegnet hingegen datenschutzrechtlichen Bedenken. Soweit jedoch die Speicherung der Film-Nummer vom Kunden gewünscht wird, um das doppelte Ausleihen von Filmen zu vermeiden, ist dies mit schriftlich zu erteilender Einwilligung des Betroffenen möglich.
Da das entsprechende Computerprogramm von einem Software-Anbieter als Standard-Programm für Videotheken vertrieben wurde, wies die Aufsichtsbehörde sowohl den Software-Anbieter als auch die entsprechende Videothek auf diese Rechtslage sowie darauf hin, daß nach § 4 Abs. 2 des Gesetzes über Personalausweise eine Verwendung der Personalausweisnummer insoweit unzulässig ist, als mit ihrer Hilfe ein Abruf personenbezogener Daten aus Dateien der eine Dateienverknüpfung möglich ist. Der Software-Anbieter hat sein Programm daraufhin entsprechend geändert.

1.2.6 Verarbeitung von **Mitgliederdaten** durch Vereine

Im Berichtszeitraum wandte sich ein Sportverein mit der Bitte um Beratung an eine Aufsichtsbehörde wegen der Frage, ob die Übermittlung von Mitgliederdaten an eine Sparkasse zur Inanspruchnahme eines "Sparkassen-Vereins-Service" datenschutzrechtlich zulässig sei. Mit diesem Vereinsservice bot eine Sparkasse den Vereinen in ihrem Einzugsbereich eine Dienstleistung an,

mit der den Vereinen eine Hilfe zur rationellen und wirtschaftlichen Finanzverwaltung, insbesondere durch den Einzug von Mitgliederbeiträgen, geleistet werden sollte. Die Frage wurde wie folgt beurteilt:
Die Weitergabe der personenbezogenen Daten der Mitglieder des Sportvereins an den "Sparkassen-Vereins-Service" stellt eine Übermittlung i.S.d. § 2 Abs. 2 Nr. 2 BDSG dar, weil sie für eine Geschäftsbesorgung bestimmt ist.

Liegt die Einwilligung des Betroffenen in die Verarbeitung seiner personenbezogenen Daten nicht vor, so ist deren Übermittlung zulässig "im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen oder soweit es zur Wahrung berechtigter Interessen der übermittelnden Stelle oder eines Dritten oder der Allgemeinheit erforderlich ist und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden".

Die Mitgliedschaft in einem Verein wird als vertragsähnliches Vertrauensverhältnis anzusehen sein, das die Übermittlung rechtfertigen kann, soweit sich dies aus der Vereinssatzung ergibt. Ansonsten beurteilt sich die Zulässigkeit der Übermittlung danach, ob ein berechtigtes Interesses vorliegt. Danach muß bei der Übermittlung abgewogen werden zwischen dem berechtigten Interesse der übermittelnden Stelle, eines Dritten oder der Allgemeinheit und den schutzwürdigen Belangen des Betroffenen.
Da eine Einzelfallabwägung regelmäßig nicht stattfindet, kann auch eine Beeinträchtigung schutzwürdiger Belange im Einzelfall nicht ausgeschlossen werden. Soweit jedoch vertraglich sichergestellt ist, daß die Sparkasse die Mitgliederdaten ausschließlich nach Wei-

sung des Sportvereins verarbeitet, erscheint es ausreichend, wenn der Verein einen entsprechenden Beschluß über die beabsichtigte Weitergabe herbeiführt mit Festlegungen darüber, welche personenbezogenen Daten an die Sparkasse zu welchen Zwecken übermittelt werden.

Ein solcher Beschluß müßte den Vereinsmitgliedern bekanntgegeben werden mit dem Hinweis, daß die Daten weitergegeben werden, sofern kein Widerspruch erfolgt. Damit wird den Vereinsmitgliedern die Möglichkeit gegeben, der Weitergabe zu widersprechen. Daten von Mitgliedern, die einer Weitergabe widersprechen, dürfen nicht an die Sparkasse weitergegeben werden. Neu-Mitglieder sollten bei Unterzeichnung der Aufnahmeerklärung auf diesen Beschluß sowie auf die Möglichkeit des Widerspruchs hingewiesen werden.

Die Aufsichtsbehörde unterrichtete den Sportverein in diesem Sinne. -

Im 1. Tätigkeitsbericht (vgl. Ziff. 7.10 S. 79) wurde angesprochen, ob bei **Gruppenversicherungsverträgen**, die als Rahmenverträge zwischen Vereinen und Versicherungsunternehmen den Vereinsmitgliedern den Abschluß von Einzelversicherungsverträgen zu günstigeren als den üblichen Konditionen ermöglichen, der Verein Daten der Vereinsmitglieder an die Versicherung weitergeben darf, damit diese die Vereinsmitglieder zwecks Abschlusses von Einzelversicherungen umwerben kann. In diesen Fällen bedarf es einer schriftlichen Einwilligung bzw. der Einräumung einer Widerspruchsmöglichkeit.

Im Rahmen der Erörterungen des "Düsseldorfer Kreises" ist in diesem Zusammenhang von einer Aufsichtsbehörde eine auf den ersten Blick vielleicht weniger Fragen des Datenschutzes berührende Sachverhaltsvariante angesprochen worden:

Anläßlich des Abschlusses des Versicherungsvertrages wurde - wie die Aufsichtsbehörde feststellte - Vereinsmitgliedern auch eine Zuwendungserklärung zu Gunsten des Vereins vorgelegt, mit der ein Anspruch des Vereinsmitgliedes auf Rückerstattung von Prämienanteilen (aus der Überschußbeteiligung) an den Verein - freiwillig - abgetreten werden konnte.

Es stellte sich die auch datenschutzrechtliche Frage, ob die Einwilligung zur Datenübermittlung auch diesen **weiteren**, die Vereinsmitglieder möglicherweise zudem überraschenden Zweck umfaßt.

Trotz unterschiedlicher Auffassungen insbesondere zur Frage, ob Belange des Datenschutzes berührt sind, konnte die betreffende Aufsichtsbehörde mit einem Versicherungsunternehmen eine Einigung dahin erzielen, daß die Vereinsmitglieder **zuvor schriftlich** auf die Möglichkeit einer Zuwendung und darauf **hingewiesen** werden, daß der Abschluß des Versicherungsvertrages nicht von der Abgabe der Zuwendungserklärung abhängt.

1.2.7 **Versichertendaten**

Wie im 1. Tätigkeitsbericht ausgeführt (vgl. Ziff. 9.2.4, S. 96), konnten Schweigepflichtentbindungsklauseln in den Bereichen Kranken-, Unfall- und Lebensversicherung abschließend mit der Versicherungswirtschaft vereinbart werden.

Im Berichtszeitraum fanden Verhandlungen der obersten Aufsichtsbehörden mit der Versicherungswirtschaft über andere Versicherungssparten betreffende Schweigepflichtentbindungsklauseln statt (Haftpflicht-, Reiserücktrittskosten-, Berufsunfähigkeits- und Pflegerentenversicherung). Auch bei diesen Klauseln soll die Entbindung von der Schweigepflicht auf das unumgänglich Notwendige beschränkt werden. Die Verhandlungen sind noch nicht in bezug auf alle Versicherungssparten abgeschlossen.

1.3 **Datensicherung und organisatorische Schutzvorschriften** (Einzelfragen)

Bei den oben unter Ziff. 1.1.4 umschriebenen Mängeln gilt es weiterhin, auf Verbesserungen hinzuwirken. Die Erfahrungen der Aufsichtsbehörden zeigen, daß auch im Berichtszeitraum im privaten Bereich im wesentlichen gleichartige Probleme auftraten wie im öffentlichen Bereich (vgl. hierzu 1. Tätigkeitsbericht: Ziff. 8.1 S. 85). Zur Vermeidung von Wiederholungen wird daher insoweit auch auf die Berichte des Landesbeauftragten für den Datenschutz Nordrhein-Westfalen verwiesen.

Beispielhaft seien für den nicht-öffentlichen Bereich im folgenden einige Punkte herausgegriffen:

1.3.1 Die Aufsichtsbehörden wurden immer wieder von betrieblichen Datenschutzbeauftragten auf die Problematik des Datenschutzes und der Datensicherung beim Einsatz von Personal-Computern (PC) angesprochen.

Der zunehmende Einsatz von PCs, insbesondere bei der elektronischen Verarbeitung von individuell verwalteten Dateien, macht besondere Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit erforderlich.

Aus folgenden Gründen ist eine besondere Gefährdung des Datenschutzes durch die PCs anzunehmen:

- Die meist hohen Speicherkapazitäten kompakter und preiswerter PCs sowie der kleinen Datenträger (Disketten)
- die Möglichkeit des Anschlusses an Datenbanken und Rechenzentren bzw. der lokalen Vernetzung ohne ausreichende Kontrollierbarkeit des Datenflusses
- die Möglichkeit für geübte Anwender, Anwendungsprogramme und Dateien ohne ausreichende Dokumentation zu erstellen oder zu kopieren
- die meist nicht mögliche Protokollierung und damit fehlende Nachprüfbarkeit der durchgeführten Aktivitäten.

Es sei darauf hingewiesen, daß die gebotene Protokollierung im PC-Bereich seitens der Betriebssoftware kaum unterstützt wird und die Speicherkapazitäten hierzu bis vor einiger Zeit nicht ausreichten. Es bleibt abzuwarten, ob künftig die Betriebssoftware eine ausreichende Protokollierung zuläßt. Hier ergibt sich eine Forderung an die Hersteller.

Für den Datenschutzbeauftragten im Großbetrieb ist es schwieriger geworden festzustellen, wo überall im Betrieb welche Systeme zu welchem Zweck eingesetzt werden. Es sollte sichergestellt werden, daß hier eine umfassende Unterrichtung des betrieblichen Datenschutzbeauftragten stattfindet.

Anders als bei der Datenverarbeitung mit Großrechnern und mit Systemen mittlerer Größe ist der Benutzer eines Personal-Computers oft gleichermaßen Bediener, Programmierer, Dateiverwalter und Sachbearbeiter in einer Person, woraus sich besondere Probleme für die gebotene Funktionstrennung ergeben. -

1.3.2 Nicht nur im PC-Bereich erfordern eine ordnungsgemäße Datenverarbeitung sowie ein datenschutzrechtlich verantwortlicher Umgang mit personenbezogenen Daten eine übersichtlich beschriebene Arbeitsplatzorganisation, die zu einer **Trennung** verschiedener **Funktionen** innerhalb des Unternehmens führt. Bei den Routinekontrollen durch die Aufsichtsbehörde hat sich gezeigt, daß in Klein- und Mittelbetrieben vielfach ohne genaue Arbeitsplatzbeschreibung gearbeitet wird. Einer genauen Arbeitsteilung/Funktionstrennung bereiten oft die vorgegebene Personalausstattung oder räumliche Gegebenheiten Schwierigkeiten. Hier waren Empfehlungen der Aufsichtsbehörden gefragt, die von den geprüften Unternehmen in entsprechende Maßnahmen umgesetzt werden konnten.

1.3.3 Die Frage der Datensicherheit stellt sich insbesondere im Fall der Benutzung von Wählleitungen (der Sicherheitsstandard von Standleitungsverbindungen ist höher zu bewerten, da Manipulationen ein "Anzapfen" mit erheblichem technischen Aufwand erfordern). In vielen Fällen wurde bemängelt, daß der Verbindungsaufbau nicht durch das zentrale DV-System, z. B. durch Rückruf, erfolgte. Wenn ein Rückrufsystem nicht besteht, so sollten die gültigen Paßworte nur befristet genutzt werden. Außerdem wurde gefordert, die Anzahl von möglichen Fehlversuchen zu begrenzen.
Bei ihren Überprüfungen empfahlen die Aufsichtsbehörden, beim Verbindungsaufbau darauf zu achten, daß Fehlzugriffsversuche besonders aufgezeichnet und deren Ursachen nachgegangen wird. Nur bei besonderer Aufzeichnung lassen sich Fehlzugriffsversuche umgehend feststellen, um die Funktionsfähigkeit von Sicherungsmaßnahmen überprüfen zu können. -

Die **Verschlüsselung** zur Datensicherung ist bei der Verarbeitung personenbezogener Daten noch nicht sehr verbreitet. Als wirksamer Schutz intern gespeicherter Daten, zur gesicherten Datenübertragung von einem Datenverarbeitungssystem oder Speichermedium zu einem anderen, insbesondere bei Nutzung von Wählverbindungen, gewinnen Chiffriertechniken künftig zunehmend an Bedeutung.
Software-Lösungen für Großrechner und auch für PC-Anwendungen sind mittlerweile vorhanden. Im Rahmen der Aufsicht wurde festgestellt, daß solche Verschlüsselungssoftware schon häufig bei Großunternehmen anzutreffen ist. -

1.3.4 **Betriebliche Datenschutzbeauftragte** begegneten in der täglichen Praxis in einigen Fällen Schwierigkeiten, weil sie am **Informationsfluß** innerhalb des Unternehmens nicht ausreichend beteiligt wurden. Das neue BDSG bestimmt nunmehr, daß der betriebliche Datenschutzbeauftragte über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten ist.

Fragen gab es wiederholt zur "beratenden Mitwirkung" des betrieblichen Datenschutzbeauftragten bei der Auswahl der in der Verarbeitung personenbezogener Daten tätigen Personen. Hier vertraten Unternehmen oftmals den Standpunkt, daß es ausreichend sei, wenn schon die Personalabteilung bei Einstellungen und Versetzungen kritisch die Belange des Datenschutzes in ihre Überlegungen einbeziehe, ohne daß es der besonderen Mitwirkung des betrieblichen Datenschutzbeauftragten bedürfe.

Wie immer die Verfahren unternehmensintern auch aussehen mögen, bleibt festzuhalten, daß nach dem Gesetz der betriebliche Datenschutzbeauftragte **verpflichtet** ist, bei der Auswahl der bei der Verarbeitung personenbezogener Daten tätigen Personen beratend mitzuwirken. Auch im Hinblick auf die durch die Novelle des BDSG beabsichtigte Stärkung der Stellung des betrieblichen Datenschutzbeauftragten würden solche Verfahren Bedenken begegnen, die dessen Mitwirkungspflicht in Frage stellen könnten.

Die **Schulung der Mitarbeiter** durch den betrieblichen Datenschutzbeauftragten wurde nicht immer, vor allem in Klein- und Mittelbetrieben, ausreichend durchgeführt. Oft beschränkte man sich dabei auf eine einmalige Belehrung im Zusammenhang mit der Verpflichtung auf das Datengeheimnis. Anders stellt sich die Sachlage in den meisten Großunternehmen dar. Dort sind von den betrieblichen Datenschutzbeauftragten oder in deren Auftrag Schulungsunterlagen erstellt worden. Seminarveranstaltungen, Arbeitskreise oder spezielle Informationsdienste gewährleisten eine ordnungsgemäße Schulung. Dabei wird im Unternehmen auch der Nachschulungsbedarf überwacht. -

Insgesamt bestätigte sich auch im Berichtszeitraum, daß Mängel mit zunehmender Betriebsgröße abnehmen. Die Aufsichtsbehörden werden daher auch in Zukunft kleineren und mittleren (sowie selbstverständlich auch den großen) Unternehmen beratend zur Seite stehen.

2. **Das neue Bundesdatenschutzgesetzes** (BDSG)

Das mit Gesetz vom 20. Dezember 1990 (BGBl. I S. 2954) novellierte Bundesdatenschutzgesetz ist - mit Ausnahme einer Vorschrift zum automatisierten Abrufverfahren - am 1. Juni 1991 in Kraft getreten.

2.1 Vereinzelt ist die Meinung vertreten worden, die Novelle des BDSG habe zum Ziel, die Datenverarbeitung z.B. der Vereine und Verbände vom **Anwendungsbereich** auszunehmen.

Begründet wird dies damit, daß der im Gesetz nach wie vor enthaltene Begriff der "geschäftsmäßigen" Datenverarbeitung, der bislang die auf Dauer oder auf Wiederholung angelegte Datenverarbeitung betraf, nunmehr i.S.v. "geschäftlich", d.h. auf Erwerbszwecke ausgerichtet, zu verstehen sei. Diese Betrachtungsweise verkennt - wie auch die oben geschilderten Fälle zur Datenverarbeitung der Vereine zeigen mögen (s.o. Ziff. 1.2.6) - die Auswirkungen, die sich für das Recht auf informationelle Selbstbestimmung von Vereinsmitgliedern auch aus der Verarbeitung von Daten durch einen Verein ergeben können.

Nach einhelliger Meinung der im "Düsseldorfer Kreis" vertretenen Aufsichtsbehörden der Länder kommt dem Begriff "geschäftsmäßig" derselbe Sinngehalt zu wie dem in der alten Gesetzesfassung wortgleich enthaltenen Begriff. Der Gesetzgeber hat den Begriff "geschäftsmäßig" unverändert in die Novelle übernommen. Vereine und Verbände werden daher auch weiterhin der Aufsicht nach dem BDSG unterliegen. -

2.2 Das novellierte BDSG führt zu einer **Erweiterung der Befugnisse** der Aufsichtsbehörden:

- In den Bereichen, in denen die behördliche Überprüfung bislang die Beschwerde eines Betroffenen voraussetzte, kann nunmehr auch ohne Vorliegen einer solchen Beschwerde lediglich aufgrund **hinreichender Anhaltspunkte** für eine Verletzung von Datenschutzbestimmungen eine Überprüfung vorgenommen werden. Die Behörde kann demnach auch aus eigener Initiative, wenn sich hier Anhaltspunkte für die Verletzung datenschutzrechtlicher Bestimmungen ergeben, tätig werden (sog. **"erweiterte Anlaßaufsicht"**).

  Es sollte hier allerdings nicht unerwähnt bleiben, daß die Aufsichtsbehörden schon in der Vergangenheit Hinweisen häufig dann nachgegangen sind, wenn Eingaben von Nichtbetroffenen vorlagen. Die Unternehmen waren vielfach - dies ist erfreulich - auch in diesen Fällen bereit, den Behörden Auskunft über ihre Datenverarbeitung zu geben und Anregungen zur Verbesserung des Datenschutzes aufzugreifen.

  Eine Überprüfung durch die Aufsichtsbehörden sieht das Gesetz jedoch nur vor, soweit personenbezogene Daten in oder aus **Dateien** verarbeitet bzw. genutzt werden. Daten in Akten unterfallen dem Anwendungsbereich des Gesetzes nur, soweit diese **offensichtlich** aus einer Datei entnommen sind. Mit dieser grundsätzlichen Beschränkung des Datenschutzes auf Dateien, die nur begrenzt Akten einbezieht, bleibt die Novelle hinter den Erwartungen zurück.
  Der Bürger zeigt wenig Verständis, wenn eine ihn betreffende Datenverarbeitung je nachdem, ob sie in einer Datei oder einer Akte ihren Niederschlag findet,

einer behördlichen Überprüfung unterzogen bzw. nicht unterzogen werden kann, obwohl die Betroffenheit des Rechts auf informationelle Selbstbestimmung sowohl in dem einen als auch in dem anderen Fall gleichermaßen denkbar ist.

Dessenungeachtet, die Aufsichtsbehörde kann, sofern sie Bedenken gegen eine nicht-dateimäßige Verarbeitung hegt, im Wege der Empfehlung oder Beratung auf das Unternehmen zugehen. Dies setzt allerdings voraus, daß das Unternehmen freiwillig auch in den nicht der Kontrolle der Aufsichtsbehörden unterliegenden Bereichen Auskunft gibt.

Die Aufsichtsbehörden waren in der Vergangenheit mit Erfolg darum bemüht, in den Unternehmen Verständnis dafür zu wecken, daß nicht durch eine gleichsam künstliche Segmentbildung der Datenschutz von vornherein restriktiv gehandhabt wird. Von diesem Verständnis geht in der Grundtendenz offenbar auch das neue BDSG aus, wenn es künstliche Trennlinien zwischen Akten und Dateien zu vermeiden sucht, indem es die Anwendung des BDSG auf Akten auch dann vorsieht, wenn die Daten offensichtlich aus einer Datei stammen (s.o.).

Bei Beschwerden dürften die Unternehmen auch mit Ansehensverlusten zu rechnen haben, wenn sie in bedenklichen Fällen unter Hinweis auf die eingeschränkte Geltung des BDSG eine Überprüfung verweigern würden, nur weil eine nicht-dateimäßige Verarbeitung vorliegt.

- Erstmalig werden den Aufsichtsbehörden **Eingriffsbefugnisse** eingeräumt, die allerdings auf den Bereich der Datensicherheit und auf die Gewährleistung einer ordnungsgemäßen betrieblichen Selbstkontrolle beschränkt bleiben. So kann die Aufsichtsbehörde im Bereich der Datensicherheit die Beseitigung technischer oder organisatorischer Mängel **anordnen**. Bei schwerwiegenden Mängeln kann sie den Einsatz einzelner Verfahren **untersagen**, wenn der Beseitigungsanordnung nicht Folge geleistet wird. Schließlich kann die **Abberufung** des betrieblichen Beauftragten für den Datenschutz **verlangt** werden, wenn er die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit nicht besitzt.

  Die Praxis wird zeigen, inwieweit die Aufsichtsbehörden von diesen neuen Befugnissen Gebrauch machen, die in ganz erheblicher Weise in den Betriebsablauf eines Unternehmens einzugreifen vermögen.

  Soweit angenommen werden kann, daß die Unternehmen auch in Zukunft bereit sind, Beanstandungen und Empfehlungen der Aufsichtsbehörden zu entsprechen, dürfte sich die praktische Anwendung der neuen Eingriffsbefugnisse in Grenzen halten. Mit einer Anwendung müssen die Unternehmen rechnen, die trotz Beanstandung nicht zu einer Behebung der gerügten Mängel bereit sind.

  Die Unternehmen sollten alle Möglichkeiten zur Verbesserung z.B. der Datensicherheit ausschöpfen. In diesem Bereich bedarf es nach wie vor weiterer Anstrengungen (vgl. oben Ziff. 1.1.4 sowie Ziff. 1.3).

Ebenso liegt es im Interesse der Unternehmen, wenn sie ausschließlich geeigneten Personen die verantwortungsvolle Aufgabe des betrieblichen Datenschutzbeauftragten übertragen.

Es muß betont werden, daß das Gesetz auch weiterhin an der besonderen Bedeutung dieser im Unternehmen angesiedelten **Selbstkontrolle** festhält.

Hier hat der betriebliche Datenschutzbeauftragte einen wichtigen Beitrag zum Datenschutz zu leisten. Schon im Unternehmen sollen die Probleme des Datenschutzes und der Datensicherheit erkannt und gelöst werden. In dem Maße, in dem es gelingt, von vornherein geeignete Datenverarbeitungsverfahren zu installieren oder erkannte Probleme mit dem Datenschutz selbst abzustellen, nimmt die Notwendigkeit für behördliche Aufsichtsmaßnahmen ab. In Bereichen, in denen die Umsetzung gebotener Datenschutzstandards unmittelbar Auswirkungen auf das unternehmerische Handeln entfaltet, sind selbstkonzipierte und insoweit auch akzeptierte Regelungen, sofern sie geeignet sind, Vorgaben aufgrund einer externen Kontrolle vorzuziehen.

Die Stellung des Beauftragten für den Datenschutz innerhalb des Unternehmens ist mit der Novelle gestärkt worden. Vielleicht geht das Gesetz davon aus - dies wäre aus Sicht der Aufsichtsbehörden zu begrüßen -, daß der Ausbau seiner Stellung nicht nur zur Bewältigung der gestiegenen Anforderungen beitragen soll, sondern auch zur Optimierung der Selbstkontrolle insgesamt zu führen vermag. Hier sind den Aufsichtsbehörden auch alle weitergehenden Anstrengungen der Wirtschaft recht, die auf eine Optimierung der Selbstkontrolle abzielen.

Das Gesetz sieht, auch dies kann aus der Sicht der Aufsichtsbehörden nur gutgeheißen werden, weiterhin die Möglichkeit für den betrieblichen Datenschutzbeauftragten vor, sich in Zweifelsfällen an die Aufsichtsbehörde wenden zu können.

Diese Möglichkeit des eher präventiven **Zusammenwirkens von Betrieb und Behörde** hat schon im Berichtszeitraum eine Ausweitung erfahren (vgl. oben Ziff. 1.1.3); sie sollte weiterhin verstärkt genutzt werden.

Gemeinsam durch Zusammenwirken von Verwaltung und Wirtschaft Lösungen zu erarbeiten, war auch im Berichtszeitraum eine der besonderen Aufgaben des "Düsseldorfer Kreises". In Verhandlungen mit den Spitzenverbänden der Wirtschaft, die einer freiwilligen Selbstbindung der den Dachverbänden angeschlossenen Unternehmen im Sinne einer möglichst datenschutzfreundlichen Handhabung des Gesetzes dienen, konnten weitere Fortschritte erzielt werden (vgl. hierzu z.B. Ziff. 4.).

Vor diesem Hintergrund mag die Praxis damit zurechtkommen, daß der Gesetzgeber sich nicht entschließen konnte, den Aufsichtsbehörden weitere, im materiellrechtlichen Bereich liegende Eingriffsbefugnisse an die Hand zu geben. Die Aufsichtsbehörden können auch in Zukunft nicht bei Verstößen gegen das materielle Datenschutzrecht die Erhebung, Verarbeitung und Nutzung personenbezogener Daten untersagen und die Löschung gespeicherter Daten anordnen. Insoweit bleibt es dabei, daß die Aufsichtsbehörden die datenverarbeitenden Stellen von der Notwendigkeit bestimmter Maßnahmen **überzeugen** müssen, ohne daß sie in der Lage wären, ihre Vorstellungen einseitig in hoheitlicher Form durchzusetzen.

Bei Datenschutz**verstößen** wird es daher auch in Zukunft Sache des Betroffenen bleiben, sich aus **eigener Initiative** ggf. mit gerichtlicher Hilfe gegen eine unzulässige Datenverarbeitung bzw. -nutzung zu wehren.

2.3 Weitere Änderungen bringt die Novelle u.a. in folgenden Punkten:

- Die Daten**erhebung** ist nunmehr ausdrücklich geregelt; Daten dürfen - wie bereits in der Datenschutzkonvention des Europarates vom 28.01.1981 vorgesehen - nur nach Treu und Glauben und auf rechtmäßige Weise erhoben werden. Auch die eigentliche Datenverarbeitung verlangt rechtmäßig erhobene Daten.

- Auch eine **Nutzung** personenbezogener Daten ("jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt") kann nur nach Vorliegen der gesetzlichen Voraussetzungen durchgeführt werden.

- Ausdrücklich wird festgeschrieben, daß die **Rechte** der Betroffenen auf Auskunft, Berichtigung, Löschung oder Sperrung **nicht** durch Rechtsgeschäft ausgeschlossen oder beschränkt werden können.

- Für einen Schadensersatzanspruch ist eine **Umkehr der Beweislast** eingeführt worden.

- Das Gesetz sieht eine **Vermutung** vor, daß bei Daten, die sich z.B. auf gesundheitliche Verhältnisse, strafbare Handlungen, Ordnungswidrigkeiten, religiöse oder politische Anschauungen sowie auf arbeitsrechtliche Rechtsverhältnisse beziehen, ein einer listenmäßigen Übermittlung entgegenstehendes Interesse des Betroffenen besteht.
  Zu Lasten des Bürgers kann aus der Regelung nicht etwa im Wege eines Umkehrschlusses gefolgert werden, daß bei anderen als den vorgenannten Daten ein Interesse an dem Ausschluß einer Übermittlung nicht bestehe. Unschwer lassen sich andere, sehr sensible personenbezogene Daten vorstellen, gegen deren Übermittlung der Betroffene sehr wohl ein schutzwürdiges Interesse besitzt.

- **Widerspricht** der Betroffene der **Nutzung** oder **Übermittlung** seiner Daten für **Zwecke der Werbung oder der Markt- oder Meinungsforschung**, ist eine Nutzung oder Übermittlung für diese Zwecke unzulässig bzw. sind für diese Zwecke die Daten zu sperren."

Insgesamt enthält die Novelle - weitgehende Veränderungen der materiellen Datenschutzregelungen sind ausgeblieben - weitere Schritte zur Sicherung des Persönlichkeitsrechts. Nach wie vor erscheinen aber zusätzliche, detaillierte Regelungen in sensiblen Bereichen (z.B. zum Arbeitnehmerdatenschutz) unverzichtbar.

Auch die ständig wachsenden Möglichkeiten zur Zusammenfassung und Auswertung einer Fülle von Daten über einzelne Personen "in einer Hand" (z.B. im Bereich des automatisierten Zahlungsverkehrs oder auch im Bereich der Direktwerbung) werfen - nicht zuletzt mit Blick auf die Rechtssicherheit - die Frage auf, inwieweit die novellierten Vorschriften neuen Entwicklungen Rechnung tragen können (vgl. auch 1. Tätigkeitsbericht Ziff. 2.2.3 und 2.2.4, S. 10 und 11).

Die Auswirkungen der Novelle auf die Praxis bedürfen daher einer aufmerksamen Beobachtung. Die Zukunft wird zeigen, welchen Beitrag die Novelle zur Verbesserung des Datenschutzes in der Praxis zu leisten vermag.

Der "Düsseldorfer Kreis" wird über die Novellierung betreffende Grundsatzfragen beraten, um eine Abstimmung der Länder untereinander herbeizuführen.

Schon jetzt ist abzusehen, daß die Praxis mit Aufmerksamkeit den weiteren Arbeitsergebnissen des "Düsseldorfer Kreises" entgegensieht.

Es zeigt sich im übrigen recht deutlich am Beispiel der Novelle, daß von der gemeinsamen Arbeit der obersten für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörden der Länder entscheidende Impulse für den Vollzug des BDSG ausgehen.

3. Vorschlag der EG-Kommission für eine "Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten"

Die Absicht der EG-Kommission, eine Richtlinie vorzubereiten, die sich zum Ziel setzt, ein hohes Datenschutzniveau in der gesamten Europäischen Gemeinschaft sicherzustellen, ist, nachdem in der Vergangenheit immer wieder eine Initiative der EG gefordert wurde, zu begrüßen und verdient Unterstützung.

Die Kommission bekennt sich ausdrücklich zum Grundrechtscharakter des Schutzes personenbezogener Daten, den es europaweit zu sichern gilt.

Ein Handlungsbedarf wird gesehen, weil die unterschiedliche Ausgestaltung des Datenschutzes in den Mitgliedstaaten den freien Verkehr von Waren, Dienstleistungen und Kapital in der Gemeinschaft behindern kann. Die Kommission geht - auch hierin ist ihr zu folgen - davon aus, daß die mit der Richtlinie verbundene Rechtsangleichung in der EG nicht zu einer Verringerung des Schutzniveaus führen darf, das in den Mitgliedstaaten bereits gewährleistet wird.

Mit den sich bei unterschiedlichen Datenschutzstandards ergebenden Problemen des grenzüberschreitenden Datenverkehrs war der "Düsseldorfer Kreis" verstärkt im Berichtszeitraum befaßt. Da die Novelle des BDSG keine Regelung über den grenzüberschreitenden Datenverkehr enthält, ist es grundsätzlich zu begrüßen, daß auf der Ebene der Europäischen Gemeinschaft Regelungen des Transfers von Daten sowohl innerhalb der EG als auch in Drittländer vorgesehen sind (hierzu nachfolgend Ziff. 4).

Der Richtlinienvorschlag geht in Teilen über die Datenschutzkonvention des Europarates hinaus und übernimmt bewährte Regelungen und Instrumente des deutschen Datenschutzrechts (vgl. auch Beschluß der Datenschutzbeauftragten des Bundes und der Länder vom 29.01.1991, als Anlage 3 abgedruckt im 10. Tätigkeitsbericht des LfD).

Es ergeben sich, wie der Bundesrat in seiner Stellungnahme vom 14.12.1990 beschlossen hat (Drucksache 690/90), jedoch noch einige Verbesserungswünsche, die u. a. eine Angleichung an die Konzeption des Bundesdatenschutzgesetzes zum Ziel haben. Die Bundesregierung ist auch aufgefordert sicherzustellen, daß wegen der Regelungen der Richtlinie die in der Bundesrepublik Deutschland bestehende Organisation der Datenschutzkontrolle nicht in Frage gestellt wird. Die Bundesregierung soll ferner dafür Sorge tragen, daß in den von der Richtlinie vorgesehenen EG-Gremien die Hälfte der Sitze, die der Bundesrepublik Deutschland zustehen, mit gemeinsamen Vertretern der Länder besetzt werden kann. Da die Länder von der Arbeit der vorgesehenen Gremien in erheblichem Ausmaß betroffen sein werden, ist es wichtig, daß sie ihre Erfahrungen unmittelbar in die Beratungen einbringen können.

Zu welchem Ergebnis die weiteren Beratungen der Richtlinie innerhalb der EG-Organe führen, ist noch nicht abzusehen. Deren endgültige Ausgestaltung im einzelnen muß z.Zt. als noch offen bezeichnet werden.

4. Grenzüberschreitender Datenverkehr und "Vertragsmodell"

Im ersten Tätigkeitsbericht (Vgl. Ziff. 10, S. 102 u. S. 103) wurde die Empfehlung an die Wirtschaft ausgesprochen, in Zusammenarbeit mit den Aufsichtsbehörden für den grenzüberschreitenden Datenverkehr Lösungskonzepte zu entwickeln, um bei einem Datenexport in Länder mit schwächerem oder gar fehlendem Datenschutz der Gefährdung schutzwürdiger Belange der von der Verarbeitung ihrer Daten betroffenen Personen entgegenzuwirken.

Im Berichtszeitraum haben die **SCHUFA** sowie mit ihr der **Zentrale Kreditausschuß** in enger und konstruktiver Zusammenarbeit mit dem "Düsseldorfer Kreis" ein Auslandskonzept erarbeitet, wonach die SCHUFA ihre Vertragspartner im Ausland unabhängig davon, ob in dem jeweiligen Empfängerland ein Datenschutzgesetz und mit welchem Standard besteht, bezüglich der von der SCHUFA übermittelten Daten u.a. darauf verpflichtet, die in der **Datenschutzkonvention des Europarates** enthaltenen Grundsätze einzuhalten.

Insbesondere sehen die vertraglichen Verpflichtungen vor, daß die im Ausland ansässigen Vertragspartner Daten nur **ausschließlich** zu dem bei der Anfrage angegebenen **Zweck** nutzen dürfen; sie sind **gegen** eine **Weitergabe** an Dritte sowie eine **unbefugte Nutzung abzusichern**. Der im Ausland ansässige Vertragspartner muß **Auskunfts-, Berichtigungs- und Löschungsverlangen** entsprechen. Auf Anfrage hat der Vertragspartner der SCHUFA - ggf. bei einem Informationsbesuch der SCHUFA - die **Einhaltung der Vertragspflichten nachzuweisen** sowie erkannte **Mängel zu beseitigen**.

Schließlich ist bei Verstoß gegen die im Interesse der Betroffenen übernommenen Vertragspflichten (s.o.) **Schadensersatz** den Betroffenen gegenüber vorgesehen.

Um die Einhaltung der Vertragspflichten regelmäßig zu **überwachen**, muß der Vertragspartner der SCHUFA im Ausland einen SCHUFA-Beauftragten bestellen, der in regelmäßiger Verbindung mit der SCHUFA steht.

Dieses Vertragskonzept enthält Elemente eines Vertrages zu Gunsten Dritter, nämlich zu Gunsten des Betroffenen, wobei darüber hinausgehend der in der beim Kreditantrag vom Kreditinstitut vorzulegenden und vom Kunden zu unterzeichnenden "SCHUFA-Klausel" enthaltene Hinweis auf Auskunfts-, Berichtigungs- und Löschungsansprüche darauf hindeutet, daß es sich insoweit um unmittelbar dem Rechtsverhältnis Kunde/Kreditinstitut entspringende Ansprüche handeln soll.

Der Betroffene wird in einem auf Wunsch zur Verfügung zu stellenden Merkblatt über die Verpflichtung des im Ausland ansässigen Vertragspartners auf die o.a. Grundsätze unterrichtet.

Mit diesem Modell ist ein wichtiger Schritt zur Sicherung des Rechts auf informationelle Selbstbestimmung beim Datenexport ins Ausland unternommen worden.

Erfahrungen in der Praxis müssen noch abgewartet werden.

Solange und soweit verbindliche Regelungen für den Datenexport innerhalb der EG und in Drittländer noch nicht vorhanden sind, können "Vertragsmodelle" einen Beitrag zur Verbesserung des Datenschutzes leisten. Sie vermögen allerdings nicht, da sie letztlich nur in Teilbereichen zu Verbesserungen führen, inhaltlich umfassende, entweder für alle oder bereichsspezifisch für einzelne Wirtschaftszweige geltende Datenschutzregelungen der EG zu ersetzen oder den dahingehenden Handlungsbedarf in Frage zu stellen.

Einen großen Schritt zur Lösung der mit dem grenzüberschreitenden Datenverkehr verbundenen Probleme sieht der Richtlinienvorschlag vor (vgl. o. Ziff. 3), indem er für den Datentransfer innerhalb der EG einen auf seiner Grundlage in den Mitgliedstaaten verwirklichten Datenschutzstandard voraussetzt und für den Datentransfer in Drittländer ein "angemessenes" Schutzniveau verlangt. Von der Ausgestaltung der Richtlinie im einzelnen wird es abhängen, welche Bedeutung "Vertragsmodellen" in Zukunft zukommen wird.

Bei dem hier zustandegekommenen Modell ist die Bereitschaft der Wirtschaft zu begrüßen, aus eigener Initiative weitere Schritte zur Sicherung des Rechts auf informationelle Selbstbestimmung zu unternehmen.

Dieser Bereitschaft zur Initiative und letztlich zur Selbstbindung kommt auch in Zukunft große Bedeutung zu.

Den Aufsichtsbehörden wäre daran gelegen, wenn dieser Schritt eine Signalwirkung auch für andere Wirtschaftszweige setzen könnte.

Der "Düsseldorfer Kreis" befindet sich bereits in weiteren Verhandlungen mit anderen Wirtschaftsverbänden.

LANDTAG NORDRHEIN-WESTFALEN
11. Wahlperiode

Drucksache 11/3175

05.02.1991

Unterrichtung

durch die Landesregierung

- zur Beratung -

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

Schreiben des Innenministers vom 01. Februar 1992:

Die Landesregierung hat in der Kabinettsitzung am 07. Januar 1992 den Zweiten Bericht über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörden beschlossen.

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

Der Bericht wurde als Anlage zu Drucksache 11/3175 nur an die Mitglieder des Landtags verteilt.

Datum des Originals: 01.02.1992/Ausgegeben: 06.02.1992