Unterrichtung

Der Niedersächsische Minister des Innern
— 51.2-05440/4-5 —

Hannover, den 10. 3. 1986

An den
Herrn Präsidenten des Niedersächsischen Landtages
Hannover

Betr.: **Tätigkeits- und Erfahrungsbericht der niedersächsischen Aufsichtsbehörden zu Fragen des Datenschutzes im nicht-öffentlichen Bereich**

Anlg.: 2

Sehr geehrter Herr Präsident!

Die SPD-Fraktion hatte am 14. 2. 1985 beantragt (Drs 10/3898), die Landesregierung aufzufordern, dem Landtag einen Tätigkeits- und Erfahrungsbericht über die Arbeit der niedersächsischen Aufsichtsbehörden zu Fragen des Datenschutzes im nicht-öffentlichen Bereich vorzulegen. Unabhängig davon, daß eine Berichtspflicht für die Aufsichtsbehörden im nicht-öffentlichen Bereich — im Gegensatz zu den jährlichen Berichten des Niedersächsischen Datenschutzbeauftragten für den Bereich der öffentlichen Verwaltung — gesetzlich nicht vorgesehen ist, wurde die Vorlage eines solchen Berichts anläßlich der ersten Beratung des Entschließungsantrages am 8. 3. 1985 von mir zugesagt.

Wegen der Zusammenfassung mit einer Reihe von weiteren Vorlagen zum Datenschutz hat eine abschließende Beratung des Antrages bisher noch nicht stattgefunden. Gleichwohl hat das Landesministerium in seiner Sitzung am 25. 2. 1986 beschlossen, den Bericht auch ohne einen förmlichen Landtagsbeschluß bereits jetzt zu erstatten, um eine Beratung noch vor dem Ende der Legislaturperiode zu ermöglichen.

Dem Beschluß des Kabinetts entsprechend übersende ich zur Unterrichtung des Niedersächsischen Landtages anliegend den zugesagten Tätigkeits- und Erfahrungsbericht in 2facher Ausfertigung.

Mit freundlichen Grüßen
Dr. Möcklinghoff

Datenschutzaufsicht in der Wirtschaft

(Tätigkeits- und Erfahrungsbericht der niedersächsischen Aufsichtsbehörden)

Inhaltsverzeichnis:

		Seite
Vorbemerkung		4
1.	Ausgestaltung der staatlichen Datenschutzaufsicht im nicht-öffentlichen Bereich	4
1.1	Vorgeschichte und Regelungskonzept	4
1.2	Organisation der Datenschutzaufsicht in Niedersachsen	5
1.2.1	Zuständige Behörden	5
1.2.2	Abgrenzung zum Niedersächsischen Datenschutzbeauftragten	5
1.3	Aufgaben und Befugnisse der Aufsichtsbehörden	6
1.3.1	Anlaßaufsicht nach § 30 BDSG	6
1.3.2	Beratungsfunktion der Aufsichtsbehörde	6
1.3.3	Regelmäßige Kontrolle nach § 40 BDSG	7
2.	Überwachungs- und Prüftätigkeit der Aufsichtsbehörden in Niedersachsen	7
2.1	Umfang der Prüfungstätigkeit	7
2.2	Bearbeitung von Eingaben und Beschwerden	8
2.3	Einzelne Schwerpunkte der Überwachungstätigkeit	8
2.3.1	Auskunfteien	8
2.3.1.1	Informationsbeschaffung, Arbeitsweise	8
2.3.1.2	Handels- und Wirtschaftsauskunfteien	9
2.3.1.3	Kreditschutzauskunfteien	9
2.3.1.4	Rechtmäßigkeit der Datenspeicherung und Übermittlung	11
2.3.1.5	Nutzung von Daten aus dem Inkassobereich für Auskunfteizwecke	11
2.3.1.6	Benachrichtigung, Auskunftserteilung über gespeicherte Daten	12
2.3.1.7	Berichtigung, Sperrung, Löschung von gespeicherten Daten	13
2.3.2	Handel	13
2.3.2.1	Adressenhandel und Direktwerbung	13
2.3.2.2	Versandhandel	14
2.3.3	Versicherungswirtschaft	15
2.3.3.1	Ermächtigungsklauseln in Versicherungsverträgen	15
2.3.3.2	Zentrale Dateien der Versicherungswirtschaft	16
2.3.4	Banken und Sparkassen	19
2.3.5	Privatärztliche Verrechnungsstellen	19
2.3.6	Service-Rechenzentren	20
2.3.7	Datenschutz im Arbeitsverhältnis	21

2.4	Erfahrungen aus der Überwachungstätigkeit	22
2.4.1	Datenschutzbewußtsein	22
2.4.2	Datensicherheit	23
2.4.3	Defizite der Datenschutzkontrolle	25
3.	Zusammenarbeit der Aufsichtsbehörden der Länder	26
4.	Zusammenarbeit mit der Wirtschaft	26
5.	Novellierung des BDSG	27
Anlage	Aufsichtsbehörden der Länder	29

Vorbemerkung

Die SPD-Fraktion des Niedersächsischen Landtages hat am 14. 2. 1985 (Drs 10/3898) beantragt, die Landesregierung aufzufordern, dem Landtag einen Tätigkeits- und Erfahrungsbericht über die Arbeit der niedersächsischen Aufsichtsbehörden zu Fragen des Datenschutzes im nicht-öffentlichen Bereich vorzulegen. Der Bericht soll sich nicht in der Darstellung von Einzelproblemen erschöpfen, sondern die für den Bürger bedeutsamen Grundsatzfragen berücksichtigen.

Die Landesregierung hat diese Initiative ausdrücklich begrüßt, obwohl eine Berichtspflicht für die Aufsichtsbehörden im nicht-öffentlichen Bereich — im Gegensatz zu den jährlichen Berichten des Niedersächsischen Datenschutzbeauftragten im Bereich der öffentlichen Verwaltung — nicht vorgesehen ist, erhält sie doch so Gelegenheit, die Öffentlichkeit über ihre Erfahrungen bei der Anwendung des Bundesdatenschutzgesetzes (BDSG) zu unterrichten. Zwar steht eine abschließende Beratung des Antrages noch aus; die Landesregierung hat aber keinen Zweifel, daß der Landtag dem Antrag folgen wird. Deshalb hat sie beschlossen, den Bericht auch ohne einen förmlichen Landtagsbeschluß bereits jetzt zu erstatten.

Die Aufsichtsbehörden in Niedersachsen haben ihre Tätigkeit mit Inkrafttreten des BDSG am 1. 1. 1978 aufgenommen. Der nachfolgende Bericht erfaßt ihre Tätigkeit bis Mitte 1985.

1. Ausgestaltung der staatlichen Datenschutzaufsicht im nicht-öffentlichen Bereich

1.1 Vorgeschichte und Regelungskonzept

Art, Umfang und Ausgestaltung der Aufgaben der Aufsichtsbehörden waren in den parlamentarischen Beratungen über das BDSG lange umstritten; vor allem war streitig, ob auch in dem im Dritten Abschnitt des Gesetzes geregelten Bereich der Datenverarbeitung für eigene Zwecke neben der Kontrolle durch den Betroffenen und den betrieblichen Datenschutzbeauftragten außerdem noch eine behördliche Überwachung notwendig sei. Der Regierungsentwurf sah Aufsichtsbehörden nur für den Vierten Abschnitt (Datenverarbeitung für fremde Zwecke) vor (BT-Drs 7/1027).

Diese Regelung des Regierungsentwurfs stieß auf breite Zustimmung der Wirtschaft, die kein Bedürfnis für Aufsichtsbehörden bei der Datenverarbeitung für eigene Zwecke sah (z. B. Stellungnahme des Bundesverbandes der Deutschen Industrie). Auch die Länder machten Bedenken gegen eine Ausweitung der Aufgaben der Aufsichtsbehörden geltend, vor allem wegen der Schwierigkeiten und Belastungen, die mit der Einrichtung solcher Behörden verbunden wären; es müßten qualifiziertes Personal und ausreichende Sachmittel bereitgestellt werden (Stellungnahme des Bundesrates vom 28. 6. 1976, BT-Drs 7/5497, S. 5).

In den abschließenden Beratungen des Bundestags-Innenausschusses und des Vermittlungsausschusses wurden diese Einwände nicht berücksichtigt. Die Abgeordneten wünschten eine wirksame Kontrolle. Vom Bürger könne aber in aller Regel nicht erwartet werden, daß er über die zur Ausübung seiner Kontrollrechte erforderlichen Kenntnisse der Datenverarbeitung verfüge, d.h. den Ablauf des Verarbeitungsprozesses und die jeweilige Unternehmens- oder Verbandsorganisation durchschauen könne; darüber hinaus könne er den für eine wirksame Kontrolle unumgänglichen Aufwand an Zeit und Mitteln nicht aufbringen. Auch der betriebliche Datenschutzbeauftragte sei kein ausreichender Ausgleich. Seine Anbindung an die datenverarbeitende Stelle bringe Konflikte mit sich, die die Wirksamkeit seines Auftrages beeinträchtigen könnten. Daher entschied sich der Gesetzgeber letztlich, zur Überwachung der datenverarbeitenden Stellen Aufsichtsbehörden vorzusehen, die als neutrale staatliche Stellen an der Verwirklichung des Datenschutzes mitwirken sollen.

1.2 Organisation der Datenschutzaufsicht in Niedersachsen

Nach Artikel 30 GG ist die Ausübung der staatlichen Befugnisse und die Erfüllung der staatlichen Aufgaben grundsätzlich Angelegenheit der Länder. Dementsprechend legt das BDSG fest (§§ 30 Abs. 5 und 40 Abs. 2), daß die Landesregierungen die für die Überwachung der Durchführung des Datenschutzes zuständigen Behörden bestimmen.

1.2.1 Zuständige Behörden

Aufsichtsbehörden nach §§ 30, 40 BDSG sind die Bezirksregierungen (Runderlaß vom 29.11.1977 — Nds. MBl. S. 1488 —; Beschluß des Landesministeriums vom 13.12.1983 — Nds. MBl. 1984, S. 10 —). Bei der Durchführung von Prüfungen und Beratungen, für die spezielle Kenntnisse der automatisierten Datenverarbeitung erforderlich sind, bedienen sie sich einer Prüfgruppe, die für diesen Zweck beim Niedersächsischen Landesverwaltungsamt vorgehalten wird. Die Fachaufsicht über die Bezirksregierungen als Datenschutz-Aufsichtsbehörden obliegt dem Minister des Innern.

Maßgebend für die Zuordnung der Datenschutzkontrolle im nicht-öffentlichen Bereich zu den Bezirksregierungen war die Überlegung, daß Berührungen zum Gewerberecht bestehen, für das die Bezirksregierungen zuständig sind, und daß von der Kontrolltätigkeit hauptsächlich Unternehmen der Wirtschaft betroffen sein würden.

Eine ähnliche Organisation für die staatliche Datenschutzaufsicht im privaten Bereich haben die Länder Bayern, Hessen, Nordrhein-Westfalen und Rheinland-Pfalz gewählt.

Eine Zusammenstellung der Aufsichtsbehörden in den einzelnen Ländern ist als Anlage beigefügt.

1.2.2 Abgrenzung zum Niedersächsischen Datenschutzbeauftragten

Während die Bezirksregierungen die Einhaltung der Vorschriften des BDSG im privaten Bereich überwachen, obliegt die Kontrolle der öffentlichen Stellen, im wesentlichen der öffentlichen Verwaltung, dem Niedersächsischen Datenschutzbeauftragten. Bei den öffentlich-rechtlichen Wirtschaftsunternehmen ist die Kontrolle geteilt: diese Unternehmen unterliegen grundsätzlich der Überwachung durch den Niedersächsischen Datenschutzbeauftragten; für die meisten und wichtigsten öffentlich-rechtlichen Wirtschaftsunternehmen, so die öffentlich-rechtlichen Banken, die Sparkassen und die öffentlich-rechtlichen Versicherungen, soweit sie Wettbewerbsunternehmen sind, sieht § 15 des Niedersächsischen Datenschutzgesetzes allerdings eine Ausnahme vor: diese Unternehmen unterliegen der Kontrolle der Aufsichtsbehörden nach §§ 30, 40 BDSG.

Für alle öffentlich-rechtlichen Unternehmen gilt, daß sich die Zulässigkeit der Datenverarbeitung nicht nach den für die übrigen öffentlichen Stellen geltenden Vorschriften des Niedersächsischen Datenschutzgesetzes, sondern nach den für die Wirtschaft geltenden Vorschriften des BDSG richtet. Für die im Wettbewerb stehenden Banken und Versicherungen ist darüber hinaus die geschilderte abweichende Aufsichtsregelung getroffen worden, um auch insoweit eine Gleichbehandlung mit den konkurrierenden Unternehmen der Privatwirtschaft herzustellen. Der Wettbewerb dürfte die geschäftliche Tätigkeit und das Erscheinungsbild dieser Unternehmen so prägen, daß dagegen die öffentlich-rechtliche Trägerschaft zurücktritt. Die Regelung hat den Vorteil, daß für die schwierigen Probleme der Datenverarbeitung bei den Banken und Versicherungen nicht neben den Aufsichtsbehörden auch noch entsprechender Sachverstand beim Niedersächsischen Datenschutzbeauftragten vorgehalten werden muß.

Auch in ihrer Stellung gegenüber der Landesregierung unterscheiden sich die Kontrollinstanzen. Der Niedersächsische Datenschutzbeauftragte ist bei seiner Tätigkeit fachlich unabhängig und untersteht nur der Rechtsaufsicht des Landesministeriums; er unterliegt also keiner Fachaufsicht, für seine Tätigkeit dürfen ihm keine Weisungen erteilt werden. Dagegen sind die Bezirksregierungen weisungsabhängige Behörden, für deren Handeln der zuständige Ressortminister parlamentarisch verantwortlich ist. Anders als der Niedersächsische Datenschutzbeauftragte, der als exekutiv-internes Kontrollorgan Empfehlungen und Beanstandungen aussprechen kann, denen keine unmittelbare rechtliche Wirkung zukommt, können die Bezirksregierungen auch Verwaltungsakte und Bußgeldbescheide erlassen.

1.3 Aufgaben und Befugnisse der Aufsichtsbehörden

Zweck des Datenschutzes ist es, den Bürger vor einer Beeinträchtigung seiner schutzwürdigen Belänge bei der Datenverarbeitung zu bewahren. Das BDSG schränkt seinen Anwendungsbereich allgemein auf personenbezogene Daten ein, die in Dateien gespeichert, verändert, gelöscht oder aus Dateien übermittelt werden (§ 1 Abs. 2 BDSG). Diese Beschränkung bildet zugleich den Rahmen für die Kontrolltätigkeit der Aufsichtsbehörden. Grundlegend ist weiter die Unterscheidung zwischen Stellen, die Datenverarbeitung für eigene Zwecke betreiben (z.B. Banken, Industrie, Handel, Versicherungen, Vereine) und Stellen, die personenbezogene Daten für fremde Zwecke verarbeiten (z.B. Auskunfteien, Werbewirtschaft, Adreßhandel, Markt- und Meinungsforschungsinstitute, Service-Rechenzentren). Die Pflichten und Befugnisse der Aufsichtsbehörden sind für beide Bereiche unterschiedlich geregelt.

1.3.1 Anlaßaufsicht nach § 30 BDSG

Stellen, die personenbezogene Daten für eigene Zwecke verarbeiten, unterliegen nach § 30 Abs. 1 BDSG lediglich der Anlaßaufsicht. Die Aufsichtsbehörde darf nur tätig werden, wenn sich ein von der Datenverarbeitung betroffener Bürger oder der betriebliche Datenschutzbeauftragte der jeweiligen Stelle aus konkretem Anlaß an sie wendet. Obwohl bei diesen Stellen der weitaus umfangreichere Teil der privatwirtschaftlichen Verarbeitung personenbezogener Daten liegt (z.B. Daten von Kunden, Arbeitnehmern, Lieferanten, Mitgliedern), was sich auch an der Vielzahl der Eingaben und Beschwerden aus diesem Bereich messen läßt, sind in der Praxis der niedersächsischen Aufsichtsbehörden Prüfungen vor Ort nur in einem verhältnismäßig geringem Umfang erforderlich gewesen (vgl. 2.1).

Die Aufsichtsbehörde beschränkt sich bei der Anlaßaufsicht in der Regel auf die Prüfung der an sie herangetragenen Einzelfälle. Sie ist jedoch nicht gehindert, in diesem Zusammenhang weiteren Verstößen gegen Datenschutzbestimmungen nachzugehen. Sie ist berechtigt, die zur Prüfung erforderlichen Auskünfte zu verlangen, die Geschäftsräume des Unternehmens zu betreten, dort Prüfungen und Besichtigungen vorzunehmen und in Geschäftsunterlagen, insbesondere in die gespeicherten personenbezogenen Daten und Datenverarbeitungsprogramme, Einsicht zu nehmen. Dagegen hat sie nicht die Befugnis, bestimmte Datenschutzmaßnahmen durchzusetzen. Die Erfahrung hat aber gezeigt, daß in der weit überwiegenden Zahl der Fälle die Feststellung von Verstößen bereits ausreichte, um die datenverarbeitende Stelle zur Abhilfe zu veranlassen. In den übrigen Fällen kann die Aufsichtsbehörde dem Betroffenen nur empfehlen, zur Durchsetzung seiner Rechte die Zivilgerichte anzurufen.

1.3.2 Beratungsfunktion der Aufsichtsbehörden

Das BDSG mißt der Selbstkontrolle der datenverarbeitenden Stelle ein besonderes Gewicht bei. Es verpflichtet deshalb Unternehmen, deren Datenverarbei-

tung ein bestimmtes Volumen überschreitet, einen betrieblichen Datenschutzbeauftragten zu bestellen. Die Beratung der betrieblichen Datenschutzbeauftragten stellt eine wesentliche Aufgabe der Aufsichtsbehörden dar (§ 30 Abs. 1 Satz 2 BDSG). Ihr kam besonders in den ersten Jahren nach dem Inkrafttreten des BDSG große Bedeutung zu. Wenn das Gesetz auch nur von der Unterstützung des betrieblichen Datenschutzbeauftragten spricht, so würde man doch den Zweck des Gesetzes verfehlen, wenn nur er als Gesprächspartner der Aufsichtsbehörde in Betracht gezogen würde. Daher hat auch die Beratung der vielen kleineren Unternehmen, die wegen des geringen Umfangs ihrer Datenverarbeitung keinen Datenschutzbeauftragten zu bestellen brauchen, großes Gewicht für die Umsetzung des Datenschutzrechts in die Praxis. Durch frühzeitige Kontakte mit den Aufsichtsbehörden können mögliche Konfliktsituationen erkannt und im Interesse aller Beteiligten spätere Beanstandungen vermieden werden.

1.3.3 Regelmäßige Kontrolle nach § 40 BDSG

Einer weitergehenden staatlichen Aufsicht unterliegen die Stellen, die personenbezogene Daten für fremde Zwecke verarbeiten. Dazu gehören vor allem Wirtschafts- und Handelsauskunfteien, Adreßhandels- und Direktwerbeunternehmen, Markt- und Meinungsforschungsinstitute sowie Service-Rechenzentren. Diese Stellen unterliegen nach § 40 BDSG neben den Kontrollmaßnahmen nach § 30 BDSG einer ständigen Überwachung, die die Aufsichtsbehörde von Amts wegen wahrnimmt. Hier liegt auch der Schwerpunkt der Tätigkeit der niedersächsischen Aufsichtsbehörden.

Die genannten Unternehmen haben die Aufnahme oder Beendigung ihrer Tätigkeit innerhalb eines Monats bei der Aufsichtsbehörde anzumelden, die hierüber ein von jedermann einsehbares Register führt. Von der Einsichtnahme wird allerdings nur in wenigen Fällen Gebrauch gemacht. Aufgrund dieses Registers legen die Aufsichtsbehörden einen Überwachungsturnus fest, der je nach Art und Umfang der Datenverarbeitung in den Unternehmen zwischen 3 und 5 Jahren liegt.

2. Überwachungs- und Prüftätigkeit der Aufsichtsbehörden in Niedersachsen

2.1 Umfang der Prüfungstätigkeit

Der regelmäßigen Kontrolle der Aufsichtsbehörden unterliegen derzeit rd. 220 Unternehmen, von denen fast die Hälfte im Regierungsbezirk Hannnover angesiedelt ist. Während des Berichtszeitraumes wurden insgesamt 339 Prüfungen durchgeführt; dabei handelte es sich in 34 Fällen um Wiederholungsprüfungen. Der Unterschied zwischen der Zahl der gemeldeten Stellen und der der Prüfungen ergibt sich daraus, daß das Melderegister einer ständigen Fluktuation unterliegt, weil meldepflichtige (und bereits geprüfte) Unternehmen ihren Betrieb aufgegeben haben, andere ihre Tätigkeit umgestellt haben oder bei der Prüfung festgestellt wurde, daß die Unternehmen sich irrtümlich gemeldet hatten und lediglich der Anlaßaufsicht nach § 30 BDSG unterlagen.

Die zum Register gemeldeten Unternehmen wurden nach und nach einer ersten Prüfung unterzogen, die im Hinblick auf die verhältnismäßig neue Materie „Datenschutz" zunächst vor allem der Bestandsaufnahme diente. Es wurde der Vollständigkeit der Registermeldungen, der Bestellung eines betrieblichen Datenschutzbeauftragten — soweit erforderlich — und den nach dem BDSG erforderlichen Verpflichtungen der jeweiligen Mitarbeiter auf das Datengeheimnis nachgegangen. Ferner wurden die dem BDSG unterliegenden Datenverarbeitungsverfahren sowie die vom Unternehmen getroffenen Datensicherungsmaßnahmen einer Prüfung unterzogen. Inzwischen haben die Aufsichts-

behörden turnusmäßig mit einer zweiten Prüfrunde begonnen (s.o.), in der verstärkt Schwerpunkte gesetzt werden. Ausgangsbasis hierfür sind die Schwachstellen, die im Rahmen der ersten Prüfungen wiederholt festgestellt wurden.

Besonderes Augenmerk gilt dabei der Bestellung des betrieblichen Datenschutzbeauftragten, vor allem auch seiner Zuverlässigkeit und Fachkunde, sowie bestimmten Datensicherungsmaßnahmen, die nach den Erfahrungen der ersten Prüfrunde als verbesserungsbedürftig erkannt wurden. Im übrigen werden die Aufsichtsbehörden verstärkt auf den Einzelfall entsprechend dem jeweiligen Geschäftsablauf eingehen und dabei auch feststellen, ob die im Rahmen der ersten Prüfung ausgesprochenen Beanstandungen inzwischen ausgeräumt sind. Während die meldepflichtigen Unternehmen mit wenigen Ausnahmen inzwischen mindestens einmal geprüft wurden, waren daneben Prüfungen im Rahmen der Anlaßaufsicht sowohl bei ihnen als auch bei Unternehmen, die Datenverarbeitung für eigene Zwecke betreiben, nur selten erforderlich.

2.2 Bearbeitung von Eingaben und Beschwerden

Neben den regelmäßigen Prüfungen hatten die Aufsichtsbehörden zahlreiche mündliche und schriftliche Eingaben von Bürgern zu bearbeiten. Genaue Zahlenangaben dazu liegen aber nicht vor und lassen sich auch nicht ohne unverhältnismäßigen Verwaltungsaufwand ermitteln.

Etwa die Hälfte der Eingaben betraf die Datenverarbeitung nach dem 3. Abschnitt des BDSG (also vor allem Versicherungen, Kreditinstitute und Handelsunternehmen); von den übrigen waren in der Mehrzahl Auskunfteien betroffen. Die Eingaben lassen sich unterscheiden in

— Beschwerden über bestimmte Datenverarbeitungsvorgänge,

— Anfragen zur Rechtmäßigkeit der Datenverarbeitung in konkreten Einzelfällen,

— allgemeine Auskünfte zum Datenschutz.

Die weit überwiegende Zahl der Beschwerden und Anfragen zur Rechtmäßigkeit der Datenverarbeitung konnte schon dadurch erledigt werden, daß eine umfassende Auskunft gegeben wurde und die Betroffenen auf die ihnen zustehenden Rechte hingewiesen wurden. Soweit dies nicht ausreichte, konnte den Beschwerden in der Regel durch fernmündliche oder schriftliche Kontakte mit den datenverarbeitenden Unternehmen abgeholfen werden. Insgesamt waren weniger als 5 % aller Beschwerden begründet; in den übrigen Fällen stand die Datenverarbeitung im Einklang mit den Bestimmungen des BDSG. Vielen Beschwerden lag offensichtlich nur ein allgemeines Unbehagen an der Verarbeitung der eigenen personenbezogenen Daten und eine unvollständige Kenntnis der vom Gesetz eingeräumten Kontrollrechte zugrunde.

2.3 Einzelne Schwerpunkte der Überwachungstätigkeit

2.3.1 Auskunfteien

Gemessen an der Zahl der Anfragen und Eingaben nahmen die Auskunfteien die größte Aufmerksamkeit der Bürger in Anspruch. Hier werden am ehesten Beeinträchtigungen von Persönlichkeitsrechten befürchtet. Aus diesem Grund soll der Bereich der Auskunfteien in diesem Bericht ausführlicher behandelt werden.

2.3.1.1 Informationsbeschaffung, Arbeitsweise

Auskunfteien sind gewerbliche Einrichtungen, die solche Daten sammeln und speichern, die Aussagen über die Kreditfähigkeit und Kreditwürdigkeit von

Einzelpersonen und Firmen ermöglichen, und die diese Informationen Interessenten auf Anfrage zur Verfügung stellen. Auf diese Weise sollen Kreditgeber oder Stellen, die wirtschaftliche Vorleistungen erbringen, vor finanziellen Verlusten geschützt werden. Zu diesem Zweck werten Auskunfteien systematisch alle verfügbaren allgemein zugänglichen Quellen (z.B. Telefon- und Adreßbücher, Zeitungen, öffentliche Register) aus. Eine der wichtigsten Informationsquellen der Auskunfteien ist das bei den Vollstreckungsgerichten geführte Schuldnerverzeichnis nach § 915 ZPO, in dem alle Personen aufgeführt sind, die eine eidesstattliche Versicherung abgegeben haben oder gegen die eine Haftanordnung im Rahmen der Vollstreckung ergangen ist. Die Eintragungen im Schuldnerverzeichnis sind spätestens nach 3 Jahren, gerechnet vom Schluß des Jahres der Eintragung, zu löschen. Nachdem die Aufsichtsbehörden mehrfach festgestellt hatten, daß Auskunfteien Auszüge aus dem Schuldnerverzeichnis, die gelöscht sein mußten, weiterhin gespeichert hatten, sind die Gerichte dazu übergegangen, einzelne Auskunfteien, die die gesetzlichen Löschungsfristen mißachtet hatten, von der Belieferung mit weiteren Auszügen auszuschließen. Darüber hinaus ist beabsichtigt, die Bestimmungen über die Führung des Schuldnerverzeichnisses und über die Erteilung von Auskünften bzw. Abschriften aus dem Schuldnerverzeichnis zu ändern. Der Bundesminister der Justiz hat bereits einen Referentenentwurf vorgelegt.

Neben der Auswertung dieser Quellen bedienen sich die Auskunfteien meist noch fest angestellter oder freiberuflicher Rechercheure, die in Fällen, in denen allgemein zugängliche Informationen nicht vorliegen — vor allem bei Privatpersonen — den Betroffenen selbst, aber auch Personen, die diesen kennen, befragen. Die gesammelten Informationen werden in einem Archiv aufbewahrt, um sie bei Anfragen wieder verwenden zu können. Allerdings muß die Richtigkeit der Informationen bei jeder Anfrage erneut geprüft werden.

2.3.1.2 Handels- und Wirtschaftsauskunfteien

Der weit überwiegende Teil des Auskunftsverkehrs bei den Handels- und Wirtschaftsauskunfteien betrifft Geschäftsleute und Handelsunternehmen, die sich über die Bonität anderer Geschäftsleute oder Firmen vergewissern wollen, mit denen sie in Geschäftsverbindung zu treten beabsichtigen. Die Beteiligung am Wirtschaftsverkehr bedingt die Offenlegung einer Reihe personenbezogener Informationen; deshalb haben die Geschäftsleute und Unternehmen ein eigenes Interesse an der Informationsspeicherung und stellen den Auskunfteien betriebliche Informationen teilweise selbst zur Verfügung.

Ein relativ kleiner Teil der Auskünfte wird auch über nicht gewerblich tätige Privatpersonen erteilt. Zu den Informationsempfängern zählen hier vor allem der Versandhandel (zur Absicherung bei Käufen auf Rechnung oder bei Ratenzahlungen), Autovermieter und Kaufhäuser; Voraussetzung ist, daß sie wegen eines geschäftlichen Risikos ein konkretes Interesse darlegen können (vgl. auch 2.3.1.3).

2.3.1.3 Kreditschutzauskunfteien

Im Bereich des Bankwesens gibt es eine Kreditschutzorganisation, die Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA). Sie besteht aus einer Reihe über das gesamte Bundesgebiet verteilter Einzelgesellschaften. Diese erhalten aufgrund vertraglicher Abmachungen ihre Informationen vor allem von den Banken und Sparkassen, denen sie wiederum als Gegenleistung Informationen zur Beurteilung der Kreditwürdigkeit potentieller Kunden aus ihrem Datenbestand zur Verfügung stellen. Die Banken und Sparkassen lassen sich zu der Datenübermittlung von ihren Kunden ermächtigen; dazu unterschreibt

der Kunde — in der Regel bei der Kontoeröffnung oder der Beantragung eines Kredits — eine entsprechende Klausel. Die bisher verwendete Klausel war mit den Aufsichtsbehörden der Länder abgestimmt und lautete wie folgt:

„Das Kreditinstitut ist berechtigt, der Schutzgemeinschaft für allgemeine Kreditsicherung Daten des Kreditnehmers und etwaiger Mitschuldner über die Aufnahme (Kreditbetrag, Laufzeit, Ratenbeginn) und die Abwicklung dieses Kredites zur Speicherung zu übermitteln."

Die Datenschutzaufsichtsbehörden der Länder gingen trotz Meinungsverschiedenheiten mit der Kreditwirtschaft über den Charakter der Klausel (Einwilligung oder bloße Unterrichtung) davon aus, daß mit dieser Formulierung ein vertretbarer Kompromiß zwischen dem Interesse des Kreditgewerbes an größtmöglicher Absicherung gegen Kreditausfälle und dem Recht der Kunden auf Geheimhaltung ihrer finanziellen Verhältnisse gefunden sei. Inzwischen ist die sog. „SCHUFA-Klausel" jedoch vom Bundesgerichtshof mit Urteil vom 19. 9. 1985 für rechtswidrig erklärt worden. Der Bundesgerichtshof bestätigt zwar seine bisherige Rechtsprechung, daß die Übermittlung von Kreditinformationen an ein Kreditinformationssystem zulässig sei, weil dessen Ziel, künftigen Kreditgebern die Beurteilung der Kreditwürdigkeit eines Kreditnehmers zu erleichtern, im Interesse sämtlicher Beteiligter liege. Notwendig sei jedoch, daß die übermittelnde Bank Aussagekraft und Berechtigung einer bestimmten Einzelmitteilung unter sorgfältiger Interessenabwägung prüft und außerdem das Kreditinformationssystem so organisiert ist, daß die gespeicherten Daten insgesamt ein möglichst vollständiges, aktuelles Bild der Kreditwürdigkeit bieten und die Weitergabe sich auf Anschlußnehmer beschränkt, die ein berechtigtes Interesse haben, über die Kreditwürdigkeit eines Betroffenen unterrichtet zu werden.

Nach dem Urteil verstößt die bisher verwendete Klausel gegen § 9 des Gesetzes zur Regelung des Rechts der allgemeinen Geschäftsbedingungen (AGBG), weil sie den Kunden unangemessen benachteiligt. Diese Benachteiligung liegt darin, daß die Klausel mit wesentlichen Grundgedanken des BDSG nicht vereinbar ist. Nach Auffassung des Bundesgerichtshofes liegt eine wesentliche Benachteiligung vor, „wenn eine formularmäßige Einwilligung sich nicht auf bestimmte Kreditdaten beschränkt, sondern pauschal unter der Bezeichnung „Daten des Kreditnehmers über die Abwicklung des Kredits„ auch Angaben über einseitige Maßnahmen des Kreditgebers zur Durchsetzung vermeintlicher Ansprüche gegen den Kreditnehmer, beispielsweise Mahnungen, Kündigungen, Mahnbescheide... umfassen soll und den Kreditgeber uneingeschränkt ermächtigt, auch derartige Negativmerkmale ohne Interessenabwägung im Einzelfall und sogar in Fällen, in denen eine solche Abwägung negativ ausfallen würde, an ein Kreditinformationssystem zu übermitteln."

Dies bedeutet zum einen, daß eine SCHUFA-Klausel keine pauschale Ermächtigung zur Übermittlung nicht näher spezifizierter Merkmale enthalten darf, sondern genau aufzählen muß, welche Merkmale an die SCHUFA übermittelt werden dürfen. Es bedeutet aber zum anderen auch, daß bestimmte Negativmerkmale nicht mit einer differenzierteren Einwilligung, sondern nur nach einer Einzelfallabwägung der Interessen der übermittelnden Stelle, eines Dritten oder der Allgemeinheit mit den schutzwürdigen Belangen des Betroffenen an die SCHUFA übermittelt werden dürfen.

Unter Berücksichtigung dieser Grundsätze ist zwischen den obersten Aufsichtsbehörden der Länder und den Verbänden des Kreditwesens inzwischen eine neue SCHUFA-Klausel vereinbart worden, die in Kürze Verwendung finden soll. Sie bedarf zunächst allerdings noch der Abstimmung mit der SCHUFA.

Noch nicht abschließend geklärt worden sind allerdings die Auswirkungen des Urteils auf andere Vertragspartner der SCHUFA, denn neben den Kreditinstituten haben auch Wirtschaftsunternehmen aller Branchen, vor allem Versand- und Kaufhäuser, — allerdings eingeschränkten — Zugang zu den Informationen der SCHUFA, wenn sie sich ihr mit sogenannten B-Verträgen anschließen. Im Gegensatz zu den A-Verträgen der Kreditinstitute berechtigen die B-Verträge nur zum Bezug bestimmter Negativinformationen, d.h. über die vertragswidrige Abwicklung von Kreditverträgen, nicht jedoch über das Bestehen von Kredit- oder Bürgschaftsverpflichtungen.

2.3.1.4 Rechtmäßigkeit der Datenspeicherung und Übermittlung

Das BDSG erlaubt die Erteilung von Auskünften ohne die Einwilligung des Betroffenen, soweit kein Grund zu der Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden. Generelle Aussagen darüber, wann schutzwürdige Belange beeinträchtigt werden, sind nicht möglich; dies kann nur im Einzelfall festgestellt werden. Eine Beeinträchtigung schutzwürdiger Belange ist jedoch im allgemeinen dann nicht anzunehmen, wenn lediglich für Kreditentscheidungen bedeutsame Daten gesammelt und übermittelt werden und wenn diese Daten richtig sind. Wer solche Informationen haben möchte, muß ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft darlegen. Die Gründe für das Vorliegen eines berechtigten Interesses und die Mittel für ihre glaubhafte Darlegung sind von der Auskunftei aufzuzeichnen.

Die Aufsichtsbehörden haben im Rahmen von Stichproben geprüft, ob die Datenverarbeitung der Auskunfteien den genannten Voraussetzungen entspricht. Nur in wenigen Fällen war es erforderlich, Einzelspeicherungen zu beanstanden.

Allerdings war häufiger festzustellen, daß Auskunfteien auch Informationen speichern, die keine konkreten Aussagen zur Kreditwürdigkeit des Betroffenen enthalten (z.B. „geschieden", „verheiratet in zweiter Ehe", „besitzt (mehrere) Autos"). Während die Auskunfteien davon ausgehen, daß solche Angaben durchaus von Bedeutung für die Beurteilung der Kreditwürdigkeit sind, weil sie z.B. auf bestehende Unterhaltsverpflichtungen des Betroffenen hinweisen könnten, vertreten die obersten Aufsichtsbehörden die Auffassung, daß diese Daten Anlaß zu Spekulationen geben können und dadurch schutzwürdige Belange des Betroffenen beeinträchtigen. Eine Einigung in diesem Punkt steht noch aus.

2.3.1.5 Nutzung von Daten aus dem Inkassobereich für Auskunfteizwecke

Verschiedene Handelsauskunfteien treten gegenüber Betroffenen zugleich als zugelassene Inkassobüros auf und fordern die Betroffenen auf, Schulden zu begleichen. Gleichzeitig weisen sie darauf hin, daß sich das Verhalten der Betroffenen bei der Schuldbegleichung auf den Inhalt etwaiger Auskünfte auswirken werde.

Die Vertreter der Handelsauskunfteien erklärten dazu, daß die im Zusammenhang mit dem Inkassogeschäft gewonnenen Daten mit den Daten, die Auskunftszwecken dienen, grundsätzlich nicht vermengt würden. Die Handelsauskunfteien könnten allerdings solche Informationen nicht ignorieren, die wesentliche Aussagen über die Kreditwürdigkeit eines Betroffenen enthielten. Auch könne davon ausgegangen werden, daß dem Auftraggeber des Inkassogeschäfts bekannt sei, daß Inkassobüro und Handelsauskunftei miteinander verbunden sind, und daß dieser — soweit er nicht ausdrücklich etwas anderes bestimmt habe — damit einverstanden sei, daß die für das Inkassogeschäft bekanntgegebenen Daten auch für Auskunfteizwecke verwendet werden.

Eine Benachrichtigung des Betroffenen anläßlich der erstmaligen Übermittlung der Daten vom Inkassobüro an die Auskunftei sei entbehrlich, da der vom Inkassobüro angeschriebene Betroffene aus dem Schreiben selbst entnehmen könne, daß die Auskunftei die Daten ebenfalls speichere.

Die Datenschutzreferenten haben Bedenken gegen dieses Verfahren. Da Handelsauskunftei und Inkassobüro datenschutzrechtlich als zwei verschiedene Stellen anzusehen sind, dürfen Daten vom Inkassobüro an die Handelsauskunftei nur unter den Zulässigkeitsvoraussetzungen des § 24 BDSG übermittelt werden.

Eine Übereinstimmung zu dieser Frage wurde bisher nicht erzielt.

2.3.1.6 Benachrichtung, Auskunftserteilung über gespeicherte Daten

Das BDSG räumt dem betroffenen Bürger verschiedene Rechte ein, durch deren Wahrnehmung er einem Mißbrauch der zu seiner Person gespeicherten Daten entgegenwirken kann.

So ist die Auskunftei verpflichtet, wenn erstmals Daten übermittelt werden, den Betroffenen davon zu unterrichten, daß Daten über ihn gespeichert sind, es sei denn, der Betroffene hat bereits auf andere Weise von der Datenspeicherung Kenntnis erhalten (z.B. durch eine Unterrichtung bei Vertragsabschluß; vgl. 2.3.1.3). In den meisten Fällen wird diese Benachrichtigung mit der Aufforderung verbunden, weitere Auskünfte zu erteilen, um von vornherein eine Speicherung unrichtiger Daten zu vermeiden. Diese Aufforderungen erweckten allerdings gelegentlich den Anschein, als sei der Betroffene verpflichtet, eine derartige „Selbstauskunft" zu erteilen. Inzwischen ist in Zusammenarbeit der Aufsichtsbehörden der Länder und der Spitzenverbände der Auskunfteien erreicht worden, daß solche irreführenden Aufforderungen nicht mehr verschickt werden, sondern auf die Freiwilligkeit der Beantwortung hingewiesen wird.

Wenn ein Bürger konkret wissen will, welche Daten über ihn gespeichert sind, hat er nach dem BDSG einen Rechtsanspruch auf Auskunft über diese Daten. Für die Auskunft kann ein Entgelt verlangt werden. Die Höhe dieses Entgelts war besonders in den ersten Jahren nach Inkrafttreten des BDSG ein Schwerpunkt der Eingaben an die Aufsichtsbehörden. Nachdem die Auskunfteien überwiegend dazu übergangen sind, die Auskünfte kostenlos zu erteilen, stehen jetzt Beschwerden über die Art der Datenbeschaffung und die Frage im Vordergrund, ob die Auskunftei den Informanten und den Datenempfänger bekanntgeben muß.

Besonders die Praxis der Auskunfteien, Nachbarn der Betroffenen zu befragen, stieß auf heftige Kritik. Mit den Spitzenorganisationen der Auskunfteien konnte inzwischen Einvernehmen dahin erzielt werden, daß sich Befragungen in der Nachbarschaft, soweit nicht auf sie verzichtet werden kann, nur auf wenige Angaben wie Wohnort, Aufenthaltsdauer, Größenordnung des Einkommens, Arbeitgeber und wirtschaftliche Verhältnisse beziehen dürfen. Persönliche Beurteilungen werden nicht mehr erfragt.

Die vielen Beschwerden darüber, daß Informant und Empfänger von Auskünften nicht genannt werden, mußten die Aufsichtsbehörden dagegen abschlägig bescheiden. Diese Daten werden in der Regel nicht im Auskunftsbestand des Betroffenen gespeichert und unterliegen damit auch nicht der gesetzlichen Auskunftspflicht. Nur wenn die Daten automatisch verarbeitet werden, kann der Betroffene Auskunft auch über die Personen und Stellen verlangen, an die seine Daten regelmäßig übermittelt werden.

2.3.1.7 Berichtigung, Sperrung, Löschung von gespeicherten Daten

Stellt ein Betroffener fest, daß zu seiner Person gespeicherte Daten unrichtig sind, hat er Anspruch auf Berichtung. Dazu muß er der Auskunftei meist die richtigen Daten nennen. Er muß also abwägen, ob sein Interesse an der Berichtigung so groß ist, daß er, um den Fehler zu beseitigen, die richtigen Daten preisgibt.

Daten sind zu sperren, wenn ihre Richtigkeit bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt. Die Stelle, die das Datum gespeichert hat, muß die Richtigkeit der Daten überprüfen, wenn der Betroffene die Unrichtigkeit behauptet oder wenn sonstige Anhaltspunkte dafür vorliegen. Im Einzelfall kann schwer zu beurteilen sein, ob ein bestimmtes Datum richtig oder unrichtig ist. Vertritt die speichernde Stelle nach der Prüfung weiterhin die Auffassung, die Daten seien richtig, während der Betroffene dies bestreitet, und kann keine Seite die Richtigkeit ihrer Auffassung beweisen, so sind die Daten zu sperren, d. h. sie dürfen von der speichernden Stelle nicht mehr verwendet, insbesondere nicht an Dritte übermittelt werden. In der Praxis führte dies allerdings meist dazu, daß die Daten gelöscht wurden.

Gespeicherte Daten sind ferner am Ende des fünften Kalenderjahres nach ihrer Einspeicherung zu sperren. Der Betroffene kann auch die Löschung verlangen.

Die Stichproben der Aufsichtsbehörden haben keine Anhaltspunkte dafür ergeben, daß die Auskunfteien berechtigten Verlangen auf Berichtigung, Sperrung und Löschung nicht nachgekommen sind. Allerdings mußte wiederholt festgestellt werden, daß Daten, die älter als fünf Jahre waren, unter Hinweis auf den erheblichen organisatorischen Aufwand nicht gesperrt worden waren. Dies haben die Aufsichtsbehörden regelmäßig beanstandet. Es bleibt abzuwarten, ob bei den Wiederholungsprüfungen in diesem Punkt eine Verbesserung festgestellt werden kann.

2.3.2 Handel

2.3.2.1 Adressenhandel und Direktwerbung

Viele Beschwerden und Eingaben richteten sich gegen die Flut von unmittelbar an die Betroffenen adressiertem Werbematerial. Die Gerichte haben dazu bisher die Auffassung vertreten, daß die Direktwerbung zwar eine Belästigung sein könne, daß dadurch aber die Persönlichkeitsrechte der Betroffenen in der Regel noch nicht beeinträchtigt werden.

Da der Erfolg der Werbung wesentlich davon abhängt, daß sie den an dem angebotenen Produkt möglicherweise interessierten Personenkreis erreicht, ist ein werbendes Unternehmen an möglichst genauen Informationen über potentielle Kunden interessiert. Je mehr Informationen es besitzt, desto gezielter und erfolgversprechender kann es werben. Kenntnisse darüber, wer welche Hobbys, Interessen oder Eigenschaften hat oder wer bestimmte Materialien benötigt, lassen sich auf verschiedene Weise gewinnen; ergiebige Quellen sind z.B. Branchen- und Adreßbücher, Mitgliederverzeichnisse von Vereinen, Teilnehmerverzeichnisse spezieller Veranstaltungen usw. Häufig dienen auch Verlosungen und Preisausschreiben dem Zweck, Informationen über den Einzelnen zu erhalten, wenn die Teilnahmeberechtigung von weiteren Angaben, etwa über Hobbys, das Alter des Betroffenen o.ä., abhängig gemacht wird. Durch Auswerten allgemein zugänglicher Datenquellen, Adressenaustausch oder -verkauf und Zusammenführung des Materials läßt sich ein breites Spektrum von Informationen gewinnen. Auf diese Tätigkeit haben sich sogenannte Adressenhändler spezialisiert. Die Daten, in der Regel nach Berufen oder Berufsgruppen geordnet, werden für eine „maßgeschneiderte Regionalwerbung" teilweise auch nach Postleitzonen getrennt angeboten.

Vor dem Inkrafttreten des BDSG wurden Adressen im wesentlichen in ganzen Beständen (auf Magnetband oder Aufkleberlisten) zur einmaligen Nutzung verkauft. Neuerdings hat sich die sog. Adressenmittlung durchgesetzt. Hierbei werden die Adressen genutzt, ohne daß sie den Bereich des Adreßeigentümers verlassen. Adreßeigentümer sind Adressenverlage, können aber auch Versandhäuser oder andere Unternehmen sein. Durch einen Vermittler werden das werbende Unternehmen und der Adreßeigentümer in der Weise zusammengebracht, daß die eine Seite das Werbematerial, die andere die Adressen einbringt. Der Vermittler oder in seinem Auftrage ein sog. „Letter- Shop" adressieren das Material und geben es zur Post. Als Absender sind entweder das werbende Unternehmen oder ein Postfach des Letter-Shops angegeben. Das werbende Unternehmen erhält also die Adreßdaten nicht und weiß zunächst nur, daß eine bestimmte Anzahl von Personen in einem bestimmten Raum die Werbung erhalten hat. Erst wenn ein Adressat auf das Werbeschreiben antwortet, werden dem werbenden Unternehmen Namen und Adresse bekannt. Der Adressat offenbart damit zugleich seine Zugehörigkeit zum Kundenkreis des Adreßeigentümers. Dies ist ihm in der Regel nicht bewußt. Es kann ihm dadurch bewußt gemacht werden, daß im Werbeschreiben die Selektionskriterien genannt werden, die dazu geführt haben, ihn anzuschreiben. Wenn sich der Adressat dann gleichwohl dem werbenden Unternehmen offenbart, geschieht dies in vollem Bewußtsein der Konsequenzen der Antwort. Die Aufsichtsbehörden hatten mit dem Verband der Adressenverleger und Direktwerbeunternehmen eine entsprechende Vereinbarung getroffen. Leider hat die Praxis gezeigt, daß sich die werbenden Unternehmen nicht an diese Vereinbarung halten. Deshalb finden z.Z. erneut Verhandlungen der Aufsichtsbehörden der Länder mit der Werbewirtschaft unter Federführung des Niedersächsischen Ministers des Innern statt. Weiteres Ziel dieser Verhandlungen ist eine Verbesserung der Position des Betroffenen, insbesondere sollen die Adressen von Betroffenen, die nicht mehr umworben sein wollen, gelöscht werden.

Die Beschwerdeführer werden in der Regel darauf hingewiesen, daß eine Möglichkeit, die Zusendung unerwünschter Werbeschreiben einzudämmen, darin besteht, sich in die vom Verband der Adressenverleger und Direktwerbeunternehmer geführte „Robinson-Liste" aufnehmen zu lassen. Allerdings bietet auch diese von der Werbewirtschaft eingerichtete Liste keinen vollkommenen Schutz gegen unverlangte Werbung, weil der Verband nur etwa ein Drittel der Werbefirmen vertritt und in die Werbeadressen Namensvarianten geraten, die nicht in der Robinson-Liste verzeichnet sind.

Der Vollständigkeit halber sei darauf hingewiesen, daß auch das Kraftfahrtbundesamt Anschriften über Kraftfahrzeughalter zum Verkauf anbietet, jedoch nur dann, wenn sich diese bei der An- oder Ummeldung ihrer Fahrzeuge ausdrücklich damit einverstanden erklärt haben. Die Einwilligung ist jederzeit widerruflich. Ferner veräußert die Bundespost über die Deutsche Postreklame GmbH die in den Fernsprechbüchern veröffentlichten Angaben sowie Berufsangaben aus den Telefonanschlußanträgen. Auch diese Datenweitergabe wird eingestellt, wenn der Betroffene es verlangt.

2.3.2.2 Versandhandel

Datenschutzrechtliche Fragen aus dem Versandhandel beschäftigten die niedersächsischen Aufsichtsbehörden nur wenig. Die großen Versandhäuser haben ihren Sitz in anderen Bundesländern. So beschränkte sich die Tätigkeit der Aufsichtsbehörden in aller Regel darauf, Beschwerden an die Aufsichtsbehörden dieser Länder weiterzuleiten oder den Beschwerdeführer in allgemeiner Form über die Rechtslage zu informieren.

Immer wieder wurde der Umfang der erfragten Daten in den Bestellscheinen des Versandhandels in Frage gestellt. Die Versandhäuser fragen insbesondere bei Erstbestellungen eine Reihe von Informationen über den Kaufinteressenten ab, um sich über seine Kreditwürdigkeit zu vergewissern. So wird u.a. nach Berufstätigkeit, Familienstand, Staatsangehörigkeit und Aufenthaltsdauer gefragt. Die Antworten sind wesentliche Grundlage für die Entscheidung, ob und in welcher Höhe ein Kreditkonto als Einzel- oder Sammelbesteller eingerichtet wird (bei Ausländern z.B. ist die Aufenthaltsdauer in der Bundesrepublik von großer Bedeutung). Diese Informationen werden nicht in die Stammdaten des Kontos (z.B. Name, Adresse) übernommen oder für andere Zwecke benutzt. Bei Bestellungen, deren Wert 200 DM überschreitet oder bei Interesse an der Einrichtung eines Sammelbestellerkontos wird regelmäßig bei der SCHUFA nachgefragt. Da der neue Kunde diese Angaben im Rahmen des vorvertraglichen Vertrauensverhältnisses freiwillig abgibt, besteht kein Grund, gegen die Speicherung dieser Daten Einwendungen zu erheben, zumal, da die Erstbestellscheine nur noch für spätere Kontrollen und zur Erfüllung der handels- und steuerrechtlichen Aufbewahrungsvorschriften verwahrt werden.

2.3.3 Versicherungswirtschaft

Eingaben, die die Versicherungswirtschaft betrafen, hatten vor allem die Schweigepflicht-Entbindungsklausel und die Datenspeicherung oder den Datenaustausch der Versicherungen untereinander bei Schadensfällen zum Gegenstand.

2.3.3.1 Ermächtigungsklauseln in Versicherungsverträgen

Bei Vertragsabschluß erbitten die Versicherungsunternehmen verschiedene Informationen, die ihnen die Bearbeitung des Antrags — insbesondere das Abschätzen des zu übernehmenden Risikos — und die Durchführung des Versicherungsvertrages ermöglichen sollen. Der Versicherungsnehmer unterzeichnet in diesem Zusammenhang Ermächtigungsklauseln, mit denen er seine Zustimmung zur Verarbeitung ihn betreffender Informationen erteilt. Dabei ist zu unterscheiden zwischen einer Klausel, mit der der Versicherungsnehmer in die Verarbeitung personenbezogener Daten einwilligt, und solchen, die die ärztliche Schweigepflicht nach § 203 StGB betreffen.

Mit der Datenverarbeitungsklausel verfolgt die Versicherungswirtschaft im wesentlichen zwei Anliegen. Sie soll einmal die Zulässigkeit der Datenverarbeitung auch in den Fällen sicherstellen, in denen die Zulässigkeitstatbestände des § 23 Satz 1 und § 24 Abs. 1 BDSG nicht vorliegen oder zumindest zweifelhaft sind. Sie soll zum anderen Datenempfängern, denen das Versicherungsunternehmen Daten des Versicherungsnehmers übermittelt und die diese Daten speichern, die in § 26 Abs. 1 BDSG vorgeschriebene Benachrichtigung des Versicherungsnehmers ersparen; dieser wird in der Klausel auf die beabsichtigte Übermittlung hingewiesen, erhält also im Sinne des § 26 Abs. 1 BDSG „auf andere Weise" Kenntnis.

Daten der Versicherungsnehmer werden an viele verschiedene Empfänger, z. B. an Rückversicherer, andere Versicherungsunternehmen der Versicherungsgruppe, Verbände einer Sparte, andere Versicherungsunternehmen derselben Sparte und Versicherungsvermittler weitergegeben. Da die gesetzlichen Zulässigkeitsvoraussetzungen dieser vielfältigen Datenübermittlungen im Interesse einer zügigen Vertragsabwicklung und aus Kostengründen nicht in jedem Einzelfall zweifelsfrei festgestellt werden können, kann die Datenweitergabe nur durch die Einwilligung des Betroffenen rechtlich abgesichert werden. Voraussetzung für eine wirksame Einwilligung ist, daß der Betroffene die Konsequenzen seiner Erklärung übersehen kann. Deshalb haben die Aufsichtsbe-

hörden der Länder und die Spitzenverbände der Versicherungswirtschaft unter Beteiligung des Bundesaufsichtsamtes für das Versicherungswesen eine Klausel vereinbart, in der jedes Versicherungsunternehmen seine regelmäßigen Datenempfänger namentlich bezeichnen kann. Außerdem wurde vereinbart, daß dem Betroffenen auf Wunsch ein Merkblatt mit ausführlichen Informationen zur Datenübermittlung ausgehändigt wird.

Da kein Anspruch auf Abschluß eines Versicherungsvertrages besteht — ausgenommen ist die Kfz-Haftpflicht-Versicherung —, steht es dem Versicherungsunternehmen grundsätzlich frei, den Vertragsabschluß abzulehnen, wenn der Antragsteller die Ermächtigungsklausel streicht. Die Versicherungsunternehmen haben sich jedoch verpflichtet, in einem solchen Fall den Interessenten zunächst ausführlich über die Bedeutung der Klausel und die Gründe, die im Fall der Streichung die Durchführung des Vertrages verhindern, zu unterrichten.

Über die Schweigepflicht-Entbindungsklausel (für Ärzte) in den Lebens-, Kranken- und Unfallversicherungsverträgen ist noch keine einvernehmliche Regelung mit der Versicherungswirtschaft gefunden worden. In diesen Versicherungssparten ist die Abschätzung des gesundheitlichen Risikos ein wesentlicher Gesichtspunkt für die Tarifkalkulation und die einzelfallbezogene Vertragsgestaltung. Die Versicherungsunternehmen sind deshalb daran interessiert, von Ärzten und Krankenhäusern, von anderen Versicherungsunternehmen und auch staatlichen Stellen (z. B. den Sozialversicherungsträgern) Auskünfte über die Gesundheitsverhältnisse des Versicherungsnehmers zur Nachprüfung seiner Angaben zu erhalten.

Wegen der pauschalen Fassung der derzeit verwendeten Klausel sind jedoch die Sozialversicherungsträger gehindert, Sozialdaten an Versicherungen weiterzugeben, weil hierfür die Einwilligung des Betroffenen „im Einzelfall" erforderlich ist. Die mangelnde Bestimmtheit der Klausel sowie der Umfang der Informationswünsche der Versicherungen sind die wesentlichen Punkte in den z. Z. laufenden Verhandlungen mit den Spitzenverbänden der Versicherungswirtschaft.

2.3.3.2 Zentrale Dateien der Versicherungswirtschaft

Verschiedene Verbände der Versicherungswirtschaft haben Zentraldateien eingerichtet, aus denen Daten an alle Mitgliedsunternehmen der gleichen Sparte übermittelt werden.

— Zentrale Registrierstelle Rechtsschutz

Die Rechtsschutzversicherer und ihr Verband (HUK-Verband) haben ein Auskunftssystem eingerichtet, das den Versicherern in der Hauptsache dazu dient, vor Annahme eines Vertrages das einzugehende Risiko besser einschätzen zu können. Gemäß § 19 Abs. 2 der Allgemeinen Bedingungen über die Rechtsschutzversicherungen (ARB) ist dem Rechtsschutzversicherer die Kündigung eines Versicherungsvertrages möglich, wenn der Versicherungsnehmer seine Versicherung häufiger in Anspruch nimmt und damit kein „normales Risiko" mehr darstellt. Um beurteilen zu können, ob von einem normalen Risiko ausgegangen werden kann, hat der Versicherer zunächst nur die Angaben des Antragstellers. Nach § 16 des Versicherungsvertragsgesetzes (VVG) hat dieser alles anzugeben, was der Risikobeurteilung dient; dazu zählt auch der Verlauf von Vorversicherungen. In vielen Anträgen aber wird die Frage nach dem Vorversicherer nicht beantwortet. Die Rechtsschutzversicherer sind deshalb dazu übergegangen, alle Kündigungen nach § 19 Abs. 2 ARB dem HUK-Verband zu melden. Dieser informiert alle Rechtsschutzversicherer über die Kündigungen durch die regelmäßige Übersendung einer vollständigen Kopie der Datei. Auf diese Weise läßt sich

feststellen, ob ein Antragsteller die Angaben über eine Vorversicherung „vergessen" hat.

Gegen die Datenübermittlung an den HUK-Verband bestanden bisher keine datenschutzrechtlichen Bedenken. Es muß allerdings geprüft werden, ob nach dem Urteil des BGH zur Wirksamkeit der SCHUFA-Klausel (vgl. 2.3.1.3) die Ermächtigungsklausel in Versicherungsverträgen noch als ausreichende Ermächtigung zur Datenübermittlung an zentrale Dateien angesehen werden kann. Dagegen halten die Aufsichtsbehörden für den Datenschutz die vollständige Übermittlung der Datei an alle Rechtsschutzversicherer auch schon heute für unzulässig. Nach ihrer Auffassung ist dieses Verfahren durch die Ermächtigungsklausel nicht gedeckt, weil im Zeitpunkt der Übermittlung noch keine Einzelfallprüfung zur konkreten Risikobeurteilung ansteht und deshalb ein berechtigtes Interesse des Datenempfängers an der Kenntnis aller Kündigungen nicht dargelegt werden kann. Als Lösung haben sie eine Anfrage bei der Zentraldatei vorgeschlagen, wenn im konkreten Fall ein Versicherungsantrag vorliegt, in dem die Frage nach dem Vorversicherer nicht beantwortet ist. Die Verhandlungen der Aufsichtsbehörden mit den Versicherungsunternehmen hierzu sind noch nicht abgeschlossen.

— Sonderwagnisdatei der Lebensversicherer

Beim Verband der Lebensversicherungsunternehmen e.V. wird eine „Wagnisdatei" der Lebensversicherungsgesellschaften geführt. In dieser Datei sind die zur Identifikation einer Person erforderlichen Daten sowie ein Hinweis darauf gespeichert, daß beim Abschluß eines Lebensversicherungsvertrages ein überdurchschnittliches Risiko bestünde. Nähere Angaben über Art und Qualität des Sonderwagnisses können diesem Datensatz allerdings nicht entnommen werden. Gesundheitsdaten werden in keinem Fall übermittelt.

Der Zweck der Datei besteht darin, den Versicherern die Möglichkeit zu verschaffen, die Angaben der Antragsteller zu überprüfen, die diese bei Vertragsabschluß zu machen haben (§ 16 VVG), um die versicherten Risiken besser einschätzen und tariflich richtig einordnen zu können.

Der gesamte Bestand dieser Datei wird monatlich an alle Lebensversicherungsgesellschaften übermittelt. Diese gleichen zunächst alle bestehenden eigenen Verträge mit den übermittelten Daten ab, um zu prüfen, ob Anlaß zu einer Nachprüfung der vom Versicherungsnehmer bei Vertragsabschluß angegebenen Risiken besteht. Ferner wird jeder neu eingehende Versicherungsantrag mit diesem Dateibestand verglichen, um fehlende Angaben über Risiko und Vorversicherer aufzudecken, zu deren Mitteilung der neue Kunde nach § 16 VVG verpflichtet ist.

Gegen dieses Verfahren haben die Aufsichtsbehörden aus den zur „Zentralen Registrierstelle Rechtsschutz" genannten Gründen gleichfalls Bedenken erhoben. Auch hier dauern die Verhandlungen mit den Versicherungsunternehmen noch an.

— Meldeverfahren des Deutschen Transportversicherungsverbandes

Die Reisegepäckversicherer melden in Form von „vertraulichen Rundschreiben" dem Deutschen Transportversicherungsverband jeden auffälligen Schadensfall. Der Grund für die Auffälligkeit kann darin liegen, daß gegen strafrechtliche Vorschriften oder gegen versicherungsvertragliche Obliegenheiten verstoßen wurde. Die Originale der eingehenden Meldungen werden zu Beweiszwecken beim Verband gesammelt; dieser verteilt Kopien der Mel-

dungen an alle anderen Reisegepäckversicherer im Bundesgebiet. Auf diese Weise machen sich die Reisegepäckversicherer gegenseitig auf neue Fallgestaltungen aufmerksam, die es rechtfertigen, unredlichen Versicherungsnehmern die Leistung im Schadensfall zu verweigern oder sogar einen Strafantrag zu stellen. Darüber hinaus bieten die Mitteilungen allen anderen Versicherern die Möglichkeit, die eigenen Versicherungsbestände zu überprüfen, ob für einen Versicherungsnehmer bereits ein Schaden reguliert wurde, der ggf. erst aufgrund der Mitteilung als auffälliger Schaden oder gar als Betrug erkannt werden kann.

Auch hier bestehen die gleichen Bedenken wie bei den vorgenannten Zentraldateien. Allerdings wird man — auch im Interesse der Versichertengemeinschaft — bei den Reisegepäckversicherern ein berechtigtes Interesse des einzelnen Versicherungsunternehmens anerkennen müssen, alle anderen Versicherer über auffällige Ereignisse zu unterrichten und von diesen unterrichtet zu werden, um Betrugsfälle oder fingierte Schadensmeldungen aufzudecken.

Gleichwohl ist dem Verband empfohlen worden, das Mitteilungsverfahren auf die Erforderlichkeit im konkreten Einzelfall auszurichten und die beim Verband bestehende Datensammlung deshalb mit vermindertem Datenbestand als reine Hinweisdatei auszugestalten oder aber die Ermächtigungsklausel als Einwilligung in die Datenübermittlung umzuformulieren. Auch hier sind die Verhandlungen mit der Versicherungswirtschaft noch nicht abgeschlossen.

— Malus-Datei der Kfz-Versicherer

Der HUK-Verband hat für die Kfz-Haftpflichtversicherer zur Kontrolle der richtigen Einstufung der Verträge eine Zentraldatei errichtet.

Der Beitragssatz in der Kfz-Haftpflichtversicherung richtet sich u.a. nach der Dauer der schadensfreien Mitgliedschaft. Bei einem Versicherungswechsel legt der Versicherungsnehmer darüber in der Regel eine Bescheinigung des bisherigen Versicherers vor, um sich den sog. Bonus zu erhalten. Fehlt eine solche Bescheinigung, verlangt die vom Bundesminister für Wirtschaft genehmigte Tarifordnung eine sog. „Vorversicherer-Anfrage", um eine tarifgerechte Einstufung des Versicherungsvertrages zu ermöglichen.

Viele Kfz-Halter haben versucht, die Einstufung ihrer Versicherungsverträge in eine Schadensklasse dadurch zu verhindern, daß sie den Versicherer wechselten und beim neuen Versicherer den schadensbehafteten Vorvertrag verschwiegen. Um dies verhindern zu können, werden Daten über gekündigte Verträge, die in eine Schadensklasse eingestuft sind oder aufgrund des Schadensverlaufes im Folgejahr in eine Schadensklasse eingestuft werden müßten, an den HUK-Verband übermittelt. Diese Daten entsprechen denen, die der Versicherungsnehmer auch in seinem Antrag auf Abschluß einer Kfz-Haftpflichtversicherung zur Risikobeurteilung anzugeben hat.

Gegen dieses Verfahren bestehen aus der Sicht der Aufsichtsbehörden keine Bedenken. Der Unterschied zu den vorgenannten Zentraldateien besteht darin, daß nicht der Gesamtbestand der Malus-Datei an alle Kfz-Versicherer weitergegeben wird. Nur wenn im Einzelfall ein Antrag auf Abschluß einer Kfz-Haftpflichtversicherung keine Angaben über einen Vorversicherer enthält, werden auf Anfrage Auskünfte aus der Malus-Datei erteilt. Die anfragende Versicherung muß in der Einzelanfrage — ggf. durch den Versicherungsantrag — das berechtigte Interesse an der Kenntnis darlegen.

2.3.4 Banken und Sparkassen

Den meisten Bürgern war bislang unbekannt, daß zwischen den Banken und Sparkassen ein reger Informationsaustausch über wirtschaftliche Verhältnisse, das Zahlungsverhalten und die Kreditfähigkeit ihrer Kunden bestand. Diese Bankauskünfte wurden in aller Regel ohne Einwilligung des Kunden erteilt, der im allgemeinen auch später nicht erfuhr, daß sein Kreditinstitut Auskünfte über ihn gegeben hatte. Bankauskünfte wurden auch Kunden der Banken und Sparkassen über andere Kunden erteilt. Diese Praxis war von den Datenschutzaufsichtsbehörden mehrfach beanstandet worden. Um die Forderungen der Aufsichtsbehörden zu erfüllen, beabsichtigte die Kreditwirtschaft, die Erteilung von Bankauskünften durch eine Ergänzung ihrer Allgemeinen Geschäftsbedingungen auf eine vertragsgemäße Grundlage zu stellen und teilte dies zum Jahreswechsel 1983/84 der Öffentlichkeit mit. Die vorgesehene Änderung stieß jedoch erneut auf Bedenken der Datenschutzaufsichtsbehörden, weil sie mit wesentlichen Grundsätzen der Datenschutzgesetze nicht zu vereinbaren war und die Kunden unangemessen benachteiligte.

Die Veröffentlichung dieser Bedenken löste eine Flut von Widersprüchen beunruhigter Bankkunden aus, die auch die niedersächsischen Aufsichtsbehörden beschäftigte. In den Verhandlungen zwischen Vertretern der Behörden und der Kreditwirtschaft wurde schließlich eine einvernehmliche Regelung erzielt. Nach dem im Oktober 1984 vom Kreditausschuß und den Datenschutzkontrollinstanzen veröffentlichten „Gemeinsamen Communique über das Bankauskunftsverfahren" gelten nunmehr folgende Bedingungen:

1. Das Kreditinstitut ist berechtigt, über Geschäftskunden (juristische Personen und Kaufleute) Bankauskünfte zu erteilen, sofern ihm keine anderslautende Weisung des Kunden vorliegt.
2. Bankauskünfte über Privatkunden erteilt das Kreditinstitut nur dann, wenn diese allgemein oder im Einzelfall ausdrücklich zugestimmt haben.
3. Bankauskünfte sind allgemein gehaltene Feststellungen und Bemerkungen über die wirtschaftlichen Verhältnisse des Kunden, seine Kreditwürdigkeit und Zahlungsfähigkeit; betragsmäßige Angaben über Kontostände, Sparguthaben, Depot- oder sonstige dem Kreditinstitut anvertraute Vermögenswerte sowie Kreditinanspruchnahmen werden nicht gemacht.
4. Bankauskünfte erhalten nur eigene Kunden sowie andere Kreditinstitute für deren eigene Zwecke und die ihrer Kunden; sie werden nur dann erteilt, wenn der Anfragende ein berechtigtes Interesse an der gewünschten Auskunft glaubhaft darlegt.

Der Bankkunde wird über den Inhalt der Neuregelung durch eine Kundeninformation „Bankauskunftsverfahren" unterrichtet, die in den Kreditinstituten ausliegt. Ferner sollen die genannten Regeln in die Allgemeinen Geschäftsbedingungen der Banken und Sparkassen aufgenommen werden. Bei dieser Gelegenheit wurde außerdem vereinbart, daß der Bankkunde künftig ausführlicher und deutlicher über das Auskunftsverfahren mit der SCHUFA unterrichtet werden soll. Wegen der inhaltlichen Ausgestaltung dieser Informationen sollte zunächst noch das Urteil zur SCHUFA-Klausel (vgl. 2.3.1.3) abgewartet werden. Nachdem das Urteil inzwischen vorliegt, sind auch die Gespräche mit der Kreditwirtschaft wieder aufgenommen worden.

2.3.5 Privatärztliche Verrechnungsstellen

Wer als Privatpatient einen Arzt, Zahnarzt oder anderen Angehörigen der Heilberufe oder ein Krankenhaus aufsucht, wird nicht auf der Grundlage eines Krankenscheines behandelt, sondern erhält eine Rechnung über die erbrachten

Leistungen. Dabei stellen die meisten Ärzte die Rechnungen nicht selbst aus, sondern übermitteln die dafür benötigten Daten an eine privatärztliche Verrechungsstelle. Diese stellt die Rechnung aus, überwacht in der Regel auch die Zahlung und speichert zu diesem Zweck die entsprechenden Daten.

Die rechnungsmäßige Abwicklung des Behandlungsvertrages über privatärztliche Verrechnungsstellen und die Übermittlung der Behandlungsdaten einschließlich der Diagnose ist nach Auffassung der obersten Aufsichtsbehörden datenschutzrechtlich zulässig, weil diese Stellen der strafrechtlich geschützten Schweigepflicht nach § 203 Abs. 1 Nr. 6 des Strafgesetzbuches (StGB) unterliegen. Gleichwohl haben die obersten Aufsichtsbehörden empfohlen, die Patienten in geeigneter Weise über dieses Verfahren zu informieren (z.B. durch einen Aushang im Wartezimmer).

Inzwischen ist jedoch die Tendenz erkennbar, daß in zunehmendem Maße auch andere gewerbliche Dienstleistungsunternehmen Abrechnungen für Ärzte durchführen. Da es sich bei diesen Unternehmen in der Regel nicht um berufsständische ärztliche Vereinigungen in der Rechtsform eines Vereins von Ärzten handelt, unterliegen sie nicht der Schweigepflicht nach dem StGB. Damit ist die Weitergabe der Behandlungsdaten nur zulässig, wenn der Patient schriftlich in die Datenübermittlung einwilligt; anderenfalls würde die Weitergabe dieser Daten eine unbefugte Offenbarung eines fremden Geheimnisses im Sinne von § 203 StGB darstellen.

Den niedersächsischen Aufsichtsbehörden lagen Beschwerden zu dieser Problematik zwar noch nicht vor; sie werden die weitere Entwicklung jedoch aufmerksam verfolgen.

2.3.6 Service-Rechenzentren

Weitgehend unbeachtet von der Öffentlichkeit vollzog sich die Prüftätigkeit der Aufsichtsbehörden bei den Service-Rechenzentren.

Viele Unternehmen der Wirtschaft, vor allem kleinere Unternehmen, lassen ihre Geschäftsdaten außer Haus durch ein externes Rechenzentrum verarbeiten. Diese sogenannte „Datenverarbeitung im Auftrag" ist im BDSG ausdrücklich zugelassen. Deshalb liegt für die Verarbeitung der Kunden-, Lieferanten- oder auch Mitarbeiterdaten durch Service-Rechenzentren in der Regel keine gesonderte Einwilligung der Betroffenen vor; darum kommt der Ausgestaltung des Auftragsverhältnisses besondere Bedeutung zu.

Für die Zulässigkeit der Datenverarbeitung im Auftrag gelten zwei Voraussetzungen: zum einen hat der Auftraggeber den Auftragnehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen (§ 22 Abs. 2 BDSG), zum anderen ist dem Auftragnehmer die Verarbeitung der personenbezogenen Daten nur im Rahmen der Weisungen des Auftraggebers gestattet (§ 37 BDSG). Die Vergabe der Datenverarbeitung an ein Rechenzentrum entbindet das auftraggebende Unternehmen nicht von seinen Verpflichtungen zur Einhaltung der Datenschutzvorschriften. So bleibt es weiterhin Adressat für die dem Betroffenen zustehenden Rechte, die sich im wesentlichen aus den §§ 26, 27 BDSG ergeben. Das Rechenzentrum, das geschäftsmäßig die Datenverarbeitung im Auftrag übernimmt, unterliegt seinerseits den Vorschriften des vierten Abschnitts des BDSG (§§ 31, 37). Es muß vor allem die notwendigen Maßnahmen zur Datensicherung (§ 6 BDSG) und zur Wahrung des Datengeheimnisses (§ 5 BDSG) treffen und — bei Vorliegen der gesetzlichen Voraussetzungen — einen betrieblichen Datenschutzbeauftragten bestellen (§ 38 BDSG). Daneben unterliegt es der Meldepflicht bei der zuständigen Aufsichtsbehörde.

Da Service-Rechenzentren ausschließlich fremde Daten verarbeiten, ist deren technische und organisatorische Sicherung gegen unerlaubte Zugriffe besonders wichtig. Die Datensicherungsmaßnahmen reichen von Schutzvorkehrungen gegen äußere Schadenseinflüsse (wie Einbruch, Diebstahl, Feuer) über system- und programmtechnische Maßnahmen (Protokollierung, wer wann was eingegeben oder abgerufen hat sowie automatische Schlüssigkeitsprüfungen von solchen Aktivitäten) bis hin zu reinen organisatorischen Maßnahmen, wie Zutrittsbeschränkungen für bestimmte Mitarbeiter, genauen Beschreibungen zur Abgrenzung der Befugnisse und Verantwortlichkeiten der Mitarbeiter und Vorschriften über Entnahme und Aufbewahrung von Datenträgern. Hierzu gehören vor allem Vorkehrungen dagegen, daß die Datenbestände verschiedener Kunden miteinander vermischt werden oder daß ein Kunde auf den Bestand eines anderen Kunden zugreift.

Die Aufsichtsbehörden haben festgestellt, daß die Service-Rechenzentren im allgemeinen sehr darum bemüht sind, die notwendigen Datensicherungsmaßnahmen zu verwirklichen. Da die Verarbeitung von fremden Daten in der Regel ihre Existenzgrundlage bildet, haben sie ein großes eigenes Interesse daran, die Anforderungen des Datenschutzes zu erfüllen.

Schwachstellen mußten allerdings bei der vertraglichen Ausgestaltung der Auftragsdatenverarbeitung festgestellt werden. Das BDSG enthält keine Vorschriften über die Anforderungen an die Weisungen des Auftraggebers. So besteht keine Pflicht, die Vereinbarung mit dem Auftragnehmer schriftlich niederzulegen. Andererseits hat die Aufsichtsbehörde zu prüfen, ob dem Rechenzentrum konkrete Weisungen des Auftraggebers vorliegen und ob es die Datenverarbeitung entsprechend diesen Weisungen gestaltet hat. Sofern entsprechende Weisungen des Auftraggebers nicht vorlagen, führte dies daher zwangsläufig zu Beanstandungen. Lagen lediglich mündliche Abreden vor, wurde ausnahmslos darauf gedrungen, sie schriftlich niederzulegen. Aber auch wenn die Aufsichtsbehörde das Rechenzentrum davon überzeugen konnte, daß schriftliche Vereinbarungen im Hinblick auf mögliche Schadensersatzforderungen im eigenen Interesse lägen, kam es vor, daß Auftraggeber nicht zu schriftlichen Vereinbarungen bereit waren, offensichtlich, um langfristige Bindungen an das Rechenzentrum zu vermeiden. Den Rechenzentren blieb aus wirtschaftlichen Gründen (Verlust des Auftrages) keine andere Wahl, als auch diese Aufträge anzunehmen.

2.3.7 Datenschutz im Arbeitsverhältnis

Das Arbeitsverhältnis ist Anknüpfungspunkt einer großen Zahl von Informationsansprüchen, die bis ins einzelne gehende Angaben zur Person des Arbeitnehmers zum Gegenstand haben. Diese Informationsansprüche beruhen auf zahlreichen gesetzlichen oder tarifrechtlichen Bestimmungen in Tarifverträgen, Steuergesetzen und Vorschriften zur Kranken-, Renten-, Arbeitslosen- und Unfallversicherung. Ferner enthalten die Arbeitsschutzgesetze (Arbeitssicherheitsgesetz, Jugendarbeitsschutzgesetz, Mutterschutzgesetz, Kündigungsschutzgesetz), das Arbeitsförderungsgesetz, das Bundeskindergeldgesetz sowie das Unterhaltssicherungsgesetz — um nur einige dieser Rechtsvorschriften zu nennen — gesetzliche Grundlagen für die Erfassung und Verwendung von Arbeitnehmerdaten.

Vor allem ist der Arbeitgeber selbst an umfassenden Informationen über seine Arbeitnehmer interessiert. Sie versetzen ihn in die Lage, Arbeitsabläufe besser zu steuern und den Arbeitseinsatz — auch im Interesse der Arbeitnehmer — wirksamer zu gestalten. Angaben über Schwangerschaft oder Schwerbehinderung sind bei der Suche nach einem angemessenen Arbeitsplatz nützlich oder

sogar erforderlich. Die Einsatzmöglichkeiten der elektronischen Datenverarbeitung mußten fast zwangsläufig dazu führen, die Verarbeitung der Personalinformationen zu automatisieren. Zumindest dort, wo für viele Mitarbeiter Daten zu verwalten sind, ist — schon wegen der Fristen und Termine für Meldepflichten des Arbeitgebers — der Einsatz eines Datenverarbeitungsverfahrens kaum noch zu umgehen. So wickeln fast alle größeren Betriebe inzwischen die Lohn- und Gehaltsabrechnung mit Hilfe der automatisierten Datenverarbeitung ab. Andere Bereiche sind die reine Personalverwaltung (Einstellung, Einstufung, Kündigung, Personaleinsatz), die Produktions- und Vertriebsplanung und weiter die Gleitzeit- und Telefondatenerfassung.

Obwohl in der Öffentlichkeit vor allem über die Einführung sogenannter „Personalinformationssysteme" durchaus kontroverse Auffassungen bestehen, erhielten die niedersächsischen erhielten die Aufsichtsbehörden keine Eingaben und Beschwerden zu Personalinformationssystemen. Da die Unternehmen der Wirtschaft, bei denen bereits Personalinformationssysteme eingerichtet sind, in aller Regel nur der Anlaßaufsicht unterliegen, konnten die Aufsichtsbehörden über den Umgang mit Personalinformationssystemen keine eigenen Erkenntnisse gewinnen.

Die vereinzelt vorliegenden Anfragen zum Arbeitnehmerdatenschutz galten vorrangig der Telefondatenerfassung. Die Zulässigkeit der Speicherung von Telefondaten der Arbeitnehmer wird allgemein nicht in Frage gestellt. Die Berechtigung des Arbeitgebers zur Erfassung ergibt sich aus der Zweckbestimmung des Arbeitsverhältnisses; der Arbeitgeber hat ein berechtigtes Interesse an der Vermeidung unnötiger Telefongespräche und an einer korrekten Telefonbenutzung durch den Arbeitnehmer, vor allem wegen des von ihm zu tragenden Kostenrisikos für Amtsanschlüsse mit Fernwahlmöglichkeit. Ein Teil der Rechtsprechung hat jedoch — gerade in jüngster Zeit — Probleme in der Erfassung von Daten Dritter, also der Angerufenen, gesehen. Dies ist allerdings keine Frage des Arbeitnehmerdatenschutzes. Die Landesregierung wird die weitere Entwicklung der Rechtsprechung aufmerksam verfolgen.

2.4 Erfahrungen aus der Überwachungstätigkeit

2.4.1 Datenschutzbewußtsein

Die vielen Eingaben von Bürgern zeigen, daß sich die Bevölkerung der Gefahren für die Persönlichkeitsrechte bewußt ist, die mit den neuen Informationstechniken verbunden sind. Allerdings handelt es sich dabei selten um ein rechtlich fundiertes Bewußtsein. Überwiegend wird nur ein allgemeines Unbehagen über die Datenverarbeitung zum Ausdruck gebracht (vgl. 2.2). Häufig wird übersehen, daß die Datenschutzgesetze die Verarbeitung personenbezogener Daten nicht generell untersagen, sondern nur an bestimmte Voraussetzungen knüpfen, und daß die Datenverarbeitung dazu dient, Aufgaben und Geschäftszwecke der betreffenden Unternehmen — nicht zuletzt auch zum Vorteil des Bürgers — rationeller zu erfüllen. Hier konnten die Aufsichtsbehörden aufklären. Dies wird auch eine der wichtigsten Aufgaben der künftigen Tätigkeit bleiben.

Bei den gewerblichen Unternehmen ist das Datenschutzbewußtsein recht unterschiedlich ausgeprägt. Die Aufsichtsbehörden haben festgestellt, daß es mit der Größe der Unternehmen und mit der Qualifikation der Mitarbeiter zunimmt. Unternehmen, die einen hauptberuflichen Datenschutzbeauftragten beschäftigen oder bei denen der betriebliche Datenschutzbeauftragte einen bedeutenden Teil seiner Arbeitszeit auf den Datenschutz verwenden kann, wenden sich häufiger mit schriftlichen und telefonischen Anfragen an die Auf-

sichtsbehörde; auch bei den Aufsichtsprüfungen wurde festgestellt, daß sich solche Unternehmen sehr um die Einhaltung der datenschutzrechtlichen Vorschriften bemühen. Dagegen entstand der Eindruck, daß bei kleineren Unternehmen der Datenschutz häufiger als eine lästige Pflicht betrachtet wird und nur gelegentlich in das Bewußtsein der Unternehmer rückt, vor allem dann, wenn sich die Aufsichtsbehörde zur Prüfung anmeldet. Dies zeigte sich auch darin, daß häufig erst nach der Anmeldung zur Aufsichtsprüfung Änderungsmeldungen zum Datenschutzregister gefertigt wurden, obwohl die Monatsfrist längst überschritten war. Bei diesen Unternehmen fehlte den Datenschutzbeauftragten auch öfter die erforderliche Fachkunde. Da der betriebliche Datenschutzbeauftragte bei Prüfungen anwesend ist, war leicht festzustellen, ob es sich um einen geeigneten Mitarbeiter handelte, der die ihm im BDSG zugewiesenen Aufgaben auch tatsächlich erfüllen konnte. Die Wiederholungsprüfungen werden zeigen, inwieweit die Tätigkeit der Aufsichtsbehörden dazu beigetragen hat, auch in diesem Punkte zu Verbesserungen beizutragen.

Die geringe Zahl von Anlaßprüfungen und die Ergebnisse der regelmäßigen Prüfungen zeigen, daß die Wirtschaft im großen und ganzen den Anforderungen des Datenschutzes gerecht wird. Viele der von den Aufsichtsbehörden in den Anfangsjahren beanstandeten Schwachstellen waren auf die noch mangelnde Erfahrung mit dem BDSG zurückzuführen. Die Aufsichtsbehörden haben sich deshalb auch nicht nur als Kontrollinstanz, sondern vor allem auch als beratende Stellen verstanden. Die Betriebe und ihre Datenschutzbeauftragten zeigten sich dabei in der Regel aufgeschlossen, Anregungen aufzunehmen und Beanstandungen nachzukommen. Dies beweist auch der Umstand, daß erst in zehn Fällen die Verhängung eines Bußgeldes wegen Verstößen gegen die Meldepflicht oder ähnliche formale Datenschutzbestimmungen erforderlich war.

Hinzu kommt, daß die Unternehmen erkannt haben, daß sich viele Anforderungen des Datenschutzes durchaus positiv auf die internen Geschäftsabläufe auswirken können, indem z. B. Arbeitsabläufe besser gesteuert und transparenter gestaltet, durch Programm- und Verfahrensprüfungen kostenintensive Wiederholungsläufe vermieden und durch Programmdokumentationen personelle Veränderungen besser und schneller aufgefangen werden.

2.4.2 Datensicherheit

Die datenverarbeitenden Personen und Stellen sind nach § 6 BDSG verpflichtet, die zur Ausführung des Gesetzes erforderlichen technischen und organisatorischen Maßnahmen zu treffen. Datenverarbeitungsprogramme und -anlagen müssen gegen Verlust, Verfälschung und Beschädigung gesichert sein, unabhängig davon, ob diese Schäden durch bewußte Eingriffe (Mißbrauch, Sabotage) oder sonstige Einwirkungen (Fehler, Zufall, Katastrophen) eintreten könnten. Für die automatische Datenverarbeitung hat der Gesetzgeber in der Anlage zu § 6 BDSG Anforderungen an die Datensicherung für die wichtigsten Verarbeitungsbereiche vorgesehen. Dabei handelt es sich nicht um eine abschließende Aufzählung der Anforderungen; ob und ggf. welche Sicherungsmaßnahmen erforderlich sind, kann nur im konkreten Einzelfall beurteilt werden. Als Maßstäbe für Datensicherungsmaßnahmen nennt § 6 Abs. 1 BDSG zum einen die Erforderlichkeit, zum anderen das angemessene Verhältnis zwischen dem Aufwand für die Datensicherungsmaßnahme und dem angestrebten Schutzzweck. Zu berücksichtigen sind etwa die Sensitivität der gespeicherten Daten, die jeweilige Aufgabe, der Nutzwert der Daten für die eigenen Interessen, den Betroffenen oder unberechtigte Dritte sowie die Mißbrauchsgefahr.

Nach den Erfahrungen der niedersächsischen Aufsichtsbehörden haben vor allem Mittel- und Kleinbetriebe Schwierigkeiten, die geforderten Datensiche-

rungsmaßnahmen zu verwirklichen. Dies hat mehrere Gründe. Nach den bei den Prüfungen gewonnenen Einblicken in diese Unternehmen ist der Personalbestand in der Datenverarbeitung häufig so gering, daß kaum Kapazitäten für die Erarbeitung entsprechender Maßnahmen frei sind. Oft wird auch die Notwendigkeit von Datensicherungsmaßnahmen nicht richtig eingeschätzt oder aus Wirtschaftlichkeitsüberlegungen der Aufwand dafür gescheut. Dabei kann Datensicherheit häufig schon durch einfache Mittel herbeigeführt werden, etwa durch die Beschaffung abschließbarer Metallschränke, den Austausch von herkömmlichen Türschlössern gegen Sicherheitsschlösser, die Sicherung von Fenstern durch Panzerglas oder Vergitterungen oder die Installierung einer Alarmanlage.

Je nach Art der Datenverarbeitung müssen unterschiedliche Anforderungen an die Datensicherheit gestellt werden. So ist z.B. die Speicherkontrolle, d.h. die Verhinderung unbefugter Eingaben in einen Datenspeicher sowie der unbefugten Kenntnisnahme, Veränderung oder Löschung gespeicherter Daten, in der Regel bei Unternehmen, die ausschließlich Mikroverfilmung betreiben, ohne Belang. Die Ausführungen dieses Berichts beschränken sich daher auf die Bereiche, die für die überwiegende Zahl der datenverarbeitenden Unternehmen von Bedeutung sind.

Die Aufsichtsbehörden stellten als wesentliche Mängel vor allem fest, daß Unbefugten der Zugang zu Datenverarbeitungsanlagen nicht immer verwehrt wird (Zugangskontrolle). So waren Zugangswege nicht gesichert, und vielfach wurde die Erteilung von Zugangsberechtigungen an die Mitarbeiter sehr großzügig gehandhabt. In einigen Fällen gab es überhaupt keine Regelung, und eine Antwort auf die Frage nach dem Kreis der Zugangsberechtigten konnte erst nach einer Diskussion zwischen dem betrieblichen Datenschutzbeauftragten und dem Leiter der Datenverarbeitung gegeben werden. Weitere Schwachpunkte ergaben sich aus dem Fehlen von Richtlinien für das Vorgehen bei Verlust von Schlüsseln oder Code-Karten oder daraus, daß keine Regelung für nicht uneingeschränkt Zugangsberechtigte (Wartungs- und Reinigungspersonal, Besucher) vorlag.

Auch die Handhabung der Abgangskontrolle (Aufbewahrung der Datenträger und die Verhinderung ihrer unbefugten Entfernung) führte in vielen Fällen zu Beanstandungen. Die Aufbewahrung einer Kartei mit personenbezogenen Daten in Schuhkartons unter dem Sofa im Wohnzimmer eines Ein-Mann-Betriebes war zwar nur ein Extremfall; wenn Datenträger jedoch — und das ist kein Einzelfall — in unverschlossenen Schränken lagern und die Entnahme nicht protokolliert wird, kann dies keine ausreichende Sicherheit bieten.

In allen Betrieben mit On-line-Anwendungen waren die Benutzer- und Zugriffsberechtigungen festgelegt worden; Legitimation und Kontrolle der Benutzer wurden in der Regel durch Kennwörter sichergestellt. Zusätzliche Maßnahmen, z.B. das Abschließen der Datenstationsräume oder der Terminals, gab es dagegen selten. Dies wurde vor allem dann beanstandet, wenn die Kennwörter selten oder nie geändert wurden und die Wirksamkeit ihrer Kontrollfunktion dadurch unzureichend erschien.

Ein weiterer Mängelschwerpunkt lag bei der Auftragskontrolle. Hierzu wird auf die Ausführungen unter 2.3.6 verwiesen.

Dagegen war die Transportkontrolle, die gewährleisten soll, daß personenbezogene Daten bei ihrer Übermittlung sowie beim Transport entsprechender Datenträger nicht unbefugt gelesen, verändert oder gelöscht werden können, überwiegend zufriedenstellend geregelt.

Verbesserungsbedürftig war in vielen Fällen die Organisationskontrolle, die den datenverarbeitenden Stellen auferlegt, ihre Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird. Sie reicht von der Gliederung des Unternehmens bis zur Organisation des Datenträgerarchivs und erfaßt nicht nur den Verarbeitungsprozeß als solchen, sondern bereits Entwicklungsphasen der Programmierung von der Planung bis zur Außerdienststellung der Programme. Die wichtigste Maßnahme besteht in der Funktionentrennung. Dadurch soll erreicht werden, daß die unbefugte Kenntnisnahme von Daten und ihre unbefugte Verarbeitung oder Nutzung ausgeschlossen oder zumindest erschwert wird, indem bei der Verarbeitung jeweils nur bestimmte Personen unter bestimmten Bedingungen und in begrenztem Umfang genau abgegrenzte Funktionen wahrnehmen. Eine weitere wichtige Aufgabe besteht in der genauen und aktuellen Dokumentation von Aufbau- und Ablaufstrukturen. Dies ist eine wesentliche Voraussetzung rationeller Organisation, die schon im eigenen Interesse des Unternehmens liegt. Sie ist zugleich ein notwendiges Instrument des Datenschutzes, denn nur wenn der vorgesehene Ablauf einschließlich der Funktionen der einzelnen Mitarbeiter genau aufgezeichnet ist, lassen sich tatsächliche Abweichungen erkennen und unter Datenschutzgesichtspunkten prüfen.

Während die Organisationskontrolle in größeren Betrieben in der Regel nicht zu beanstanden war, wurde sie vor allem bei kleinen und mittleren Betrieben nur unzureichend vorgenommen. Äußerst selten waren Arbeitsplatzbeschreibungen zur genauen Abgrenzung der Kompetenzen und Verantwortlichkeiten zu finden. Hier wird ein weiterer Schwerpunkt der Wiederholungsprüfungen liegen.

Eine zusammenfassende Beurteilung der bei den geprüften Betrieben vorgefundenen Datensicherungsmaßnahmen ist kaum möglich. Die Ursachen dafür sind vielfältig. Wo das Bewußtsein für die Notwendigkeit der Datensicherung ausgeprägt war, zeigten sich zumindest Ansätze für Datensicherungsmaßnahmen. Dann konnte auch feststellt werden, daß diese Maßnahmen nicht zur Behinderung der organisatorischen Abläufe führen müssen, sondern über den eigentlichen Sicherungszweck hinaus sogar Nutzen bringen können. Dort, wo man dagegen der Datensicherung eher mit Gleichgültigkeit gegenüberstand, was nicht selten auf einen mangelhaften Informationsstand zurückzuführen war, und wo man lediglich den Aufwand der Datensicherung sah, waren überwiegend auch die geschilderten Mängel anzutreffen. Aufklärung und praxisbezogene Beratung sind daher Voraussetzung einer weiteren Verbesserung der Datensicherung.

2.4.3 Defizite der Datenschutzkontrolle

Viele Eingaben und Beschwerden sind auf ein bestimmtes Handeln der Aufsichtsbehörden zur Durchsetzung von Forderungen gegenüber datenverarbeitenden Stellen gerichtet und lassen erkennen, daß die Befugnisse der Datenschutzbehörden in der Regel überschätzt werden.

Die Befugnisse der Aufsichtsbehörden sind beschränkt. Sie können die Erteilung von Auskünften, den Zutritt zu den Geschäftsräumen und die Einsicht in die Geschäftsunterlagen fordern und erzwingen. Wer diesen Forderungen nicht nachkommt, handelt außerdem ordnungswidrig; die Ordnungswidrigkeit kann von der Aufsichtsbehörde mit einem Bußgeld geahndet werden. Damit stehen ihr hinreichende Möglichkeiten zur Verfügung, die Durchführung ihrer Prüfungen sicherzustellen. Dagegen hat sie keine Befugnis, Vorkehrungen zur Beseitigung festgestellter Mißstände zu verlangen und durchzusetzen. Das stößt auch beim Bürger auf wenig Verständnis. Dieses Problem wird im Rahmen der Novellierungsbemühungen zum BDSG gelöst werden müssen (vgl. 5.).

Im übrigen ist es Sache des Betroffenen, im Einzelfall seine Rechte gegenüber der datenverarbeitenden Stelle durchsetzen. Hat die Aufsichtsbehörde festgestellt, daß eine Rechtsverletzung gegenüber dem Beschwerdeführer vorliegt, verweist sie ihn zur Geltendmachung seiner individuellen Rechte an die Zivilgerichte. Es ist nicht ihre Aufgabe, private Rechte des Beschwerdeführers durchzusetzen. Würde die Aufsichtsbehörde vom Amts wegen — möglicherweise gegen den Willen des Betroffenen — gegen ein bestimmtes Verhalten des Unternehmens vorgehen, könnten dadurch, vor allem durch gerichtliche Verfahren, erneut schutzwürdige Belange des Betroffenen beeinträchtigt werden.

3. **Zusammenarbeit der Aufsichtsbehörden der Länder**

Die Datenschutzreferenten der Länder haben vereinbart, durch regelmäßige Abstimmungsgespräche eine möglichst einheitliche Anwendung der datenschutzrechtlichen Vorschriften in den Ländern sicherzustellen. Diese Abstimmungsgespräche zwischen den obersten Aufsichtsbehörden der Länder finden seit nunmehr acht Jahren regelmäßig unter Federführung des Innenministeriums des Landes Nordrhein-Westfalen statt. Niedersachsen ist in dieser Runde durch den Minister des Innern vertreten. Im Hinblick auf den Tagungsort hat sich für die Runde inzwischen die Bezeichnung „Düsseldorfer Kreis" eingebürgert.

In dieses Gremium werden die Erfahrungen der Aufsichtsbehörden der einzelnen Länder eingebracht. Es behandelt Datenschutzprobleme von überregionaler Bedeutung. Als eines der wichtigsten Ergebnisse der Koordinierungsbemühungen der Aufsichtsbehörden sind die „Vorläufigen Verwaltungsvorschriften zum BDSG" zu nennen. Obwohl die Mitglieder des Düsseldorfer Kreises keinem Einigungszwang unterliegen, ist es bisher trotz teilweise zunächst unterschiedlicher Auffassungen gelungen, zu allen wesentlichen Rechtsfragen übereinstimmende Auslegungen zu finden und dadurch eine einheitliche Vorgehensweise der Aufsichtsbehörden sicherzustellen. Dies ist im Hinblick auf den Gleichheitsgrundsatz und darauf, daß die datenverarbeitenden Stellen die Praxis der Aufsichtsbehörden in den einzelnen Ländern kritisch beobachten und vergleichen, von besonderer Bedeutung. Die Beschlüsse des Düsseldorfer Kreises werden den Aufsichtsbehörden in den Ländern und den betroffenen Wirtschaftsverbänden bekanntgegeben. Die dadurch erreichte Transparenz aufsichtsbehördlichen Handelns wird von der Wirtschaft begrüßt.

Daneben bestehen von Fall zu Fall enge Kontakte der einzelnen Aufsichtsbehörden der Länder untereinander, vor allem hinsichtlich der Unternehmen, die in verschiedenen Bundesländern tätig sind.

4. **Zusammenarbeit mit der Wirtschaft**

Eine wichtige Aufgabe des Düsseldorfer Kreises ist es, Ansprechpartner der Wirtschaftsverbände zu sein, wenn diese besondere Problembereiche des Datenschutzes erörtern wollen. Zu diesem Zweck werden von Fall zu Fall Arbeitsgruppen gebildet, die die Fragen zusammen mit Vertretern der Wirtschaft aufbereiten und dem Düsseldorfer Kreis zur abschließenden Beschlußfassung vorlegen. In der Regel werden dabei übereinstimmende Ergebnisse erzielt.

Die Aufsichtsbehörden in Niedersachsen nehmen darüber hinaus regelmäßig an den Sitzungen regionaler ERFA-Kreise (Erfahrungsaustausch-Kreise) teil. Dies sind Untergruppierungen der Gesellschaft für Datenschutz und Datensicherheit e.V., eines gemeinnützigen Vereins, dessen Mitglieder aus allen Bereichen der Wirtschaft und der Verwaltung kommen. Hier treffen sich vor allem die Datenschutzbeauftragten zahlreicher niedersächsischer Unternehmen zu einem Erfahrungsaustausch über aktuelle Probleme des Datenschutzes. Die Teil-

nahme der Aufsichtsbehörden an diesen Sitzungen dient dem ständigen Dialog mit diesem Personenkreis und bietet Gelegenheit, allgemeine Auslegungs- und Anwendungsfragen des Datenschutzes praxisbezogen zu erörtern.

5. **Novellierung des Bundesdatenschutzgesetzes**

Seit der Verabschiedung des BDSG durch den Deutschen Bundestag am 10.11.1976, der jahrelange intensive Beratungen in den Ausschüssen des Bundestages sowie Anhörungen der Vertreter von Wirtschaft und Verwaltung vorausgegangen waren, werden das Gesetz und seine Ziele in der Öffentlichkeit lebhaft diskutiert. Vor allem die Generalklauseln, die in den Erlaubnistatbeständen verwendet werden, waren von Anfang an umstritten. So ist es nicht verwunderlich, daß schon kurze Zeit nach der Verabschiedung des Gesetzes erste Novellierungswünsche geäußert wurden. Der ständige technische Fortschritt auf dem Gebiet der Informationsverarbeitung mag dazu beigetragen haben, daß erste Novellierungsentwürfe zum BDSG erst Anfang 1980 aus der Mitte des Bundestages vorgelegt wurden. Sie konnten in der damaligen Legislaturperiode allerdings nicht mehr behandelt werden. Auch ein nachfolgender Referentenentwurf aus dem Jahre 1982, der eine in vielen Punkten sehr kontroverse Diskussion auslöste, kam über dieses Stadium nicht hinaus.

Ein weiterer Gesetzentwurf zur Novellierung des BDSG wurde im Frühjahr 1984 von der SPD-Bundestagsfraktion eingebracht. Zu dem Entwurf fand im Sommer 1985 eine öffentliche Anhörung vor dem Innenausschuß des Deutschen Bundestages statt, die bisher noch nicht abgeschlossen werden konnte. Inzwischen haben auch die Bundestagsfraktionen von CDU/CSU und FDP und die Bundesregierung einen gemeinsamen Entwurf im Bundestag eingebracht (BT-Drs 10/4737).

Die beiden letzten Gesetzentwürfe werden wesentlich durch das Urteil des Bundesverfassungsgerichts vom 15.12.1983 zum Volkszählungsgesetz 1983 geprägt. Das Bundesverfassungsgericht hat sich mit der Erhebung personenbezogener Daten unter Androhung von Zwang zu statistischen Zwecken und mit der Zulässigkeit ihrer Nutzung zu sonstigen Zwecken befaßt. Über diesen Anlaß hinaus trifft das Urteil Aussagen von grundsätzlicher Bedeutung für alle Rechtsbereiche, in denen personenbezogene Daten verarbeitet werden. Prüfungsmaßstab des Bundesverfassungsgerichts war das aus den Grundrechten der Artikel 2 Abs. 1 und Artikel 1 Abs. 1 Grundgesetz abgeleitete „Recht auf informationelle Selbstbestimmung" des einzelnen. Dieses Recht umfaßt die Befugnis des einzelnen, „grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden" (a.a.O. C II 1.).

Der Urteilstenor, der nach § 31 Abs. 2 Bundesverfassungsgerichtsgesetz Gesetzeskraft hat, betrifft allerdings ausschließlich das Volkszählungsgesetz 1983. Die Bindungswirkung ist auf die tragenden Gründe des Urteils beschränkt, d. h. auf jene Entscheidungsteile, die unbedingt erforderlich sind, um die gefällte Entscheidung begründen zu können. Nicht von der Bindungswirkung erfaßt sind u. a. die Ausführungen, die eine die Entscheidung tragende Begründung verallgemeinern. Auch behandelt das Urteil nur das Verhältnis zwischen Bürger und Staat. Im Verhältnis der Privatrechtsträger untereinander gelten die Grundrechte nicht unmittelbar, so daß auch das „Recht auf informationelle Selbstbestimmung" kein unmittelbar im Privatrechtsverkehr geltendes Recht ist. Die Grundrechte können aber als Ordnungsgrundsätze bzw. objektive Wertentscheidungen der Verfassung mittelbar Drittwirkungen insofern entfalten, als Regelungen der Rechtsbeziehungen zwischen Privatpersonen in ihrem Geiste ausgelegt werden müssen, vor allem nicht im Widerspruch zu Grund-

rechten stehen dürfen. Inwieweit die Ausführungen des Bundesverfassungsgerichts unter diesem Gesichtspunkt auch für den privaten Bereich von Bedeutung sein können, muß im Rahmen der parlamentarischen Beratungen sorgfältig geprüft werden. Dabei muß berücksichtigt werden, daß der Private, der Daten anderer erhebt und speichert, selbst Grundrechtsträger ist und sich seinerseits auf das Grundrecht der allgemeinen Handlungsfreiheit und andere Grundrechte berufen kann. Deshalb muß häufig ein Ausgleich zwischen verschiedenen Grundrechten gesucht werden.

Die Landesregierung ist der Auffassung, daß es nach den bisherigen Erfahrungen mit dem BDSG einer grundlegenden Umgestaltung seiner für den nichtöffentlichen Bereich geltenden Regelungen oder einer wesentlichen Erweiterung seines Anwendungsbereiches nicht bedarf; das schließt nicht aus, Regelungsdefizite oder Unklarheiten zu beseitigen. Hierfür liegt die Gesetzgebungskompetenz — anders als für den öffentlichen Bereich — beim Bund.

Im Vordergrund stehen Anpassungen an den technischen Fortschritt, etwa im Hinblick auf den zunehmenden Einsatz von Kleincomputern (sog. Personal-Computer), die gerade auch dadurch erweiterten Möglichkeiten einer dezentralen Datenverarbeitung im Rechnerverbund sowie die wachsende Bedeutung von On-line-Verbindungen. Die Landesregierung unterstützt ferner die in den Novellierungsentwürfen zum Ausdruck gebrachten Bemühungen um eine Verbesserung des Datenschutzes im privaten Bereich, die — neben der Anpassung an neue technische Gegebenheiten — die Datenverarbeitung durchsichtiger machen und dem Bürger mehr Rechte geben sollen.

Das gilt einmal für das Auskunftsrecht der Bürger. In Fällen, in denen unrichtige Angaben übermittelt wurden, ist es für den Betroffenen heute nur schwer möglich, eine Richtigstellung bei den Datenempfängern zu erreichen. Es ist daher beabsichtigt, das Auskunftsrecht auf die Angabe der Datenlieferanten und -empfänger auszuweiten, um den Betroffenen in den Stand zu setzen, seine Rechte auch gegenüber diesen Stellen zu wahren. Die Auskünfte sollen in der Regel unentgeltlich erteilt werden. Bei Unternehmen, die Daten für fremde Zwecke verarbeiten, soll aber weiterhin ein Entgelt verlangt werden können, wenn etwa die Einholung einer Auskunft durch den Betroffenen offensichtlich nur dazu dient, die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken zu nutzen (so wurde beobachet, daß einzelne Unternehmen dazu übergehen, statt selbst eine — kostenpflichtige — Auskunft einzuholen, die Vorlage einer Selbstauskunft von dem Betroffenen zu verlangen). Auf diese Weise sollen vor allem die Auskunfteien gegen eine mißbräuchliche Ausübung des Auskunftsrechts geschützt werden. Im Rahmen der Novellierung wird auch eine Stärkung der Kontrollinstanzen angestrebt. So ist an eine Stärkung der Position des betrieblichen Datenschutzbeauftragten durch einen verbesserten Kündigungsschutz und Benachteiligungsverbote gedacht. Auch sollen die Aufsichtsbehörden — im Bereich der Anlaßaufsicht — nicht nur auf Eingaben Betroffener angewiesen, sondern auch aus anderem Anlaß zur Prüfung befugt sein. Vor allem sollen sie aber die Abstellung von Mängeln in der Datenverarbeitung auch durchsetzen können. So sollen sie Maßnahmen zur Beseitigung technischer und organisatorischer Mängel anordnen, einzelne Verfahren untersagen oder die Abrufung von betrieblichen Datenschutzbeauftragten, die die gesetzlichen Voraussetzungen nicht erfüllen, verlangen können.

Aufsichtsbehörden der Länder für den nicht-öffentlichen Bereich nach §§ 30, 40 BDSG

Land	Oberste Aufsichtsbehörde	regional zuständige Aufsichtsbehörden
Baden-Württemberg	Innenministerium Baden-Württemberg Dorotheenstr. 6 7000 Stuttgart 1	
Bayern	Bayerisches Staatsministerium des Innern Odeonsplatz 3 8000 München 22	Regierung von Oberbayern Maximilianstr. 39 8000 München 22 Regierung von Niederbayern Regierungsplatz 540 8300 Landshut Regierung der Oberpfalz Emmeransplatz 8/9 8400 Regensburg Regierung von Oberfranken Ludwigstr. 20 8580 Bayreuth Regierung von Mittelfranken Schloß 8800 Ansbach Regierung von Unterfranken Peterplatz 9 8700 Würzburg Regierung von Schwaben Fronhof 10 8900 Augsburg
Berlin	Senator für Inneres Fehrbelliner Platz 2 1000 Berlin 31	
Bremen	Der Landesbeauftragte für Datenschutz Arndtstraße 1 2850 Bremerhaven 1	
Hamburg	Hamburgischer Daten- schutzbeauftragter Karl-Muck-Platz 1 2000 Hamburg 36	
Hessen	Hessischer Minister des Innern Friedrich-Ebert-Allee 12 6200 Wiesbaden	Regierungspräsident Darmstadt Luisenplatz 2 6100 Darmstadt Regierungspräsident Gießen Landgraf-Philipp-Platz 1 6300 Gießen Regierungspräsident Kassel Steinweg 6 3500 Kassel
Niedersachsen	Niedersächsischer Minister des Innern Lavesallee 6 3000 Hannover	Bezirksregierung Hannover Am Waterlooplatz 11 3000 Hannover Bezirksregierung Braunschweig Bohlweg 38 3300 Braunschweig Bezirksregierung Lüneburg Auf der Hude 2 2120 Lüneburg Bezirksregierung Weser-Ems Theodor-Tantzen-Platz 8 2900 Oldenburg

Land	Oberste Aufsichtsbehörde	regional zuständige Aufsichtsbehörden
Nordrhein-Westalen	Innenminister des Landes Nordrhein-Westfalen Haroldstr. 5 4000 Düsseldorf	Regierungspräsident Köln Zeughausstr. 4–8, 5000 Köln (zuständig auch für Regierungsbezirk Düsseldorf) Regierungspräsident Arnsberg 5770 Arnsberg, Seibertzstr. 1 (zuständig auch für Regierungsbezirke Detmold und Münster)
Rheinland-Pfalz	Ministerium des Innern für Sport des Landes Rheinland-Pfalz Schillerplatz 5 6500 Mainz	Bezirksregierung Koblenz Stresemannstr. 3–5 5400 Koblenz Bezirksregierung Trier Mustorstr. 14 5500 Trier Bezirksregierung Rheinhessen-Pfalz Friedrich-Ebert-Str. 14 6730 Neustadt/Weinstraße
Saarland	Saarland Der Minister des Innern Der Landesbeauftragte für Datenschutz Sophienstr. 12 6600 Saarbrücken	
Schleswig-Holstein	Innenminister des Landes Schleswig-Holstein Düsternbrookerweg 70/90 Landeshaus 2300 Kiel	