Innenministerium des Landes Nordrhein-Westfalen

Innenministerium NRW, 40190 Düsseldorf

An den
Präsidenten des Landtags
Nordrhein-Westfalen

40221 Düsseldorf

Haroldstraße 5,
40213 Düsseldorf

Telefon
(0211) 871 01
Durchwahl
(0211) 871 2599

Aktenzeichen
I A 5--1.2.11.2

3 .12.1999

Betr.: Stellungnahme der Landesregierung zum 14. Tätigkeitsbericht der Landesbeauftragten für den Datenschutz Nordrhein-Westfalen
6. Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörden

Die Landesregierung hat am 2. November 1999 die Stellungnahme zu dem 14. Tätigkeitsbericht der Landesbeauftragten für den Datenschutz Nordrhein-Westfalen sowie den 6. 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 die Stellungnahme sowie den Bericht vor (jeweils in 300-facher Ausfertigung).

(Dr. Fritz Behrens)

LANDTAG
NORDRHEIN-WESTFALEN
12. WAHLPERIODE

VORLAGE
12/ 3083
alle Drs.

E-mail: poststelle@im.nrw.de Telefax (0211) 871 3355
Straßenbahnlinien 704, 709 und 719 bis Haltestelle Poststraß

Stellungnahme der Landesregierung

zum

14. Tätigkeitsbericht der Landesbeauftragten für den Datenschutz

Nordrhein-Westfalen

(LfD)

„Datenschutzbericht 1999“

für die Zeit vom 1. Januar 1997 bis zum 31. Dezember 1998

A. Vorbemerkung

Der 14. Tätigkeitsbericht der Landesbeauftragten für den Datenschutz bezieht sich auf den Zeitraum 01. Januar 1997 bis 31. Dezember 1998. Neben der Darstellung von Einzelfällen, in denen nach Auffassung der Landesbeauftragten Datenschutzverstöße festgestellt wurden, sind besondere Schwerpunktthemen des Berichts u.a. Technik und Medien, die Tätigkeit der Sicherheitsbehörden sowie Datenschutzanforderungen im Gesundheitsbereich und bei der Tele-Heimarbeit.

Im Zusammenhang mit der Darstellung technischer und rechtlicher Aspekte der Medienentwicklung wird in dem Bericht auf die Gefahren hingewiesen, die sich aus dem immer größer werdenden Einfluss von Informations- und Telekommunikationstechnik ergeben. Insbesondere wird auf das Problem von Datenspuren und die daraus wachsende Gefahr des Missbrauchs und der Zusammenführung von Einzelinformationen zu komplexen Persönlichkeitsprofilen hingewiesen. Der Forderung im Bericht nach datenschutzfreundlichen Techniken und Verfahren, nach Erweiterung der anonymen Nutzung, Datenvermeidung und Datenreduzierung ist auch aus Sicht der Landesregierung zuzustimmen. Den Ausführungen der Landesbeauftragten zur Tätigkeit der Sicherheitsbehörden, die zum Teil auf bundesgesetzlicher Rechtsgrundlage erfolgt, kann nicht in allen Punkten gefolgt werden, zumal die im Rahmen von Kontrollbesuchen oder aufgrund von Beschwerden und Anfragen von Bürgerinnen und Bürgern festgestellten Probleme noch nicht abschließend aufgearbeitet sind und weiterer Diskussion bedürfen. Hinsichtlich der Nutzung von Gesundheitsnetzen, die die Kommunikation zwischen den Institutionen des Gesundheitswesens verbessern sollen, weist der Bericht auf die speziellen Risiken hin, die solche Netze im Hinblick auf einen möglichen Missbrauch persönlicher Gesundheitsinformationen beinhalten. Grundsätzlich wird die Auffassung geteilt, insoweit die Risikofaktoren durch individuelle Sicherheitskonzepte zu minimieren. Einen breiten Raum in dem Bericht nehmen die datenschutzrechtlichen Hinweise zur Tele-Heimarbeit ein. In Nordrhein-Westfalen laufen zwei Modellprojekte bei den Bezirksregierungen Düsseldorf und Münster, die von der Landesbeauftragten beratend begleitet werden.

Zur Beachtung des Datenschutzes in der Praxis führt der Bericht zahlreiche Einzelfälle auf, in denen nach Auffassung der Landesbeauftragten Datenschutzverstöße festgestellt wurden. Nicht in jedem dieser Fälle kann dem Bericht gefolgt werden; insgesamt jedoch stimmt die Landesregierung in vielen Positionen mit der Landesbeauftragten überein. Daher wird nicht zu allen im Tätigkeitsbericht angesprochenen Punkten Stellung genommen. Vielmehr beschränkt sich die Stellungnahme – von Ausnahmen abgesehen - auf die Punkte, in denen unterschiedliche Einschätzungen bestehen, sowie auf ergänzende Ausführungen zu bestimmten im Bericht aufgegriffenen Fragen.

Insgesamt ist festzustellen, dass in vielen Bereichen Übereinstimmung mit der Landesbeauftragten hinsichtlich Datenschutz und Datensicherheit besteht. Auch wurde in zahlreichen Fällen bereits im Vorfeld der Entwicklung neuer Techniken von ihrer Beratungstätigkeit Gebrauch gemacht. Die Landesregierung räumt dem Recht auf informationelle Selbstbestimmung einen hohen Stellenwert ein. Dies zeigt sich auch im Zusammenhang mit der anstehenden Novellierung des Datenschutzgesetzes Nordrhein-Westfalen. In diesem Zusammenhang ist beabsichtigt, nicht nur die zwingende Anpassung an die EG-Datenschutzrichtlinie vorzunehmen, sondern darüber hinaus das Datenschutzrecht in Nordrhein-Westfalen grundlegend zu reformieren.

B. Zum Tätigkeitsbericht im einzelnen

Übersicht

Bericht der LfD Abschnitt, Seite			Stellungnahme Seite
1.	S. 2	**Zur Situation im Datenschutz: Gestalten statt verwalten**	--
2.	S. 8	**Technische und rechtliche Aspekte der Medienentwicklung**	8
2.1	S. 8	Datenschutzfreundliche Technologien	9
2.2.1	S. 11	Kryptographie – Schlüsseltechnologie für Informationssicherheit und vertrauenswürdige Kommunikation – Einführung	10
2.2.2	S. 12	Verschlüsselungsverfahren	10
2.4.2.2	S. 30	Telekommunikation - Verstärkte Überwachungstendenzen auf Kosten des Datenschutzes	11
3.	S. 49	**Polizei und Verfassungsschutz**	12
3.1	S. 49	Sicherheit auf Kosten der Grundrechte?	12
3.2	S. 51	Der große Lauschangriff	13
3.3	S. 52	DNA-Analysedatei	14
3.5.1	S. 54	Wachsende Zahl von Telefonüberwachungen	16
3.5.3	S. 56	Unzureichende Benachrichtigungen von Abhörmaßnahmen	18
3.6	S. 57	Verfassungsschutz und polizeilicher Staatsschutz	18
3.6.1	S. 57	Bereich Verfassungsschutz	19
3.6.2	S. 59	Bereich Sicherheitsüberprüfung	23
3.6.3	S. 61	NADIS-Personenzentraldatei (PZD)	26
3.6.4	S. 61	Erfassung einfacher Mitglieder von Organisationen	27
3.6.5	S. 62	Staatsschutz, Verfassungsschutz und die Versammlungsfreiheit	30
3.7.1	S. 66	Schengener Informationssystem (SIS)	38
3.7.2	S. 71	Europol – Strafrechtliche Immunität der Europol-Angehörigen	38

3.8.2	S. 80	Identifizierung mit Hilfe von Fotos	39
4.	S. 83	**Die Bürgerinnen und Bürger und die Justiz**	40
4.5	S. 85	Formulare bei Familiengerichten	40
5.	S. 87	**Bürgerämter**	41
5.1.1	S. 87	Das neue Melderecht	41
6.	S. 93	**Ausländerinnen und Ausländer**	43
6.2	S. 93	Der Echtheitsgrad von Ehen	43
6.4	S. 95	Familienzusammenführung mit unzulänglichem Datenschutz	44
7.	S. 98	**Sozialbereich**	45
7.1	S. 99	Sozialämter schießen über das Ziel hinaus	46
7.2	S. 100	Prüfung von Pflegeleistungen	46
7.3	S. 101	Datenabrufe erfordern Ermittlungsbefugnisse	48
7.6	S. 105	Mehr Bürgernähe bei den Rentenversicherungsträgern	50
8.	S. 107	**Gesundheit**	51
8.1	S. 107	Trotz guter Zusammenarbeit noch ungelöste Probleme	51
9.	S. 118	**Statistik – Kommt wieder eine Volkszählung?**	--
10.	S. 121	**Bildung und Wissenschaft**	52
10.1.2	S. 123	Die Schulen und das Internet – Nutzungsordnungen	52
10.2	S. 124	Keine Wahl beim Studierendenausweis mit Chip?	52
10.3	S. 125	Forschung	53
11.	S. 128	**Öffentlicher Dienst**	54
11.1	S. 128	Verlust von Personalakten	54
11.2	S. 129	Bewerbungsverfahren	54

11.4	S. 130	Tele-Heimarbeit – Hinweise für eine datenschutzgerechte Einführung	55
11.4.1	S. 131	Allgemeines	55
11.4.2	S. 131	Grundsätzliche Anforderungen/Hinweise	55
11.4.3	S. 133	Anforderungen an technische und organisatorische Maßnahmen	57
12.	S. 137	**Verkehr, Wirtschaft und öffentliche Unternehmen**	61
12.2.3	S. 140	Geldwäsche	61

Zu 2. Technische und rechtliche Aspekte der Medienentwicklung (Seite 8)

Der Bericht der LfD beschreibt in diesem Abschnitt verschiedene „datenschutzfreundliche" Techniken, wie z.B. Verschlüsselungsverfahren, digitale Signatur und Firewallsysteme. Diesen technischen Ausführungen kann weitestgehend zugestimmt werden; sie geben aber lediglich den derzeitigen Stand der Technik wieder.

Es ist darauf hinzuweisen, dass auf Grund der dynamischen Entwicklung in diesem Bereich künftig und teilweise bereits heute technische Alternativen zur Verfügung stehen, mit denen die gesetzlichen Anforderungen hinsichtlich Datensicherheit und Datenschutz ebenfalls erfüllt werden können. Der Landesregierung muss deshalb weiterhin die Entscheidung überlassen bleiben, geeignete technische Systeme und Verfahren zur Erfüllung ihrer Aufgaben auszuwählen.

Allgemein ist zu der Darstellung der LfD darauf hinzuweisen, dass immer dann, wenn Technologien und Verfahren des Datentransfers diskutiert werden, hiermit einhergehend Missbrauchsmöglichkeiten und damit sowohl für das Individuum als auch für den Sicherheitsapparat eines Staates Risiken verbunden sind.

Am Beispiel der Verschlüsselungsverfahren (2.2.1, 2.2.2) sowie der Abhandlung zum IMSI-Catcher (2.4.2.3) sei verdeutlicht, inwieweit durch die aufgezeigten Technologien die Interessenlage der Nachrichtendienste tangiert wird.

In der Einführung zum Thema Kryptographie auf Seite 11 formuliert die LfD unter 2.2.1, erster Absatz a. E.: "Attribute wie vertraulich, integer und authentisch sind als Eigenschaften der Daten anzusehen, die unabhängig vom aktuellen Aufenthaltsort der Daten sowie der Art und dem Stadium ihrer Verarbeitung gesichert werden müssen". Aussagen wie diese erwecken den Eindruck, die Kommunikationsfreiheit des Individuums genieße immer und vor allen anderen Rechtsgütern den Vorrang. Dass Technologien wie die Kryptographie auch von Kriminellen und Staatsfeinden zum Informationsaustausch genutzt werden und den Sicherheitsbehörden hierdurch die Wahrnehmung ihrer Aufgaben wesentlich erschwert, wenn nicht

völlig vereitelt wird - dass es deshalb wie zu jeder Regel auch hier eine Ausnahme geben muss - bleibt unerwähnt.

Entsprechendes gilt zur Darstellung des IMSI-Catchers. Hier wird der Eindruck erweckt, es ginge ausschließlich um eine Erweiterung der Befugnisse der Sicherheitsbehörden. Dass diese Technik eine Reaktion darstellt auf Ausweichmöglichkeiten, die infolge neuer Techniken für Terroristen/Extremisten geschaffen wurden - etwa sich durch Austausch von Telefonkarten einer G-10-Maßnahme entziehen zu können - bleibt ebenfalls unerwähnt. Es ist verständlich, dass aus der Sicht des Verfassungsschutzes eine Gesetzesänderung, welche den Einsatz solcher Verfahren gestattet, befürwortet wird, und zwar aus Gründen des Schutzes der Gemeinschaft vor Einzelnen, die die neuen Technologien gemeinschaftsschädigend missbrauchen.

Zu 2.1 Datenschutzfreundliche Technologien (Seite 8)

Der Grundsatz der Datenvermeidung, der im Einklang mit der Europäischen Datenschutzrichtlinie steht, wird bei der Entwicklung neuer IT-Verfahren so weit wie möglich beachtet. Gleiches gilt für die in dem Bericht enthaltenen technischen Anregungen und Hinweise. Beispielsweise werden im Justizbereich mit dem vorgelegten Referentenentwurf eines Strafverfahrensänderungsgesetzes (StVÄG 1999) bei den Staatsanwaltschaften und der Strafgerichtsbarkeit bestehende Rechtsunsicherheiten bei der Verarbeitung personenbezogener Daten beseitigt und die notwendigen Grundlagen für einen weiteren Ausbau der Informationstechnik im Bereich der Strafverfolgung und der Strafgerichtsbarkeit geschaffen.

Zu 2.2 Kryptographie - Schlüsseltechnologie für Informationssicherheit und vertrauenswürdige Kommunikation (Seite 11)

Zu 2.2.1 Einführung (Seite 11)

Zu den Bemerkungen hinsichtlich der Überwachungsmöglichkeiten des Staates im Spannungsfeld der Nutzung von Verschlüsselungsmöglichkeiten durch den Bürger hat der Arbeitskreis II „Innere Sicherheit" der Innenministerkonferenz auf seiner Sitzung am 10./11. Mai 1999 festgestellt, dass die polizeiliche Arbeit – insbesondere die Telekommunikationsüberwachung – gegenwärtig durch den Missbrauch von Verschlüsselungsprodukten noch nicht wesentlich beeinträchtigt wird. Für die Zukunft sei jedoch eine stetige Zunahme der Nutzung und damit auch des Missbrauchs zu erwarten. Durch die Verbreitung der Verschlüsselung dürften die gesetzlichen Befugnisse der Strafverfolgungs- und Sicherheitsbehörden jedoch nicht ausgehöhlt werden. Die zuständigen Behörden würden deshalb weiterhin aufmerksam verfolgen, welcher spezifische Sicherheitsbedarf durch die zunehmende Verbreitung von Verschlüsselung entsteht und ggf. durch bestehende Gesetze nicht abgedeckt wird.

Zu 2.2.2 Verschlüsselungsverfahren (Seite 12)

Zu 2.2.2.1 Symmetrische Verschlüsselungsverfahren (Seite 12)

Zu 2.2.2.2 Asymmetrische Verschlüsselungsverfahren (Seite 13)

Zu den Verschlüsselungsverfahren wird auch auf die einleitende Bemerkung der Stellungnahme zu Abschnitt 2 verwiesen.

Zu 2.4.2 Telekommunikation (Seite 29)

Zu 2.4.2.2 Verstärkte Überwachungstendenzen auf Kosten des Datenschutzes (Seite 30)

Die Befürchtung, dass das Telekommunikationsnetz in der Gefahr stehe, „... verstärkt als Fahndungsnetz eingesetzt zu werden", wird nicht geteilt. Zwar hat sich die Anzahl der strafprozessualen Telekommunikationsüberwachungen in Nordrhein-Westfalen im Berichtszeitraum erhöht, jedoch muss ausdrücklich darauf hingewiesen werden, dass Telekommunikationsüberwachungen nur nach Einzelfallprüfungen und Vorliegen aller gesetzlichen Voraussetzungen zulässig sind. Der Eindruck, dass Strafverfolgungsbehörden das Telekommunikationsnetz wie ein „Schleppnetz" benutzen könnten, um so eine Vielzahl von Personen undifferenziert strafprozessualen Maßnahmen zu unterziehen, trifft nicht zu. Es ist festzustellen, dass das Telekommunikationsnetz durch die Strafverfolgungsbehörden keinesfalls als „Fahndungsnetz" eingesetzt wurde oder wird.

Es wird auch auf die Stellungnahme zu 3.1 verwiesen.

Zu 3. Polizei und Verfassungsschutz (Seite 49)

Zu 3.1 Sicherheit auf Kosten der Grundrechte? (Seite 49)

In diesem Abschnitt übt die LfD Kritik an gesetzlichen Vorschriften des Bundes und ihrer Ausführung durch Dienststellen des Bundes wie den Bundesnachrichtendienst. Die Landesregierung hält sich nicht für berufen, dazu Stellung zu nehmen. Eine Stellungnahme der Landesregierung ist nur gefordert, soweit ein Zusammenhang mit der Ausführung von Bundesgesetzen durch das Land besteht. Soweit etwa die LfD eine stetige Erweiterung der Bestimmungen über die Telefonüberwachung beklagt, ist aus der Sicht der Landesregierung darauf aufmerksam zu machen, dass die reale Entwicklung im Verfassungsschutzbereich eine andere Richtung genommen hat. Die Anzahl der Speicherungen ist kontinuierlich zurückgefahren worden. Von daher wurde der Grundrechtsschutz tendenziell gestärkt.

Die Befugnisse des Verfassungsschutzes sind nicht "stets" ausgedehnt worden. So wurde beispielsweise das Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G 10) seit seinem Inkrafttreten am 1. November 1968 insgesamt 11mal geändert. Im Gegensatz zu der von der LfD angesprochenen Änderung der entsprechenden strafrechtlichen Vorschriften bedeuteten die Änderungen im G 10 nicht automatisch eine Erweiterung der staatlichen Eingriffsbefugnisse. Erweitert wurde der Straftatenkatalog lediglich durch die erste Änderung vom 13.09.1978. Mit ihr wurden in Nr. 1 des Artikels 1 § 2 Abs. 1, in Nr. 5 die §§ 87 und 89 StGB sowie in Nr. 6 der 1976 in Kraft getretene § 129 a StGB (Bildung terroristischer Vereinigungen) in den Straftatenkatalog einbezogen. Darüber hinaus wurde in Nr. 7 des § 2 G 10 § 47 Abs. 1 Nr. 7 des Ausländergesetzes, der in Artikel 11 Abs. 1 des Gesetzes zur Neuregelung des Ausländerrechts vom 09.07.1990 durch § 92 Abs. 1 Nr. 8 Ausländergesetz (heute § 92 Abs. 1 Nr. 7 Ausländergesetz) ersetzt wurde, erstmalig aufgenommen. Die übrigen Änderungen des G 10 führten nicht zu einer Erweiterung des Straftatenkatalogs zugunsten der Verfassungsschutzbehörden.

Nicht unerwähnt bleiben darf in diesem Zusammenhang, dass G 10-Gesetzesänderungen auch Regelungen zum Gegenstand hatten, in denen die Rechte der Betroffenen erweitert

wurden. So wurde durch das Verbrechensbekämpfungsgesetz die Regelung in § 5 Abs. 5 Satz 3 G 10 a.F. gestrichen. Nach dieser Vorschrift unterblieb die Benachrichtigung eines Betroffenen, wenn auch nach Ablauf von fünf Jahren seit Beendigung der Maßnahme eine Gefährdung des Zwecks der Maßnahme nicht ausgeschlossen werden konnte. Dies hat zur Folge, dass beendete G 10-Maßnahmen heute zeitlich unbegrenzt auch nach Ablauf von 5 Jahren auf eine Benachrichtigung des Betroffenen hin überprüft werden müssen.

Zu 3.2 Der große Lauschangriff (Seite 51)

Inhaltlich befaßt sich dieser Abschnitt nur mit dem "großen Lauschangriff" im Zusammenhang mit der Strafverfolgung. Die durch Art. 13 Abs. 4 GG normierten Befugnisse des Verfassungsschutzes werden von der LfD nicht angesprochen. In diesem Zusammenhang ist lediglich darauf hinzuweisen, dass in Nordrhein-Westfalen aufgrund der Grundgesetzänderung z. Zt. nicht beabsichtigt ist, auch das Verfassungsschutzgesetz Nordrhein-Westfalen (VSG NW) zu ändern. Dies spiegelt das Verständnis der Verfassungsschutzbehörde für einen zurückhaltenden Einsatz dieses nachrichtendienstlichen Mittels wider.

Die von der LfD gegen die gesetzliche Regelung der akustischen Wohnraumüberwachung vorgetragenen Bedenken sind im Gesetzgebungsverfahren eingehend geprüft worden. Sie haben nicht zuletzt auch dazu beigetragen, dass die Voraussetzungen für eine Anordnung gemäß § 100 c Abs. 1 Nr. 3 StPO sehr eng sind und nur eine restriktive Anwendung dieser Maßnahme als gleichsam „ultima ratio“ zulassen. Dass Staatsanwaltschaften und Gerichte nicht Ermittlungen um jeden Preis durchführen bzw. anordnen, lässt sich dadurch belegen, dass in Nordrhein-Westfalen bislang seit dem Inkrafttreten des Gesetzes bis Ende März 1999 lediglich in einem Fall eine akustische Wohnraumüberwachung stattgefunden hat. Insgesamt werden die Zahlen bundesweit voraussichtlich den einstelligen Bereich nicht überschreiten.

Zur Zeit befasst sich eine vom Strafrechtsausschuss der Konferenz der Justizministerinnen und –minister eingesetzte Arbeitsgruppe unter dem Vorsitz Nordrhein-Westfalens mit der vom Deutschen Bundestag am 16. Januar 1998 im Zusammenhang mit den Beratungen zum großen Lauschangriff geäußerten Bitte

- um Prüfung, wie Zahl, Art, Umfang und Verlauf von Telefonüberwachungen und Wohnungsüberwachungen sich nach einheitlichen Grundsätzen statistisch erfassen lassen, und

- um Vorlage von Vorschlägen zur Verbesserung des Verfahrens der richterlichen Anordnung.

Es ist beabsichtigt, zur Herbstkonferenz der Justizministerinnen und –minister einen Abschlussbericht vorzulegen, der sich insbesondere zu der geforderten Verbesserung der statistischen Erfassung der Telefonüberwachungsmaßnahmen verhält und Möglichkeiten der Erfolgskontrolle aufzeigen soll.

Zu 3.3 DNA-Analysedatei (Seite 52)

Im Zusammenhang mit den Ausführungen zur DNA-Analysedatei wird der Begriff Genanalyse verwendet und dies mit der Feststellung verbunden, dass die nicht-codierenden DNA-Abschnitte bei Verwandten Ähnlichkeiten aufweisen (Seite 53, 1. Absatz). Diese Aussage ist so unzutreffend. Richtig ist einerseits, dass es sich bei der DNA um erbliche Strukturen handelt, es besteht demnach keine Ähnlichkeit, sondern sogar eine Identität einiger Merkmale zwischen blutsverwandten Personen. Die DNA besteht andererseits aus codierenden und nicht-codierenden Regionen, und es werden ausschließlich nicht-codierende Bereiche zur DNA-Analyse ausgewertet und forensisch genutzt. Der Begriff Genanalyse ist insoweit falsch, denn Gene befinden sich nur im codierenden Bereich, der forensisch außer Betracht bleibt.

Weiterhin wird auf Seite 53, 2. Absatz, angedeutet, dass sich durch die wissenschaftliche Forschung in Zukunft Erkenntnisse ergeben könnten, aufgrund derer die derzeit gespeicherten Analyseergebnisse eine Erstellung von Persönlichkeitsprofilen ermöglichen: „Schließlich wären angesichts der besonderen Sensibilität der Daten aus DNA-Analysen klare gesetzliche Vorgaben für die Verarbeitungs- und Nutzungsbefugnisse am Platze gewesen." Aus wissenschaftlicher Sicht kann bezüglich der für die DNA-Analysedatei relevanten Auswertungsverfahren, als deren Ergebnis lediglich Zahlenwerte über die Längenvarianten der DNA entste-

hen, ausgeschlossen werden, dass diese jetzt oder in Zukunft Informationen über das Aussehen, sonstige Eigenschaften oder die Persönlichkeit des Betroffenen liefern könnten.

Zur Forderung der LfD, es bedürfe einer Einengung des zu weit gefassten Straftatenkatalogs, ist Folgendes auszuführen: Um eine nach rechtsstaatlichen Grundsätzen angemessene Nutzung der DNA-Analysedatei zur Verbrechensbekämpfung sicherzustellen, hat der Gesetzgeber in § 81 g StPO die Voraussetzungen für eine Entnahme von Körperzellen und ihre molekulargenetische Untersuchung zur Speicherung in der DNA-Analysedatei an den Begriff der „Straftat von erheblicher Bedeutung" geknüpft und ihn durch Regelbeispiele näher definiert. Der Begriff „Straftat von erheblicher Bedeutung" findet sich als Voraussetzung für die Anordnung bestimmter Ermittlungshandlungen an mehreren Stellen der Strafprozessordnung, so unter anderem in den §§ 98 a, 110 a. Die Straftat muss demnach mindestens dem mittleren Kriminalitätsbereich zuzurechnen sein, den Rechtsfrieden empfindlich stören und geeignet sein, dass Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen. Die nötige Klarstellung und Eingrenzung findet der Begriff der erheblichen Straftat durch die aufgeführten Regelbeispiele, die verdeutlichen, dass es sich bei den in Betracht kommenden Delikten nicht um Straftaten geringerer Kriminalität handelt. Eine weitergehende Einengung ist im Interesse einer effektiven Verbrechensbekämpfung nicht geboten.

Soweit ein ausdrückliches Verbot der Speicherung von Analyseergebnissen gefordert wird, die auf der freiwilligen Abgabe von Speichelproben beruhen, meint der Bericht offensichtlich die sogenannten DNA-Reihenuntersuchungen. Diese Untersuchungen setzen in jedem Einzelfall die freiwillige Abgabe von Speichelproben voraus. Jeder Freiwillige wird darüber belehrt, dass für ihn keine gesetzliche Verpflichtung zur Abgabe besteht und er im Falle der Nichtabgabe mit keinerlei Nachteilen zu rechnen hat, dass die gewonnenen DNA-Identifizierungsmuster nicht in der DAD gespeichert oder recherchiert werden und die Probe einschließlich der erhobenen Daten nach Ausschluss der Täterschaft vernichtet wird. Für eine mögliche weitergehende Speicherung der gewonnenen Proben gibt es im DNA-Identitätsfeststellungsgesetz keine gesetzliche Grundlage. Ihre Vernichtung ist zwingend geboten. Gesetzgeberischer Handlungsbedarf ist aus der Sicht der Landesregierung nicht gegeben.

Die gesetzlichen Vorgaben für die Verarbeitungs- und Nutzungsbefugnisse sind nach Einschätzung der Landesregierung nicht unklar. Hinsichtlich der Verarbeitung und Nutzung der aufgrund des DNA-Identitätsfeststellungsgesetzes gewonnenen DNA-Identifizierungsmuster verweist das Gesetz auf das Bundeskriminalamtgesetz. Demzufolge gelten die umfangreichen bereichsspezifischen Datenschutzbestimmungen des Bundeskriminalamtgesetzes für die als Verbunddatei des polizeilichen Informationssystems geführte zentrale DNA-Analysedatei beim Bundeskriminalamt, insbesondere die dortigen Regelungen über Verantwortlichkeiten, Datenschutzkontrolle, Schadensersatz, Auskunftserteilung, Berichtigung und Löschung.

Zu 3.5 Ermittlungsinstrument Telefon (Seite 54)

Zu 3.5.1 Wachsende Zahl von Telefonüberwachungen (Seite 54)

Die von der LfD geäußerte Kritik an der wachsenden Zahl von Telefonüberwachungen ist aus der Sicht der Landesregierung unbegründet.

Die Aussage, die Anzahl der Überwachungsanordnungen sei im Jahr 1997 gegenüber dem Vorjahr um mehr als 20 % angestiegen, bedarf der Klarstellung. Der unbefangene Leser muss sie gleichermaßen auf die Polizei und auf den Verfassungsschutz beziehen, da an keiner Stelle der Ausführungen zur "Telefonüberwachung" zwischen Polizei und Verfassungsschutz differenziert wird.

Tatsächlich wurden von der Verfassungsschutzbehörde NRW im Berichtszeitraum gegen 15 Betroffene Maßnahmen durchgeführt. Dies zeigt, dass das Mittel der G 10-Maßnahme von der Verfassungsschutzbehörde in Nordrhein-Westfalen sehr restriktiv gehandhabt wird, so dass von einer inflationären Entwicklung im Umgang mit G 10-Maßnahmen für den Bereich des Verfassungsschutzes keine Rede sein kann.

Aber auch im Polizei- und Justizbereich werden Maßnahmen der Fernmeldeüberwachung gemäß § 100 a StPO von den Gerichten nicht in ausufernder Weise angeordnet; sie gehören auch nicht zum Standardrepertoire von Ermittlungsmaßnahmen.

Die im Jahr 1997 gemeldeten einschlägigen 7.776 Verfahren machen im Verhältnis zu einer Gesamtzahl von 4.421.659 durch die Staatsanwaltschaften bundesweit erledigten Ermittlungsverfahren einen prozentual sehr geringen Anteil (von nur 0,17 %) aus. In Nordrhein-Westfalen ist die Zahl der Verfahren, in denen Telefonüberwachungen angeordnet worden sind, im Jahr 1998 gegenüber 1997 von 216 um 43 % auf 316 und die Zahl der von solchen Maßnahmen Betroffenen von 432 um ca. 90 % auf 829 gestiegen. Gleichwohl rechtfertigt auch dies die Sorge um die Wahrung der Grundrechte nicht. Konkrete Anhaltspunkte dafür, dass die vom Gesetzgeber bewusst vorgenommenen Beschränkungen der Anwendbarkeit der Maßnahme unterlaufen bzw. missachtet werden, liegen nicht vor. Der augenfällige Anstieg der Anordnungen hat seine Ursache im Wesentlichen in der Bekämpfung der Organisierten Kriminalität (OK). Die der OK zuzurechnenden, überörtlich agierenden Straftäter bedienen sich verstärkt der technischen Möglichkeiten im Bereich der Telekommunikation und sie gestalten ihre Straftatenvorbereitung und -durchführung organisatorisch so, dass weniger einschneidende Ermittlungsansätze als Telefonüberwachungsmaßnahmen nicht vorhanden sind. Von den im Jahr 1998 gemeldeten 319 Ermittlungsverfahren mit Anordnungen gemäß § 100 a StPO bezogen sich allein 70 %, nämlich 224 Verfahren, auf schwere Betäubungsmittelstraftaten, d. h. typische OK-Delikte.

In Nordrhein-Westfalen lassen sich – jedenfalls für den Bereich der Generalstaatsanwaltschaft Düsseldorf – auch Aussagen über den Erfolg der Telefonüberwachung treffen: Von insgesamt 177 beendeten Maßnahmen waren 143 (= 80,8 %) erfolgreich, nur 34 (= 19,2 %) führten nicht zur Begründung eines die Erhebung der öffentlichen Klage rechtfertigenden Tatverdachts bzw. zu Ansatzpunkten für weitere erfolgreiche Ermittlungen.

Dies belegt nach Auffassung der Landesregierung nachdrücklich die überragende Bedeutung dieses strafprozessualen Hilfsmittels gerade im Kampf gegen die Organisierte Kriminalität. Aus diesem Grund unterstützt die Landesregierung auch alle Maßnahmen, die in einem für die Belange der Praxis vertretbaren Rahmen die Transparenz und Akzeptanz dieser Maßnahmen in der Bevölkerung erhöhen. Vor dem Hintergrund entsprechender Beschlüsse der Konferenz der Justizministerinnen und -minister ist in verschiedenen Arbeitsgruppen ihres Strafrechtsausschusses geprüft worden, wie sich das strafprozessuale Instrument der Fernmeldeüberwachung nicht im Sinne einer rechtspolitisch gebotenen Ausweitung des Deliktskatalo-

ges, sondern auch im Sinne einer restriktiven Handhabung optimieren lässt. Dabei ist überwiegend ein gesetzgeberischer Handlungsbedarf verneint worden.

Zu 3.5.3 Unzureichende Benachrichtigungen von Abhörmaßnahmen (Seite 56)

Für die Verfassungsschutzbehörden normiert § 5 Abs. 5 G 10 eine Benachrichtigungspflicht gegenüber den Betroffenen. Diese ist entsprechend der Aufgabenstellung des Verfassungsschutzes an andere Voraussetzungen geknüpft als die in § 101 StPO genannten. Nach § 5 Abs. 5 Satz 1 G 10 sind Beschränkungsmaßnahmen den Betroffenen nach ihrer Einstellung mitzuteilen, wenn eine Gefährdung der Beschränkung ausgeschlossen werden kann. Für den Fall, dass im Zeitpunkt der Einstellung der Maßnahme noch nicht abschließend beurteilt werden kann, ob diese Voraussetzungen vorliegen, bestimmt § 5 Abs. 5 Satz 2 G 10, dass diese Mitteilung vorzunehmen ist, **sobald** eine Gefährdung des Zwecks der Beschränkung ausgeschlossen werden kann.

Die vom Gesetz geforderte möglichst frühzeitige Benachrichtigung der Betroffenen wird beim Verfassungsschutz in NRW dadurch gewährleistet, dass sämtliche Verfahren bei ihrer Beendigung und daran anschließend spätestens alle 6 Monate daraufhin überprüft werden, ob unter den oben genannten Voraussetzungen eine Benachrichtigung des Betroffenen erfolgen kann. Häufig muss eine Benachrichtigung, die noch im zeitlichen Zusammenhang zu der Maßnahme steht, unterbleiben, weil die Betroffenen auch weiterhin in die Szene eingebunden sind und durch eine Benachrichtigung der Zweck der Beschränkung nachhaltig gefährdet würde. Die Rechte der betroffenen Personen werden insofern jedoch durch die regelmäßige und in kurzen Zeitabständen erfolgende Überprüfung gewahrt.

Zu 3.6 Verfassungsschutz und polizeilicher Staatsschutz (Seite 57)

Allgemein kann hierzu gesagt werden, dass bei den Besuchen der Mitarbeiter der LfD aus Sicht des Verfassungsschutzes eine konstruktive Zusammenarbeit erfolgt ist. Insbesondere bei der Überprüfung von Einzelfällen (Auskunftsersuchen) wurden kaum Beanstandungen erhoben.

Zu 3.6.1 Bereich Verfassungsschutz (Seite 57)

1. Unterpunkt: Word-Perfect-Dateien (Seite 57)

Das Thema wurde bereits beim Kontrollbesuch der LfD in der Zeit vom 30. Juni bis 04. Juli 1997 aufgegriffen. In seiner Stellungnahme zu dem von der LfD erstellten Prüfbericht hat das Innenministerium ausgeführt, dass Rechtsgrundlage für die Erstellung der Word-Perfect-Dateien § 5 Abs. 1 VSG NW ist. Nach dieser Vorschrift darf die Verfassungsschutzbehörde die zur Erfüllung ihrer Aufgaben erforderlichen Informationen einschließlich personenbezogener Daten verarbeiten. Die von der LfD aufgezeigten Probleme der Word-Perfect-Dateien werden auch hier gesehen. Der Hinweis, das Problem im Rahmen der Neuorganisation der automatisierten Datenverarbeitung bei der Verfassungsschutzbehörde zu lösen, ist richtig. Die neue Datenbank wird es ermöglichen, Organisations- und Objektbezüge zu erfassen. Sie wird komfortable Möglichkeiten der Wiedervorlage, Sperrung, Löschung, Protokollierung und Zugriffsbegrenzung der Daten aufweisen. Mit der Fertigstellung des Programms "Neue Kartei" ist nach dem jetzigen Planungsstand Anfang des vierten Quartals diesen Jahres zu rechnen.

2. Unterpunkt: Einsichtnahme in Register gemäß § 16 Abs. 3 VSG NW (Seite 57)

Die von der LfD vorgenommene Schlußfolgerung, es handele sich bei § 16 Abs. 3 VSG NW um eine überflüssige Rechtsvorschrift, da sie bisher in der Praxis keine Anwendung gefunden hat, wird nicht geteilt.

Nach § 16 Abs. 2 VSG NW darf die Verfassungsschutzbehörde die in § 16 Abs. 1 VSG NW genannten Stellen (Gerichte, Behörden und Einrichtungen des Landes, Gemeinden, Gemeindeverbände und sonstige der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts) unter drei alternativen Voraussetzungen um Übermittlung der zur Erfüllung ihrer Aufgaben erforderlichen Informationen einschließlich personenbezogener Daten ersuchen, nämlich dann, wenn diese Informationen nicht aus allgemein zugänglichen Quellen erhoben werden können, wenn sie nur mit übermäßigem Aufwand oder nur durch eine den Betroffenen stärker belastende Maßnahme erhoben werden können.

Nach § 16 Abs. 3 VSG NW darf die Verfassungsschutzbehörde amtliche Register einsehen, aber - unter weiteren Einschränkungen - nur dann, wenn durch die Übermittlung nach Absatz 2 der Zweck der Maßnahme gefährdet oder der Betroffene unverhältnismäßig beeinträchtigt würde. Die Forderung der LfD nach Beseitigung des § 16 Abs. 3 VSG NW ist daher nicht sachgerecht, da in einer Übermittlung von personenbezogenen Daten nach dieser Vorschrift unter Berücksichtigung datenschutzrechtlicher Aspekte auch ein schonenderes Mittel gesehen werden kann.

§ 16 Abs. 3 Satz 3 VSG NW hat bisher noch keine Anwendung gefunden. Es handelt sich hierbei um eine weitreichende Maßnahme und einen schwerwiegenden Eingriff in das informationelle Selbstbestimmungsrecht. Dass von einer derartigen Datenübermittlung bisher noch kein Gebrauch gemacht wurde, zeigt deutlich, dass die Verfassungsschutzbehörde Nordrhein-Westfalen normgerecht schonend verfahren ist. Hieraus kann aber nicht die Schlußfolgerung gezogen werden, die Vorschrift zu streichen, denn die Notwendigkeit, sie zu praktizieren, ist für die Zukunft nicht ausgeschlossen.

3. Unterpunkt: Übermittlung von Daten an Stellen außerhalb des öffentlichen Bereichs (Seite 58)

§ 17 Abs. 4 VSG NW regelt einen anderen Sachverhalt als der von der LfD angesprochene § 6 des Verfassungsschutzgesetzes vom 21. Juli 1981. Die Begründung des VSG NW in der derzeit gültigen Fassung weist darauf hin, dass durch die Vorschrift des § 17 Abs. 4 "nicht die Weitergabe personenbezogener Daten im Rahmen von Befragungen erfaßt werden (soll). Rechtsgrundlage hierfür ist § 5 Abs. 1". Damit sind die Fälle, in denen im Rahmen nachrichtendienstlicher Arbeit des Verfassungsschutzes (§ 5 Abs. 2 Nr. 4 VSG NW) Daten z.B. an Quellen weitergegeben werden müssen, nicht nach § 17 VSG NW zu behandeln.

Ausgenommen aus dem Geltungsbereich des § 17 VSG NW ist außerdem die Übermittlung personenbezogener Daten, deren Bekanntgabe im Rahmen der Öffentlichkeitsarbeit "für das Verständnis des Zusammenhangs oder der Darstellung der Organisationen erforderlich ist",

aber auch nur dann, wenn "die Interessen der Allgemeinheit das schutzwürdige Interesse des Betroffenen überwiegen". Datenübermittlungsgrundlage ist dann § 15 Abs. 2 VSG NW.

Des weiteren ist die Übermittlung personenbezogener Daten im Rahmen von Sicherheitsüberprüfungen kein Anwendungsfall des § 17 Abs. 4 VSG NW. Hier greifen als Spezialvorschriften insbesondere § 15 Abs. 1 und 2 sowie § 28 Sicherheitsüberprüfungsgesetz (SÜG).

Fallgestaltungen, in denen bei dieser inzwischen sehr differenzierenden Rechtslage § 17 Abs. 4 VSG NW Übermittlungsgrundlage sein könnte, sind nicht schlechthin auszuschließen, wenn sie auch sehr selten sein werden. Sie müssen außerdem nach § 17 Abs. 4 Satz 2 VSG NW in einem Nachweis erfaßt werden, für den wiederum inhaltliche, formale sowie Sicherungs- und Vernichtungsvorschriften gelten.

Seit Inkrafttreten des neuen Gesetzes ist noch keine Entscheidung auf der Grundlage des § 17 Abs. 4 VSG NW erforderlich geworden; der im Gesetz vorgesehene Nachweis brauchte deshalb bisher nicht angelegt zu werden.

4. Unterpunkt: Speicherungen im NADIS (Seite 58)

Bei den NADIS-Speicherungen und damit auch bei deren Protokollierung wird § 6 BVerfSchG auf eine Verbunddatei in Bundesregie angewandt. Rechtsgrundlage ist § 5 i.V.m. § 6 BVerfSchG. Der von der LfD in diesem Zusammenhang zitierte § 10 Abs. 3 Satz 2 VSG NW betrifft dagegen die internen Speicherungen bei der Verfassungsschutzbehörde Nordrhein-Westfalen und ist hier nicht anwendbar. Nordrhein-Westfalen wird jedoch bei einer etwaigen Änderung der NADIS-Richtlinien auf eine Verkürzung der Protokollierungsfristen hinwirken.

5. Unterpunkt: Löschung von Daten (Seite 58)

Nach den Ausführungen zu den Löschungspflichten gemäß § 11 Abs. 3 VSG NW strebt die LfD eine Löschung von personenbezogenen Daten aus Organisationsakten an. Klarstellungs-

bedürftig sind die Ausführungen insofern, als darauf hingewiesen wird, der Verfassungsschutz wolle Organisationsakten "von der zeitgleichen Löschungspflicht freigestellt" wissen. Dies erweckt den Eindruck, der Verfassungsschutz wolle einer gesetzlichen Löschungspflicht nicht nachkommen. Tatsächlich bezieht sich die derzeit gültige gesetzliche Regelung in § 11 Abs. 3 VSG NW aber nicht generell auf Akten des Verfassungsschutzes, z.B. Organisationsakten, sondern lediglich speziell auf "zur Person geführte Akten". Das Anliegen der LfD ist somit ein rechtspolitisches Anliegen, das nur im Wege einer Gesetzesänderung zu erreichen wäre.

Der Begriff "zur Person geführte Akten" in § 11 Abs. 3 VSG NW kann auch nicht erweitert ausgelegt und damit auf Organisationsakten bezogen werden. Die Ausführungen der LfD laufen zwar auf eine solche erweiterte Auslegung hinaus. Diese beruht aber auf einer Vermischung der Begrifflichkeiten aus § 11 Abs. 1 und 2 und § 11 Abs. 3 VSG NW und widerspricht Wortlaut, Systematik und Regelungszweck des § 11 VSG NW. § 11 VSG NW differenziert nämlich bewusst zwischen "personenbezogenen Daten in Akten" (Absätze 1 und 2) und "zur Person geführten Akten" (Absatz 3). Diese Differenzierung trägt dem Umstand Rechnung, dass sich in allen Akten des Verfassungsschutzes - d.h. sowohl in Sach- bzw. Organisationsakten als auch in zur Person geführten Akten - personenbezogene Daten befinden. Dies ergibt sich aus der Natur der Sache, da alle "Bestrebungen" im Sinne des § 3 Abs. 1 VSG NW von Personen getragen werden. Das Vorhandensein personenbezogener Daten auch in nicht "zur Person geführten Akten" des Verfassungsschutzes ist somit kein Einzelfall, sondern die Regel. Eine umfassende Löschungspflicht für personenbezogene Daten würde Sach- und Organisationsakten regelmäßig unbrauchbar machen. In einigen Arbeitsbereichen des Verfassungsschutzes würde eine Löschung von für sich betrachtet "nicht mehr erforderlichen" personenbezogenen Daten aus Sach- bzw. Organisationsakten die in den Akten enthaltenen Sachinformationen bis zur Unkenntlichkeit durchlöchern. Sachzusammenhänge könnten nicht mehr nachvollzogen werden, wie z.B. die Entwicklung einzelner Gruppierungen des sog. "Antiimperialistischen Widerstandes" über Jahre mit wechselnden Aktivisten, ihr bewusstes gleichzeitiges Entfalten von legalen und illegalen Aktivitäten oder ihr Streben nach taktischen Bündnissen mit unverdächtigen Organisationen und Personen. Um dies zu vermeiden, ordnet § 11 VSG NW für nicht "zur Person geführte Akten" gerade keine Löschung einzelner personenbezogener Daten an - auch nicht für den Fall, dass sie "nicht mehr

erforderlich" sind -, sondern ermöglicht für Einzelfälle unter den Voraussetzungen der Absätze 1 und 2 die Berichtigung oder Sperrung.

Im Übrigen hätte die geforderte Verfahrensweise die unpraktikable Folge, dass man z.B. auch Namen aus Zeitungsartikeln oder Gerichtsurteilen, die in den Sachakten enthalten sind, unkenntlich machen müsste. Außerdem sind in jeder Verwaltungsakte außerhalb des Verfassungsschutzes ebenfalls personenbezogene Daten enthalten.

Zu 3.6.2 Bereich Sicherheitsüberprüfung (Seite 59)

Soweit die LfD ihren Eindruck wiedergibt, bei den sicherheitsüberprüften Personen handele es sich um im Sinne der Aufgabenstellung des Verfassungsschutzes besonders verdächtige Personen, weil diese in NADIS gespeichert würden, ist darauf hinzuweisen, dass NADIS ein reines Fundstellenverzeichnis und keine "Verdächtigtendatei" ist.

Gemäß § 21 Abs. 2 letzter Satz SÜG NW ist eine solche Speicherung in gemeinsam genutzten Verbunddateien ausdrücklich zulässig. Um Geheimnisträger, die im Rahmen der Aufgabenstellung des Verfassungsschutzes auffällig werden, jederzeit als solche ausmachen zu können, ist die Speicherung im NADIS auch notwendig.

1. Unterpunkt: Einzubeziehende Lebenspartner (Seite 60)

Die LfD sieht die Datenschutzrechte der in das Verfahren möglicherweise einzubeziehenden Partnerinnen und Partner unzureichend gewahrt. Auch bei einer Verweigerung der Einwilligung in die Einbeziehung würden die Daten der Partnerinnen und Partner einer Abfrage im Informationssystem des Verfassungsschutzes unterzogen. Tatsächlich wird aber in einem solchen Fall keine Sicherheitsüberprüfung durchgeführt. Der Einsatz der betroffenen Person in einer sicherheitsempfindlichen Tätigkeit ist dann nicht möglich. Insoweit sind auch keine Daten zu löschen, da gar keine Daten gespeichert sind.

Die Verweigerung des Ehepartners der zu überprüfenden Person hat nach dem Gesetz nur auf die Überprüfung nach § 9 SÜG NW (einfache Sicherheitsüberprüfung) keine Auswirkung.

Die Erkenntnisse der Verfassungsschutzbehörden des Bundes und der Länder zum Ehepartner der zu überprüfenden Person können auch ohne Einwilligung abgefragt werden. Zur Zulässigkeit dieser Verfahrensweise wird auf die Gesetzesbegründung zu § 13 Abs. 2 SÜG NW verwiesen. Danach ist die bloße Anfrage bei den Verfassungsschutzbehörden nach den evtl. dort vorliegenden Erkenntnissen zur Ehefrau oder Lebenspartnerin oder zum Ehemann oder Lebenspartner und den anderen in der Sicherheitserklärung genannten Personen oder Objekten nicht als Einbeziehung dieser Person in die Sicherheitsüberprüfung zu betrachten.

Die Einwilligung dieses Personenkreises ist somit nicht Voraussetzung für die Abfrage bei den Verfassungsschutzbehörden.

2. Unterpunkt: Sicherheitserheblichkeit von Ermittlungsverfahren und Straftaten (Seite 60)

Die Auffassung der LfD, Verkehrsstraftaten, wie z. B. fahrlässige Körperverletzung im Straßenverkehr, könnten ohne eingehende Begründung nicht als sicherheitserhebliche Erkenntnisse weitergegeben werden, läßt außer Betracht, dass fahrlässiges Verhalten im Straßenverkehr ebenso wie fahrlässiger Umgang im Verkehr mit Verschlußsachen auf die fehlende oder unzureichende Beachtung von Rechtsvorschriften zurückzuführen ist. Es bedarf bei einer am Zweck des SÜG orientierten Betrachtungsweise keiner näheren Erläuterung, dass die Bereitschaft zum fahrlässigen Umgang mit Regelungen auch für Geheimschutzfragen von sicherheitserheblicher Bedeutung ist.

Gleiches gilt für nicht abgeschlossene Ermittlungsverfahren, auch wenn diese schwebenden Verfahren stets ungesicherte Daten enthalten. Aus dem Umstand, dass gegen die überprüfte Person ein Strafverfahren eingeleitet wurde, ist zumindest im Sinne von § 6 Abs. 2 SÜG NW ein Anhaltspunkt für ein Sicherheitsrisiko erkennbar. Der betroffenen Person bleibt in jedem Fall, unabhängig davon, ob die Erkenntnisse als sicherheitserheblich oder als sicherheitserheblich, aber noch nicht abschließend bewertet eingestuft werden, die Möglichkeit, hierauf im Rahmen des § 15 Abs. 4 SÜG NW zu reagieren.

Die Tatsache, dass ein Ermittlungsverfahren eingeleitet wurde, ist keine ungesicherte Erkenntnis. Sie wird im übrigen nicht "verbreitet", sondern lediglich dem Geheimschutzbeauftragten der zuständigen Stelle zweckgebunden mitgeteilt. Dieser hat sodann die Möglichkeit, diesem Anhaltspunkt im Rahmen des Sicherheitsüberprüfungsverfahrens nachzugehen.

3. Unterpunkt: Sicherheitsüberprüfung ehrenamtlich tätiger Personen im Bereich des Strafvollzugs (Seite 60)

Die Behauptung, die Sicherheitsüberprüfung ehrenamtlich tätiger Personen im Bereich des Strafvollzuges erfolge derzeit insgesamt ohne Rechtsgrundlage, ist nicht nachvollziehbar. Rechtsgrundlage ist § 2 Buchstabe d) bb) in Verbindung mit § 2 letzter Satz SÜG NW in Verbindung mit der Verordnung zur Bestimmung der lebens- oder verteidigungswichtigen Einrichtungen vom 03. November 1995 (GV.NW. S. 1148). Danach übt eine sicherheitsempfindliche Tätigkeit aus, wer an einer sicherheitsempfindlichen Stelle einer lebens- oder verteidigungswichtigen Einrichtung beschäftigt ist. Lebenswichtig sind u.a. solche Einrichtungen, die für das Funktionieren des Gemeinwesens unverzichtbar sind. Hierzu zählen nach der genannten Verordnung auch die Justizvollzugsanstalten des geschlossenen und des offenen Vollzugs.

Unter dem Begriff "beschäftigt" nur solche Personen zu verstehen, die in einem Beamten- oder Angestelltenverhältnis stehen, wie es die LfD offensichtlich macht, geht am Sinn und Zweck des SÜG NW vorbei.

Trennung der Datenverarbeitung (Seite 60, letzter Absatz)

Eine Trennung der Datenverarbeitung zwischen Verfassungsschutzbehörde und der an einer Sicherheitsüberprüfung mitwirkenden Behörde, wie es die LfD vorschlägt, würde § 3 Abs. 2 VSG NW verletzen, wonach die Verfassungsschutzbehörde auch bei der Sicherheitsüberprüfung mitwirkt. Der Grund für die einheitliche Datenverarbeitung in NADIS ist bereits oben ausgeführt.

Zu 3.6.3 NADIS-Personenzentraldatei (PZD) (Seite 61)

Die Aussage der LfD, dass im NADIS gemäß § 6 Abs. 2 BVerfSchG nur solche Identifizierungsdaten gespeichert werden dürfen, ohne die ein Auffinden der zu einer bestimmten Person angelegten Akten nicht möglich wäre, ist richtig. Genau nach diesem Prinzip nimmt auch die nordrhein-westfälische Verfassungsschutzbehörde ihre Speicherung im NADIS vor. Aus diesem Grunde wurde auch das Speicherverhalten nicht aufgrund der erfolgten förmlichen Beanstandung durch die LfD geändert.

NADIS-Speicherungen und INPOL-Speicherungen sind nicht vergleichbar. Für die Speicherung in INPOL stehen sichere Personendaten, nämlich die genannten, zur Verfügung. Die Verfassungsschutzbehörden erhalten häufig "weiche", unvollständige und nicht überprüfbare Daten. Sie müssen deshalb, um Datenschutz im Sinne der Identifizierung der wirklich betroffenen Personen praktizieren zu können, auf Merkmale außerhalb der engsten personenbezogenen Daten zurückgreifen.

Beim Verfassungsschutz liegen häufig nur einzelne Daten wie etwa ein Kfz-Kennzeichen oder eine Schließfachnummer vor. Es ist daher erforderlich, auch diese Daten zu speichern. Häufig ist es nur mit Hilfe eines vorhandenen Kfz-Kennzeichens, einer Telefonnummer oder einer Schließfachangabe möglich, die Identifizierung einer bestimmten Person vorzunehmen. In diesen Fällen muss es dann aber auch, um die Aufgabenerfüllung der Verfassungsschutzbehörden nicht zu gefährden, möglich sein, diese Daten zu speichern. Dies läuft nicht dem Gesetzeswortlaut entgegen, da dieser nur auf die Daten zur Identifizierung abstellt und ein solches Datum im Einzelfall auch in der Angabe einer Telefonnummer oder eines Kfz-Kennzeichens gegeben sein kann. Gerade aus Datenschutzgründen kann es im Einzelfall notwendig sein, diese Daten zu speichern, nämlich dann, wenn es bei Vorliegen nur weniger Identifizierungsmerkmale zu Personenverwechslungen kommen könnte.

Die Datenschutzbeauftragten der anderen Länder haben - soweit hier bekannt ist - ebenso wie der BfD ihre diesbezüglichen Bedenken zurückgestellt.

Zu 3.6.4 Erfassung einfacher Mitglieder von Organisationen (Seite 61)

Hierzu heißt es im ersten Absatz unter anderem:

"Danach werden die Daten einfacher Mitglieder solcher Organisationen zwar in den Akten der Organisation erfasst, die Speicherung des Datensatzes in den elektronischen Dateien erfolgt jedoch nur dann, wenn das Mitglied die Organisation durch Aktivitäten nachdrücklich unterstützt."

Diese Aussage beschreibt die Datenverarbeitungspraxis der Auswertungsreferate, die sich nach den Bestimmungen des VSG NW (§ 8 Abs. 1 Nr. 1 u. 2 i.V.m. § 3 Abs. 1 u. 3 VSG NW) richtet, ungenau. Eine Speicherung personenbezogener Informationen erfolgt hier bei folgenden Konstellationen, wobei in Fällen des § 8 Abs. 1 Nr. 1 VSG NW die Entscheidung über Speicherung und Dauer der Speicherung grundsätzlich die Intensität der vorliegenden tatsächlichen Anhaltspunkte für den Verdacht, dass eine Person in einem oder für einen Personenzusammenschluss im Sinne des § 3 VSG NW handelt, berücksichtigt:

- Mitgliedschaft in extremistischen Parteien

Bei extremistischen Gruppierungen mit fest gefügten Organisationsstrukturen wie den rechtsextremistischen und linksextremistischen Parteien werden auch "einfache" Mitglieder durchweg gespeichert. Dies steht auch in Einklang mit der Rechtslage (§ 8 Abs. 1 Nr. 1 i.V.m. § 3 Abs. 1 u. Abs. 3 Satz 1 Buchst. c) 1. Alt. VSG NW). Auch in Zukunft werden hier "einfache" Mitglieder aller rechts- und linksextremistischen Parteien gespeichert.

- Betätigung in extremistischen Gruppierungen ohne formalisierte Mitgliedschaft

Neben den extremistischen Parteien betätigen sich Extremisten aber auch in Personenzusammenschlüssen, die - z.T. typischerweise - keine formalisierte bzw. keine offen bekannte Mitgliedschaft kennen. Insofern kann bei einer Speicherung auch nicht zwischen "einfachen" und aktiven Mitgliedern unterschieden werden. So sind z.B. alle Personen, die regelmäßig im

Namen der Informationsstelle Kurdistan (ISKU) auftreten, z.B. als Mitarbeiter in der Geschäftsstelle, im Rahmen logistischer und organisatorischer Arbeit oder als Organisatoren von Versammlungen, "Angehörige" dieses dem sog. "Antiimperialistischen Widerstand" zuzurechnenden Personenzusammenhangs, handeln also "in" einem Personenzusammenschluss; ihre Daten werden nach § 8 Abs. 1 Nr. 1 i.V.m. § 3 Abs. 1 u. Abs. 3 Satz 1 Buchst. c) 1. Alt. VSG NW gespeichert.

- Betätigung für extremistische Gruppierungen

Falls nach den dem Verfassungsschutz vorliegenden Erkenntnissen bei einem Personenzusammenschluss nicht von "Angehörigen" im Sinne der oben dargestellten Alternativen ausgegangen werden kann, insbesondere bei Gruppierungen ohne feste Organisationsstrukturen, also auch ohne "Mitgliedschaft im klassischen Sinne", wird geprüft, ob das Kriterium "Handeln für einen Personenzusammenschluss durch nachdrückliche Unterstützung" (§ 8 Abs. 1 Nr. 1 i.V.m. § 3 Abs. 1 u. Abs. 3 Satz 1 Buchst. c) 2. Alt. und Abs. 3 Satz 2 VSG NW) erfüllt ist. Dieses Tatbestandsmerkmal ist auch auf Fälle anzuwenden, in denen Personen Bestrebungen eines möglicherweise auch fest strukturierten Personenzusammenschlusses wie einer Partei nachdrücklich unterstützen, ohne jedoch Mitglied zu sein.

Was im Einzelfall unter "nachdrücklicher Unterstützung" zu verstehen ist, kann nicht für alle Gruppierungen einheitlich festgestellt werden. Abhängig ist dies auch von der Ausrichtung, Gefährlichkeit oder evtl. Konspiration der jeweiligen Gruppierungen. Unter anderem bei Personengruppen mit hoher Militanz und Gewaltbereitschaft - wie bei Teilen der Neonazis und der Skinheads - wird die entsprechende Schwelle relativ niedrig angesetzt. Bei nicht militanten, aber konspirativen Zirkeln kann schon der einmalige Besuch einer Veranstaltung ausreichend sein. In diesem Zusammenhang können für die Bewertung auch Informationen über Ablauf und Inhalt der jeweiligen Veranstaltung relevant sein. In dem Beispielsfall der Informationsstelle Kurdistan (ISKU) werden Personen gespeichert, die Veranstaltungen der ISKU besuchen und diese Bestrebung dadurch nachdrücklich unterstützen, und zwar bei mehrfach festgestellten Besuchen wegen höherer Intensität der Anhaltspunkte für den Verdacht einer extremistischen Bestrebung mit längerer Speicherungsdauer als bei einmaligem Besuch.

- Kontaktpersonen von Beobachtungsobjekten

Nach § 8 Abs. 1 Nr. 2 i.V.m. § 3 Abs. 1 u. Abs. 3 VSG NW werden solche personenbezogenen Informationen gespeichert, die für die Erforschung und Bewertung von Bestrebungen oder Tätigkeiten nach § 3 Abs. 1 VSG NW erforderlich sind. Dies kann im Beispielsfall der Informationsstelle Kurdistan (ISKU) für Kontaktpersonen von Angehörigen oder Unterstützern der ISKU zutreffen. So ist es z.B. erforderlich zu beobachten, mit welchen - auch unverdächtigen - Personen die ISKU versucht, taktische Bündnisse etwa im Rahmen von themenbezogenen Kampagnen einzugehen. Entsprechende personenbezogene Daten werden allerdings regelmäßig nur in Sachakten und Sachdateien verarbeitet. Eine Speicherung der betroffenen Personen in der elektronischen Personendatei allein wegen ihrer Kontakte zu Angehörigen oder Unterstützern der beobachteten Gruppierung erfolgt nicht.

- Einzelpersonen, die nicht in einem oder für einen Personenzusammenschluss handeln

Daten zu Einzelpersonen werden insbesondere erfasst, wenn diese zur Verfolgung eigener extremistischer Ziele Gewalttaten begehen, begangen haben oder planen oder sie sich an gewalttätigen Aktionen im Zusammenhang mit extremistischen Aktivitäten beteiligen, beteiligt haben oder dies planen. Dasselbe gilt, wenn ihr Verhalten aufgrund seiner Wirkungsweise geeignet ist, ein Schutzgut des § 3 Abs. 1 VSG NW erheblich zu beschädigen (§ 3 Abs. 3 letzter Satz VSG NW). Diese Speicherungen kommen in der Praxis nicht so häufig vor.

- Daten von Mitgliedern extremistischer Organisationen in Sachakten

Soweit im Abschnitt 3.6.4 beklagt wird, dass aus Organisationsakten auch die Daten einzelner Mitglieder herausgelesen werden könnten, ist die dahinterstehende inhaltliche Aussage richtig. Dies ist jedoch unvermeidbar und auch nicht änderungsbedürftig. Insoweit wird auf die o.a. Position zur Unterscheidung zwischen Organisations- und Personenakten verwiesen. Soweit im letzten Absatz des Abschnitts 3.6.4 bezüglich der Erfassung und Verarbeitung von personenbezogenen Daten einfacher Mitglieder ein weiteres Beispiel für die Notwendigkeit der datenschutzkonformen Neugestaltung der Verarbeitung personenbezogener Daten in Organisationsakten gesehen wird, ist dem nicht zuzustimmen. Organisationsakten ohne die Na-

mensnennung von Personen sind weder praktikabel noch wünschenswert und rechtlich nach dem oben Gesagten nicht geboten (siehe dazu grundsätzlich auch oben - Stellungnahme zu Abschnitt 3.6.1).

Zu 3.6.5 Staatsschutz, Verfassungsschutz und die Versammlungsfreiheit (Seite 62)

Zu den im Rahmen von Kontrollbesuchen von der LfD angenommenen Datenschutzproblemen liegen ihr inzwischen Stellungnahmen aus Sicht des Polizeilichen Staatsschutzes vor. Ohne einer mehr auf Fachebene von der LfD ggf. noch für erforderlich gehaltenen Einzelerörterung vorzugreifen, bedarf es einiger Erläuterungen:

Befürchtungen der LfD, dass mit Blick auf die fundamentale Bedeutung des Grundrechts aus Art. 8 GG die Verarbeitung personenbezogener Daten im Zusammenhang mit der Anmeldung von Versammlungen im Grundsatz einer Korrektur bedarf, können nicht bestätigt werden.

Die Aufgabentrennung von Polizei und Verfassungsschutz wird gewahrt. Weder kommt es zu einer Überschneidung von polizeilichen Aufgaben mit denen des Verfassungsschutzes noch wird – wie der Bericht unzutreffend ausführt – die datenschutzrechtliche Prüfung, ob die Voraussetzungen für eine Übermittlung an den Verfassungsschutz vorliegen, von der Polizei auf den Verfassungsschutz verlagert.

Der Bericht erweckt überdies schon in der Überschrift auf Seite 62 den – unzutreffenden – Eindruck, dass der Polizeiliche Staatsschutz außerhalb jeglicher Organisationsbindung an die Kreispolizeibehörde, gleichsam neben ihr und dem Verfassungsschutz stehe. Er ist, wie andere Organisationseinheiten auch, Teil der Kreispolizeibehörde und wirkt in dieser Einbindung an den Aufgaben der Gefahrenabwehr mit und nimmt Aufgaben der Kriminalitätsbekämpfung wahr.

Im Einzelnen ist anzumerken:

- Weder ist von einer im Rechtssinne „regelmäßigen" oder von einer ohne Prüfung erfolgenden Weitergabe personenbezogener Daten innerhalb der Kreispolizeibehörden noch von einer solchen Übermittlung insbesondere an den Verfassungsschutz auszugehen. Zweck, Umfang und Ausgestaltung der einzelnen Verarbeitungsschritte, die auf der Grundlage insbesondere des Polizeigesetzes erfolgen, richten sich jeweils an der **Erforderlichkeit** im datenschutzrechtlichen Sinne aus. Datenverarbeitungen „auf Vorrat" finden nicht statt.

- Datenverarbeitungen – insbesondere Anfragen bei anderen Behörden – anläßlich der Anmeldung einer Versammlung dienen – bei der Unterabteilung Polizeilicher Staatsschutz nicht anders als in anderen Bereichen der als Versammlungsbehörde zuständigen Kreispolizeibehörde – dem Ziel, **dem Versammlungsrecht soweit als möglich Geltung zu verschaffen.** Sie dienen der Überprüfung, ob und mit welchen Störungen der angemeldeten Versammlung zu rechnen ist und welche versammlungsrechtlichen Schutzvorkehrungen getroffen werden können.

- Soweit die Polizei personenbezogene Daten speichert, geschieht dies ebenso wie bei Anfragen an Dritte **ausschließlich** zur Erfüllung der der **Polizei** nach dem Polizeigesetz und dem Versammlungsgesetz zugewiesenen Aufgaben. Die Zulässigkeit der Speicherung personenbezogener Daten bei der Polizei – auch über eine Einzelveranstaltung hinaus – hängt nach dem Polizeigesetz davon ab, ob und inwieweit die Informationen für Zwecke der Gefahrenabwehr und/oder Kriminalitätsbekämpfung von Bedeutung sind.

- Soweit Daten unrichtig sind, müssen - hierüber haben Meinungsverschiedenheiten nicht bestanden - die Stellen, die die Daten erhalten haben, gemäß dem Polizeigesetz unterrichtet werden. Dies gilt auch, soweit Daten über Teilnehmer an Versammlungen bei der Polizei überhaupt in Listen zusammengefaßt werden.

- Der weitere Umgang mit von der Polizei an den Verfassungsschutz zu übermittelnden personenbezogenen Daten richtet sich nach den Aufgaben, die nach dem Verfassungsschutzgesetz dort wahrzunehmen sind.

Bei alledem kann nicht ausgeschlossen werden, dass in Einzelfällen der Umfang der Datenverarbeitung aufgrund einer kritischen Überprüfung im Nachhinein auch anders beurteilt werden kann. Hierbei ist aber zu berücksichtigen, dass die in Rede stehenden Verfahrensweisen auf der Grundlage überwiegend prognostischer Einschätzungen zu sehen sind.

Zusammenfassend ist festzustellen, dass, auch soweit der Darstellung der LfD nicht gefolgt wird, deren Bewertungen dennoch als Anregung an die Behörden mit dem Ziel weitergege-

ben werden, die eigene Praxis unter datenschutzrechtlichen Gesichtspunkten auch in Zukunft aufmerksam und kritisch zu überprüfen.

3. Unterpunkt: Datenübermittlung durch den polizeilichen Staatsschutz an den Verfassungsschutz (Seite 63)

Die Ausführungen der LfD bezüglich der Weitergabe der Informationen über die Anmeldung von Versammlungen laufen im Ergebnis darauf hinaus, dass der Staatsschutz und in der Folge der von dort zu informierende Verfassungsschutz nur dann Meldungen erhalten sollen, wenn "im Einzelfall konkrete Anhaltspunkte für Staatsschutzdelikte oder sonstige politisch motivierte Straftaten vorliegen" (S. 63, 1. Unterpunkt). Diese Forderung verkennt die Aufgabenstellung des Verfassungsschutzes. Der Verfassungsschutz hat Informationen zu Bestrebungen im Sinne des § 3 VSG NW zu sammeln und auszuwerten. Die Verfassungsschutzrelevanz bemisst sich demnach nicht nach der "Friedlichkeit" einer Versammlung oder der Frage, ob in diesem Zusammenhang Straftaten zu erwarten sind, sondern danach, ob eine Versammlung eine Aktivität im Rahmen einer Bestrebung im Sinne des § 3 Abs. 1 VSG NW ist, solche Aktivitäten unterstützen soll oder Anlass zu Aktivitäten von verfassungsfeindlichen Bestrebungen ist. Hat eine Versammlung nach diesen Kriterien Verfassungsschutzrelevanz, hat der Verfassungsschutz alle Informationen zu sammeln und auszuwerten, die der Aufklärung der verfassungsfeindlichen Bestrebung dienen, insbesondere ihrer Organisation, Vorgehensweise, Personenstärke und Struktur.

Im Tätigkeitsbericht (S. 64, letzter Absatz, und S. 65, 1. Absatz) wird u.a. ausgeführt, dass die geschilderten Verfahrensweisen das Bestreben deutlich machten, dass der Umfang der Erkenntnisse über Anmelderinnen und Anmelder sowie Teilnehmerinnen und Teilnehmer von Versammlungen zwischen Verfassungsschutz und Staatsschutz identisch sein solle. Dies entspricht nicht der Praxis. Weder weiß der Verfassungsschutz, was dem Staatsschutz über Anmelder und Teilnehmer von Versammlungen alles bekannt ist, noch umgekehrt. Übermittlungen erfolgen jeweils nur im Rahmen der gesetzlichen Vorgaben. Durch den Verfassungsschutz werden dem Staatsschutz nur insoweit Erkenntnisse übermittelt, als dies für dessen Aufgabenerfüllung erforderlich ist. In concreto liegen dem Verfassungsschutz häufig über einzelne Demonstrationsanmelder viel mehr Erkenntnisse vor, als dem Staatsschutz mit-

geteilt werden. Diesem werden in der Regel nur die zur Gefahrenabwehr erforderlichen Erkenntnisse mitgeteilt. Im Hinblick auf die Datenübermittlung durch den Staatsschutz an den Verfassungsschutz wird der Eindruck erweckt, dass beim polizeilichen Staatsschutz der Grundsatz zu gelten scheine, "Staatsschutzrelevanz gleich Verfassungsschutzrelevanz". Dies trifft nicht zu und wird beim Staatsschutz so auch nicht gesehen. Aus dem Umstand, dass die Polizei weitgehend ihren Informationsverpflichtungen aus § 16 Abs. 1 Satz 2 VSG NW nachkommt, derartige Rückschlüsse zu ziehen, ist nicht gerechtfertigt.

Nicht geteilt wird auch die Auffassung der LfD, wonach es auf die **objektive** Erforderlichkeit der Datenübermittlung ankommen soll. Inwieweit eine Information tatsächlich Relevanz hat, kann oft nur im Nachhinein beurteilt werden. Deshalb stellt z.B. auch § 28 Abs. 2 Polizeigesetz NW für die Datenübermittlung im Bereich der Gefahrenabwehr darauf ab, ob - im Übermittlungszeitpunkt - die Kenntnis der Daten zur Aufgabenerfüllung erforderlich **erscheint**. Die Feststellung, ob die Übermittlung objektiv erforderlich **ist**, liegt in den problematisierten Fällen somit nach eindeutiger Rechtslage nicht im Verantwortungsbereich der Polizei. Die Prüfung der objektiven Verfassungsschutzrelevanz fällt dem Verfassungsschutz zu und kann auch nur dort sachgerecht durchgeführt werden. Dabei ergibt sich aus der Tatsache, dass die Polizeibehörden nicht über die gleiche Informationsbasis über extremistische Bestrebungen verfügen wie der Verfassungsschutz, dass die endgültige Bewertung durch den Verfassungsschutz auch zu dem Ergebnis kommen kann, dass trotz anfänglicher Hinweise auf extremistische Bestrebungen im Einzelfall keine Verfassungsschutzrelevanz gegeben ist.

Wird bei der Prüfung der Übermittlungspflichten der Polizeibehörden nach § 16 Abs. 1 VSG NW der Begriff der Verfassungsschutzrelevanz in der hier beschriebenen Weise zutreffend zugrunde gelegt und dementsprechend die von der LfD geforderte "Einzelfallprüfung" durchgeführt, erübrigt sich die Diskussion über eine "Verlagerung" der Prüfung der Zulässigkeit der Übermittlung auf die Verfassungsschutzbehörden. Es muss dann weiterhin eine Übermittlung der Daten zu angemeldeten Versammlungen erfolgen, die einen thematischen oder personellen Bezug zu Bestrebungen im Sinne des § 3 Abs. 1 VSG NW erkennen lassen, unabhängig von einer erkennbaren Staatsschutzrelevanz bzw. der zu erwartenden Friedlichkeit oder Unfriedlichkeit der Veranstaltung. Letztlich handelt es sich um eine anlassbezogene Datenübermittlung auf Grundlage von § 16 Abs. 1 VSG NW bzw. § 28 Abs. 1 u. Abs. 2 Poli-

zeigesetz NW. Eine **regelmäßige** Datenübermittlung im Sinne des § 9 Abs. 8 DSG NW findet somit nicht statt.

Im Übrigen handelt es sich bei den Mitteilungen durch den polizeilichen Staatsschutz an den Verfassungsschutz im Zusammenhang mit Demonstrationen in vielen Fällen um Erkenntnisanfragen der Polizei, die nicht beantwortet werden könnten, wenn sie keine personenbezogenen Daten enthielten.

5. Unterpunkt: Relevanzprüfung durch den Verfassungsschutz (Seite 64)

Die Relevanzprüfung kann in den unterschiedlichen Bereichen des Verfassungsschutzes im Ergebnis zu unterschiedlichen Relationen von relevanten zu irrelevanten Daten führen. Dies ist bedingt durch Unterschiede vor allem in den Strukturen und Aktionsformen der vom Verfassungsschutz beobachteten Bestrebungen und liegt somit in der Natur der Sache.

Im mittleren Absatz auf Seite 64 des Tätigkeitsberichts ist in diesem Zusammenhang davon die Rede, dass in einem Bereich des Verfassungsschutzes davon ausgegangen werde, dass ca. 80 % der Staatsschutzmeldungen für den Verfassungsschutz nicht verwertbar seien. Es dürfte sich hierbei um die missverständliche Wiedergabe einer Information aus dem Bereich des Rechtsextremismus anlässlich eines Kontrollbesuchs der LfD handeln. Im Kontext des Tätigkeitsberichts wird damit der Eindruck erweckt, dass sich dies auf Anmelder und Teilnehmer an Versammlungen beziehe. Die entsprechenden Angaben bezogen sich jedoch ganz allgemein auf das Gesamtaufkommen der Staatsschutzmeldungen im Bereich des Rechtsextremismus; ins Auge gefasst wurden hierbei insbesondere die zahlreichen Meldungen über rechtsextremistische Schmierereien durch unbekannte Personen und über Propagandadelikte durch zum Teil ebenfalls unbekannte Täter. Diese haben einen Aussagewert hinsichtlich allgemeiner Entwicklungstendenzen, nicht aber bezüglich personenbezogener Daten.

Im Übrigen können bei einer einzigen Veranstaltung einzelne Aufgabenbereiche des Verfassungsschutzes unterschiedlich betroffen sein. Im Hinblick auf Teilbereiche des politischen Extremismus ist auch die Information des Verfassungsschutzes über beabsichtigte nichtextremistische Veranstaltungen von Bedeutung, da häufig nur dann geprüft werden kann, ob

Extremisten hiergegen gerichtete Störaktionen planen (z.B. gegen Veranstaltungen der CDU im Bundestagswahlkampf 1998 oder im Rahmen der Unterschriftenkampagne). Soweit der Verfassungsschutz auch über Veranstaltungen nicht extremistischer Organisationen und Personen unterrichtet wird, geschieht dies in aller Regel ausdrücklich mit der Intention, etwaige Gegenaktionen von Extremisten in Erfahrung zu bringen, welche die ordnungsgemäße Durchführung gefährden könnten. Dieses Vorgehen beeinträchtigt das Grundrecht nicht, sondern schützt den Grundrechtsträger bei der Verwirklichung seines Grundrechts. Die Datenübermittlung dient somit gerade dem Schutz des Grundrechts auf Versammlungsfreiheit.

Zum anderen kommt es im Bereich der kampagnenbezogenen Arbeit häufig vor, dass Versammlungen durch unverdächtige Organisationen veranstaltet bzw. durch unverdächtige Personen angemeldet werden und voraussichtlich friedlich verlaufen. Verfassungsschutzrelevant sind diese Veranstaltungen unter dem Aspekt der Beeinflussung durch extremistische Gruppierungen und der Frage, inwieweit taktische Bündnisse mit unverdächtigen Organisationen und Personen gezielt zur Erreichung extremistischer Ziele eingesetzt werden, z.B. indem man sich durch die beschriebene Vorgehensweise größere Akzeptanz in der Öffentlichkeit erhofft. Aus den mit der Anmeldung einer Versammlung vorliegenden Informationen lässt sich die Verfassungsschutzrelevanz zunächst häufig nur aufgrund thematischer Bezüge erkennen. Dies muss für die die Anmeldung entgegennehmende Stelle – nach entsprechender Prüfung - Anlass genug sein, eine Übermittlung aller die Veranstaltung betreffenden Daten an den Verfassungsschutz nach § 16 Abs. 1 Satz 2 VSG NW vorzunehmen. Eine weitere Klärung der Verfassungsschutzrelevanz erfolgt dann nach Prüfung und Abgleich mit weiteren dem Verfassungsschutz vorliegenden Informationen. Dies ist Aufgabe des Verfassungsschutzes und Inhalt seiner Arbeit.

Die Begriffswahl der LfD ("Erst- und Einzeltäter") ist mit der gesetzlichen Aufgabenstellung des Verfassungsschutzes nicht vereinbar. Verfassungsschutzrelevanz steht nicht in Korrelation zu Straftaten.

Verarbeitung der mitgeteilten Daten durch den Verfassungsschutz (Seite 65, 2. Absatz)

Die Bewertung der LfD, dass ein sehr hoher Anteil der an den Verfassungsschutz übermittelten personenbezogenen Datensätze von Anmeldern und Teilnehmern von Versammlungen zur Aufgabenerfüllung des Verfassungsschutzes objektiv nicht erforderlich sei, ist zu pauschal und nicht gerechtfertigt.

Neben der Frage, welche Versammlungsdaten die Polizei an den Verfassungsschutz melden soll, problematisiert die LfD schließlich die Frage des Umgangs mit den gemeldeten Daten beim Verfassungsschutz.

Im letzten Absatz auf Seite 62 wird im Abschnitt 3.6.5 beklagt, dass für Anmelderinnen und Anmelder von Versammlungen das Risiko bestehe, zehn Jahre lang bei Polizei und Verfassungsschutz gespeichert zu sein, selbst wenn die angemeldete Versammlung friedlich, "d.h. ohne zusätzliche polizeiliche oder verfassungsschutzrelevante Erkenntnisse, verlaufen ist". Hierdurch wird der Eindruck erweckt, alle gemeldeten Teilnehmerdaten würden hier für den Zeitraum von zehn Jahren gespeichert. Im ersten Absatz auf Seite 63 des Berichts wird Entsprechendes für die Teilnehmerinnen und Teilnehmer von derartigen Versammlungen moniert, wenn auch nach dem Wortlaut lediglich die entsprechende Praxis des Staatsschutzes und dessen Übermittlung an den Verfassungsschutz, nicht aber die Speicherungspraxis des Verfassungsschutzes selbst, kritisiert wird.

Zunächst ist klarzustellen, dass die Speicherung von Anmelderinnen und Anmeldern von Versammlungen extremistischer Organisationen im Einklang mit der derzeitigen Gesetzeslage erfolgt. Ob eine Versammlung "friedlich" und ohne die Begehung von Straftaten verläuft, besagt zunächst gar nichts über eine mögliche Verfassungsschutzrelevanz. Bestrebungen im Sinne von § 3 Abs. 1 VSG NW müssen nicht notwendigerweise mit der Begehung von Straftaten einhergehen.

Die nach entsprechender Prüfung als verfassungsschutzrelevant bewerteten Informationen werden entsprechend den oben zu Ziffer 3.6.4. ausgeführten Kriterien behandelt. Das heißt, dass eine Speicherung in der elektronischen Personendatei erfolgt, wenn Personen hier bereits

als einer extremistischen Bestrebung zugehörig gespeichert sind oder sich bei bisher hier unbekannten Personen aus dem Sachzusammenhang tatsächliche Anhaltspunkte für den Verdacht extremistischer Bestrebungen ergeben. Im letztgenannten Fall der Erstspeicherung werden grundsätzlich kurze Speicherungsfristen vorgesehen.

Eine Speicherung von Demonstrationsanmeldern extremistischer Organisationen erfolgt beim Verfassungsschutz in aller Regel nicht für zehn Jahre, sondern je nach betroffener Organisation für zwei bis fünf Jahre. Im Bereich des Rechtsextremismus beispielsweise stammt die ganz überwiegende Anzahl von Versammlungsanmeldungen aus dem Bereich der rechtsextremistischen Parteien. In diesen Fällen ist die Löschungsfrist meistens mit zwei Jahren zu bemessen. Bei Versammlungsanmeldungen aus dem Neonazibereich, die allerdings in der jüngeren Vergangenheit extrem selten waren, ist die Frist allerdings häufig mit fünf Jahren zu bemessen. Eine Löschung nach Ablauf dieser Fristen ist jedoch selbstverständlich davon abhängig, dass nach der entsprechenden Speicherung keine weiteren neuen Erkenntnisse angefallen sind.

Ergeben sich bei Prüfung der übermittelten Daten dagegen keine Anhaltspunkte für extremistische Bestrebungen der Anmelder einer Versammlung, werden deren Daten nicht in der elektronischen Personendatei gespeichert, auch wenn die Veranstaltung im oben beschriebenen Sinne durch extremistische Gruppierungen beeinflusst wird oder der Versuch der Beeinflussung stattfindet.

Soweit Meldungen über Versammlungen nach weiterer Prüfung als nicht verfassungsschutzrelevant betrachtet werden, werden sie hier vernichtet bzw. gelöscht. Die von der LfD vorgeschlagene "Rückgabe" von Unterlagen wäre in diesem Fall weder zweckmäßig noch ausreichend, da die betreffenden Meldungen durch elektronische Post übermittelt werden, die Vernichtung der betreffenden Daten also nur durch Löschung beim Verfassungsschutz erfolgen kann.

Zu 3.7 Polizeiliche Datenverarbeitung – Spiel ohne Grenzen? (Seite 66)

Zu 3.7.1 Schengener Informationssystem (SIS) (Seite 66)

Der Bericht stellt an dieser Stelle durchaus zutreffend Rechtsgrundlagen, Inhalte und Aufgabenstellung des Schengener Informationssystems (SIS) dar. Ebenfalls zu Recht stellt der Bericht unter Ziffer 3.7.1.4 fest, dass die Datenschutzkontrolle durch ein völkerrechtlich und gesetzlich festgelegtes Gremium, die sogenannte „Gemeinsame Kontrollinstanz", wahrgenommen wird. Im Folgenden zitiert der Bericht lediglich Feststellungen der Gemeinsamen Kontrollinstanz. Ein Bezug zum Tätigwerden nordrhein-westfälischer öffentlicher Stellen oder eine Betroffenheit nordrhein-westfälischer Bürger wird nicht festgestellt. Die Abstellung ggf. festgestellter Mängel wäre nicht Angelegenheit der Landesregierung. Entscheidend ist hier das Tätigwerden des Bundesbeauftragten für den Datenschutz, der, zusammen mit dem hessischen Datenschutzbeauftragten als Vertreter der Länder, deutsches Mitglied in der Gemeinsamen Kontrollinstanz ist.

Zu 3.7.2 Europol – Strafrechtliche Immunität der Europol-Angehörigen (Seite 71)

Der Bericht kommentiert an dieser Stelle die Rechtsentwicklung und das Gesetzgebungsverfahren hinsichtlich der Europol-Konvention und des Gesetzes über das sogenannte „Europol-Immunitäten-Protokoll".

Dieser Berichtsteil gibt lediglich einen Teil der Argumente wieder, die während des Gesetzgebungsverfahrens zu den Europol-Gesetzen von einem Teil der öffentlichen Meinung vorgebracht wurden. Die Landesregierung sieht daher von einer Stellungnahme ab.

Zu 3.8 Überwachung auf Schritt und Tritt? (Seite 76)

Zu 3.8.2 Identifizierung mit Hilfe von Fotos (Seite 80)

Hier führt der Bericht auf Seite 81 unten aus, dass bei der Verfolgung einer Verkehrsordnungswidrigkeit vor einer Identifizierung anhand des Personalausweisregisters die Polizei vergeblich versucht haben muss, eine Identifizierung durch Befragung anderer Personen vorzunehmen. Dies ist nach Auffassung der Landesregierung nicht mit dem Grundsatz der Verhältnismäßigkeit zu vereinbaren, wonach bei mehreren Möglichkeiten des Eingriffs in das Persönlichkeitsrecht des Betroffenen nur der geringstmögliche Eingriff zulässig ist. Dass ein Lichtbildabgleich bei einer zu Amtsverschwiegenheit verpflichteten Behörde einen geringeren Eingriff darstellt als die Befragung der Nachbarschaft durch Polizeibeamte, dürfte auf der Hand liegen (vgl. Schäpe, Grenzen der Fahrerermittlung durch die Behörde, DAR 1999, 186 ff.). Der Bitte, ihre datenschutzrechtlichen Bedenken gegen diese Rangfolge zu begründen, ist die LfD bisher nicht nachgekommen.

Zu 4. Die Bürgerinnen und Bürger und die Justiz (Seite 83)

Zu 4.5 Formulare bei Familiengerichten (Seite 85)

Der dargestellte Problembereich, die Verwendung von Formularen in der Familiengerichtsbarkeit, ist im Sinne der LfD behandelt worden und daher nicht Gegenstand einer Beanstandung. Im Übrigen dürfte sich die Angelegenheit mit Inkrafttreten des Kindesunterhaltsgesetzes am 1. Juli 1998 erledigt haben. § 643 ZPO n. F. regelt Einzelheiten der prozessualen Auskunftspflicht der Parteien und bestimmter Dritter in Unterhaltsverfahren, insbesondere auch die Pflicht des Gerichtes, die Partei auf die Möglichkeit, bei den in der Vorschrift genannten Dritten Auskünfte einzuholen, hinzuweisen. Es gibt aber – auch eingedenk des Bestrebens, praktikable und einvernehmliche Lösungen zu erreichen – Anlass, darauf hinzuweisen, dass nach der Auffassung der Landesregierung, die vom Justizministerium auch bei Bearbeitung des dem Bericht zugrundeliegenden konkreten Vorganges geäußert wurde, ein Kontrollrecht der LfD in dieser Frage nicht bestand, da keine Verwaltungsaufgaben nach § 2 Abs 1 Satz 2 DSG NW tangiert waren. Vielmehr gehört die Entwicklung und Versendung von Formularen zur Einholung von Einkommensauskünften in Unterhaltsverfahren zur Rechtspflegetätigkeit. Rechtspflegeaufgaben sind Rechtsprechungsaufgaben und zusätzlich die ihnen nur mittelbar dienenden – sie vorbereitenden oder ihnen nachfolgenden – Sach- und Verfahrensentscheidungen, wie sie von der höchstrichterlichen Rechtsprechung in den Schutzbereich der richterlichen Unabhängigkeit einbezogen werden (vergleiche BGH, Beschluss vom 30. Juli 1990 – NotZ 19/89 -, NJW 1991, 568 f). Entwicklung und Einsatz der Formulare gehören – im Rahmen der Gesetze – zur Aufbereitung des streitentscheidenden Sachverhaltes durch das Gericht.

Zu 5. Bürgerämter (Seite 87)

Zu 5.1.1 Das neue Melderecht (Seite 87)

Zu **Gruppenauskünften an Parteien** im Zusammenhang mit Wahlen wendet sich die LfD unter Hinweis auf einen Beschluss des OVG Magdeburg gegen die von der Landesregierung in der Antwort auf die Kleine Anfrage 1116 vertretene Auffassung, derartige Auskünfte dürften von den Meldebehörden angesichts des meldegesetzlichen Widerspruchsrechts der Betroffenen nicht aus Gründen des Datenschutzes abgelehnt werden. Das OVG Magdeburg beruft sich für seine gegenteilige Auffassung u.a. auf einen Beschluss des OVG Münster vom 23. Mai 1989. Zwar hatte das OVG Münster in diesem Beschluss Datenschutzaspekte als Ablehnungsgrund anerkannt, jedoch hatte der Gesetzgeber zum Zeitpunkt dieser Gerichtsentscheidung das Widerspruchsrecht noch nicht in das Meldegesetz NW aufgenommen. Der Beschluss des OVG Münster kann daher die Auffassung des OVG Magdeburg nicht stützen.

Die von der LfD zitierte Textpassage aus dem Beschluss des OVG Magdeburg trägt nicht dem Umstand Rechnung, dass der Gesetzgeber in Sachsen-Anhalt – vergleichbar wie der Gesetzgeber in Nordrhein-Westfalen – im Landesmeldegesetz ausdrücklich geregelt hat, in welcher Weise die Bürgerinnen und Bürger von ihrem Widerspruchsrecht unterrichtet werden sollen. Der Ausgleich etwaiger Wahrnehmungsdefizite bei Betroffenen durch datenschutzrechtlich begründete Versagung von Auskünften an Parteien liefe auf eine Korrektur der dem Ermessen vorgelagerten Entscheidung des Gesetzgebers zum Informationsverfahren hinaus. Eine derartige Versagung wäre auch in der Sache nicht mit der Wertung des Gesetzgebers zu vereinbaren, dem Parteienprivileg angemessen Rechnung zu tragen und demgemäß Parteien und anderen Trägern von Wahlvorschlägen unter Beachtung des Gleichheitssatzes Auskünfte durch Meldebehörden zu ermöglichen. Insoweit hält das OVG Brandenburg in seinem Beschluss vom 24. September 1998 (DÖV 1999,35) zu Recht fest, in Ansehung der den Parteien in Art. 21 GG eingeräumten Stellung als verfassungsrechtliche Institution müssten die Parteien gerade im Vorfeld von Wahlen grundsätzlich die Möglichkeit haben, in verschiedenster Form direkt mit dem Wähler in Kontakt zu treten.

Die Auffassung der LfD, durch die Erweiterung des Kreises der im automatisierten Abrufverfahren berechtigten Datenempfänger in der **Meldedatenübermittlungsverordnung NW** (MeldDÜV NW) sei eine Tendenz in Richtung eines übergreifenden Einwohnerinformationssystems fortgesetzt worden, wird nicht geteilt. Zusätzlich abrufberechtigt durch die Änderung der MeldDÜV NW im Jahre 1997 wurden lediglich die Staatsanwaltschaften und Gerichte sowie die Leitstellen für den Feuerschutz und den Rettungsdienst. Insoweit dürfen nur die Adressdaten, der Tag der Geburt und Übermittlungssperren abgerufen werden. Die nach der MeldDÜV NW abrufberechtigten Stellen dürfen allein bilateral im Verhältnis zur Meldebehörde bestimmte, in der Verordnung jeweils enumerativ aufgeführte Meldedaten abrufen, dies auch nur, wenn die Kenntnis der Daten im Einzelfall zur Erfüllung der ihnen übertragenen Aufgaben erforderlich ist. Der Gesetzgeber hat im Meldegesetz die Einrichtung automatisierter Abrufverfahren ausdrücklich zugelassen. Derartige Verfahren werden dem Datenschutz prinzipiell besser gerecht als regelmäßige Datenübermittlungen herkömmlicher Art, bei denen die Meldebehörden von sich aus ganze „Datenpakete" versenden.

Zu der Ansicht der LfD bezüglich des von ihr genannten Beispielsfalles zur **Speicherung der Religionszugehörigkeit**, eine Löschung wäre rechtlich ebenso vertretbar gewesen, ist auf die Regelung in § 7 Satz 3 MG NW zu verweisen. Danach entfällt die Prüfung der Beeinträchtigung schutzwürdiger Interessen, wenn die Verarbeitung (u.a. die Datenspeicherung) durch Rechtsvorschrift vorgeschrieben ist. Dies war vorliegend der Fall, denn die Speicherung der Religionszugehörigkeit gehört zu dem Katalog der nach § 3 Abs. 1 MG NW im Melderegister zu speichernden Daten. Die Meldebehörde hielt sich daher an die bindenden Vorgaben des Gesetzgebers. Es kann davon ausgegangen werden, dass die Angabe der Religionszugehörigkeit von den Meldebehörden allgemein nach Recht und Gesetz verwendet wird.

Zu 6. Ausländerinnen und Ausländer (Seite 93)

Zu 6.2 Der Echtheitsgrad von Ehen (Seite 93)

Die Verfahrensweise der Ausländerbehörden im Zusammenhang mit der Frage nach dem Echtheitsgrad von Eheschließungen binationaler Paare ist nach den Ermittlungen des Innenministeriums nicht zu beanstanden.

Die befragten Ausländerbehörden verfahren entsprechend der Lage des Einzelfalles. Grundsätzlich finden Überprüfungen nur statt, wenn konkrete und ausreichende Verdachtsmomente dafür bestehen, dass eine Ehe nur geschlossen wurde, um einen Aufenthaltstitel für einen Partner zu erlangen. Solche Verdachtsmomente können unterschiedliche Meldeanschriften der Ehepartner sein, sofern die Eheleute hierfür keine plausible Erklärung abgeben, oder sich aus glaubwürdigen Angaben Dritter ergeben. Als nicht ausreichend angesehen wurde etwa ein großer Altersunterschied der Eheleute oder die Tatsache, dass ein Abschiebeverfahren durch die Eheschließung unterbrochen wird, sofern diese Anhaltspunkte allein vorliegen.

Auch die Ermittlungsmaßnahmen werden dem Einzelfall angemessen gestaltet. Als Maßnahmen wurden Gespräche mit einem oder beiden Partnern, getrennte Befragungen der Eheleute oder auch im Einzelfall Hausbesuche (nur mit Einwilligung der Wohnungsinhaber) genannt.

Die Ausländerbehörden orientieren sich auch an der im Amtsblatt Nr. C 382 der Europäischen Gemeinschaften vom 16.12.1997 veröffentlichten Entschließung des Rates vom 04.12.1997 über Maßnahmen zur Bekämpfung von Scheinehen, die u.a. verschiedene Anhaltspunkte für den Verdacht einer Scheinehe auflistet.

Angesichts dessen und der Tatsache, dass Eingriffsschwelle und erforderliche Maßnahmen immer dem Einzelfall angepasst werden müssen, hält die Landesregierung eine generelle Regelung nicht für erforderlich. Dies hat das Innenministerium der LfD bereits im März 1999 mitgeteilt.

Zu 6.4 Familienzusammenführung mit unzulänglichem Datenschutz (Seite 95)

Mit Erlass vom 04.02.1998 (Az. I B 2/43.337) hat das Innenministerium die Ausländerbehörden in Nordrhein-Westfalen darüber unterrichtet, dass von Seiten der Universität Münster zum Nachweis von Verwandtschaftsverhältnissen ein Speicheltest angeboten wird. Datenschutzrechtliche Verfahrensregelungen wurden in dem Erlass nicht getroffen.

Der Speicheltest wird ausschließlich auf freiwilliger Basis durchgeführt. Die Ausländerbehörde erhält nur dann von dem Betroffenen das entsprechende Gutachten, sofern dieser es als Beweismittel im Sinne des § 70 AuslG vorlegen will. Die Ausländerbehörden entscheiden lediglich über die Eignung als Beweismittel im aufenthaltsrechtlichen Verfahren zur Familienzusammenführung.

Die Datenverarbeitung im Rahmen des Speicheltests selbst sowie die damit verbundene Einhaltung datenschutzrechtlicher Bestimmungen obliegt der den Test durchführenden Einrichtung.

Zu 7. Sozialbereich (Seite 98)

Nach Auffassung der LfD bröckelt das Sozialgeheimnis. In diesem Zusammenhang weist sie auf zwei im Jahre 1998 in Kraft getretene Rechtsänderungen hin (Änderung des § 68 Abs. 1 Satz 1 des Zehnten Buches Sozialgesetzbuch – SGB X – und Sozialhilfedatenabgleichsverordnung zu § 117 BSHG).

Die ablehnende Haltung der LfD gegenüber der Änderung des § 68 SGB X wird von der Landesregierung nicht geteilt. Die Übermittlungsbefugnis nach dieser Vorschrift ist auf Ersuchen im Einzelfall beschränkt, so dass jedenfalls Regelanfragen oder ganze Fahndungslisten bei den Sozialleistungsträgern unzulässig sind. Wie bisher hat der ersuchte Sozialleistungsträger die Grenzen der Amtshilfe nach § 4 Abs. 3 SGB X zu beachten, insbesondere wenn durch die Amtshilfe die Erfüllung seiner eigenen Aufgaben ersichtlich gefährdet würde. Über § 4 Abs. 3 SGB X hinaus ist die ersuchte Sozialbehörde nach § 68 Abs. 1 Satz 2 SGB X zur Auskunftserteilung auch dann nicht verpflichtet, wenn sich die ersuchende Stelle die Angaben auf andere Weise beschaffen kann. Wie bisher darf ferner kein Grund zur Annahme bestehen, dass durch die Auskunftserteilung schutzwürdige Interessen der Betroffenen beeinträchtigt werden.

Eine besonders sorgfältige Interessenabwägung ist bei Auskunftsersuchen geboten, welche die Klientel des Jugendamtes betreffen. Die Erfahrung der Praxis zeigt, dass immer dann, wenn das Jugendamt Kontakt mit gefährdeten Jugendlichen und jungen Erwachsenen hat und damit die Nähe zur Polizei gegeben ist, die Gefahr besteht, dass das Vertrauensverhältnis in ein Misstrauensverhältnis übergeht und eine perspektivische pädagogische Arbeit nicht mehr möglich ist. Solche Fälle müssen von beiden Seiten mit Sensibilität behandelt werden.

Zur Sozialhilfedatenabgleichsverordnung, die auf § 117 Abs. 1 und 2 BSHG beruht, ist anzumerken, dass die Bundesregierung diese Verordnung u. a. mit dem Bundesbeauftragten für den Datenschutz abgestimmt hat, um datenschutzrechtliche Gesichtspunkte zu berücksichtigen. So ist z. B. in die Rechtsverordnung die Verpflichtung zur unverzüglichen Löschung der zum Abgleichsverfahren gespeicherten Daten nach Abschluss des Datenabgleichs aufge-

nommen worden. Bei den bisher durchgeführten Datenabgleichen sind der Landesregierung bislang keine Probleme bekannt geworden.

Zu 7.1 Sozialämter schießen über das Ziel hinaus (Seite 99)

Die Auffassung der LfD hinsichtlich der Auskunftsermächtigungen über Kontenbewegungen bei Banken und Sparkassen wird geteilt.

Zu 7.2 Prüfung von Pflegeleistungen (Seite 100)

Die LfD hält die leistungsscharfe Abrechnungspraxis im Bereich der professionellen ambulanten Pflege für problematisch. Bezugspunkt für die Auffassung der LfD ist die Rahmenvereinbarung zwischen Leistungsanbieter- und Kostenträgerseite nach § 89 SGB XI. Diese Vereinbarung setzt auf der Landesebene die bundesgesetzlichen Vorgaben über die Vergütung erbrachter ambulanter Sachleistungen um, für das Abrechnungsverfahren gelten hingegen die Vorschriften der §§ 94 Abs. 1, 104, 105 SGB XI.

Die Leistungserbringer sind danach berechtigt und verpflichtet, im Falle der Abrechnung pflegerischer Leistungen die für die Erfüllung der Aufgaben der Pflegekassen und ihrer Verbände erforderlichen Angaben über die Leistungen aufzuzeichnen und den Kassen oder den Verbänden zu übermitteln. In den Abrechnungsunterlagen sind die erbrachten und abrechnungsfähigen Leistungen unter anderem nach Art, Menge und Preis anzugeben. Einzelheiten über das Verfahren sind hierbei nach § 105 Abs. 2 SGB XI von den Spitzenverbänden der Pflegekassen im Einvernehmen mit den Verbänden der Leistungserbringer festzulegen.

Die Vereinbarung nach § 89 SGB XI über ambulante Pflegesachleistungen für das Land Nordrhein-Westfalen begründet hingegen in erster Linie den Vergütungsanspruch für den einzelnen Pflegedienst gegenüber den Pflegekassen für erbrachte Leistungen. Die Leistungen werden dabei, entsprechend den Bundesempfehlungen der Spitzenverbände der Pflegekassen vom 8. November 1996, in sogenannten Leistungskomplexen ausdifferenziert, die sich eng am Pflegebegriff des § 14 SGB XI orientieren. Bereits hier finden sich diejenigen Verrichtungen, insbesondere im Bereich der Körperhygiene, die von der LfD problematisiert werden.

Diese Art der Vergütungskonkretisierung ist, neben möglichen anderen Varianten (z. B. Einzelverrichtungsbeschreibung), gemäß § 89 Abs. 3 SGB XI zulässig. Zudem gilt für das Vergütungsverhandlungsgeschehen im Rahmen des SGB XI das Vereinbarungsprinzip, so auch für den ambulanten Bereich (§ 89 Abs. 1 SGB XI).

Festzuhalten ist also zunächst, dass die Vereinbarungspartner in Nordrhein-Westfalen nach § 89 SGB XI im Rahmen des geltenden Bundesrechts zu einer der Vergütung zugrundeliegenden Leistungsbeschreibung gekommen sind. Eine in diesen Kontext fallende Entscheidung des Sozialgerichts Düsseldorf, mit dem die Rahmenvereinbarung aufgehoben worden ist, kann an dieser Auffassung auch keinen weiteren Zweifel begründen, da lediglich die nicht ausreichende Begründung der Schiedsstellenentscheidung streitentscheidend war. Ein aufsichtsrechtliches Einschreiten im Hinblick auf die Vereinbarung nach § 89 SGB XI kommt daher mangels Rechtsverletzung des SGB XI, auch hinsichtlich der aufgrund des Urteils des Sozialgerichts Düsseldorf zu erwartenden Neuvereinbarung, nicht in Betracht. Darüber hinaus ist zu beachten, dass durch die Landesaufsicht nur auf die landesunmittelbaren Kassen zugegriffen werden könnte, nicht jedoch auf bundesunmittelbare Pflegekassen (Knappschaft etc.) oder die Leistungsanbieterseite.

Ebensowenig kommt ein Einschreiten gegen das in Nordrhein-Westfalen praktizierte Abrechnungsverfahren in Betracht, welches sich strikt an den Vorgaben der §§ 94, 104 f. SGB XI orientiert. So werden nach Auskunft der AOK Rheinland Abrechnungsvordrucke verwandt, die für den einzelnen Versicherten lediglich Bezug auf die Leistungskomplexe, das Datum sowie die Menge der erbrachten Leistungen enthalten. Die Pflegedokumentation verbleibt beim Versicherten und würde nur bei begründeten Zweifeln mit Einverständnis des betroffenen Versicherten angefordert werden. Begründete Zweifel könnten etwa bei Anhaltspunkten für Leistungsmissbrauch oder gefährlicher Pflege entstehen. Nicht zutreffend ist in diesem Zusammenhang die Feststellung der LfD, nur der Medizinische Dienst der Krankenversicherung (MDK) könne die in der Pflegedokumentation enthaltenen personenbezogenen Daten durch Einsichtnahme zur Kenntnis nehmen; vielmehr hat der MDK gemäß § 80 Abs. 4 SGB XI auch die Befugnis, diese Daten im Rahmen der Qualitätsprüfung an die beauftragende Pflegekasse weiterzuleiten.

Die LfD wird in Kürze über diese Rechtsauffassung unterrichtet werden. Darüber hinaus wird ihr vorgeschlagen werden, zu den bislang geltenden bundesgesetzlichen Bestimmungen über das Abrechnungsverfahren bei professionellen Pflegeleistungen Alternativen abzustimmen, um diese im Wege einer anstehenden technischen Novelle des SGB XI über den Bundesrat in das Gesetzgebungsverfahren einzubringen.

Zu 7.3 Datenabrufe erfordern Ermittlungsbefugnisse (Seite 101)

Die LfD äußert Bedenken gegen ein Modellprojekt der Versorgungsverwaltung, mit dem eine verbesserte Zusammenarbeit zwischen Versorgungsämtern und Kommunen bei Auskunfts- und Beratungsleistungen nach dem Schwerbehindertengesetz angestrebt wird. Die kommunalen Beratungsstellen sollen in die Lage versetzt werden, im Rahmen einer vernetzten ADV-Lösung bei den Versorgungsämtern gespeicherte Sozialdaten abrufen zu können.

Dies vollzieht sich auf dem Hintergrund einer für den Bürger nur schwer durchschaubaren Aufgabenverteilung der beteiligten Verwaltungsträger. Die staatliche Versorgungsverwaltung vollzieht das Verfahren nach dem Schwerbehindertengesetz, stellt den Grad der Behinderung fest, entscheidet über das Vorliegen von Nachteilsausgleichen und stellt Schwerbehindertenausweise aus. Die kommunale Sozialverwaltung kann Schwerbehindertenausweise verlängern und entscheidet über die Anwendung der festgestellten Nachteilsausgleiche, wenn sie etwa Parkerleichterungen oder die Befreiung von der Rundfunkgebührenpflicht ausspricht. Zudem kommt ihr eine wichtige Rolle bei der Frage der Eingliederungshilfen für Schwerbehinderte zu.

Nach Auffassung der Landesregierung enthält das Zehnte Buch des Sozialgesetzbuchs hierzu die notwendigen rechtlichen Regelungen.

Eine Einschränkung des in § 35 SGB I formulierten Sozialgeheimnisses ist nur nach Maßgabe des 2. Kapitels des Zehnten Buches zulässig. Nach § 67 b SGB X ist die Nutzung von Sozialdaten zulässig, soweit die nachfolgenden Vorschriften des Gesetzbuches es erlauben oder soweit der Betroffene eingewilligt hat. § 69 SGB X hält eine Übermittlung von Sozialdaten

u. a. für zulässig, soweit sie erforderlich ist für die Erfüllung einer gesetzlichen Aufgabe der übermittelnden Stelle nach diesem Gesetzbuch oder einer solchen Aufgabe des Empfängers, wenn er eine in § 35 des 1. Buches genannte Stelle ist.

Beide alternativ genannten Voraussetzungen liegen in dem Modellprojekt vor. Die Versorgungsverwaltung hat die Pflicht, die Bürgerinnen und Bürger im Verwaltungsverfahren bei der Gestaltung der Anträge, bei Zweifelsfragen im laufenden Verwaltungsverfahren zu informieren und zu beraten (§§ 13 bis 15 SGB I). Darüber hinaus besteht nach § 17 SGB I eine Rechtspflicht, darauf hinzuwirken, dass jeder Berechtigte die ihm zustehenden Sozialleistungen umfassend und schnell erhält. Als übermittelnde Stelle erfüllt sie damit ihre gesetzliche Aufgabe.

Die Auskunft und Beratung ist aber auch eine gesetzliche Aufgabe des Empfängers. Die Kommune ist als Sozialleistungsträger im Sinne von § 35 SGB I rechtlich verpflichtet, anfragende Behinderte zu beraten und zu informieren.

Darüber hinaus bestimmt § 15 SGB I, dass die Kommunen – die nach Landesrecht zuständigen Auskunftsstellen – verpflichtet sind, über alle Angelegenheiten nach dem Sozialgesetzbuch Auskünfte zu erteilen. Die Auskunftspflicht erstreckt sich neben der Benennung der für die Sozialleistungen zuständigen Leistungsträger auf alle Sach- und Rechtsfragen, die für den Auskunftsuchenden von Bedeutung sein können. Um eine möglichst umfassende Auskunftserteilung sicherzustellen, sind die Kommunen verpflichtet, mit anderen Trägern zusammenzuarbeiten.

Wenn die Einrichtung eines automatisierten Verfahrens im Sinne von § 79 SGB X zwischen Sozialleistungsträgern im Sinne von § 35 SGB I zulässig ist, ist nicht erkennbar, dass schutzwürdige Interessen der Behinderten berührt sein können, wenn eine Kommune ihnen auf ihre Nachfrage Auskünfte erteilt, die sie sonst nur unter größerem Aufwand erlangen können.

Im Übrigen ist das von der LfD geforderte Datensicherheitskonzept erstellt worden.

Zu 7.6 Mehr Bürgernähe bei den Rentenversicherungsträgern (Seite 105)

Das von der LfD angesprochene Dialogverfahren der Träger der gesetzlichen Rentenversicherung war bereits Gegenstand einer Anzeige der Landesversicherungsanstalten Rheinprovinz und Westfalen nach § 80 Abs. 3 SGB X. Die beteiligten Rentenversicherungsträger haben umfangreiche technische und organisatorische Maßnahmen getroffen, um die Anforderungen der datenschutzrechtlichen Bestimmungen zu erfüllen. So wurde mit der Bundesversicherungsanstalt für Angestellte und der Bundesknappschaft eine Vereinbarung über die gegenseitige Beauftragung nach § 88 SGB X geschlossen. Der Text der Vereinbarung wurde ebenfalls mit dem Bundesversicherungsamt abgestimmt, das u. a. darauf Wert gelegt hatte, im Rahmen der Beauftragung dem anfordernden Versicherungsträger keinen unmittelbaren, verändernden Zugriff auf die Konten anderer Versicherungsträger einzuräumen.

Darüber hinaus hatte der Verband deutscher Rentenversicherungsträger im Vorfeld die datenschutzrechtlichen Probleme mit dem Bundesbeauftragten für den Datenschutz erörtert. Die vom Bundesbeauftragten vorgeschlagenen Maßnahmen haben die Landesversicherungsanstalten Rheinprovinz und Westfalen nach Feststellung des Landesversicherungsamtes umgesetzt.

Daher besteht derzeit unter datenschutzrechtlichen Gesichtspunkten kein weiterer Handlungsbedarf.

Zu 8. Gesundheit (Seite 107)

Zu 8.1 Trotz guter Zusammenarbeit noch ungelöste Probleme (Seite 107)

Bei der auf Seite 108 im zweiten Absatz angesprochenen Regelungslücke bezüglich der Übernahme von Patientenunterlagen eines verstorbenen niedergelassenen Radiologen handelt es sich zunächst um einen Einzelfall. Das Ministerium für Frauen, Jugend, Familie und Gesundheit ist derzeit darum bemüht, diesen Fall im Einvernehmen mit der betroffenen Ärztekammer zu lösen und diese zu einer freiwilligen Übernahme der Unterlagen zu bewegen.

Darüber hinaus wird im Rahmen einer Novellierung des Gesundheitsdatenschutzgesetzes Nordrhein-Westfalen geprüft werden, ob und wie eine Verpflichtung zur Übernahme und Aufbewahrung von Patientenakten durch die Ärztekammer oder eine andere öffentliche Stelle gesetzlich festgelegt werden kann.

Zu 10. Bildung und Wissenschaft (Seite 121)

Zu 10.1 Die Schulen und das Internet (Seite 121)

Zu 10.1.1 Basisinformation der Schülerinnen und Schüler (Seite 121)

Zu 10.1.2 Nutzungsordnungen (Seite 123)

Die Ausführungen der LfD entsprechen der Auffassung des Ministeriums für Schule und Weiterbildung, Wissenschaft und Forschung.

Es wird begrüßt, dass Mitarbeiterinnen und Mitarbeiter der LfD in der Projektgruppe „NRW–Schulen ans Netz" mitwirken. Insbesondere wird begrüßt, dass die Dienststelle der LfD sich an der Erarbeitung einer Internet-Nutzungsordnung für Schulen beteiligt.

Zu 10.2 Keine Wahl beim Studierendenausweis mit Chip? (Seite 124)

Die LfD fordert, im Gesetzgebungsverfahren für ein neues Hochschulgesetz müsse die gesetzliche Regelung für einen maschinenlesbaren Studierendenausweis in einzelnen konkret genannten Punkten bestimmte Mindestbedingungen erfüllen, um das Recht der Studierenden auf informationelle Selbstbestimmung zu gewährleisten. Diese Forderung kann nicht berücksichtigt werden. Es ist Aufgabe der Hochschulen, die näheren datenschutzrechtlichen Bestimmungen zum Studierendenausweis durch Satzung zu treffen. Dabei ist das Datenschutzgesetz zu beachten. Weiterer konkreter Bestimmungen im Hochschulgesetz bedarf es nicht; das würde auch dem Ziel der Deregulierung zuwiderlaufen.

Problematisch erscheint die Forderung, den Studierenden müsse die Wahl eingeräumt werden, auf die Nutzung der Chipkarte insgesamt oder einzelner ihrer Funktionen verzichten zu können. Die mit einem neugestalteten Studierendenausweis für die Erledigung der Verwaltungsaufgaben der Hochschulen verbundenen Vorteile würden wesentlich beeinträchtigt, wenn daneben andere Studierende Ausweise ohne Chip benutzen könnten.

Zu 10.3 Forschung (Seite 125)

Die Ausführungen des Tätigkeitsberichts zu diesem Punkt werden im Grundsatz auch vom Ministerium für Schule und Weiterbildung, Wissenschaft und Forschung geteilt.

Ergeben sich bei einem konkreten Forschungsvorhaben datenschutzrechtliche Bedenken, so wird unter Abwägung der in Artikel 5 Abs. 3 des Grundgesetzes gewährleisteten Freiheit der Forschung gegen den Grundsatz des Rechts auf informationelle Selbstbestimmung im Wege der verfassungsrechtlich konkordanten Auslegung eine Lösung gefunden werden müssen.

Zu 11. Öffentlicher Dienst (Seite 128)

Zu 11.1 Verlust von Personalakten (Seite 128)

Der Datenschutzbericht beschreibt, dass Personalakten einer Bezirksregierung in der Poststelle der Staatskanzlei für das damalige Ministerium für Arbeit, Gesundheit und Soziales (ohne Empfangsbestätigung) abgegeben wurden und sich dort „trotz umfangreicher Recherchen die Spur der Personalakten" verlor.

Tatsächlich konnte nicht festgestellt werden, dass die Personalakten überhaupt in der Poststelle der Staatskanzlei angekommen waren. Vor diesem Hintergrund sind ergänzende Sicherheitsvorschriften für den Transport und Versand von Personalakten nicht erforderlich.

Zu 11.2 Bewerbungsverfahren (Seite 129)

Die bundeseinheitliche Vorschrift zur ärztlichen Beurteilung der Polizeidiensttauglichkeit und der Polizeidienstfähigkeit (PDV 300) wurde überarbeitet. Dabei wurde den Bedenken der LfD Rechnung getragen, soweit dies aus medizinischer und beamtenrechtlicher Hinsicht möglich erschien.

Mit Beschluss vom 10.09.1998 hat der Arbeitskreis II „Innere Sicherheit" der IMK empfohlen, die überarbeitete Fassung der PDV 300 einzuführen. Die Auslieferung der Neufassung der PDV 300 wird erst nach Vorliegen der Einführungserlasse aller Länder und des Bundes erfolgen. Nach Eingang wird das Innenministerium der LfD ein Exemplar unaufgefordert übersenden.

Zu 11.4 Tele-Heimarbeit – Hinweise für eine datenschutzgerechte Einführung (Seite 130)

Der „Leitfaden zur datenschutzgerechten Planung und Einführung von Telearbeit“ (Abschnitte 11.4 bis 11.4.3) stimmt weitgehend mit den Vorstellungen der Landesregierung überein. Nur in einigen Punkten muss der Darstellung allgemein oder aus der Sicht einzelner Ressorts widersprochen werden.

Zu 11.4.1 Allgemeines (Seite 131)

In diesem Abschnitt wird ausgeführt, die Besonderheit der Tele-Heimarbeit liege darin begründet, dass die öffentliche Stelle die unmittelbare Verfügungsgewalt über die Daten verliere, die an Tele-Heimarbeitsplätzen bearbeitet werden. Diese Aussage ist jedenfalls für die Steuerverwaltung nicht zutreffend, soweit es sich um elektronisch gespeicherte Daten handelt. Die Daten des Besteuerungsverfahrens bleiben auch bei Tele-Heimarbeit in vollem Umfang im lokalen Netzwerk des Finanzamts erhalten. Am Arbeitsplatz findet lediglich eine Terminal-Emulation statt. Auch bei Übergang zu einer windows-orientierten Dialogverarbeitung (Projekt „WinGF“) ist im Tele-Heimarbeitsbereich an eine gleichartige Verarbeitung (Nutzung der sog. Thin-Client-Technik) gedacht. Die ordnungsgemäße Verarbeitung personenbezogener Daten der Bürgerinnen und Bürger wird also nicht dadurch berührt, dass sie von einem Arbeitsplatz außerhalb der Dienststelle des Bearbeiters geschieht.

Soweit es sich um andere als elektronisch gespeicherte Daten handelt (z. B. Steuerakten), überschreiten mögliche Gefährdungen der Datensicherheit nicht diejenigen, die auch bei Heimarbeit ohne Nutzung der Informationstechnik entstehen (z. B. im Betriebsprüfungsbereich).

Zu 11.4.2 Grundsätzliche Anforderungen/Hinweise (Seite 131)

Im 2. Unterpunkt auf Seite 132, 1. Absatz, wird gefordert, dass "personenbezogene Daten, die Berufs- oder besonderen Amtsgeheimnissen unterliegen", nicht in Tele-Heimarbeit verarbei-

tet werden sollten. Der Aussage kann in dieser Ausschließlichkeit nicht zugestimmt werden. Bei den genannten Daten handelt es sich weitgehend um "sensible" personenbezogene Daten im Sinne des Art. 8 der (in Umsetzung befindlichen) EG-Datenschutzrichtlinie, darüber hinaus auch z.B. um Steuerdaten, die im Bereich der Finanzverwaltung in Tele-Heimarbeit verarbeitet werden. Letzteres ist aus der Sicht der Landesregierung unbedenklich, zumal die gebotenen Sicherheitsstandards beachtet werden. Die Verarbeitung sensibler Daten in Tele-Heimarbeit wird auch von der LfD nicht generell abgelehnt, wie sich aus den Ausführungen zur Authentifizierung auf Seite134, vorletzter Absatz, und auf Seite 135, 1. Absatz, ergibt, die konkrete Vorgaben für solche Fälle enthalten. Die Frage sollte daher nicht generell negativ entschieden, sondern jeweils im Einzelnen geprüft werden.

Die Landesregierung weiß sich dabei einer datenschutzfreundlichen Haltung verpflichtet und legt nicht nur bei der Verarbeitung sensibler personenbezogener Daten, sondern überhaupt bei der Verarbeitung personenbezogener Daten in Tele-Heimarbeit einen strengen Maßstab an. Dies zeigt z.B. die Regelung im Geschäftsbereich des Ministeriums für Wirtschaft und Mittelstand, Technologie und Verkehr, wo Tätigkeiten, bei denen schwerpunktmäßig personenbezogene Daten verarbeitet werden, von der Telearbeitsform ausgeschlossen sind. Im Übrigen enthält dort die Dienstvereinbarung zur Telearbeit (DV-TA) eine ausdrückliche Regelung zum Datenschutz und zur Datensicherung, in der die Telearbeiterinnen/Telearbeiter auf ihre besondere Verpflichtung zum Datenschutz gerade am heimischen Telearbeitsplatz hingewiesen werden. Ansonsten gilt die ADV-Dienstanweisung an der häuslichen Arbeitsstätte. Da die DV-TA Inhalt der Arbeitsverträge (bei Tarifkräften) bzw. Bestandteil der Dienstanweisung (bei Beamtinnen/Beamten) geworden ist, sind die Telearbeiterinnen/Telearbeiter zum Datenschutz individualrechtlich verpflichtet worden.

Vergleichbare Vorgaben enthalten auch die einschlägigen Erlasse des Innenministeriums für die Telearbeit – Modellversuche der Bezirksregierungen Arnsberg, Düsseldorf und Münster - und dort geschlossene Dienstvereinbarungen.

Im Ministerium für Frauen, Jugend, Familie und Gesundheit, wo Telearbeitsplätze für Schreibkräfte eingerichtet worden sind, werden diesen ausschließlich Vorgänge ohne personenbezogene Daten zur Bearbeitung zugewiesen.

Im 8. Unterpunkt (Seite 132, 7. Absatz) wird gefordert, die Dienststelle müsse für sich selbst und für die LfD ein Kontrollrecht in der Wohnung der Tele-Heimarbeiterin oder des Tele-Heimarbeiters ausbedingen. Jedenfalls im Hinblick auf die LfD erscheint diese Forderung als zu weitgehend; die Kontrollrechte der LfD nach § 26 Abs. 1 DSG NW sind insoweit auf Diensträume beschränkt.

Im 9. Unterpunkt (Seite 132, vorletzter Absatz) wird die Unterrichtung der LfD über die Einrichtung von Tele-Heimarbeitsplätzen gefordert. Insoweit ist klarzustellen, dass diese Unterrichtung sich nur auf die grundsätzliche Entscheidung zur Einrichtung von Tele-Heimarbeitsplätzen beziehen kann. Eine Mitteilung über jede Einrichtung eines Tele-Arbeitsplatzes im Einzelfall wird nicht für erforderlich gehalten.

Hinsichtlich der Arbeitszeitdaten und -ergebnisse (11. Unterpunkt, Seite 133 oben) ist anzumerken, dass eine Aufzeichnung zwar stattfindet. Im Geschäftsbereich des Ministeriums für Wirtschaft und Mittelstand, Technologie und Verkehr z.B. haben die Telearbeiterinnen/Telearbeiter ihre häuslichen Arbeitszeiten in einem Arbeitstagebuch festzuhalten und auf dem Wege eines Korrekturbelegs geltend zu machen. Eine über die konkreten Arbeitsergebnisse hinausgehende Verhaltens- oder Leistungskontrolle findet jedoch nicht statt.

Zu 11.4.3 Anforderungen an technische und organisatorische Maßnahmen (Seite 133)

Die in diesem Abschnitt genannten Anforderungen sind weitgehend mit den allgemein verfügbaren technischen Komponenten realisierbar und tatsächlich realisiert worden. Auf Ausnahmen wird im Folgenden eingegangen. Es fragt sich allerdings, ob die Ausführungen der LfD zu den einzelnen technischen Punkten – die sich weitgehend wie ein technisches Handbuch lesen – in den Datenschutzbericht hätten aufgenommen werden sollen. Das BSI deckt nämlich weitgehend diese Aufgabenstellung ab, so dass die am Schluss gegebenen Hinweise auf die IT-Technik-Empfehlungen genügt hätten.

Die Forderung im 1. Unterpunkt (Seite 133, vorletzter Absatz), alle IT-Komponenten (einschließlich der Anwendungssoftware) müssten im Eigentum der Dienststelle stehen und die Verwendung privater Komponenten müsse untersagt werden, kann jedenfalls für den Bereich der Finanzverwaltung nicht akzeptiert werden. Im Bereich der steuerlichen Betriebsprüfung ist die Nutzung von prüfereigenen CD-ROM mit fachbezogenen Inhalten (z. B. steuerrechtliche Fachinformationssysteme) zugelassen, weil hierfür ein praktisches Bedürfnis besteht. Gleiches kann sich auch bei der Tele-Heimarbeit im Übrigen ergeben. In diesem Zusammenhang ist auch auch auf den Umstand hinzuweisen, dass ein Telefon eine IT-Komponente ist, die am Tele-Heimarbeitsplatz genutzt wird. Die Forderung, dieses Telefon nur nutzen zu dürfen, wenn es im Eigentum der Dienststelle steht, ist nicht sachgerecht.

Im 1. Unterpunkt (Seite 133, vorletzter Absatz) wird weiter gefordert: "Die Nutzung nicht freigegebener Software ist durch technische Maßnahmen zu verhindern." Nach dem heutigen Stand der Technik kann jedoch nicht mit Sicherheit ausgeschlossen werden, dass auch nicht freigegebene Software auf dem Rechner genutzt wird. Die dazu erforderlichen Kenntnisse kann sich jeder z.B. über das Internet beschaffen.

Die Forderung, "Kenntnisnahme, Nutzung und Manipulation von personenbezogenen Daten durch Mitbewohnerinnen und Mitbewohner oder Besuchspersonen" auszuschließen (3. Unterpunkt auf Seite 134, 1.Absatz) ist nicht realisierbar. Jeder, der sich den Zugang zu dem Rechner verschafft, ist grundsätzlich in der Lage, auch den Zugriff zu den Daten zu erlangen. Konsequenz dieser Tatsache ist auch, dass die Möglichkeit, Protokolle zu manipulieren (16. Unterpunkt auf Seite 136, 1. Absatz) nicht mit Sicherheit verhindert werden kann. Durch technische Maßnahmen können Manipulationen an den Systemen zwar erschwert, aber nicht mit Sicherheit verhindert werden.

Zu der Forderung, bei Datenfernübertragung die im Anschluss an die Authentifizierung zu übertragenden Daten zu verschlüsseln (8. Unterpunkt auf Seite 134, vorletzter Absatz), wird von Seiten des Ministeriums für Wirtschaft und Mittelstand, Technologie und Verkehr bemerkt, dass die Datenfernübertragung auf der Grundlage der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierten Technik und Komponenten für Telearbeit erfolgt. Eine Verschlüsselung ist im allgemeinen nicht erforderlich, da die eingesetzte Router-

Technik die Authentifizierung garantiert. Die Kontrolle durch ein Quittungsverfahren (9. Unterpunkt auf Seite 134, letzter Absatz) wird durch das landesweit in der Landesverwaltung eingesetzte externe Mail-Verfahren nach dem X.400- Standard garantiert.

Im 10. Unterpunkt (Seite 135, 1. Absatz) wird empfohlen, zur Authentifizierung des Anwenders ein chipkartenbasiertes Verfahren zu wählen. Diese Maßnahme ist nach Auffassung der Landesregierung nicht generell erforderlich. Ihr wird z.B. für den Bereich der Finanzverwaltung ausdrücklich widersprochen. Die dort weiterhin erhobene Forderung, bei sensiblen personenbezogenen Daten den Einsatz biometrischer Authentifizierungsverfahren zu prüfen, wird ebenfalls nicht generell unterstützt und für den Bereich der Finanzverwaltung wegen des damit verbundenen erheblichen Aufwandes zurückgewiesen. Auch aus der Sicht des Ministeriums für Wirtschaft und Mittelstand, Technologie und Verkehr wird das dort gewählte Authentifizierungsverfahren von allen Beteiligten als absolut ausreichend angesehen; es entspricht den Anforderungen des BSI. Der Einsatz von biometrischen Verfahren würde weit über den Schutzbedarf hinausgehen.

Die im 11. Unterpunkt (Seite 135, 2. Absatz) geforderte Bildschirmsperre nach einem Timeout mit anschließender Entsperrung durch Authentifizierung kann nicht für alle Bereiche der Tele-Heimarbeit befürwortet werden. In der Finanzverwaltung besteht die Bearbeitung von steuerlichen Vorgängen nicht aus einer kontinuierlichen Dateneingabe; hier sind vielmehr Eingabevorgänge und personell zu bearbeitende Schritte im Wechsel zu erledigen. Eine Bildschirmsperre würde den Arbeitsablauf empfindlich stören. Im Geschäftsbereich des Ministeriums für Wirtschaft und Mittelstand, Technologie und Verkehr erzwingt dagegen die Software der Telearbeiter-PC – wie im Ministerium selbst – eine Sperrung des Bildschirms nach 15 Minuten Inaktivität. Im übrigen kann dort der PC jederzeit in den Sperrmodus versetzt werden.

Die Forderungen bezüglich der Protokollierung zur Gewährleistung der Revisionssicherheit (16. Unterpunkt auf Seite 136 oben) erscheinen nicht zwingend. Im Geschäftsbereich des Ministeriums für Wirtschaft und Mittelstand, Technologie und Verkehr werden Protokolle der Datenverarbeitung am Telearbeitsplatz nicht durchgeführt. Sie werden einvernehmlich abgelehnt. Vereinbart sind Selbstaufschreibungen nach Art und Umfang der geleisteten Tä-

tigkeiten. Selbst wenn - was sich nicht klar ergibt - Protokollierungen nur im Falle der Verarbeitung von personenbezogenen Daten durchgeführt werden sollen, wäre diese Frage auch vor dem Hintergrund personal- und arbeitsrechtlicher Regelungen zu prüfen.

Zu 12. Verkehr, Wirtschaft und öffentliche Unternehmen (Seite 137)

Zu 12.2 Bekämpfung von missbräuchlicher Betätigung in Verwaltung und Wirtschaft (Seite 138)

Zu 12.2.3 Geldwäsche (Seite 140)

Nach Auffassung der LfD kommen Überwachungsinstrumente, die einem Kreditinstitut einen automatisierten Datenabgleich von typisierten geldwäscheträchtigen Indikatoren mit dem gesamten Datenbestand eines Kreditinstitutes ermöglichen, um vermeintliche Geldwäschesachverhalte herauszufiltern, einer Rasterfahndung gleich, die das Geldwäschegesetz nicht zulässt. Diese Aussage führt leicht zu Missverständnissen, weil sie nicht zwischen der technischen Installation eines Überwachungssystems und den verschiedenen Möglichkeiten seiner praktischen Anwendung unterscheidet.

Nach § 14 Abs. 1 und Abs. 2 Nr. 2 des Geldwäschegesetzes (GwG) sind Kreditinstitute verpflichtet, Vorkehrungen dagegen zu treffen, dass sie zur Geldwäsche missbraucht werden. In der Praxis wird von Kunden der Kreditwirtschaft vermehrt von der Möglichkeit Gebrauch gemacht, Transaktionen auf elektronischem Wege in Auftrag zu geben. In diesen Fällen erfolgt der weitere Geschäftsablauf in den Kreditinstituten ohne eine Wahrnehmung des entsprechenden Geschäftsvorfalls durch einen Angestellten rein elektronisch. Hierdurch wird eine Verhinderung von Geldwäschehandlungen, ja selbst die Verdachtschöpfung im Sinne von § 11 GwG unmöglich. Soweit Kreditinstitute solche Verfahren ermöglichen, sind sie nach § 14 GwG zu entsprechenden Ausgleichsmaßnahmen zur Verhinderung der Geldwäsche bzw. zur Ermöglichung der Verdachtschöpfung verpflichtet (Verlautbarung des Bundesaufsichtsamtes für das Kreditwesen vom 30.03.1998, Ziff. 34 d). Diese Ausgleichsmaßnahmen können nur mit elektronischer Unterstützung stattfinden. Die durch den Gesetzgeber in § 14 Abs. 2 GwG allgemein formulierten Maßnahmen der Kreditinstitute zur Geldwäschebekämpfung sind primär auf die Verhinderung von Geldwäschehandlungen gerichtet. Der Begriff der „internen Verfahren und Kontrollen zur Verhinderung der Geldwäsche" schließt elektronische Verfahren und Kontrollen ein.

Bei der Entwicklung von Grundsätzen, Verfahren und Kontrollen nach § 14 Abs. 2 Nr. 2 GwG haben die Kreditinstitute allerdings zwischen den Zielen des Geldwäschegesetzes und den Erfordernissen des Datenschutzes abzuwägen. Eine permanente Überwachung aller Kunden- und Kontobeziehungen, darin ist der LfD zuzustimmen, wäre nicht zulässig. Automatisierte Überwachungssysteme müssen daher den einzelnen Instituten angemessenen Spielraum zur Entscheidung über einen flexiblen Einsatz geben.. Der Bankenfachverband hat dem „Düsseldorfer Kreis", der Arbeitsgemeinschaft der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, ein Research-System zur Prävention der Geldwäsche vorgestellt, das den Anforderungen des Bundesaufsichtsamtes für das Kreditwesen entsprechen und zugleich den Kreditinstituten den erforderlichen Entscheidungsspielraum bei der Anwendung geben soll. Das System wird derzeit vom „Düsseldorfer Kreis" geprüft.

Mit einem Zitat aus dem „Lagebild Finanzermittlungen für 1997" stellt die LfD in ihrem Bericht auf Seite 140 fest, dass in Nordrhein-Westfalen insgesamt 1.156 Verdachtsanzeigen erstattet wurden, die nur in 3% der Fälle als Geldwäschedelikt konkretisiert werden konnten. Dies ist mit dem Hinweis verbunden, dass die Zahl unerledigter Fälle stetig wächst. Richtig ist, dass in Nordrhein-Westfalen im Kalenderjahr 1997 (nicht seit 1993) 1.156 Ermittlungsverfahren aufgrund von Verdachtsanzeigen in Bearbeitung waren. In 26 % der abgeschlossenen Verfahren führten die Ermittlungen zur Aufdeckung von Straftaten (zu den 3 % Geldwäschesachverhalten kamen weitere Delikte gemäß Betäubungsmittelgesetz, Abgabenordnung sowie sonstige Straftaten). Inzwischen dürfte die Geldwäsche gemäß § 261 StGB lediglich als Auffangtatbestand einzuschätzen sein. Die Zunahme unerledigter Verfahren war auf eine konstant hohe Zahl eingehender Verdachtsanzeigen zurückzuführen. Die Zahl unerledigter Verfahren konnte inzwischen weiter reduziert werden (Jahresende 1997: 440 Verfahren; Jahresende 1998: 312 Verfahren).

Datenschutz
im nicht-öffentlichen Bereich

Sechster Bericht

der Landesregierung Nordrhein-Westfalen

über die Tätigkeit der für den

Datenschutz im nicht-öffentlichen Bereich

zuständigen Aufsichtsbehörden

an den Landtag

Nordrhein-Westfalen

Berichtszeitraum
01. Januar 1997 bis 31. Dezember 1998

GLIEDERUNG

		Seite
Einleitung		5
1.	**Übersicht über die Kontrolltätigkeit in Zahlen**	7
1.1	Meldungen zum Register	7
1.2	Beschwerden	9
1.3	Anfragen und Beratungsersuchen	12
1.4	Überprüfungen vor Ort	13
1.5	Bußgeldverfahren/Verwaltungsverfahren nach § 38 Abs. 5 BDSG	15
2.	**Entwicklungen in den einzelnen Bereichen**	16
2.1	Zwanzigjähriges Bestehen des „Düsseldorfer Kreises“	16
2.2	Tele- und Mediendienste	20
2.3	Kontrollzuständigkeiten nach dem Telekommunikationsgesetz	23
2.4	Telefonverzeichnisse auf CD-ROM	25
2.5	Scoring-Verfahren bei der SCHUFA	27
2.6	SCHUFA-Selbstauskünfte von Mietinteressenten	29
2.7	Kreditinformation	30
2.8	Adresshandel und Direktmarketing	31
2.9	Elektronische Geldbörse („GeldKarte“)	33
2.10	Outsourcing bei Kundenbefragungen von Banken	35
2.11	Geldwäschegesetz	37
2.12	Aufgabe einer Arztpraxis/Verbleib der ärztlichen Unterlagen	39
2.13	Apothekenrechenzentren	41
2.14	Videoüberwachung	42

3.	**Einzelfälle aus der aufsichtsbehördlichen Praxis**	44
3.1	Unerlaubte Abfrage von SCHUFA-Daten	44
3.2	Erhebung personenbezogener Daten durch ein Kreditinstitut	45
3.3	Allgemeine Geschäftsbedingungen einer Lotteriegesellschaft	47
3.4	Negativdatei über Hotelgäste	48
3.5	Unzulässige Einträge in die Kundendatei	50
3.6	„Schwarze Liste" der Transportunternehmen	52
3.7	Weitergabe von Arbeitnehmerdaten	53
4.	**Stand der Novellierung des Bundesdatenschutzgesetzes (BDSG)**	54

Einleitung

Der vorliegende 6. Bericht gibt einen Überblick über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörden in Nordrhein-Westfalen. Die Berichterstattung erstreckt sich auf die Jahre 1997 und 1998.

Die Berichtsjahre zeigen kein einheitliches Bild von der Entwicklung des Datenschutzes im nicht-öffentlichen Bereich. Es gibt ermutigende Zeichen von datenverarbeitenden Stellen und bei Bürgerinnen und Bürgern, die von einem gewachsenen Bewusstsein des Grundrechts auf Datenschutz zeugen. Andererseits ist eine erhebliche Nachlässigkeit im täglichen Umgang mit personenbezogenen Daten feststellbar. Der Rang, den die Bürger ihrem Grundrecht auf informationelle Selbstbestimmung einräumen, ist hoch. Viele sehen sich derzeit vor allem bei der Datenverarbeitung durch private Stellen in ihrer persönlichen Sphäre beeinträchtigt und wünschen sich einen verstärkten Schutz.

Auf dem Weg in eine globale Informations- und Kommunikationsgesellschaft kommen auf den Datenschutz in den nächsten Jahren schwierige Aufgaben zu. Ohne einen funktionierenden Datenschutz und eine ausreichende Datensicherheit werden die Bürger den Weg in die Informationsgesellschaft nicht mitgehen, wenn sie dies mit dem Verlust ihrer Privatsphäre und dem Abbau ihrer Grundrechte bezahlen müssen. Das neue Problembewusstsein hat dazu geführt, dass sich die Bürger heutzutage weniger von öffentlichen Stellen bedroht fühlen als von den für sie kaum noch überschaubaren Missbrauchsmöglichkeiten in einer globalen Netzwelt der Wirtschaft. Aus der Sicht des Datenschutzes sind Schutzmaßnahmen zum sicheren Datentransfer und die Klärung der damit verbundenen Datenschutzfragen zwingend erforderlich. Die EG-Datenschutzrichtlinie, die in den Mitgliedstaaten der Europäischen Union in nationales Recht umgesetzt werden muss, ist ein Schritt auf dem Weg zu einem multinationalen Datenschutz– und Sicherheitskonzept. Dadurch werden jedoch noch nicht alle Probleme gelöst, da in der Privatwirtschaft Datenschutz oft Bestandteil der privatautonomen Gestaltung der Rechtsbeziehungen ist, sei es durch Einwilligung, sei es durch Vertrag.

Allerdings haben auch die Wirtschaftsunternehmen inzwischen erkannt, dass Datenschutz und Datensicherheit keine Belastungen darstellen, sondern im Gegenteil einen Wettbewerbsvorteil bieten.

Auch im Berichtszeitraum bestätigte sich weiterhin die Bereitschaft der Privatwirtschaft zum konstruktiven Dialog mit den Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich, die im „Düsseldorfer Kreis“ und seinen Unterarbeitsgemeinschaften vertreten sind. Dies zeigt, dass Datenschutz und Datensicherheit mehr und mehr als gemeinsames Anliegen gesehen werden.

1. Übersicht über die Kontrolltätigkeit in Zahlen[1]

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

1.1 Meldungen zum Register

Mit Stand 31.12.1998 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 (19)	29 (24)
- Branchen- bzw. Kreditinformationsdienste (Wirtschaftsauskunfteien, SCHUFA, Warndienste)	58 (42)	57 (56)
Gesamt:	76 (61)	86 (80)

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

	Arnsberg	Köln
- Markt- und Meinungsforschungsinstitute	22 (15)	20 (19)

[1] Zahlen in Klammern sind hier und auf den folgenden Seiten Vergleichszahlen aus dem 5. Tätigkeitsbericht.

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

Arnsberg	Köln
445 (403)	672 (546)

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

d) Gemeldete Unternehmen nach a) bis c) insgesamt

Arnsberg	Köln
543 (479)	778 (645)

Die Zahlen lassen erneut eine deutliche Zunahme erkennen. Der Anstieg der gemeldeten Stellen liegt wohl im Wesentlichen an der wachsenden Auslagerung von Geschäftsbereichen mit dem Schwerpunkt Datenverarbeitung auf spezialisierte Dienstleistungsunternehmen (Outsourcing), die dann als „Auftragsdatenverarbeiter" nach § 32 Abs. 1 Nr. 3 BDSG meldepflichtig werden.

1.2 Beschwerden

In den Jahren 1997 und 1998 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 271 (178) Beschwerden und bei der Bezirksregierung Köln 423 (370) 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 80 (94) Beschwerden und bei der Bezirksregierung Köln 111 (98) 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	54 (39)	68 (53)
- Industrie/Großunternehmen	26 (11)	36 (38)
- Krankenhäuser, Ärzte, privatärztliche Verrechnungsstellen	25 (20)	28 (18)
- Kreditinstitute/-vermittler	21 (16)	73 (85)
- Versicherungen	30 (17)	71 (83)
- Vereine, Verbände	17 (26)	43 (27)
- Sonstige	98 (49)	104 (66)
Gesamt	271 (178)	423 (370)

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

	Arnsberg	Köln
- Adresshandel, Direktmarketing	17 (24)	46 (34)
- Auskunfteien, Warndienste	27 (51)	55 (46)
- Konzerndatenverarbeiter	5 (9)	-- (--)
- Markt- und Meinungsforschungsinstitute	10 (5)	1 (3)
- Rechenzentren (Auftragsdatenverarbeiter)	8 (5)	9 (15)
- Sonstige	13 (-)	-- (--)
Gesamt	80 (94)	111 (98)

Auffallend ist die stetige Zunahme der Beschwerden insgesamt von 488 in den Jahren 1993 und 1994 über 740 in den Jahren 1995 und 1996 auf 885 im Berichtszeitraum. Der Schwerpunkt der Zunahme liegt noch mehr als in den Vorjahren im Bereich der Datenverarbeitung für **eigene** Zwecke und hierbei insbesondere in den Bereichen Handel/Handwerk, Kreditinstitute, Versicherungsunternehmen. Hier wirkt sich die wachsende Sensibilisierung der Bürgerinnen und Bürger für den Datenschutz aus, die sich in einer großen Anzahl von Anfragen und Beschwerden niederschlägt. Ebenso stand im Vordergrund vieler Beschwerden nach wie vor die Verarbeitung und Weitergabe von personenbezogenen Daten zu Werbezwecken (Marketing).

Beschwerden zu Datenverarbeitungen für **fremde** Zwecke betrafen schwerpunktmäßig unverändert die Tätigkeit von Auskunfteien (z.B. zur Zulässigkeit und Dauer der Speicherung von „Negativ"-Merkmalen). Die geschäftsmäßige Verarbeitung personenbezogener Daten zu Werbezwecken hat vor allem infolge der zunehmenden Flut unerbetener Werbung zu vermehrten Anfragen und Beschwerden in Bezug auf Herkunft, Verarbeitung und Auswertung des Adressenmaterials und sonstiger Daten geführt.

Bei den insgesamt 885 Beschwerden kam es in 181 Fällen zu Beanstandungen oder Empfehlungen der Aufsichtsbehörden, denen **sämtlich** entsprochen wurde; in den übrigen Fällen er-

gab sich kein Grund zu Beanstandungen; vereinzelt wurden auch die Beschwerden aus verschiedenen Gründen (z.B. wegen Einstellung der Geschäftstätigkeit) nicht weiter verfolgt.

Beschwerden vermitteln den Aufsichtsbehörden einen Einblick zunächst nur in die durch die Beschwerden bekannt gewordenen Fälle. Soweit Beschwerden nicht erhoben werden, kann nicht etwa angenommen werden, in diesen Bereichen ergäbe sich auch kein Grund zu Beanstandungen oder Empfehlungen. Der Anteil der begründeten Beschwerden an der Gesamtzahl der Beschwerden liegt unter Einbeziehung der Zahlen aus den Vorjahren bei etwa 20 bis 25 %. Würde dieses Verhältnis auf die Gesamtzahl der stattfindenden Datenverarbeitungen hochgerechnet, dürfte sich in absoluten Zahlen eine eindrucksvolle Anzahl kritischer oder verbesserungsbedürftiger Fälle ergeben.

1.3 Anfragen und Beratungsersuchen

Die Aufsichtsbehörden erhielten wieder zahlreiche schriftliche Anfragen und Beratungsersuchen, die Datenverarbeitungen sowohl für eigene Zwecke (§ 28 BDSG) als auch für fremde Zwecke (§ 32 Abs. 1 BDSG) betrafen. Es ergibt sich folgende Aufschlüsselung:

	Arnsberg		Köln	
	§ 28	§ 32 Abs. 1	§ 28	§ 32 Abs. 1
Anfragen von				
- betriebl. Datenschutzbeauftragten	37 (16)	14 (11)	37 (29)	14 (16)
- Geschäftsleitungen	68 (23)	59 (9)	68 (51)	59 (48)
- Betriebsräten	14 (9)	8 (4)	14 (8)	8 (3)
- Einzelpersonen, Vereinen, Verbänden	84 (44)	65 (6)	84 (57)	65 (49)
Gesamt	203 (92)	146 (30)	203 (145)	146 (116)

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

1.4 Überprüfungen vor Ort

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

		Arnsberg	Köln
a)	Regelmäßige Überwachung nach § 38 Abs. 2 BDSG bei Stellen mit Datenverarbeitung für fremde Zwecke		
	- Adresshandel/Direktmarketing	6	9
	- Akten- und Datenvernichtungsunternehmen	14	27
	- Auskunfteien/SCHUFA	7	12
	- Brancheninformationsdienste	-	2
	- Buchführungshelfer/Schreibbüros	8	51
	- Datenerfassungsbüros	3	31
	- Markt- und Meinungsforschungsinstitute	4	5
	- Mikroverfilmungsinstitute	5	7
	- Rechenzentren (incl. Konzerndatenverarbeitung)	42	43
	- Sonstige	1	-
	Gesamt	90 (92)	187 (152)

		Arnsberg	Köln
b)	konkrete Anlässe (§ 38 Abs. 1 BDSG) bei Stellen mit Datenverarbeitung		
	für **eigene** Zwecke	2 (1)	93 (86)
	für **fremde** Zwecke	- (2)	22 (20)
	Gesamt	2 (3)	115 (106)
	Gesamt a) und b)	92 (95)	302 (258)

Bei den insgesamt 277 (244) regelmäßigen Überprüfungen kam es in 83 (94) Fällen zu Beanstandungen und in 71 (71) Fällen zu Empfehlungen, denen die Unternehmen ebenso wie bei den Beschwerden (Ziffer 1.2) in **sämtlichen** Fällen gefolgt sind.

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

Wie in den Vorjahren betrafen die Überprüfungen vor Ort technische Fragen der Datensicherheit und organisatorische Schutzvorkehrungen (hierzu im einzelnen zuletzt 4. Tätigkeitsbericht, Ziff. 1.4, S. 15).

Die bereits in den Vorjahren festgestellte hohe Quote von Mängeln besteht nach wie vor. Zur Hochrechnung der Mängelquote gilt das unter Ziffer 1.2 Ausgeführte entsprechend. Ziel der aufsichtsbehördlichen Kontrollen in Verbindung mit einer intensiven Beratung muss es weiterhin sein, die eigenen Bemühungen der verantwortlichen Stellen um Datensicherheit und organisatorische Schutzvorkehrungen nachhaltig zu stärken.

1.5 Bußgeldverfahren/Verwaltungsverfahren nach § 38 Abs. 5 BDSG

Im Berichtszeitraum wurde gegen ein Unternehmen aus dem Bereich des Adresshandels und Direktmarketings ein Ordnungswidrigkeitenverfahren gem. § 44 Abs. 1 Ziffer 6 BDSG durchgeführt und ein Bußgeld von 5.000,-- DM wegen Auskunftverweigerung festgesetzt sowie nach erfolglosem Einspruch für die Landeskasse vereinnahmt. Da davon auszugehen ist, dass dieses Verfahren vermutlich in dem gesamten Umfeld für erhöhte Aufmerksamkeit gesorgt hat, kann darin im Hinblick auf künftige Fälle ein Signal für auskunftsunwillige Stellen gesehen werden.

In der Regel wurden indes die festgestellten Mängel nach Beanstandung oder Empfehlung von den Betroffenen ausgeräumt, so dass sich die Notwendigkeit der Durchführung von Bußgeldverfahren nicht ergab.

2. Entwicklungen in einzelnen Bereichen

2.1 Zwanzigjähriges Bestehen des „Düsseldorfer Kreises"

Der „Düsseldorfer Kreis" ist ein Koordinierungsgremium der obersten Aufsichtsbehörden für den Datenschutz in der Privatwirtschaft. Im Herbst 1997 konnte er auf sein 20jähriges Bestehen zurückblicken.

Damals kamen die Innenministerien der Länder überein, sich bezüglich auftretender Zweifelsfragen untereinander abzustimmen und ihre Erfahrungen auszutauschen, um eine möglichst einheitliche Auslegung und Anwendung des Bundesdatenschutzgesetzes vom 27.01.1977 zu gewährleisten. Aus einer zunächst lose zusammengetretenen Gesprächsrunde entstand eine ständige Arbeitsgemeinschaft der Vertreter der obersten Aufsichtsbehörden der Länder für den Datenschutz im nicht-öffentlichen Bereich. Dem Gremium gehören die Datenschutzreferenten der Innenministerien der Flächenstaaten sowie teilweise Datenschutzbeauftragte der Länder, die auch für den Datenschutz in der Privatwirtschaft zuständig sind, an. Den Vorsitz führt das Innenministerium Nordrhein-Westfalen, das die in der Regel zweimal jährlich stattfindenden Sitzungen in Düsseldorf ausrichtet.

Vorrangiges Ziel des „Düsseldorfer Kreises" ist die Erarbeitung einheitlicher Positionen zu Datenschutzfragen von überregionaler Bedeutung sowie die Führung eines ständigen Dialogs mit der Privatwirtschaft, um den Datenschutz zu fördern. In der Anfangsphase stand die Interpretation unbestimmter Rechtsbegriffe des Datenschutzes im Vordergrund, später befasste sich das Gremium mit datenschutzrechtlichen Einzelfragen, z. B. bei Kreditwirtschaft und Versicherungswirtschaft, SCHUFA, Handelsauskunfteien, Adresshandel und Direktwerbung, Arbeitnehmer- und Patientendatenschutz sowie Versandhandel.

Im Berichtszeitraum standen insbesondere datenschutzrechtliche Fragen der modernen Informationstechnik, etwa auf den Feldern Telekommunikationsdienste, CD-ROM, Internet oder Chipkartenanwendung im Vordergrund.

Ein weiterer Schwerpunkt waren die Beratungen im Rahmen der Umsetzung der Europäischen Datenschutzrichtlinie 95/46/EG des Europäischen Parlaments und des Rates in jeweils nationales Recht für Bund und Länder zur Rechtsangleichung in der Europäischen

Gemeinschaft und die Auswirkungen auf die anstehende Novellierung des Bundesdatenschutzgesetzes.

Von Anfang an suchte der „Düsseldorfer Kreis" engen Kontakt zu den Spitzenorganisationen der Wirtschaft, insbesondere vor dem Hintergrund der überregionalen und länderübergreifenden Datenverarbeitung großer Wirtschafts- und Dienstleistungsunternehmen. Mit den Verhandlungen sollte eine Selbstbindung der den Dachverbänden angeschlossenen Unternehmen im Sinne einer möglichst datenschutzgerechten und praktikablen Handhabung des BDSG erreicht werden. Auf zahlreichen wichtigen Gebieten konnten in diesen Verhandlungen Verbesserungen im Datenschutz herbeigeführt werden. Beispielhaft sind hier zu nennen:

Neugestaltung des Bankauskunftsverfahrens

Mit der Kreditwirtschaft konnte Einigung über die Neugestaltung des Bankauskunftsverfahrens (Auskünfte an eigene Kunden sowie andere Kreditinstitute, für deren eigene Zwecke und die ihrer Kunden, nicht aber beispielsweise Auskunfteien) erzielt werden. Danach werden Bankauskünfte über Privatkunden nur noch mit deren ausdrücklicher Einwilligung im Einzelfall erteilt. Bankauskünfte über Geschäftskunden - u. a. juristische Personen sowie im Handelsregister eingetragene Kaufleute - dürfen gegeben werden, sofern keine anderslautende Weisung des betroffenen Kunden vorliegt. Die Auskunftverweigerung wegen fehlender Einwilligung ist so zu formulieren, dass sie nicht als nachteilige Auskunft verstanden werden kann. Auf Verlangen des Betroffenen hat das Kreditinstitut diesem den Inhalt einer erteilten Auskunft mitzuteilen.

SCHUFA-Klauseln

Gemeinsam mit dem Zentralen Kreditausschuss und der Bundes-SCHUFA wurden neue SCHUFA-Klauseln entwickelt, die u. a. für Kontoeröffnung, Kreditaufnahme und Bürgschaftserklärung Verwendung finden und zusammen mit einem Merkblatt für die Kunden die Transparenz der Datenverarbeitung wesentlich erhöhen. Da das SCHUFA-Informationssystem seine Legitimation ausschließlich aus der Beurteilung der Kreditwürdigkeit bezieht, wurde der Kreis der Systembenutzer grundsätzlich auf Kreditinstitute und solche Wirtschaftsunternehmen, die Konsumenten Geld- oder Warenkredite zur Verfügung stellen, beschränkt. Ausgeschlossen wurden danach u. a. Immobilienvertreter, Getränkegroßhändler, Lesezirkel,

Fernschulen und Möbelspeditionen. Versicherungsunternehmen dürfen am SCHUFA-Verfahren nur insoweit teilnehmen, als sie Darlehen (zur Wohnbaufinanzierung) gewähren.

Schweigepflichtentbindungsklauseln und Einwilligungsklausel in der Versicherungswirtschaft

Mit der Versicherungswirtschaft konnten Schweigepflichtentbindungsklauseln in den Bereichen Kranken-, Unfall- und Lebensversicherungen sowie Haftpflicht-, Reiserücktrittskosten-, Berufsunfähigkeits- und Pflegerentenversicherungen konzipiert werden. Zugleich wurden hinsichtlich der Zulässigkeit der Datenverarbeitung eine neue Einwilligungsklausel und ein Merkblatt mit einer Übersicht über die Datenverarbeitungprozesse zur Unterrichtung der Kunden in der Versicherungswirtschaft formuliert.

Grenzüberschreitender Datenverkehr

In Anlehnung an ein mit der Privatwirtschaft entwickeltes Vertragsmodell für die Datenübermittlung in Länder mit schwächerem oder fehlendem Datenschutz erarbeiteten SCHUFA und Zentraler Kreditausschuss gemeinsam mit dem „Düsseldorfer Kreis" ein Auslandskonzept, wonach die SCHUFA ihre Vertragspartner unabhängig davon, ob in dem jeweiligen Empfängerland ein Datenschutzgesetz besteht, darauf verpflichtet, die in der Datenschutzkonvention des Europarates enthaltenen Grundsätze einzuhalten (insbesondere hinsichtlich Zweckbindung, Weitergabe an Dritte, unbefugter Nutzung sowie Auskunfts-, Berichtigungs- und Löschungsverlangen).

„Allfinanzklauseln" in der Kreditwirtschaft

In Beratungen zwischen der Arbeitsgruppe Kreditwirtschaft des „Düsseldorfer Kreises" und dem Zentralen Kreditausschuss konnten kombinierte Hinweis- und Einwilligungsklauseln bei der Datenverarbeitung zu vermittelten Verträgen erreicht werden (Einwilligungsklauseln zur Datenweitergabe für Kundenberatung und –werbung im Rahmen von „Allfinanz-Konzepten"). Mit ausführlicher Einwilligung des Bankkunden wird eine Übermittlung von Daten an mit einem Kreditinstitut als Verbundpartner kooperierende Unternehmen, z. B. eine Bausparkasse, ermöglicht. Da in diesem Zusammenhang auch besonders schützenswerte Daten,

wie z. B. Kontostände, übermittelt werden, wurde in den Verhandlungen besonderes Gewicht auf Transparenz und Freiwilligkeit der Einwilligungserklärungen gelegt.

Zur rationelleren Bewältigung seiner Aufgaben hat der „Düsseldorfer Kreis" Arbeitsgruppen gebildet, die nach Bedarf einberufen werden, so etwa die Arbeitsgruppen „Kreditwirtschaft", „Versicherungswirtschaft", „Auskunfteien", „Telekommunikation" und „Internationaler Datenverkehr". Die Ergebnisse der Arbeitsgruppen werden im Gesamtgremium beraten.

Der „Düsseldorfer Kreis" hält auch Kontakt mit den für den öffentlichen Bereich zuständigen Datenschutzbeauftragten des Bundes und der Länder, soweit diese nicht bereits Mitglied des Gremiums sind, sowie mit dem auf Bundesebene für die Datenschutzgesetzgebung zuständigen Bundesministerium des Innern. So nehmen an den Sitzungen regelmäßig Vertreter des Bundesministeriums des Innern und des Bundesbeauftragten für den Datenschutz teil. Bei wesentlichen Berührungspunkten mit dem Datenschutz im öffentlichen Bereich werden auch Mitarbeiter der Datenschutzbeauftragten der Länder in Arbeitsgruppen des „Düsseldorfer Kreises" eingeladen.

Im Rahmen der Umsetzung der Datenschutzrichtlinie der Europäischen Gemeinschaft im Bundesdatenschutzgesetz hat der „Düsseldorfer Kreis" zahlreiche Vorschläge erarbeitet. Die Novellierung des Bundesdatenschutzgesetzes sowie der Länderdatenschutzgesetze und die Entwicklung eines einheitlichen Datenschutzstandards in den EG-Mitgliedstaaten werden auch künftig einen Schwerpunkt in den Beratungen des „Düsseldorfer Kreises" bilden.

2.2 Tele- und Mediendienste

Bereits im 5. Tätigkeitsbericht wurde auf die Gesetzgebungsmaßnahmen hingewiesen, welche die rechtlichen Rahmenbedingungen der modernen Informations- und Kommunikationstechnik regeln sollen. Am 1. August 1997 sind als neue Regelwerke der Mediendienste-Staatsvertrag der Länder und das Informations- und Kommunikationsdienste-Gesetz des Bundes (IuKDG) in Kraft getreten. Der Mediendienste-Staatsvertrag regelt die rechtlichen Bedingungen der an die **Allgemeinheit** gerichteten Mediendienste, z.B. des elektronischen Zeitungsangebots oder der Textanzeigedienste im Fernsehprogramm, wobei kein individueller Leistungsaustausch stattfindet. Das IuKDG besteht aus einem Gesetzesbündel, insbesondere dem Teledienstegesetz und dem Teledienstedatenschutzgesetz. Diese befassen sich mit elektronischen Informations- und Kommunikationsdiensten, die für eine **individuelle** Nutzung bestimmt sind. Als Beispiele sind Einrichtungen wie Telebanking und Online-Shopping zu nennen, bei denen ein individueller Leistungsaustausch stattfindet.

Die genannten Regelwerke weisen die Aufsicht für den Bereich des Datenschutzes den Aufsichtsbehörden nach § 38 des Bundesdatenschutzgesetzes, in Nordrhein-Westfalen mithin den Bezirksregierungen Arnsberg und Köln zu. Diese haben dadurch einen beträchtlichen qualitativen und quantitativen Zuwachs an Arbeit erhalten, der im Folgenden verdeutlicht wird:

Der Rechtsverkehr mittels elektronischer Medien vollzieht sich gleichzeitig in verschiedenen Schichten, für die unterschiedliche Rechtsvorschriften gelten. Beispielsweise gilt bei den Geschäftsbeziehungen zwischen Versandhandelsunternehmen und ihren Kunden für den Umgang mit Kundendaten, die an das Unternehmen übermittelt und dort gespeichert werden - Name, Anschrift u.ä. - das Bundesdatenschutzgesetz (obere Schicht). Vollzieht sich die Kommunikation zwischen den Geschäftspartnern auf elektronischem Wege durch Inanspruchnahme eines Anbieters von Telediensten, gilt zusätzlich für die Verarbeitung der im Zuge des Kommunikationsvorgangs anfallenden Daten das Teledienstedatenschutzgesetz (mittlere Schicht). Soweit dabei das Leitungsnetz eines Anbieters von Telekommunikationsdiensten (also eine Telefonleitung) benutzt wird, gilt für den Umgang mit den dabei anfallenden Daten zusätzlich das Telekommunikationsgesetz (untere Schicht). Aufsichtsbehörde für den Telekommunikationsbereich ist aber nicht die Bezirksregierung Arnsberg oder Köln, sondern der Bundesbeauftragte für den Datenschutz. Verkehrt der Kunde nicht durch Vermittlung eines Teledienstes individuell mit dem Versandhandelsunternehmen, sondern nimmt

er einen an die Allgemeinheit gerichteten Mediendienst in Anspruch (Teleshopping ohne direkte Bestellmöglichkeit auf elektronischem Wege), gelten die Bestimmungen des Mediendienste-Staatsvertrages.

Das Beispiel zeigt, dass die datenschutzrechtliche Beurteilung eines relativ einfachen, auf elektronischem Wege abgewickelten Geschäftsvorganges komplizierte Sachverhaltsermittlungen erfordern und rechtlich schwierige Zuordnungs- und Abgrenzungsprobleme mit sich bringen kann. (Handelt es sich im Einzelfall um einen Tele- oder einen Mediendienst? Zu welcher „Schicht" gehört der datenschutzrelevante Vorgang? Welche Vorschrift ist anzuwenden und welche Aufsichtsbehörde ist zuständig?)

Zu diesen qualitativen Erschwernissen kommt hinzu, dass die Aufsicht nach dem Teledienstedatenschutzgesetz und dem Mediendienste-Staatsvertrag nicht wie die Aufsicht nach dem Bundesdatenschutzgesetz anlassbezogen, sondern auf Dauer auch ohne konkreten Anlass ausgeübt wird und damit auch quantitativ einen erheblich höheren Arbeitsaufwand erfordert.

Die erweiterte Aufgabenstellung hat die Bezirksregierung Köln veranlasst, einen Schwerpunkt der Datenschutzaufsicht auf die neuen Technologien zu legen. Die Bezirksregierung hat eine Prüfungsstrategie für diesen Bereich entwickelt und mit dem Innenministerium NRW sowie der Bezirksregierung Arnsberg abgestimmt.

Im Anschluß daran führte die Bezirksregierung Köln eine Umfrage bei 35 Unternehmen aus der Branche der Tele- und Mediendienste in ihrem Aufsichtsbezirk durch, mit dem Ziel, den Stand der Umsetzung der neuen Gesetze und die auftretenden Probleme stichprobenartig zu erfassen. Als Ergebnis der Umfrage wurde eine Fülle von Erkenntnissen zu der Umsetzung der neuen Gesetze in den befragten Unternehmen gewonnen. Als Folgereaktion der Unternehmen wurden konkrete Verbesserungen für den Datenschutz durch Änderung von Allgemeinen Geschäftsbedingungen und Verträgen erreicht. Die Fragebogenaktion stieß in der Fachöffentlichkeit sowie bei den Datenschutzaufsichtsbehörden anderer Länder und auf Bundesebene auf großes Interesse. Sie wurde in einer Fachpublikation veröffentlicht sowie ins Internet eingestellt.

Da ein großes Informationsbedürfnis der Unternehmen im Spektrum der neuen Technologien bestand, wurde von der Bezirksregierung Köln eine Informationsbroschüre zur Datenschutzaufsicht in diesem Bereich erstellt. Die Broschüre wurde in Zusammenarbeit mit der

Industrie- und Handelskammer Köln Unternehmen aus dem Bereich der Tele- und Mediendienste zur Verfügung gestellt. Sie fand erhebliches Interesse und wurde inzwischen über 600mal an Unternehmen, Behörden und Fachverlage verteilt.

Weitere Informations- und Öffentlichkeitsarbeit in diesem Bereich leistete die Bezirksregierung Köln durch die Übernahme eines Forums zur Datenschutzaufsicht auf der DAFTA, der größten Datenschutzfachtagung in Deutschland, und durch den Besuch weiterer Veranstaltungen.

An die konzeptionelle Arbeit schlossen sich erste praktische Prüfungen der Unternehmen vor Ort an. Diese ergaben, dass die geprüften Unternehmen notwendige Datenschutzmaßnahmen durchaus ergriffen hatten. Andererseits wurden aber auch Mängel festgestellt. Allgemein ist noch von einem erheblichen Informations-, Beratungs- und Umsetzungsbedarf im Bereich der Unternehmen in den neuen Technologien auszugehen.

Die alsbald nach Verabschiedung der Gesetze zutage tretenden Umsetzungsprobleme haben das zuständige Bundesministerium veranlasst, einen Arbeitskreis einzurichten, der sich mit der Evaluierung des IuKDG befasst und etwa notwendige Gesetzesänderungen vorbereitet. Die Erfahrungen aus der Datenschutzpraxis wurden auch in diesen Arbeitskreis eingebracht.

2.3 Kontrollzuständigkeiten nach dem Telekommunikationsgesetz

In Abschnitt 2.2 wurde bereits über Rechtsprobleme berichtet, die sich bei der Abgrenzung von Tele- und Mediendiensten hinsichtlich der anzuwendenden Vorschriften und der Kontrollzuständigkeiten ergeben. Ähnliche Probleme sind auch bei der Anwendung des Telekommunikationsgesetzes (TKG) aufgetreten.

§ 91 Abs. 4 TKG trifft für die Verarbeitung personenbezogener Daten bei der geschäftsmäßigen Erbringung von Telekommunikationsdiensten eine auf den ersten Blick klare und eindeutige Regelung: An die Stelle der Kontrolle nach § 38 des Bundesdatenschutzgesetzes (BDSG), die in Nordrhein-Westfalen den Bezirksregierungen Arnsberg und Köln obliegt, tritt eine Kontrolle durch den Bundesbeauftragten für den Datenschutz. Dennoch kann es in Grenzbereichen schwierig werden zu entscheiden, ob bei bestimmten Sachverhalten die Aufsichtsregelungen nach § 91 Abs. 4 TKG oder nach § 38 BDSG greifen. Das wird an folgenden Beispielen deutlich, bei denen es zu Kompetenzkonflikten zwischen dem Bundesbeauftragten für den Datenschutz und den Aufsichtsbehörden der Länder gekommen ist:

Ein Anbieter von Kommunikationsdiensten (vereinfacht ausgedrückt: eine Telefongesellschaft) kann sich zur Akquisition neuer Kunden eines Vertragsvermittlers bedienen, der die Kundin oder den Kunden wirbt und die Bestandsdaten für die Vertragsbegründung und -gestaltung erhebt. Die Tätigkeit des Vertragsvermittlers ist als Datenverarbeitung im Auftrag des Diensteanbieters zu werten, so dass die Verarbeitung der Bestandsdaten der Kontrolle des Bundesbeauftragten für den Datenschutz unterliegt. Fraglich wird die Kontrollzuständigkeit beim weiteren Umgang mit den beim Vermittler gespeicherten Bestandsdaten, wenn etwa kein Vertrag zustande kommt und der Vermittler die Daten für Zwecke verwendet, für die sie nicht erhoben worden sind. Hier kann sich ein Anwendungsbereich für das Bundesdatenschutzgesetz mit der Folge ergeben, dass die Aufsichtsbehörde nach § 38 BDSG zuständig ist.

Probleme ergeben sich auch bei der Wahrnehmung der Kontrollkompetenz gegenüber Unternehmen, die Nebenstellenanlagen betreiben und diese für Privatgespräche ihrer Klientel zur Verfügung stellen (z.B. Krankenhäuser, Hotels). Nach Auffassung des Bundesbeauftragten für den Datenschutz wirkt das Unternehmen dabei an der Erbringung von Telekommunikationsdiensten mit und unterliegt insoweit seiner Aufsicht. Die Aufsichtsbehörden der Länder reklamieren dagegen ihre Zuständigkeit, weil in diesen Fällen keine geschäftsmäßige Erbrin-

gung von Telekommunikationsdiensten vorliegt, die Haupt- oder wesentlicher Geschäftszweck des Unternehmens ist.

Zwischen dem Bundesbeauftragten für den Datenschutz und den obersten Aufsichtsbehörden der Länder besteht Übereinstimmung, dass durch diese noch nicht entschiedenen Zweifelsfragen die wirksame Ausübung der Kontrolle nicht leiden darf. Es darf z.B. nicht vorkommen, dass sich unterschiedliche Behörden nacheinander zu Kontrollbesuchen bei einem Unternehmen anmelden, das Nebenstellenanlagen betreibt. Für die Fälle einer möglichen Überschneidung der Kontrollzuständigkeiten ist deshalb vereinbart worden, dass der Bundesbeauftragte für den Datenschutz und die Aufsichtsbehörden der Länder sich bei datenschutzrechtlichen Maßnahmen gegenseitig unterrichten und ihr Vorgehen miteinander abstimmen. Gleiches gilt in Überschneidungsbereichen für die Herausgabe allgemeiner Verlautbarungen und die Abgabe von Stellungnahmen.

2.4 Telefonverzeichnisse auf CD-ROM

Mit der Entwicklung der Informationstechnik sind neben den herkömmlichen gedruckten Telefonbüchern zunehmend elektronische Telefonverzeichnisse auf CD-ROM auf den Markt gekommen. Solche Verzeichnisse werden nicht nur von den Anbietern von Telekommunikationsdiensten (z.B. der Deutschen Telekom), sondern auch von anderen Unternehmen („Informationsdiensten") herausgegeben, die nicht selbst Telekommunikationsdienste anbieten. Diese Unternehmen unterliegen nicht, wie die Anbieter von Telekommunikationsdiensten, der Kontrolle des Bundesbeauftragten für den Datenschutz, sondern der Kontrolle der Aufsichtsbehörden der Länder. Bereits der 5. Tätigkeitsbericht hat auf datenschutzrechtliche Probleme mit Produkten dieser Art hingewiesen. Solche Probleme beschäftigten die Aufsichtsbehörden weiterhin im Berichtszeitraum:

Die Telekommunikationsanbieter unterliegen bei der Herausgabe ihrer Verzeichnisse gesetzlichen Auflagen durch das Telekommunikationsgesetz (TKG) und die Telekommunikationsdienstunternehmen-Datenschutzverordnung (TDSV). Sie haben z. B. den Willen von Kunden, die eine Aufnahme in das Verzeichnis nicht wünschen, zu beachten und zu dokumentieren. Auch darf über Namen und andere Daten von Kunden, wenn bei Nachfrage nur die Telefonnummer angegeben wird, keine Auskunft gegeben werden; folgerichtig darf es auch nicht ermöglicht werden, mittels einer Telefon-CD-ROM durch Eingabe einer Telefonnummer Namen und weitere Daten des Anschlussinhabers zu ermitteln („Invertsuche").

Während sich die Anbieter von Telekommunikationsdiensten durchweg an die gesetzlichen Auflagen halten, mussten die Aufsichtsbehörden für den Datenschutz feststellen, dass andere Herausgeber von Telefonverzeichnissen auf CD-ROM sich sichtlich nicht daran gebunden fühlen. Sie bieten eine Vielzahl von Suchmöglichkeiten an, darunter auch die Invertsuche. Wer in einer Zeitungsanzeige, wie es häufig vorkommt, nicht seinen Namen und seine Adresse, sondern nur eine Telefonnummer angibt, hat damit nicht mehr die Gewähr, dass er anonym bleibt.

Es ist umstritten, ob Unternehmen, die nicht selbst Telekommunikationsdienste anbieten, überhaupt Telefonverzeichnisse auf CD-ROM herausgeben dürfen, es sei denn, sie könnten eine datenschutzrechtlich korrekte Einwilligung aller Betroffenen nachweisen. Die Aufsichtsbehörden der Länder vertreten, wie auch der Bundesbeauftragte für den Datenschutz, einheit-

lich die Rechtsauffassung, dass jedenfalls die Herausgabe von CD-ROM, welche die Invertsuche ermöglichen, datenschutzrechtlich unzulässig ist, weil sonst schutzwürdige Belange der Betroffenen verletzt würden. Wer insoweit in seinen Rechten verletzt wird, kann sich durch Inanspruchnahme der Gerichte dagegen wehren. Den Aufsichtsbehörden sind dagegen weitgehend die Hände gebunden, weil ihre Zuständigkeit sich nach dem Sitz der Vertriebsfirma richtet und die beanstandeten Produkte, die auf den deutschen Markt kommen, regelmäßig von Niederlassungen der betreffenden Unternehmen im Ausland vertrieben werden.

Am Rande sei vermerkt, dass die Herausgabe von Telefonverzeichnissen auf CD-ROM auch urheberrechtliche Fragen aufwirft. Die Herausgeber haben sich die benötigten Daten in der Vergangenheit teilweise durch Einscannen von Telefonbüchern und teilweise auch auf die Weise verschafft, dass sie alle deutschen Telefonbücher durch Hunderte von Arbeitskräften aus Ostasien abschreiben ließen. Der Bundesgerichtshof hat inzwischen entschieden, dass derartige Praktiken das sogenannte Leistungsschutzrecht des Urhebers verletzen. Gewerbliche Anbieter von Telefonverzeichnissen auf CD-ROM bedürfen somit für die Übernahme von Kundendaten aus Telefonbüchern einer Lizenz des Inhabers des Leistungsschutzrechts. Dabei stellt sich die Frage, ob der Lizenznehmer von datenschutzrechtlichen Bindungen freigestellt werden kann, denen der Lizenzgeber unterliegt.

2.5 Scoring-Verfahren bei der SCHUFA

Im fünften Tätigkeitsbericht der Landesregierung für den Berichtszeitraum 1995/1996 wurde bereits die Einführung des „Scoring-Verfahrens" bei der SCHUFA behandelt. Aus datenschutzrechtlicher Sicht wurde die grundsätzliche Zulässigkeit des Verfahrens aufgezeigt, aber auch über Einzelprobleme berichtet, die sich aus einer mangelnden Durchschaubarkeit des Verfahrens für den Kunden ergaben. Diese Probleme haben die Aufsichtsbehörden weiter beschäftigt.

Scoring ist ein Punktbewertungsverfahren (Score = Punktzahl), das auf mathematisch-statistischen Analysen der Daten beruht, die der SCHUFA vorwiegend von ihren Anschlusspartnern – soweit erforderlich, mit Einwilligung der Betroffenen – übermittelt worden sind. In dem Scorewert spiegelt sich der Grad des Risikos einer Kundenbeziehung wider. Der aktuelle Scorewert eines Kunden kann sich mit der Aktualisierung des Datenbestandes über seine Person laufend ändern und wird den SCHUFA-Anschlusspartnern im Rahmen einer beantragten Auskunft stichtagsbezogen mitgeteilt.

Aus der Sicht der Aufsichtsbehörden ist bedenklich, dass die Betroffenen über die Verarbeitung ihrer Daten in einem Scoring-Verfahren keine Mitteilung erhalten und auch nicht erfahren können, welche Scorewerte dem Unternehmen, bei dem sie Kunde sind, wann und wie oft übermittelt worden sind. Im Berichtszeitraum haben sich betroffene Bürgerinnen und Bürger vermehrt an die Aufsichtsbehörden gewandt und beanstandet, dass im Rahmen einer kostenpflichtigen Selbstauskunft keine Score-Informationen gegeben würden.

Die SCHUFA hält die Durchführung des Scoring-Verfahrens durch die von den betroffenen Kunden unterzeichnete allgemeine Einwilligungsklausel für rechtlich abgedeckt, auch ohne dass das Scoring-Verfahren ausdrücklich darin erwähnt wird; sie hält sich auch nicht für verpflichtet, den Betroffenen über die ermittelten Scorewerte Auskunft zu geben, weil diese veränderlich sind und nicht in den Datensätzen der Betroffenen bei der SCHUFA gespeichert werden.

In den Verhandlungen des „Düsseldorfer Kreises" mit der SCHUFA wurde angestrebt, eine bessere Transparenz des Verfahrens für die Betroffenen zu erreichen. Inzwischen zeichnet sich ein Erfolg ab. Bei der anstehenden Weiterentwicklung und Modernisierung der

„SCHUFA-Klausel" soll nunmehr in diese auch eine Information über das Scoring-Verfahren aufgenommen werden. Weitere Informationen zum Scoring sollen einem Merkblatt zu entnehmen sein, das den Kunden der SCHUFA-Anschlusspartner von diesen auf Verlangen ausgehändigt wird. In Bezug auf die Mitteilung von Scorewerten an Betroffene verweist die SCHUFA darauf, dass die Kunden ihre Scorewerte bei dem Unternehmen erfahren können, das sie erhalten hat. Ob dies zur Unterrichtung der Kunden ausreicht, bedarf noch der Klärung und der Beobachtung der weiteren Entwicklung durch die Aufsichtsbehörden.

2.6 SCHUFA-Selbstauskünfte von Mietinteressenten

Auch im Berichtszeitraum mussten sich die Aufsichtsbehörden im nicht-öffentlichen Bereich wiederum mit der Praxis einiger Vermieter befassen, von Mietinteressenten regelmäßig die Vorlage einer SCHUFA-Selbstauskunft zu verlangen. Dies ist aus datenschutzrechtlicher Sicht nicht unproblematisch. Es ist zwar anzuerkennen, dass die Wohnungswirtschaft daran interessiert ist, „schwarze Schafe" vor dem Abschluss eines Mietvertrags zu erkennen, und ihr daher an einer Bonitätsprüfung gelegen ist.

Ausgehend vom Grundsatz der Erforderlichkeit benötigt jedoch die Wohnungswirtschaft lediglich in den Fällen, in denen die ansonsten vorgelegten Unterlagen für eine abschließende Aussage über die Bonität des Wohnungsbewerbers nicht ausreichen, die SCHUFA-Selbstauskunft als zusätzliches Entscheidungskriterium.

Die Arbeitsgruppe „Auskunfteien", eine Unterarbeitsgemeinschaft des „Düsseldorfer Kreises", ist in Gespräche mit der SCHUFA eingetreten, um zu klären, ob ein speziell auf die Wohnungswirtschaft zugeschnittenes Auskunftsverfahren eingerichtet werden kann. Denkbar wäre etwa, ein solches Verfahren auf die Übermittlung von Negativdaten zu beschränken und vorher die Einwilligung der oder des Betroffenen einzuholen.

2.7 Kreditinformation

Ein ständiges Wachstum ist besonders auf dem Markt für Kredite und auf Kredit gewährte Produkte festzustellen. Zu den Bankkrediten und Leasinggeschäften treten zunehmend kreditähnliche Vorleistungen und Ausfallrisiken, z.B. bei Online-Diensten, Teleshopping, Mobilfunk usw., hinzu. Dadurch entsteht im zunehmendem Maß ein Bedarf an Bonitätsprüfungssystemen.

Bislang war die SCHUFA das einzige größere Kreditinformationssystem für Endverbraucher. Nunmehr soll ein neues, umfassend angelegtes Informationssystem über die Kreditwürdigkeit und Zahlungsfähigkeit von Privatpersonen eingerichtet werden, das im Gegensatz zur SCHUFA, die sich weitgehend auf Vertragspartnerschaften mit Unternehmen des Geld- und Warenkreditbereichs beschränkt, erheblich erweitert ist, z.B. auf Versicherungen, Telekommunikationsunternehmen als Vertragspartner. Die diesem System angeschlossenen Vertragspartner sollen verpflichtet werden, ihrerseits Informationen über das Zahlungsverhalten der Kunden zu liefern. Auch sollen branchenübergreifende Informationen mit öffentlich zugänglichen Informationen (wie Konkursen, Vergleichen, Haftbefehlen usw.) mit den Inkassodaten des Unternehmens und anderer Datenbanken verknüpft werden. Neben soziodemographischen Beschreibungen sollen u.a. auch Verfahren wie Credit-Scoring, Verhaltens-Scoring angeboten werden.

Das Unternehmen hatte sich mit seinem geplanten Konzept frühzeitig an die zuständige Aufsichtsbehörde für Datenschutz im nicht-öffentlichen Bereich zur datenschutzrechtlichen Bewertung gewandt. In langwierigen Verhandlungen ist es der örtlichen Aufsichtsbehörde unter Einschaltung des „Düsseldorfer Kreises", der Arbeitsgemeinschaft der obersten Datenschutzaufsichtsbehörden der Länder für den nicht-öffentlichen Bereich, gelungen, mit dem Unternehmen ein datenschutzfreundliches Konzept zu erarbeiten, um eine möglichst umfassende Transparenz gegenüber den Betroffenen sowie Freiwilligkeit bzw. Ausschlussmöglichkeiten einer Datenübermittlung zu erreichen. Die Betroffene müssen darüber informiert werden, welche Daten zu ihrer Person gespeichert werden und welchem Empfängerkreis ggf. die Daten zur Verfügung stehen. Auch ist darauf zu achten, dass anfragende Vertragspartner nur im Rahmen ihres berechtigten Interesses Informationen erhalten. Eine Verbindung von Bonitätsprüfung und Direktmarketing soll ausgeschlossen werden.

2.8 Adresshandel und Direktmarketing

Adresshandel und Direktmarketing sind eine derzeit ständig wachsende Geschäftsbranche. Unter Direktmarketing sind alle Aktivitäten zu verstehen, die es möglich machen, einem Teil der Bevölkerung durch Post, Telefon oder andere Direktmedien Waren oder Dienstleistungen anzubieten oder sonstige Mitteilungen zu übersenden, die informieren oder eine Reaktion hervorrufen sollen. Es geht darum, einen potentiellen Kunden mit Werbung direkt, d.h. persönlich, anzusprechen. Während früher Direktmarketing hauptsächlich vom Versandhandel genutzt wurde, versuchen heute alle Branchen, hierüber an zahlungskräftige Kundschaft heranzukommen. Gleichzeitig fühlen sich immer mehr Bürgerinnen und Bürger durch die Werbeflut in ihren Briefkästen belästigt. Auch Briefkastenaufkleber, wie „Keine Werbung bitte", verfehlen ihre Wirkung, zumal diese Aufkleber keinen Schutz bieten vor Werbematerial, das persönlich an die Betroffenen adressiert und per Post versandt wird.

Wer gezielt werben will, nimmt oft die Dienstleistungen eines Adressenunternehmens in Anspruch. Dieses benötigt außer der Adresse weitere Zusatzinformationen, etwa über die berufliche Tätigkeit, über Einkommens- und Vermögensverhältnisse, Familie, Gesundheit, Schulbildung, Urlaubs- und Reiseverhalten, Freizeitaktivitäten, Auto, Wohnung, Kauf- und Konsumverhalten.

Adressenunternehmen verkaufen ihre personenbezogenen Datensätze um so teurer, je detaillierter die Informationen über die potentiellen Kunden sind. Immer öfter werden deshalb bundesweit von verschiedenen Firmen „Lifestyle-Befragungen" oder „Haushaltsumfragen" durchgeführt, in denen meist weit über 100 Fragen zu den o.g. Bereichen gestellt werden. Oftmals wird eine Teilnahme an einer Verlosung in Aussicht gestellt.

Bei solchen Befragungen handelt es sich jedoch nicht um Marktforschung, sondern darum, aufgrund der erstellten Persönlichkeitsprofile eine gezielte Ansprache zu ermöglichen.

Gegen diese Praxis bestehen nur dann keine grundsätzlichen datenschutzrechtlichen Bedenken, wenn die Befragten nach umfassender Aufklärung über die vorgesehene Verwendung ihrer Daten ihre schriftliche Einwilligung erklärt haben. Der „Düsseldorfer Kreis", der sich im Berichtszeitraum aufgrund zahlreicher Beschwerden eingehend mit der Problematik befasst

hat, einigte sich einstimmig, folgende Mindestanforderungen an derartige Umfragen zu stellen:

1. Es muss klar erkennbar sein, dass die Angaben nicht nur anonym, sondern auch personenbezogen ausgewertet werden,

2. es muss ferner erkennbar sein, für welche Zwecke die Angaben verwendet werden, z.B. für persönlich adressierte Werbung,

3. weiter muss eine unterschriebene Einwilligung auf dem Fragebogen erfolgen, und zwar von allen volljährigen bzw. einsichtsfähigen Betroffenen.

2.9 Elektronische Geldbörse („GeldKarte")

Bereits der 5. Tätigkeitsbericht enthielt Ausführungen über die elektronische Geldbörse. Diese Zahlungsform ist unter dem Namen „GeldKarte" weiter auf dem Vormarsch. Wegen der damit verbundenen datenschutzrechtlichen Probleme bedarf die Angelegenheit erneuter und vertiefter Betrachtung.

Als GeldKarte dient die von den Banken ausgegebene EC-Karte, die mit einem Multifunktionschip ausgerüstet ist. Sie ist an ein Girokonto gebunden und wird an einem Ladeterminal mit einem Geldbetrag bis 400 DM aufgeladen, der von dem Girokonto abgebucht wird. Der Vorgang des Ladens wird mit Kartendaten, Betrag und Datum bei einer sog. Karten-Evidenzzentrale (KEZ) des zuständigen Spitzenverbandes der Kreditwirtschaft gespeichert. Die GeldKarte kann zum bargeldlosen Einkauf bei Händlern benutzt werden, die dem Verfahren angeschlossen sind. Die Zahlung erfolgt durch Abbuchung des Kaufbetrages von der GeldKarte in einem Händlerterminal. Die Transaktionsdaten des Händlers werden an eine sog. Händler-Evidenzzentrale (HEZ) übermittelt, die ihrerseits die aufbereiteten Daten an die zuständige KEZ weiterleitet, sie aber auch selbst bis zu einer Zeitdauer von sieben Jahren speichert. Die KEZ führt die übermittelten Daten mit den bei ihr gespeicherten Daten der GeldKarte zusammen.

Die eigentliche Zahlungsabwicklung und Buchung erfolgt - mit Hilfe der Datenverarbeitung bei den beiden Evidenzzentralen - über die Konten des Händlers bzw. des Käufers bei ihrer jeweiligen Bank. Bei den Evidenzzentralen entstehen jedoch Schattenkonten, auf denen sich im Lauf der Zeit eine Vielzahl von Daten über das Kaufverhalten der einzelnen Karteninhaber ansammeln kann. Solche Daten können z.B. für die Direktwerbung dritter Unternehmen von erheblichem Interesse sein, und ihre Weitergabe an diese würde entsprechend honoriert werden. Die Schattenkonten werden zwar nur anhand der EC-Kartennummern geführt und enthalten weder Namen noch Anschriften der Karteninhaber. Diese könnten jedoch mit Hilfe der bei den Banken gespeicherten Kundendaten identifiziert werden. Es gibt zwar derzeit keinerlei Hinweis auf derartige Absichten, die eindeutig rechtswidrig wären; denn sie würden von der Zweckbestimmung des Vertragsverhältnisses zwischen der Bank und ihren Kunden nicht gedeckt, und etwaigen darauf gerichteten Interessen würden schutzwürdige Belange der Betroffenen entgegenstehen. Da es jedoch in der Kreditwirtschaft allgemein üblich ist, Vorkehrungen zur Sicherung gegen Missbrauch zu treffen, sind entsprechende Forderungen auch hier

angebracht. Zumindest müsste die Archivierung der Daten auf die rechtlich und tatsächlich erforderliche Mindestdauer beschränkt werden. Weiter sollten die Rechtsbeziehungen zwischen den Banken und den Evidenzzentralen als Datenverarbeitung im Auftrag gestaltet werden, die den Weisungen der Banken unterliegt. Auch müsste geklärt werden, wie die Betroffenen ihre Auskunftsrechte geltend machen können.

Die technische Leistungsfähigkeit der Chipkarte ermöglicht über die Nutzung als GeldKarte hinaus vielfältige Zusatzanwendungen. So ist z.B. eine Zusatzfunktion der GeldKarte als elektronischer Fahrausweis in der Entwicklung. Hier gilt es zu verhindern, dass über das notwendige Maß hinaus Datenspuren gelegt und dem Missbrauch ausgeliefert werden. Besonders wichtig ist es in diesem Zusammenhang, dass die einzelnen Funktionen der Karte getrennt bleiben und ihre Vermischung durch technische Maßnahmen verhindert wird.

Sowohl bei der GeldKarte selbst als auch bei ihren möglichen Zusatzfunktionen lassen sich die geschilderten datenschutzrechtlichen Probleme vermeiden, wenn anstelle von kontogebundenen Karten sog. White Cards verwendet werden, die nicht durch Abbuchung von einem Konto, sondern durch Bareinzahlung aufgeladen werden und damit keine Identifizierung des Inhabers ermöglichen. Sie sind als Alternative zur kontogebundenen GeldKarte bei den Kreditinstituten erhältlich.

2.10 Outsourcing bei Kundenbefragungen von Banken

Im Berichtszeitraum hatten sich die Aufsichtsbehörden mit datenschutzrechtlichen Fragen zu befassen, die sich im Zusammenhang mit den verschiedenen Formen des „Outsourcing" ergaben. Unter diesem Begriff (engl. Auslagerung) wird die Übergabe von Firmenbereichen, die nicht das Kerngeschäft eines Unternehmens betreffen, an andere, dienstleistende Unternehmen verstanden, die auf diese Bereiche spezialisiert sind.

Eine Fallgruppe von Outsourcing stellen Kundenbefragungen von Banken dar, die nicht von diesen selbst durchgeführt, sondern auf Meinungsforschungsinstitute übertragen werden. Zwischen der Arbeitsgruppe „Kreditwirtschaft" des „Düsseldorfer Kreises" und den Spitzenverbänden der Kreditwirtschaft ist umstritten, wie die Weitergabe von personenbezogenen Kundendaten der Bank, ihre Verarbeitung bei dem Meinungsforschungsinstitut und ihre Rückgabe im Rahmen der Befragungsergebnisse datenschutzrechtlich zu qualifizieren ist. Die Vertreter der Kreditwirtschaft sehen darin eine Datenverarbeitung im Auftrag im Sinne des § 11 des Bundesdatenschutzgesetzes (BDSG), wobei die Verantwortung für die Datenverarbeitung ausschließlich bei der auftraggebenden Bank verbleibt. Dagegen betrachten die Vertreter der obersten Aufsichtsbehörden den Vorgang als Funktionsübertragung, weil solche Befragungen von den Meinungsforschungsinstituten regelmäßig in eigener Kompetenz gestaltet werden.

Die Unterscheidung ist datenschutzrechtlich aus folgenden Gründen von Bedeutung:

Bei Funktionsübertragung ist die Einwilligung aller Betroffenen in die Übermittlung personenbezogener Daten unabdingbar, da – nach Auffassung der Aufsichtsbehörden – bei den vorkommenden Fallgestaltungen regelmäßig kein Erlaubnistatbestand vorliegt, der eine Einwilligung entbehrlich macht. Im Fall der Auftragsdatenverarbeitung liegt wegen des Verbleibs der Verantwortlichkeit beim Auftraggeber und der Weisungsgebundenheit des Auftragnehmers eine einwilligungsbedürftige Übermittlung personenbezogener Daten nicht vor.

Nach Diskussion der unterschiedlichen Standpunkte besteht immerhin Einigkeit, dass die Entscheidung, ob eine Funktionsübertragung oder eine Auftragsdatenverarbeitung vorliegt, von der konkreten Gestaltung der Beziehungen zwischen dem Kreditinstitut und dem Dienstleistungsunternehmen abhängt. Wenn auch nach Auffassung der obersten Aufsichtsbehörden eine strikte Auslegung des § 11 BDSG nach wie vor grundsätzlich für Funktionsübertragung

spricht, kann in Einzelfällen von Outsourcing eine Auftragsdatenverarbeitung anerkannt werden, und zwar umso eher, je stärker die Vereinbarungen der Beteiligten folgende Merkmale aufweisen:

1. Eindeutige Festlegung der Verantwortlichkeit und der Weisungsrechte des beauftragenden Unternehmens, möglichst gesichert durch die Vereinbarung von Vertragsstrafen.

2. Beschränkung auf das unverzichtbare Maß der Bekanntgabe von personenbezogenen Daten an das Dienstleistungsunternehmen; bei Kundenbefragungen z.B. ausschließliche Mitteilung des Namens und der Anschrift des Kunden, der sodann von dem Dienstleistungsunternehmen einen Fragebogen unter Hinweis auf die Freiwilligkeit der Angaben erhält.

3. Möglichst weitgehende und möglichst frühzeitige Anonymisierung der Daten. Vom Zeitpunkt der vollständigen Anonymisierung an sind weitere Verfahrensschritte datenschutzrechtlich nicht mehr relevant.

4. Unterrichtung der betroffenen Kunden über die weitergegebenen Daten, die damit verfolgten Ziele und den Verbleib der datenschutzrechtlichen Verantwortung bei „ihrem" Institut als Vertragspartner. In einer solchen Klarstellung, die sich - auch ohne Benachrichtigungspflicht nach § 33 BDSG - am Transparenzgebot und an sonstigen schutzwürdigen Belangen der Kunden orientiert, liegt ein Indiz für eine Datenverarbeitung im Auftrag.

Unberührt bleiben etwaige zusätzliche Erfordernisse, die sich aus der Verpflichtung zur Wahrung des Bankgeheimnisses ergeben.

2.11 Geldwäschegesetz

Mit Inkrafttreten des Gesetzes über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz – GwG) vom 25. Oktober 1993 besteht für die Kredit- und Finanzinstitute sowie Spielbanken die Verpflichtung, unter bestimmten Voraussetzungen Finanztransaktionen den zuständigen Strafverfolgungsbehörden anzuzeigen (§ 11 GWG). Damit ist die aus datenschutzrechtlicher Sicht als besonders sensibel angesehene Verpflichtung der Geldinstitute gegeben, als quasi staatlicher Ermittlungshelfer Verdachtsfälle der Geldwäsche anzuzeigen.

Es handelt sich um eine verfassungsrechtlich ungewöhnliche Verpflichtung der Kreditinstitute, als quasi polizeilicher verlängerter Arm tätig zu werden. Hierbei wird es als besonders wichtig angesehen, die hohe Zahl der im Ergebnis nicht zu einer strafrechtlichen Verfolgung bzw. Ahndung führenden Verdachtsanzeigen wesentlich zu reduzieren. Mit jeder Verdachtsanzeige werden Wirtschaftsdaten von Privatpersonen und/oder Unternehmen offenbart und ein damit besonders sensibler Bereich privater, grundsätzlich staatsfreier Lebensführung offengelegt. Dies ist mit Blick auf das verfassungsrechtliche Gebot der Verhältnismäßigkeit staatlicher Eingriffsmaßnahmen nicht unproblematisch und kann auf Dauer nur hingenommen werden, wenn die „Trefferquote" der Verdachtsanzeigen bei gleichzeitig deutlicher Reduzierung der Anzahl deutlich zunehmen würde. Hier erscheint eine möglichst effektive Information der Kreditinstitute durch die Strafverfolgungsbehörden bzw. die staatlichen Aufsichtsstellen über das Kreditwesen mit einer besseren Sensibilisierung für bekannte und typische, aber auch für neue Formen der Geldwäsche notwendig.

Das Thema wurde im Berichtszeitraum in zahlreichen Gesprächen mit Vertretern der Kreditwirtschaft erörtert. Dabei wurde deutlich gemacht, dass die Kreditinstitute bei der Entwicklung von Grundsätzen, Verfahren und Kontrollen nach § 14 Abs. 2 Nr. 2 GwG zwischen den Zielen des Geldwäschegesetzes und den Erfordernissen des Datenschutzes abwägen müssen. Eine permanente Überwachung aller Kunden- und Kontobeziehungen wäre weder von den Vorschriften des Geldwäschegesetzes gedeckt noch mit dem Datenschutzrecht vereinbar. Automatisierte Überwachungssysteme müssen daher den einzelnen Instituten angemessenen Spielraum zur Entscheidung über einen flexiblen Einsatz geben. Der Bankenfachverband hat dem „Düsseldorfer Kreis" ein Research-System zur Prävention der Geldwäsche vorgestellt, das den Anforderungen des Bundesaufsichtsamtes für das Kreditwesen entsprechen und zu-

gleich den Kreditinstituten den erforderlichen Entscheidungsspielraum bei der Anwendung geben soll. Das System wird derzeit vom „Düsseldorfer Kreis“ geprüft. Die Gespräche mit der Kreditwirtschaft über dieses Thema werden fortgeführt.

2.12 Aufgabe einer Arztpraxis/Verbleib der ärztlichen Unterlagen

Eine Aufsichtsbehörde wurde über eine bereits längere Zeit andauernde unsachgemäße Lagerung von Patientenunterlagen (ca. 5.000 Karteikarten und ca. 15.000 Röntgenaufnahmen mit Patientendaten) informiert. Die sensiblen Unterlagen, die im Hinblick auf die ärztliche Schweigepflicht einer besonderen Umgangssorgfalt unterliegen, waren in einem für alle Bewohner und Besucher eines größeren Miethauses zugänglichen Kellerraum und im Kellerflur offen gelagert. Der für die Lagerung eigentlich verantwortliche Arzt und Betreiber einer Röntgenpraxis war verstorben. Die aufgrund fehlender Erben in der Zwischenzeit ausgefochtenen Streitigkeiten zwischen dem Nachlassverwalter, der Praxisnachfolgerin, die die Übernahme der Unterlagen angeblich vertraglich ausgeschlossen hatte, der Ärztekammer Nordrhein, die sich für unzuständig erklärte, und dem Hauseigentümer führten zu pressewirksamen Aktionen, wie beispielsweise einem Bericht über ein angebliches Angebot eines Lampenherstellers, der die Röntgenbilder für Lampenschirme verwenden wollte.

Nachdem die Aufsichtsbehörde Kenntnis von diesem untragbaren Zustand erhalten hatte, wurden die Unterlagen auf Veranlassung der Datenschutzaufsichtsbehörde zunächst durch das Ordnungsamt der zuständigen Kommune gesichert und anschließend bei einem geeigneten Unternehmen, das auf die datenschutzgerechte Lagerung und Vernichtung von sensiblen Unterlagen spezialisiert ist, in verplombten Behältnissen gelagert, wo sie sich noch heute befinden.

Die Prüfung, welche Person oder Stelle für die ordnungsgemäße Lagerung verantwortlich ist, hat bislang mangels gesetzlicher Regelungen für diesen Fall zu keinem abschließenden Ergebnis geführt. Nach einer Empfehlung der Bundesärztekammer sollen solche Unterlagen durch die örtliche Ärztekammer übernommen werden.

Eine Ordnungsverfügung der örtlichen Ordnungsbehörde zur Übernahme der Unterlagen durch die Ärztekammer Nordrhein war erfolglos, da in die Rechte von Hoheitsträgern – nach § 1 Satz 2 Heilberufsgesetz NW ist die Ärztekammer Nordrhein eine Körperschaft öffentlichen Rechts und mithin Hoheitsträger – mangels sachlicher Zuständigkeit der Polizei- und Ordnungsbehörden nicht eingegriffen werden darf. Weil es der örtlichen Ordnungsbehörde an der erforderlichen ärztlichen Fachkompetenz fehlt, um den Zweck der gesetzlichen Aufbewahrungspflichten (Herausgabe von Unterlagen an Patienten; Information über Krankheits-

bilder etc.) zu erfüllen, kann es bei der derzeitigen Aufbewahrung der Patientenunterlagen nicht bleiben.

Da die Ärztekammer Nordrhein nach wie vor eine freiwillige Übernahme ablehnt und die Lagerung der Patientenunterlagen noch mit nicht unbeträchtlichen Kosten für die öffentliche Hand behaftet ist, bedarf es auch im Hinblick auf künftige vergleichbare Fälle dringend einer gesetzlichen Regelung zum Umgang mit Patientenunterlagen, wie sie bereits 1995 in einem von der Aufsichtsbehörde begrüßten Entwurf zur Änderung des Gesundheitsdatenschutzgesetzes Nordrhein-Westfalen vom damaligen Ministerium für Arbeit, Gesundheit und Soziales vorgesehen war. Die vorgesehene Gesetzänderung hätte dazu geführt, dass im beschriebenen Fall die zuständige Ärztekammer nach § 31 Abs. 1 des Gesetzes zur Aufbewahrung verpflichtet gewesen wäre.

Das Innenministerium ist an das Ministerium für Frauen, Jugend, Familie und Gesundheit herangetreten und hat gebeten, wegen des dringenden Regelungsbedarfs eine entsprechende Vorschrift auf Landes- oder Bundesebene zu initiieren.

2.13 Apothekenrechenzentren

Durch den Hinweis eines Krankenkassen-Bundesverbandes ist das Innenministerium darauf aufmerksam gemacht worden, dass die Absicht besteht, bei Abrechnungszentren von Apotheken angefallene personenbezogene Daten (abrechnungs-) zweckentfremdet u.a. auch für Werbezwecke zu verwenden.

Nach der geltenden Rechtslage ist die zweckentfremdete Nutzung dieser Gesundheitsdaten (z.B. zu Werbezwecken) als Verstoß gegen die Bestimmungen des hier anzuwendenden Bundesdatenschutzgesetzes anzusehen.

Um einem Missbrauch dieser sensiblen Gesundheitsdaten außerhalb ihrer Zweckbestimmung entgegenzutreten, hat sich das Innenministerium des Landes an das Bundesministerium für Gesundheit gewandt. Dieses teilte mit, dass das Problem dort bekannt sei und derzeit geprüft werde, ob und bei welcher nächster Gelegenheit eine gesetzliche Regelung vorgeschlagen werden soll.

2.14 Videoüberwachung

Videoüberwachung im nicht-öffentlichen Bereich hat in den letzten Jahren stetig zugenommen. Während sie für staatliche Zwecke in den Polizeigesetzen von Bund und Ländern, aber auch in der Strafprozeßordnung detailliert geregelt wird, besteht nach wie vor keine Rechtsklarheit darüber, unter welchen Voraussetzungen Videoüberwachung durch private Stellen zulässig ist.

Zwar ist Videoüberwachung in Deutschland noch nicht so verbreitet wie in anderen Ländern, z.B. in Großbritannien, wo Videoüberwachungssysteme geradezu Hochkonjunktur haben und teilweise bereits flächendeckend zur Beobachtung öffentlicher Plätze und sogar ganzer Städte eingesetzt werden. Dennoch zeichnet sich auch hier eine Tendenz zu einer wachsenden Videoüberwachung insbesondere innerstädtischer Bereiche durch private Betreiber ab. So werden die Systeme etwa in Warenhäusern und Kreditinstituten, aber auch in Bahnhöfen, Parkhäusern, Taxis, Tankstellen oder auf öffentlichen Wegen eingesetzt.

Videoüberwachungen können sehr unterschiedlichen – durchaus auch positiven - Zwecken dienen, z.B. der Kontrolle von Geschäftseingängen, der Einlasskontrolle und von Nebeneingängen, der Sicherung von Personen vor Überfällen oder Unfällen, der Sicherung von Geld- und Sachwerten. Es müssen aber unterschiedliche verfassungsrechtlich geschützte Güter wie Leben, Gesundheit oder Eigentum mit dem ebenfalls geschützten Grundrecht auf informationelle Selbstbestimmung in Einklang gebracht werden.

Problematisch an der Videoüberwachung ist nicht nur, dass unbescholtene Personen in ihr Visier geraten, sondern dass dabei auch immense Mengen von Daten anfallen. Es besteht daher ein dringender datenschutzrechtlicher Regelungsbedarf zum Einsatz von Maßnahmen zur Videoüberwachung. Dabei ist klarzustellen, unter welchen Voraussetzungen eine solche Überwachung zulässig ist. Dringend notwendig ist insbesondere eine Regelung der Fälle, in denen die Bürger ausdrücklich auf die Videoüberwachung, z.B. in Geschäftsräumen oder Banken, hingewiesen werden müssen. Ferner ist zu regeln, unter welchen Voraussetzungen die Aufnahmen gespeichert und für welche Zwecke sie genutzt werden dürfen.

Es wäre zu begrüßen, wenn der Bundesgesetzgeber das neue Bundesdatenschutzgesetz, das auf diesen Bereich anzuwenden ist, um eine entsprechende Regelung ergänzen würde.

Besorgniserregende Tendenzen, den Alltag immer mehr zu entprivatisieren, sind bei einem neuen Projekt festzustellen, bei dem eine Gebäude-Bild-Datenbank aufgebaut wird, die nach Fertigstellung fast alle Gebäude – auch Wohnhäuser – im gesamten Bundesgebiet erfassen soll. Auch in einigen Großstädten Nordrhein-Westfalens sind entsprechende Bildaufzeichnungen erfolgt. Die Aufnahmen der einzelnen Gebäude werden ohne Wissen und ausdrückliche Einwilligung der betroffenen Hauseigentümer oder –bewohner gefertigt, wobei die Verwendung des Datenmaterials unklar ist.

Die denkbaren Auswirkungen einer Entwicklung, die darauf hinausläuft, im Informationszeitalter die Privatsphäre immer mehr zu beeinträchtigen, sind gravierend. Immerhin sind Erkenntnisse zu gewinnen, die einen Menschen und sein persönliches Umfeld genau beschreiben. Das bisherige Datenschutz-Instrumentarium kann mit dieser Entwicklung nicht Schritt halten.

Zum Schutz der Privatsphäre gehört im Kernbereich, dass jeder selbst darüber bestimmen kann, wer was wann bei welcher Gelegenheit über ihn weiß. Eine verfassungsrechtliche Grenze ist das Verbot, teilweise oder vollständige Persönlichkeitsprofile zu erstellen, es sei denn, die Bürger sind ausreichend informiert und haben zugestimmt. Dieses Verbot wird in Frage gestellt, wenn immer mehr verknüpfbare personenbezogene Informationen zur Verfügung stehen. Hier muss der Bundesgesetzgeber klare Grenzen aufzeigen und Eingriffsmöglichkeiten für die zuständigen Aufsichtsbehörden schaffen, damit die schutzwürdigen Belange der Bevölkerung ausreichend zur Geltung kommen.

3. Einzelfälle aus der aufsichtsbehördlichen Praxis

3.1 Unerlaubte Abfrage von SCHUFA-Daten

Ein Bürger legte dar, dass eine Bank unbefugterweise SCHUFA-Daten zu seiner Person abgerufen habe. Er belegte dies mit einer von ihm bei der SCHUFA beantragten Selbstauskunft. Hierin war eine Kreditanfrage der Bank ausgewiesen. Nach Aussage des Betroffenen hatte er bei der Bank aber keinen Kredit beantragt.

Seitens der zuständigen Aufsichtsbehörde für den Datenschutz erfolgte hierauf ein Prüfungs- und Informationsgespräch bei der Bank. Es stellte sich heraus, dass das Unternehmen telefonische SCHUFA-Anfragen durchführte. Zur Identifikation der anfragenden Stelle war es zwar erforderlich, dass Firmenname, eine Kennziffer und ein Passwort anzugeben waren. Zur Abwicklung von telefonischen Anfragen waren bei der Bank mehrere Mitarbeiter befugt. Welcher Mitarbeiter die unerlaubte Auskunft einholte, war weder bei der Bank noch bei der SCHUFA festzustellen.

Die Vorschriften zur technischen Abwicklung des SCHUFA-Verfahrens sehen zwar vor, dass bei telefonischen Auskünften der Name des Anfragenden aufgezeichnet werden soll. Dieses zusätzliche Identifizierungsmerkmal wurde in vorliegendem Fall aber nicht gespeichert. Dies ist in der Praxis auch kaum hilfreich, da ein unberechtigt Auskunftsuchender kaum seinen richtigen Namen nennen wird. Zur möglichst umgehenden Feststellung unerlaubter Anfragen werden telefonische Auskünfte durch die SCHUFA zur Nachkontrolle schriftlich bestätigt. So auch in diesem Fall. Nach Aussage der Bank hatte man dort ein entsprechendes Schreiben aber nicht erhalten.

Bei der betroffenen Bank erfolgen SCHUFA-Anfragen inzwischen grundsätzlich durch automatisierte Direktabrufe mit gleichzeitiger Zwangsprotokollierung. Zu telefonischen Anfragen ist nur noch ein Mitarbeiter besonders ermächtigt.

Zwar konnte diese Verbesserung für den damals Betroffenen nicht mehr greifen, es ist jedoch zumindest davon auszugehen, dass bei der Bank Wiederholungsfälle künftig aufklärbar sind.

3.2 Erhebung personenbezogener Daten unter Vortäuschung eines berechtigten Interesses durch ein Kreditinstitut und Übermittlung der Daten an einen Firmenkunden

Eine Beschwerde richtete sich gegen die Datenerhebung und –weitergabe durch ein Kreditinstitut. Das Kreditinstitut hatte eine Anfrage über eine Frau an eine Auskunftei gerichtet. Als berechtigtes Interesse wurde „Bonitätsprüfung" angegeben.

Die Auskunftei hatte darauf hin eine Auskunft über die personenbezogenen Daten der Betroffenen an das Kreditinstitut übermittelt. Diese Auskunft hatte das Kreditinstitut anschließend an einen seiner Kunden weitergeleitet. Geschäftsbeziehungen zwischen der Betroffenen und dem Kreditinstitut haben tatsächlich nicht bestanden.

Personenbezogene Daten müssen nach § 28 Abs. 1 Satz 2 BDSG nach Treu und Glauben und auf rechtmäßige Weise erhoben werden. Entgegen dieser Vorschrift hatte das Kreditinstitut jedoch durch die unrichtige Angabe eines berechtigten Interesses die Übermittlung von durch das Bundesdatenschutzgesetz geschützten personenbezogenen Daten, die nicht offenkundig sind, erschlichen.

Ferner hätte das Kreditinstitut als Empfänger der von der Auskunftei übermittelten Daten diese nur für den Zweck verarbeiten oder nutzen dürfen, zu dessen Erfüllung sie übermittelt wurden. Da das Kreditinstitut jedoch gegenüber der Auskunftei angegeben hatte, die Auskunft über die Betroffene nur für eine berechtigte Bonitätsprüfung zu verwenden, wäre eine Verarbeitung oder Nutzung der personenbezogenen Daten der Betroffenen für einen anderen Zweck (hier: Weitergabe an einen Firmenkunden) nur unter den Voraussetzungen des § 28 Abs. 1 und 2 BDSG zulässig gewesen.

Nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG ist die Übermittlung personenbezogener Daten an einen Firmenkunden als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Ein berechtigtes Interesse des Kreditinstitutes an der Weitergabe der personenbezogenen Daten der Betroffenen war nicht erkennbar. Ferner ging die Aufsichtsbehörde davon aus, dass durch die Weitergabe der personenbezogenen Da-

ten an einen Firmenkunden des Kreditinstitutes schutzwürdige Belange der Betroffenen berührt wurden.

Gem. § 28 Abs. 2 Satz 1 Nr. 1 a BDSG ist die Übermittlung oder Nutzung personenbezogener Daten auch zulässig, soweit sie zur Wahrung berechtigter Interessen eines Dritten oder öffentlicher Interessen erforderlich ist und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Weder zur Wahrung berechtigter Interessen des Firmenkunden des Kreditinstitutes noch zur Wahrung öffentlicher Interessen war es erforderlich, die personenbezogenen Daten der Betroffenen zu übermitteln. Darüber hinaus bestand auch Grund zu der Annahme, dass die Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hatte.

Die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich vertrat daher die Auffassung, dass sowohl die Erhebung der personenbezogenen Daten der Betroffenen durch das Kreditinstitut als auch die Übermittlung an den Firmenkunden unzulässig waren.

Das Kreditinstitut und der Firmenkunde wurden aufgefordert, die datenschutzrechtlichen Vorschriften zu beachten.

3.3 Allgemeine Geschäftsbedingungen für die Spielteilnahme mittels Online-Card einer Lotteriegesellschaft

Eine Vielzahl von Datenschutzeingaben betraf im Berichtszeitraum die von einer Lotteriegesellschaft verwendeten Allgemeinen Geschäftsbedingungen für die Spielteilnahme mittels Online-Card.

Nach Ziffer 3 der Allgemeinen Geschäftsbedingungen sollte sich der Spielteilnehmer damit einverstanden erklären, dass seine personenbezogenen Daten gespeichert und zum Zwecke der Werbung verwendet bzw. an andere Unternehmen übermittelt werden. Die Spielteilnahme mittels Online-Card wurde von der Zustimmung zu den Allgemeinen Geschäftsbedingungen abhängig gemacht. Eine Möglichkeit, der Ziffer 3 der Allgemeinen Geschäftsbedingungen zu widersprechen bzw. diesen Passus zu streichen, wurde dem Spielteilnehmer nicht eingeräumt.

Nachdem die Aufsichtsbehörde sich eingeschaltet und datenschutzrechtliche Bedenken vorgetragen hatte, wurde der Online-Card-Antrag überarbeitet, die relevanten Passagen wurden abgeändert.

3.4 Negativdatei über Hotelgäste

Mehrere Unternehmen wandten sich an eine örtliche Aufsichtsbehörde, weil sie beabsichtigen, eine Negativdatei über Hotelgäste für geschäftsmäßige Zwecke anzulegen. Aus einer solchen Datei sollen auf konkrete Anfrage eines Hotelbetriebes die gespeicherten Daten zu einer angefragten Person übermittelt werden. Durch diese Informationsweitergabe sollen Verluste für die Hotelbetreiber wegen zunehmender Kriminalität und sinkender Zahlungsmoral in der Hotelbranche reduziert werden.

Für eine Speicherung in der zentral geführten Negativdatei sind in einem Fall folgende Angaben vorgesehen:

- Name, Anschrift, Geburtsdatum und Passnummer bei ausländischen Gästen
- Vollstreckungsbescheid wegen offener Rechnungen hinsichtlich Verzehr und Übernachtung
- rechtskräftiges Urteil auf Zahlung offener Hotelrechnungen oder wegen vertragswidrigen Verhaltens
- fruchtlose Pfändung
- eidesstattliche Versicherung
- Haftbefehl zur Abgabe einer eidesstattlichen Versicherung
- noch nicht rechtshängige Forderungen bezüglich Verzehr und Übernachtung.

Die Übermittlung der gespeicherten Daten aus der zentral geführten Negativdatei soll unter den Voraussetzungen des § 29 Abs. 2 BDSG erfolgen. Hierbei werden die o.g. Daten an Hotelbetriebe weitergegeben, soweit diese darlegen, dass die angefragte Person ein Hotelzimmer mieten will. Ferner sollen nur die dem Auskunftsverfahren angeschlossenen Hotelbetriebe Informationen aus der Negativdatei erhalten. Die angeschlossenen Hotelbetriebe stellen die Angaben zur Verfügung. Der Hotelgast selbst wird bei der Buchung des Hotelzimmers informiert, dass seine Daten ggf. zur Einspeicherung in eine Negativdatei gelangen. Die angeschlossenen Hotelbetriebe sollen vertraglich verpflichtet werden, dem schutzwürdigen Interesse der Hotelgäste an dem Ausschluss der Übermittlung der Daten ausreichend Rechnung zu tragen. Ebenso wie die Speicherung, soll die Weitergabe von Informationen über Hotelgäste,

die wegen Reklamationen oder Mängeln ihre Rechnung nicht oder nicht in voller Höhe bezahlt haben, eindeutig ausgeschlossen werden.

Die datenschutzrechtliche Prüfung ergab, dass gegen Dateien der geplanten Art keine grundsätzlichen Bedenken bestehen, sofern die Speicherung und Übermittlung sich in den rechtlichen Grenzen des § 29 BDSG halten und die Vorschriften über die Benachrichtigung der Betroffenen, die Auskunft an die Betroffenen und die Berichtigung, Löschung und Sperrung von Daten beachtet werden. Ferner wurde den Betreibern der Datei mitgeteilt, dass die Speicherung und Weitergabe von Angaben über noch nicht rechtshängige Forderungen datenschutzrechtlich nicht zulässig ist. Auch wurde darauf hingewiesen, dass die beabsichtigte Speicherung der Seriennummern amtlicher Ausweise durch das Gesetz über Personalausweise und das Passgesetz eingeschränkt ist und bezüglich der geplanten Hinweisdatei die Vorschriften über die Meldepflicht (§ 32 BDSG) zu beachten sind.

3.5 Unzulässige Einträge in die Kundendatei

Die Eingabe eines Betroffenen wies darauf hin, dass in der Kundendatei eines Auslieferungsrestaurants unzulässige Zusatzinformationen gespeichert werden.

Der Beschwerdeführer berichtete, dass er ein Restaurant, das über einen Lieferservice verfügt, mit einer entsprechenden Warenlieferung beauftragt habe. Bei dem aus früheren Lieferungen bekannten Restaurant war dem Betroffenen bereits zuvor aufgefallen, dass das Unternehmen anhand der Telefonnummer „alte" Kunden erkennen und offensichtlich mit Hilfe eines Computerprogramms die Namen und Adressen abrufen konnte. Bei der letzten Bestellung wurde er jedoch von der die Bestellung entgegennehmenden Person darauf aufmerksam gemacht, dass er in der bereits erwähnten Kundendatenbank mit dem Vermerk: „Vorsicht! Unhöflich!" vermerkt sei und dass eine Belieferung bei einem zweiten Eintrag dieser Art nicht mehr erfolgen würde. Zunächst irritiert fragte der Beschwerdeführer nach, was konkret zu dieser Einschätzung geführt hatte, schließlich sei man mit der erbrachten Dienstleistung des Unternehmens immer zufrieden gewesen. Der Mitarbeiter des Restaurants konnte oder wollte darauf nicht näher eingehen und zog sich auf die Aussage zurück: „Das wäre ein Fakt". Der Beschwerdeführer sah nach dieser Diskussion von einer Bestellung ab, war aber nachhaltig verärgert und wandte sich mit der Bitte um datenschutzrechtliche Klärung an die zuständige Aufsichtsbehörde.

Von der Aufsichtsbehörde wurde daraufhin eine Überprüfung bei der Hauptverwaltung des Unternehmens durchgeführt. Hierbei wurde festgestellt, dass das Unternehmen mehrere Filialen mit Auslieferungsservice in verschiedenen Städten unterhält. Diese Restaurants sind jeweils mit eigenen Computern ausgestattet und arbeiten mit vorgegebenen Programmen weitestgehend selbständig. Diese Computer dienen grundsätzlich der Rechnungsschreibung und dem damit verbundenen Festhalten der Umsatzzahlen. Im Zusammenhang mit der Belieferung von Kunden und der Rechnungserstellung werden Daten wie Name, Anschrift, Telefonnummer und ggf. Zusatzinformationen zur Lieferanschrift gespeichert. Eine Speicherung von Bemerkungen wie im vorliegendem Fall war nach Aussage der Hauptverwaltung weder beabsichtigt noch angeordnet worden.

Eine Überwachung oder Kontrolle der Speicherungspraxis durch Vorgesetzte oder den betrieblichen Beauftragten für den Datenschutz hatte bis dahin offensichtlich nicht stattgefunden.

Die Aufsichtsbehörde hat die Verfahrensweise datenschutzrechtlich beanstandet und das Unternehmen zur Abhilfe aufgefordert. Von der Hauptverwaltung wurde danach umgehend eine schriftliche Anweisung an alle Filialleiter gegeben, die eine Speicherung von für die Lieferung nicht erforderlichen Bemerkungen zum Kunden ausdrücklich verbietet.

Neben einer schriftlichen Entschuldigung beim Betroffenen wurde der für die unzulässige Speicherung verantwortliche Mitarbeiter von der Unternehmensleitung abgemahnt.

3.6 „Schwarze Liste" der Transportunternehmen

Eine Aufsichtsbehörde hatte erfahren, dass eine Interessengemeinschaft für Subunternehmen im Transportgewerbe eine Liste der „Schwarzen Schafe" des Transportgewerbes erstellt hatte.

Alle Sub- und Kleinunternehmen, die negative Erfahrungen (z.B. verschleppte, schlechte oder keine Zahlung, dubiose Gegenforderungen, schlechte Auslastung, Knebelverträge oder Ausschließlichkeitsverträge usw.) gemacht haben, sollten dies der Interessengemeinschaft mitteilen.

In einer Liste wurden 80 Firmen aufgeführt, die der Interessengemeinschaft aufgrund dieser Informationen Anlass zu Bedenken gaben. Auf die Angabe der vorliegenden Gründe (negative Erfahrungen der Subunternehmen) wurde verzichtet.

Seitens der Aufsichtsbehörde bestanden gegen die Verwendung dieser Liste erhebliche datenschutzrechtliche Bedenken. Insbesondere das Verfahren zur Datenerhebung wurde für datenschutzrechtlich unzulässig angesehen. Jedermann konnte telefonische Angaben über eine andere Person verbreiten, ohne dass diese Angaben objektiv nachgeprüft wurden oder nachprüfbar waren (z.B. durch Vollstreckungstitel oder Vertragskopien). Somit konnte jedenfalls nicht ausgeschlossen werden, dass schutzwürdige Belange des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung offensichtlich überwogen.

Die Interessengemeinschaft sagte zu, diese oder eine ähnliche Liste nicht mehr herauszugeben.

3.7 Weitergabe von Arbeitnehmerdaten

Beschwerdeführend legte ein Bürger dar, dass sein Arbeitgeber Daten zu seiner Person an einen Assekuranz-Finanzmakler übermittelt habe und bat um Klärung der Angelegenheit. Der Personalchef habe ihm versichert, dass die Datenweitergabe gestattet sei.

Im Rahmen einer aufsichtsbehördlichen Prüfung wurde bei dem Unternehmen festgestellt, dass man dort tatsächlich personenbezogene Arbeitnehmerdaten an den Makler übermittelt hatte. Dieser sollte die Mitarbeiter der Firma über Möglichkeiten einer zusätzlichen Altersversorgung informieren. Von der Datenübermittlung habe man die Mitarbeiter durch ein der Monatsabrechnung beigefügtes Schreiben informiert.

Das Schreiben wurde insgesamt beanstandet, da die gesetzlichen Verarbeitungsschranken des BDSG eine solche Datenübermittlung nicht gestatten.

Die Verarbeitung personenbezogener Daten und deren Nutzung sind nach § 4 Abs. 1 BDSG nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift es erlaubt oder soweit der Betroffene eingewilligt hat. Mangels einer besonderen Rechtsvorschrift bzw. Einwilligung des Betroffenen war das BDSG anzuwenden. § 28 Abs. 2 Nr. 1 b BDSG erlaubt zwar die Übermittlung personenbezogener Informationen, wenn es sich um listenmäßig oder sonst zusammengefasste Daten handelt und der dort aufgeführte Katalog der sog. „Freien Daten" nicht überschritten wird. Gleichzeitig darf kein Grund zu der Annahme bestehen, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Dieses Ausschlussinteresse sieht der Gesetzgeber aber ausdrücklich bei einer Übermittlung arbeitsrechtlicher Rechtsverhältnisse durch den Arbeitgeber als gegeben an.

Das Maklerbüro sicherte den Verzicht auf eine Nutzung der übermittelten Daten zu, jedenfalls in den Fällen, in denen noch keine erfolgreiche Beratung durchgeführt wurde.

Zur ordnungsgemäßen Datenweitergabe wurden der Firma und dem Makler datenschutzfreundliche Lösungen aufgezeigt.

4. Stand der Novellierung des Bundesdatenschutzgesetzes (BDSG)

Wie bereits in den vergangenen Tätigkeitsberichten ausgeführt, sind die Datenschutzgesetze des Bundes und der Länder an die Europäische Datenschutzrichtlinie 95/46/EG vom 24. Oktober 1995 anzupassen. Die Richtlinie sieht eine Erweiterung der Informationsrechte der Bürgerinnen und Bürger vor und verpflichtet alle Mitgliedstaaten - ungeachtet des Spielraums, innerhalb dessen sie unter Beachtung des Gemeinschaftsrechts unterschiedliche nationale Regelungen treffen können - auf ein im Wesentlichen einheitliches Datenschutzniveau. Neben Elementen aus dem französischen Datenschutzrecht enthält die Richtlinie auch deutsche Regelungsmuster. Gleichwohl ist eine generelle Überarbeitung des deutschen Datenschutzrechts notwendig geworden. Der Gesetzgebungsauftrag richtet sich vor allem an den Bundesgesetzgeber, das Bundesdatenschutzgesetz (BDSG) entsprechend zu ändern, aber auch an die Landesgesetzgeber. Der ehemaligen Bundesregierung ist es nicht gelungen, die Umsetzung der EG-Datenschutzrichtlinie rechtzeitig innerhalb der Dreijahresfrist durchzuführen. Zwar versandte das federführende Bundesministerium des Innern im Dezember 1997 einen noch nicht vollständig abgestimmten Referentenentwurf an die Länder, zu dem diese auch kritisch Stellung genommen haben, doch das weitere Gesetzgebungsverfahren blieb im Jahr 1998 im Stadium von Gesprächen und ministeriellen Entwürfen stecken. Die vorgelegten Entwürfe beschränkten die Novellierung auf das Mindestmaß des Erforderlichen. So wurde die Chance vergeben, einige generelle Defizite des in seinen Grundzügen vor 25 Jahren konzipierten Bundesdatenschutzgesetzes zu beheben. Weder wurde der Forderungskatalog des „Düsseldorfer Kreises“ an den Bundesgesetzgeber noch wurden moderne technische Entwicklungen, wie z.B. die Datenverarbeitung auf Chipkarten oder der zunehmende Einsatz von Videotechnik, berücksichtigt.

Nachdem im April 1998 über einen Kabinettentwurf keine Einigung erzielt werden konnte, hat die ehemalige Bundesregierung das Projekt zwar weiterverfolgt, aber zu keinem Ergebnis gebracht. Durch die zögerliche Behandlung der Novellierung des BDSG sind auch die Länder in Verzug geraten. Auf Länderseite bestand zunächst einheitlich die Auffassung, die Novellierung des BDSG abzuwarten und erst im Anschluss daran die Ländergesetze zu ändern, um inhaltliche und begriffliche Unterschiede möglichst gering zu halten. Dies ließ sich jedoch angesichts der Vorgehensweise des Bundes nicht mehr durchhalten. Aus diesem Grund haben die meisten Länder entschieden, die Novellierung ihrer jeweiligen Datenschutzgesetze unabhängig von der Änderung des BDSG in Angriff zu nehmen. In Nordrhein-Westfalen liegt ein

Gesetzentwurf der Landesregierung vor. Das Gesetzgebungsverfahren soll noch in dieser Legislaturperiode abgeschlossen werden.

(Die neue Bundesregierung beabsichtigt nunmehr, das BDSG in zwei Phasen zu novellieren. In einem ersten Schritt soll die EG-Datenschutzrichtlinie umgesetzt werden, ergänzt um Regelungen zu Chipkarten, Videoüberwachungen, Datenschutz-Audit und Datensparsamkeit. In einer zweiten Phase soll dann das gesamte Datenschutzrecht umfassend modernisiert werden. Der inzwischen bekanntgewordene Entwurf des Bundesministeriums des Innern genügt allerdings den Anforderungen bei weitem nicht. Insoweit haben die Länder einen umfangreichen Forderungskatalog aufgestellt.)