12. Wahlperiode

Drucksache **12/3069**

HESSISCHER LANDTAG

27. 09. 88

Vorlage der Landesregierung

betreffend den Ersten Bericht über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden

Vorgelegt mit der Stellungnahme zum 16. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten – Drucks. 12/1742 – gemäß § 30 Abs. 2 Satz 2 des Hessischen Datenschutzgesetzes vom 11. November 1986

Eingegangen am 27. September 1988 · Ausgegeben am 14. Oktober 1988

Herstellung: Johannes Weisbecker, 6000 Frankfurt am Main · Auslieferung: Kanzlei des Hessischen Landtags · Postf. 3240 · 6200 Wiesbaden 1

12/3069

Inhaltsverzeichnis

1.
Anlaß des Berichts:

Das am 1. Januar 1987 in Kraft getretene neue Hessische Datenschutzgesetz verpflichtet die Landesregierung nach § 30 Abs. 2 Satz 2, zusammen mit ihrer Stellungnahme zum Tätigkeitsbericht des Datenschutzbeauftragten einen Bericht über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörden vorzulegen. In Hessen obliegt diese Aufsicht den Regierungspräsidien in Darmstadt, Gießen und Kassel. Der weitaus überwiegende Teil des Berichts betrifft den Regierungsbezirk Darmstadt mit seinen wirtschaftlichen Ballungsräumen. Dort ist eine technische Prüfgruppe eingerichtet worden, um den Sachverstand zu bündeln, der zur Kontrolle der sich rasch entwickelnden Datenverarbeitungstechnik erforderlich ist. Diese Prüfgruppe wird auch im Auftrag der beiden anderen Aufsichtsbehörden tätig.

Der Bericht über die Tätigkeit der Aufsichtsbehörden bietet Gelegenheit, die Vielfalt und Vielschichtigkeit der datenschutzrechtlichen Probleme in der Privatwirtschaft darzulegen. Dazu sind anschauliche Fälle aus allen Bereichen ausgewählt worden, in denen die Schwerpunkte der Aufsichtstätigkeit lagen. Da es sich um den ersten Bericht dieser Art in Hessen handelt, sind auch Fälle aus der Zeit vor dem Berichtsjahr einbezogen worden, soweit die Problematik nach wie vor besteht.

2.
Befugnisse der Aufsichtsbehörden

Für die Verarbeitung personenbezogener Daten durch private Stellen gilt das Bundesdatenschutzgesetz (BDSG). Anders als das Hessische Datenschutzgesetz, das auch für Akten und jede Art der Datenverarbeitung gilt, findet das BDSG nur Anwendung, wenn die Daten in einer Datei gespeichert sind und eine Speicherung, Veränderung, Übermittlung oder Löschung gegeben ist.

Die Zulässigkeit der Aufsichtstätigkeit hängt vom Zweck der Datenverarbeitung ab. Soweit Unternehmen personenbezogene Daten als Hilfsmittel für die Erfüllung ihrer eigenen Geschäftszwecke oder Ziele verarbeiten, darf die Aufsichtsbehörde nach § 30 Abs. 1 BDSG nur tätig werden, wenn ein Betroffener begründet darlegt, daß er bei der Verarbeitung seiner Daten in seinen Rechten verletzt worden ist. Von Amts wegen darf die Aufsichtsbehörde nach § 40 BDSG nur bei Unternehmen tätig werden, die Daten für fremde Zwecke verarbeiten. Dazu gehören Auskunfteien, Detekteien, Adreßverlage, Service-Rechenzentren oder Markt- und Meinungsforschungsinstitute.

Wenn die Aufsichtsbehörde einen Verstoß gegen Datenschutzvorschriften feststellt, kann sie zwar eine Beanstandung aussprechen, hat aber keinerlei Anordnungsbefugnisse. Es bleibt ihr nur die Möglichkeit, das Unternehmen in oft langwierigen Verhandlungen von der Richtigkeit ihrer Auffassung zu überzeugen. Diese Überzeugungsarbeit wird erleichtert, wenn die Aufsichtsbehörden aller Bundesländer übereinstimmende Meinungen vertreten. Um dies zu bewirken, arbeiten die obersten Aufsichtsbehörden – in der Regel sind dies die Innenministerien – seit Inkrafttreten des BDSG sehr eng zusammen. Dadurch konnte eine möglichst einheitliche Auslegung und Anwendung der zahlreichen unbestimmten Rechtsbegriffe des BDSG erreicht werden. Soweit Unternehmen bundesweit vertreten oder in einem Verband zusammengeschlossen sind, versuchen die obersten Aufsichtsbehörden auf dieser Ebene bundesweit gemeinsame Antworten auf die datenschutzrechtlichen Fragen zu finden. Wenn dies nicht gelingt, bleiben die Probleme meistens ungelöst. Eine Klärung durch die Rechtsprechung findet weitgehend nicht statt, da gegen die Entscheidungen der Aufsichtsbehörden wegen der fehlenden Durchsetzungsmöglichkeiten nicht geklagt wird.

3.
Bearbeitung von Beschwerden gegen datenverarbeitende Stellen des 3. Abschnitts des BDSG und Beratung

3.1
Bearbeitung von Beschwerden

Gegen datenverarbeitende Stellen des 3. Abschnitts gingen im Berichtsjahr 94 Beschwerden ein, die zu einer Überprüfung gemäß§ 30 BDSG führten.

Dabei sind die Fälle, bei denen sich mehrere Personen bezüglich eines Sachverhaltes beschwert haben, nur einfach gezählt worden. Darunter sind in einem Fall 14 und in einem weiteren Fall 49 Beschwerden eingegangen. Von den Beschwerden betrafen

Handel (Versand-, Einzelhandel)	34
Kreditkartenunternehmen	11
Kreditinstitute	12
Versicherungen	9
übrige	28
	94

In 12 Fällen war die Beschwerde begründet. Einige Fälle werden unter 7. geschildert.

Bei der Überprüfung von Beschwerden ist die Ermittlung des Sachverhaltes in vielen Fällen sehr arbeitsintensiv. In der Regel wenden sich die Aufsichtsbehörden zunächst schriftlich an die datenverarbeitenden Stellen, gegen die Beschwerde geführt wird. Nach § 30 BDSG haben sie weitgehende Befugnisse zur Aufklärung des Sachverhalts; entsprechend sind die Datenverarbeiter zur Auskunft verpflichtet. Diese zeigen jedoch nicht immer das erforderliche Maß an Zusammenarbeit. Häufig werden Auskünfte erst nach mehrfacher Aufforderung erteilt. So mußten bereits Ordnungswidrigkeitenverfahren wegen nicht rechtzeitiger Auskunftserteilung (§ 42 Abs. 1 Nr. 5 BDSG) eingeleitet werden.

Einige besonders krasse Fälle mangelnder Kooperationsbereitschaft werden unter 7.3 geschildert.

Alle Beteiligten erhalten nach Abschluß der Überprüfung eine schriftliche Stellungnahme mit einer rechtlichen Würdigung des festgestellten Sachverhalts. Bei Beanstandungen, die Verfahrensänderungen bei den datenverarbeitenden Stellen erfordern, wird den Beschwerdeführern auch mitgeteilt, inwieweit entsprechende Bemühungen der Aufsichtsbehörde erfolgreich waren.

Wenn sich datenverarbeitende Stellen weigern, Konsequenzen aus der Beanstandung zu ziehen, muß die Aufsichtsbehörde den Beschwerdeführern mitteilen, daß das BDSG keine Befugnis zur zwangsweisen Durchsetzung erforderlicher Änderungen gibt. Dies stößt häufig auf großes Unverständnis.

Außerdem haben die Aufsichtsbehörden schriftliche sowie zahlreiche mündliche und telefonische Anfragen erledigt, die zum Teil sofort, zum Teil erst nach weiterer Klärung der Sach- und Rechtslage beantwortet werden konnten.

3.2
Anlaßaufsicht

Die in diesem Bereich bestehende Anlaßaufsicht führte in der Vergangenheit dazu, daß die Aufsichtsbehörden in mehreren Fällen bei offensichtlichen Verstößen gegen Datenschutzvorschriften, die ihnen meist durch Presseberichte bekanntgeworden waren, entweder nicht eingreifen durften, weil keine Beschwerde eines Betroffenen vorlag, oder erst nach einiger Zeit tätig werden konnten, nachdem zwischenzeitlich eine Beschwerde eingegangen war.

Einige dieser Vorfälle betrafen mangelnde Sicherungsmaßnahmen bei der Beseitigung nicht mehr benötigter Datenträger mit personenbezogenen Daten. Ursache dafür waren Unachtsamkeit und grobe Nachlässigkeit beim Transport und der Vernichtung. So wurden z. B. Datenträger wie EDV-Ausdrucke, eingelöste Schecks, Bankbelege usw. in offenen Containern transportiert und vom Wind auf die Straße geweht oder Container mit zur Verbrennung bestimmten Bankbelegen einfach auf einer allgemein zugänglichen Hausmülldeponie abgeladen, weil die Müllverbrennungsanlage gerade repariert wurde.

Solche Vorfälle sind den Aufsichtsbehörden durch die Presse oder durch aufmerksame Passanten zur Kenntnis gelangt. Da keine Beschwerde eines Betroffenen vorlag, konnten sie jedoch nicht überprüft werden.

3.3
Beratung

Ein wesentlicher Teil der von den Aufsichtsbehörden geleisteten Arbeit war der Beratung der betrieblichen Beauftragten für den Datenschutz und der datenverarbeitenden Stellen gewidmet. Insoweit erfüllen sie den gesetzlichen Beratungsauftrag des § 30 Abs. 1 Satz 2 BDSG.

In der Vergangenheit haben außerdem mehrfach Betriebsräte um Beratung gebeten. In allen Fällen stand in den betreffenden Unternehmen der Abschluß von Betriebsvereinbarungen über die Verarbeitung von Personaldaten an.

Die Tatsache, daß die Datenschutzaufsichtsbehörde – insbesondere wegen eventueller Datensicherungsprobleme sowie Zugriffs- und Auswertungsmöglichkeiten – von Betriebsräten um Rat gefragt wurde, ist in mehrfacher Hinsicht bemerkenswert.

Sie zeigt zunächst, daß bei vielen Betriebsräten selbst nicht der erforderliche technische Sachverstand vorhanden ist, um die zugrundeliegenden technischen Sachverhalte und die vorgesehenen Regelungen durchschauen und beurteilen zu können. Bei dem Versuch, sich sachkundig zu machen, war die Einschaltung der Aufsichtsbehörde häufig das letzte Mittel, weil man sich mit den von der Unternehmensleitung gegebenen Informationen nicht zufrieden gab, keine aussagekräftigen Erläuterungen erhielt oder weil man sich auf Aussagen des betrieblichen Beauftragten für den Datenschutz nicht verlassen mochte, da er als der Geschäftsleitung nahestehend eingeschätzt wurde.

4.
Bearbeitung von Beschwerden gegen datenverarbeitende Stellen des 4. Abschnitts des BDSG und Beratung

Gegen nicht-öffentliche Stellen, die geschäftsmäßige Datenverarbeitung für fremde Zwecke betreiben (§§ 31 ff BDSG) sind im Berichtsjahr 43 Beschwerden eingegangen, die zu einer Überprüfung führten.

Davon betrafen

Kreditinformationsdienste (= Wirtschaftsauskunfteien und Schufa)	26
Adreßhandel	9
EDV-Serviceunternehmen	5
Markt- und Meinungsforschungsinstitute	2
übrige	1

In 16 Fällen waren die Beschwerden begründet. Davon 13 gegen Kreditinformationsdienste und 3 gegen Adreßhändler. Einige Fälle werden unter 7. geschildert.

Von diesen Beschwerden abgesehen, sind auch in diesem Bereich zahlreiche schriftliche sowie mündliche und telefonische Anfragen bearbeitet worden.

5.
Regelprüfungen von datenverarbeitenden Stellen des 4. Abschnitts des BDSG

5.1
Register

Die Stellen, die Daten für fremde Zwecke verarbeiten und damit dem 4. Abschnitt des BDSG unterliegen, haben nach § 39 BDSG der Aufsichtsbehörde die Aufnahme ihrer Tätigkeit anzumelden und dabei folgende Angaben zu machen:

1. Name oder Firma der Stelle,
2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzlich oder verfassungsmäßig berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
3. Anschrift,
4. Geschäftszwecke oder Ziele der Stelle und der Datenverarbeitung,

5. Art der eingesetzten automatisierten Datenverarbeitungsanlagen,
6. Name des Beauftragten für den Datenschutz,
7. Art der von ihr oder in ihrem Auftrag gespeicherten personenbezogenen Daten,
8. bei regelmäßiger Übermittlung personenbezogener Daten Empfänger und Art der übermittelten Daten.

Das Register, das von jedem eingesehen werden kann, soll sowohl der Information des Betroffenen dienen als auch der Aufsichtsbehörde die für ihre Tätigkeit erforderlichen Einsichten verschaffen.

Während die Betroffenen von der Einsicht nur in seltenen Fällen Gebrauch machen, hat sich das Register zu einem wichtigen Hilfsmittel für die Aufsichtsbehörden entwickelt. Die darin enthaltenen Angaben ermöglichen es, für die Regelprüfungen Schwerpunkte zu setzen und dementsprechend planmäßig vorzugehen.

Bisher sind zum Register der Aufsichtsbehörden folgende Stellen gemeldet:

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

Kreditinformationsdienste (= Wirtschaftsauskunftsdateien und Schufa)	34
Brancheninformationsdienste	1
Datenbanken	8
Adreßhändler, -Verleger, -Makler, -Verwalter	24
Gesamt	67

2. Stellen, die geschäftsmäßig personenbezogene Daten zum Zweck der Anonymisierung speichern und sie in dieser Form übermitteln (§ 31 Abs. 1 Nr. 2 BDSG)

Markt- und Meinungsforscher	21

3. Stellen, die geschäftsmäßig personenbezogene Daten im Auftrag als Dienstleistungsunternehmen verarbeiten (§ 31 Abs. 1 Nr. 3 BDSG)

Service-Rechenzentren allgemein	106
Banken-Rechenzentren	102
Konzern-DV	43
Sonstige Datenverarbeiter	55
Datenerfasser	56
Mikroverfilmer	9
Entsorgungsbetriebe (Datenträgervernichtung)	22
Gesamt	403
Gemeldete Unternehmen insgesamt	491

5.2
Prüfungsübersicht

Bisher wurden insgesamt 149 datenverarbeitende Stellen des 4. Abschnitts des BDSG überprüft.

Davon entfielen 54 Prüfungen auf das Berichtsjahr 1987.

Die bisher durchgeführten 149 Prüfungen (davon 7 Wiederholungsprüfungen) betrafen:

1.	Service Rechenzentren (davon 5 im Bank- und 11 im Konzernbereich)	72
2.	Datenerfasser	22
3.	Mikroverfilmer	4
4.	Datenträgervernichter	7

5.	Kreditinformationsdienste	23
6.	Brancheninformationsdienste	1
7.	Datenbanken	5
8.	Adreßhändler/Makler etc.	5
9.	Markt- und Meinungsforscher	10

Die Prüfungen brachten folgendes Ergebnis:

–	Beanstandungen	60	(darunter alle Wiederholungsprüfungen)
–	Empfehlungen	47	
–	ohne wesentliche Beanstandungen	40	
–	Prüfungsabbruch	2	

Erläuternd ist zunächst festzustellen, daß § 40 BDSG den Aufsichtsbehörden nicht die Aufgabe eines „Datenschutz-TÜV" zuweist, der etwa die DV-Konfiguration des jeweiligen Anwenders unter Datenschutz- und Datensicherungsaspekten umfassend prüft und freigibt. Die Regelprüfungen können – zumindest bei der ersten Prüfung – nur Stichproben sein, bei denen sich die Aufsichtsbehörde zunächst darauf beschränkt, festzustellen, ob funktionsfähige betriebseigene Kontrollen vorhanden sind, die den Datenschutzvorschriften entsprechen.

Die Prüfungstermine werden in der Regel 4 bis 6 Wochen vorher mit dem Unternehmen telefonisch abgestimmt und von der Aufsichtsbehörde schriftlich bestätigt. Mit der Terminbestätigung wird das Unternehmen aufgefordert, über die Registermeldung nach § 39 BDSG hinaus zur Prüfungsvorbereitung weitere schriftliche Informationen zu übersenden, damit die Prüfungshandlung selbst – auch im Interesse des Unternehmens – so kurz und effektiv wie möglich abgewickelt werden kann. Gleichzeitig wird das Unternehmen darauf hingewiesen, daß die Anwesenheit des betrieblichen Beauftragten für den Datenschutz während der Überprüfung erforderlich ist, der Geschäftsführer für ein Gespräch am Anfang der Prüfung zur Verfügung stehen soll und Mitarbeiter aus dem Organisationsbereich, der Anwendungs- und der Systemprogrammierung zeitweise für Auskünfte über Arbeitsabläufe und Sicherungsmaßnahmen benötigt werden. Zum Abbruch der Prüfung kam es bisher in zwei Fällen, weil in einem Fall weder der Geschäftsführer und der für die EDV Verantwortliche noch ein verantwortlicher Vertreter anwesend waren und im zweiten Fall keine prüffähigen schriftlichen Unterlagen vorlagen.

Nach Beendigung der Prüfung, die in der Regel 1 bis 2 Tage dauert, teilt die Aufsichtsbehörde dem Unternehmen in einem Abschlußgespräch ein vorläufiges Ergebnis oder, falls dies wegen schwieriger Abwägungen zu diesem Zeitpunkt noch nicht möglich ist, zumindest ihre ersten Eindrücke mit. Die endgültige Bewertung erhält das Unternehmen später in einem schriftlichen Prüfbericht.

Förmliche Beanstandungen erfolgen bei wesentlichen Verstößen gegen die Datenschutzvorschriften, während die Aufsichtsbehörde in Bagatellfällen den datenverarbeitenden Stellen lediglich mündliche Hinweise gibt, ohne daß dies schon zu einer schriftlichen Beanstandung führt. Wenn sie zum Beispiel feststellt, daß ein Unternehmen eine nach § 39 BDSG erforderliche Änderungsmeldung nicht abgegeben hat, leitet sie nicht in jedem Fall ein Bußgeldverfahren nach § 42 Abs. 1 Nr. 4 BDSG ein, sondern beläßt es zunächst bei einem Hinweis auf die Meldepflicht. Beanstandungen bedeuten grundsätzlich, daß Verfahrensänderungen bei der Datenverarbeitung zwingend erforderlich sind. Wird dagegen nur eine Empfehlung ausgesprochen, dann ist die Befolgung der damit verbundenen Hinweise zur Verfahrensverbesserung nicht zwingend geboten.

Folgende wesentliche Mängel wurden am häufigsten festgestellt (Reihenfolge nach Häufigkeit):

- Keine bzw. unvollständige Programm- und Verfahrensdokumentation
- Keine Fortschreibung dieser Dokumentation
- Fehlende bzw. mangelhafte Protokollierung der Verarbeitung
- Keine bzw. unzureichende Kontrolle vorhandener Protokolle

- Nichtbeachtung des Vier-Augen-Prinzips bei den einzelnen Verarbeitungsschritten
- Fehlende Eingabekontrolle
- Unzureichende Raumsicherung
- Keine geordnete Datenträgerverwaltung
- Kein Passwort bzw. ein Passwort für alle Mitarbeiter
- Fehlende bzw. unzureichende Dateiübersichten
- Keine Ergebniskontrolle vor dem Versand von Auswertungen
- Fehlende schriftliche Weisungen der Auftraggeber

Außerdem mußte beanstandet werden:

- Unvollständige Meldungen nach § 39 zum Register
- Verspätete Registermeldungen
- Nichtbestellung eines betrieblichen Beauftragten für den Datenschutz.

Weitere Erläuterungen folgen unter 8.

Da das BDSG keine Eingriffsbefugnisse gibt, können die Aufsichtsbehörden im Beanstandungsfall die erforderlichen Änderungen nicht mit Zwangsmitteln durchsetzen. Bei dem größten Teil der nach § 40 geprüften Unternehmen waren Zwangsmittel auch nicht erforderlich. Einige dieser Stellen, vor allem Kreditinformationsdienste, aber auch Service-Rechenzentren haben sich jedoch entweder geweigert oder waren erst aufgrund nachdrücklicher und manchmal sehr zeitaufwendiger Bemühungen bereit, die erforderlichen Änderungen z. B. bei Verfahrensabläufen durchzuführen.

6.
Problematik des auf Dateien beschränkten Anwendungsbereichs des BDSG

Der Anwendungsbereich des BDSG ist auf solche personenbezogenen Daten beschränkt, die in Dateien verarbeitet oder aus Dateien übermittelt werden. Nach der Legaldefinition des § 2 Abs. 3 Nr. 3 BDSG erfüllen Akten und Aktensammlungen nicht den Dateibegriff, es sei denn, daß sie durch automatisierte Verfahren umgeordnet und ausgewertet werden können.

Dies führt in der Praxis immer wieder zu Abgrenzungsproblemen, die insbesondere den betroffenen Bürgern selbst kaum verständlich gemacht werden können.

Das Persönlichkeitsrecht eines Betroffenen kann auch dann verletzt sein, wenn private Stellen seine Daten außerhalb von Dateien, z. B. in Akten oder Listen verarbeiten.

Dies soll an einigen Beispielen deutlich gemacht werden, in denen die Aufsichtsbehörde den Beschwerden der Betroffenen nicht nachgehen konnte:

Der Mitarbeiter eines genossenschaftlich organisierten Unternehmens fragte bei der Aufsichtsbehörde an, ob es datenschutzrechtlich zulässig sei, wenn die Unternehmensleitung dem Verbandsprüfer im Rahmen einer Prüfung die komplette Personalakte des Betroffenen vorlege. Mangels Zuständigkeit mußte die Beantwortung dieser Frage abgelehnt werden.

Wäre dem Prüfer dagegen ein EDV-Ausdruck der Personalstammdaten des Mitarbeiters ausgehändigt worden, wäre dieser Vorgang nach den BDSG-Vorschriften zu beurteilen gewesen. Die Personalstammdaten sind natürlich auch in der Personalakte enthalten.

Versicherungen verarbeiten die Stammdaten ihrer Versicherungsnehmer mit Hilfe der EDV, während die bei der Abwicklung eines einzelnen Versicherungsfalles zu verarbeitenden personenbezogenen Daten meist in einer Akte geführt werden.

Auch hier unterliegt die Verarbeitung der Stammdaten den Vorschriften des BDSG, die der übrigen personenbezogenen Daten, die wesentlich sensibler sind, dagegen nicht.

Eine Bankkundin wendete sich unter anderem gegen die Aufzeichnung

bestimmter personenbezogener Daten in der Zwangsversteigerungsakte ihrer Hausbank. Ein Tätigwerden der Aufsichtsbehörde war jedoch nicht möglich, weil diese Angaben allein in der Akte und nicht in einer manuellen Datei oder der EDV-Anlage der Bank gespeichert waren.

In einem anderen Fall hatte eine Firma eine Liste in der Werkshalle ausgehängt, aus der die Urlaubs- und Krankheitstage der in der Werkshalle Beschäftigten zu entnehmen waren. Eine Überprüfung des Vorgangs war nicht möglich, da Listen nicht unter den gesetzlichen Dateibegriff fallen.

Daß der Dateibegriff zu Ausgrenzungen und Ungleichbehandlungen führt, die sachlich nicht zu rechtfertigen sind, wird auch in dem später unter 7.7.5 in anderem Zusammenhang geschilderten Fall deutlich.

Dort hatte ein Heiratsvermittler Kopien von Heiratsurkunden seiner Kunden mit den personenbezogenen Daten der Eheleute sowie deren Eltern an Dritte übermittelt. Die Übermittlung der Daten der betroffenen Eheleute war nach dem BDSG zu beurteilen, da er diese Daten auch in einer Datei führte. Die Daten der betroffenen Eltern waren dagegen nicht in einer Datei gespeichert, sondern „nur" auf den Kopien der Urkunden vorhanden. Die Verletzung der Privatsphäre der Eltern war hier genauso schwerwiegend, wie der Eingriff in die Rechte der Eheleute, dennoch waren die Datenschutzvorschriften nicht anwendbar, da der Dateibegriff nicht erfüllt war.

7.
Einzelne Datenschutzprobleme

Einer der wichtigsten Problembereiche, mit denen die Aufsichtsbehörden sich immer wieder befassen müssen, ist die Verarbeitung von Kreditinformationen durch Kreditinformationsdienste und deren Vertragspartner. Mit Kreditinformationsdiensten sind hier die Wirtschaftsauskunfteien und die Schufa gemeint.

Kreditinformationsdienste sind eine wichtige Stütze des Kreditgeschäfts. Sie liefern Informationen, die die Entscheidung zur Gewährung von Krediten, seien es Barkredite, Ratenzahlungen, Warenlieferungen oder sonstige Leistungen erleichtern.

Beim Handel mit Kreditinformationen kommt es im besonderen Maße auf drei Gesichtspunkte an:

Die verarbeiteten Daten müssen vollständig, aktuell und kreditbezogen sein. Vollständig müssen die Daten sein, damit nicht durch einseitige Auswahl von Teilinformationen ein falsches Bild über den Betroffenen entsteht. Veraltete Daten lassen keine zuverlässigen Aussagen über den Betroffenen zu, da sich z. B. seine finanziellen Verhältnisse zwischenzeitlich geändert haben bzw. haben können. Informationen aus der Privatsphäre des Betroffenen, die keine zuverlässigen Aussagen über seine Kreditwürdigkeit ermöglichen, sind auch nicht kreditrelevant.

Diese Anforderungen werden aber leider nicht immer erfüllt, was die folgenden Ausführungen verdeutlichen sollen.

7.1
Wirtschaftsauskunfteien

Wirtschaftsauskunfteien sammeln Informationen über Betriebe und Privatpersonen, stellen sie zusammen und geben Auskünfte an anfragende Stellen. Die gesammelten Daten werden auch weiterhin aufbewahrt, um sie später erforderlichenfalls wieder verwenden zu können.

Eine Auskunftei wird in der Regel tätig, wenn ein Kunde bei ihr anfragt, weil er mit einem Dritten ein Geschäft abschließen will, das mit einem wirtschaftlichen Risiko verbunden ist.

Die Informationen stammen zum Teil aus allgemein zugänglichen Quellen, wie öffentlichen Registern (z. B. Handelsregister, Schuldnerverzeichnis), Presse, Adreß- und Telefonbüchern. Außerdem erhalten die Wirtschaftsauskunfteien auch von ihren Kunden, also den Empfängern der Auskünfte, weitere Daten über ihre Zahlungserfahrungen.

Sind nur wenige aussagekräftige Daten vorhanden, was bei Privatpersonen häufig vorkommt, werden möglicherweise auch Nachbarn befragt.

Keine Informationen erhalten die Auskunfteien von Behörden (Sozialämtern, Finanzämtern und anderen); ebensowenig haben sie Zugriff auf die bei der Schufa gespeicherten Daten.

Die Auskunfteien dürfen nur solchen Stellen Auskünfte geben, die gemäß § 32 Abs. 2 BDSG ein berechtigtes Interesse glaubhaft dargelegt haben. Als berechtigt anerkannt sind wirtschaftliche Interessen, also die Vermeidung geschäftlicher Risiken im weitesten Sinne, z. B. wenn Ware gegen Rechnung geliefert werden soll.

Der größte Teil des Auskunftgeschäfts betrifft Firmen und Geschäftsleute. Ein relativ kleiner Teil der Auskünfte wird über Privatpersonen erteilt.

Häufig erreichen die Aufsichtsbehörden Anfragen von Privatpersonen, die sich verärgert dagegen verwahren, daß Wirtschaftsauskunfteien Daten über sie speichern und weitergeben. Verursacht wird diese Verärgerung einerseits, weil die Betroffenen davon erfahren haben, daß in der Nachbarschaft über sie nachgefragt wurde, andererseits, weil sie grundsätzlich nicht damit einverstanden sind, daß Auskunfteien Daten über sie sammeln und verbreiten.

In solchen Fällen muß die Aufsichtsbehörde den Betroffenen verdeutlichen, daß das BDSG die Wirtschaftsauskunfteien bei der Verarbeitung personenbezogener Daten an bestimmte Regeln bindet. Wenn diese Regeln eingehalten werden, benötigen die Auskunfteien nicht die Einwilligung der Betroffenen für die Verarbeitung.

Die Betroffenen erhalten von dem Tätigwerden einer Wirtschaftsauskunftei Kenntnis durch die in § 34 Abs. 1 BDSG vorgeschriebene Benachrichtigung. Danach sind die speichernden Stellen verpflichtet, den Betroffenen über die Speicherung seiner personenbezogenen Daten dann zu benachrichtigen, wenn diese Daten erstmals übermittelt werden. Mit der Benachrichtigung wird lediglich darauf hingewiesen, daß personenbezogene Daten des Betroffenen verarbeitet werden. Dieser kann dann von seinem Auskunftsrecht (§ 34 Abs. 2) Gebrauch machen und die einzelnen über ihn gespeicherten Daten erfragen.

Die Wahrnehmung des Auskunftsrechts führt bei vielen Betroffenen zu Verärgerung, wenn sie erfahren, daß sie grundsätzlich für diese Auskunft ein Entgelt zu zahlen haben. Es darf gemäß § 34 Abs. 3 nicht über die durch die Auskunftserteilung entstandenen direkt zurechenbaren Kosten hinausgehen. Der Ärger richtet sich vor allem dagegen, daß Auskunfteien und die Schufa ein Entgelt verlangen dürfen, obwohl man die Datenspeicherung bei diesen Stellen nicht „veranlaßt" habe und auch nicht wolle und es sich schließlich ja um die „eigenen Daten" handele. Über die Einschaltung einer Wirtschaftsauskunftei sei man auch nicht informiert worden.

Mittlerweile verzichten zwar einige Auskunfteien auf ein Entgelt, wenn ein Betroffener gemäß § 34 Abs. 2 BDSG Auskunft über die zu seiner Person gespeicherten Daten verlangt, die Schufa nimmt jedoch weiterhin ein Entgelt (10,– DM für eine schriftliche, 8,– DM für eine mündliche Auskunft).

7.1.1
Recherchemethoden

Ein Teil der gegen Wirtschaftsauskunfteien vorgebrachten Beschwerden richtet sich gegen deren Recherchemethoden, genauer gesagt die Befragung von Nachbarn oder gar des Arbeitgebers.

Dies soll folgender Fall deutlich machen:

Die Beschwerdeführerin wollte mit einer Krankenversicherungsgesellschaft einen Vertrag abschließen. Die von ihr zu zahlende Versicherungsprämie sollte monatlich DM 39,50 betragen. Die von der Versicherung zur Bonitätsprüfung eingeschaltete Auskunftei befragte zwei Nachbarn und den Arbeitgeber der Betroffenen.

Derartige Befragungen greifen tief in die geschützte Privatsphäre eines Betroffenen ein, so daß sie nur in eng begrenzten Ausnahmefällen erlaubt sein dürfen. Zwar ist die Datenerhebung im Gesetz nicht ausdrücklich geregelt, ihre näheren Umstände können jedoch Auswirkungen für die Prüfung haben, ob die darauf folgende Speicherung der Daten zulässig ist.

Die Wirtschaftsauskunfteien haben sich nach Verhandlungen mit den obersten Länderaufsichtsbehörden für den Datenschutz bereit erklärt, Nachbarschaftsbefragungen zu reduzieren. Bei Bagatellfällen – soweit diese als solche erkennbar sind – soll auf Nachbarschaftsbefragungen verzichtet werden.

Die Überprüfung ergab, daß die Auskunftei im Beispielsfall, nicht nur gegen diese Vereinbarung verstoßen, sondern auch übersehen hat, daß die Versicherung bei Nichtzahlung der Prämie zur Kündigung des Versicherungsvertrages berechtigt gewesen wäre und ein Risiko somit für sie nicht vorlag.

Auch in diesem Fall konnte die Aufsichtsbehörde nur die Unzulässigkeit der Datenverarbeitung (Speicherung und Übermittlung der Daten der Betroffenen) feststellen und die Auskunftei zur Löschung der durch Nachbar- und Arbeitgeberbefragung erlangten Daten auffordern. Dieser Aufforderung ist sie nicht nachgekommen.

7.1.2
Unzureichende und vorgetäuschte Darlegung des berechtigten Interesses

Die Auskunfteien dürfen ihren Kunden gemäß § 32 Abs. 2 BDSG nur Auskünfte geben, wenn diese ein berechtigtes Interesse glaubhaft dargelegt haben. Die Gründe für die Darlegung des berechtigten Interesses sind aufzuzeichnen. Im Rahmen der regelmäßigen Prüfungen gemäß § 40 BDSG werden auch diese Aufzeichnungen von den Aufsichtsbehörden kontrolliert.

Im Massengeschäft der Wirtschaftsauskunfteien wird für die Darlegung des berechtigten Interesses keine individuelle Begründung gegeben. Der Datenempfänger (Kunde der Auskunftei) gibt lediglich einen Anfragegrund an, indem er einen von mehreren auf einem Formblatt vorgegebenen Gründen ankreuzt. Die entsprechenden Tatsachen, die zu der Anfrage geführt haben, können vorliegen oder auch nicht. Sie zu behaupten, bedeutet jedoch noch nicht, sie im Sinne des Gesetzes auch glaubhaft darzulegen.

Als Beispiel sollen mehrere Fälle dienen, in denen der Auskunftei durch den Kunden ein angebliches berechtigtes Interesse genannt wurde:

7.1.2.1
Bürgermeisterwahl

Bei einer Auskunftei wurde von einer Firma Auskunft über einen Wahlkandidaten eingeholt, wobei als Anfragegrund angegeben wurde:

Geschäftsanbahnung. Es bestanden jedoch keinerlei Beziehungen zwischen der Firma und dem Betroffenen.

7.1.2.2
Mißbräuchliche Nutzung der Informationsmöglichkeiten einer Bank durch einen ihrer Mitarbeiter

Ein Bankangestellter ließ durch die zentrale Auskunftsabteilung der Bank bei einer Wirtschaftsauskunftei für private Zwecke – im Zusammenhang mit Unterhaltsstreitigkeiten – eine Auskunft einholen. Diese mißbräuchliche Nutzung der Informationsmöglichkeiten der Bank hätte möglicherweise vermieden werden können, wenn die Anfrageberechtigung des betreffenden Angestellten bankintern genauer geprüft worden wäre.

7.1.2.3
Weinlieferung

Ein Kunde bestellte bei einem Weinhändler Wein. Der Händler sollte selbst anliefern. Zahlung bei Lieferung war vereinbart. Der Händler holte Auskunft bei einer Wirtschaftsauskunftei ein. Seine Berechtigung zur Auskunft begründete er nachträglich mit seinem Anfahrtrisiko sowie einer möglichen Bezahlung des Weins per Scheck.

Nach Feststellung der Aufsichtsbehörde lag ein nach § 32 Abs. 2 BDSG berechtigtes Interesse nicht vor, weil nicht jedes – und in diesem Fall geringes – wirtschaftliches Risiko zur Auskunfteinholung berechtigt.

In diesen Fällen konnte die Auskunftei nicht erkennen, daß kein berechtigtes Interesse für eine Auskunft vorlag, weil als Anfragegrund jeweils pauschal „Geschäftsanbahnung" angegeben worden war.

7.1.2.4
Ungenaue Bezeichnung des Anfragegrundes

Das folgende Beispiel verdeutlicht, daß auch bei Unklarheiten oder Zweifeln hinsichtlich des behaupteten berechtigten Interesses die gewünschte Auskunft ohne weitere Rückfragen erteilt wird:

Ein Anwaltsbüro holte über den Betroffenen bei einer Wirtschaftsauskunftei eine Auskunft ein. Als Anfragegrund war angegeben: „Rechtl. Angelegenheit". Die Auskunft wurde ohne weitere Rückfrage erteilt, obwohl hier ein anerkennenswertes berechtigtes Interesse noch nicht einmal im Ansatz glaubhaft dargelegt war, denn mit dieser „rechtl. Angelegenheit" mußte nicht notwendigerweise ein wirtschaftliches Risiko verbunden sein. Nur letzteres berechtigt aber zu einer Anfrage bei einer Wirtschaftsauskunftei.

7.1.2.5
Zahlung mit Scheck

Ein Versandhaus holte bei einer Wirtschaftsauskunftei eine Auskunft über einen Besteller ein. Dabei gab dieses Versandhaus eine Bonitätsprüfung als berechtigtes Interesse an. Durch verschiedene Recherchen konnte jedoch ermittelt werden, daß bei dem Versandhandel weder eine Bonitätsprüfung noch ein anderes berechtigtes Interesse vorlag. Der Betroffene hatte bei dem anfragenden Versandhaus Waren im Wert von ca. 1500,– DM bestellt und dem Bestellschreiben einen Scheck in entsprechender Höhe beigefügt. 6 Tage nach der Bestellung wurde der Scheck eingelöst und nach weiteren 4 Tagen wurde das Konto des Betroffenen belastet.

Trotzdem holte das Versandhaus 12 Tage nach der Bestellung für diese und evtl. folgende Aufträge eine Auskunft über die wirtschaftliche Lage des Betroffenen ein. Der vorgetragene Einwand, ein berechtigtes Interesse habe vorgelegen, da die Deckung des Schecks nicht feststand, konnte nicht überzeugen.

Zwar ist die Hereingabe eines Schecks noch nicht die Erfüllung der Kaufpreisforderung. Doch bot der Scheck eine ausreichende Sicherheit, indem noch vor der Lieferung seine Einlösung versucht werden konnte. Erst im Falle der Nichteinlösung wäre ein berechtigtes Interesse an einer Wirtschaftsauskunft anzuerkennen gewesen. Zudem ist aufgrund des ermittelten Sachverhaltes anzunehmen, daß das Versandhaus im Zeitpunkt der Anfrage Kenntnis von der Deckung des Schecks hatte bzw. Kenntnis haben konnte.

Auch konnte für mögliche zukünftige Aufträge kein berechtigtes Interesse an einer Auskunft über die wirtschaftliche Lage des Betroffenen anerkannt werden, da keine Anhaltspunkte für eine weitere Bestellung des Betroffenen vorlagen. Eine Anfrage ohne konkreten Grund ist aber unzulässig.

7.1.2.6
Zusammenfassung

Diese Erfahrungen zeigen: Jeder Vertragspartner einer Wirtschaftsauskunftei kann unter Vortäuschung eines berechtigten Interesses Auskünfte erhalten, ohne ein großes Entdeckungsrisiko einzugehen.

Die obersten Länderaufsichtsbehörden für den Datenschutz haben in Verhandlungen mit den Wirtschaftsauskunfteien durchgesetzt, daß wenigstens nachträglich stichprobenartige Kontrollen durchgeführt werden, d. h., bei einem Promille der erteilten Auskünfte wird das angegebene berechtigte Interesse nachträglich überprüft.

Bei den regelmäßigen Überprüfungen der Kreditinformationsdienste wird auch geprüft, ob und wie sorgfältig diese Stichprobenkontrollen von den Kreditinformationsdiensten durchgeführt werden. An der erforderlichen Sorgfalt läßt der folgende Fall zweifeln, der bei der Prüfung einer Wirtschaftsauskunftei im Berichtsjahr festgestellt wurde:

Der Kunde dieser Auskunftei, der Einfamilienhäuser errichtet und verkauft, fragte über den Betroffenen an; genannter Anfragegrund: Kreditentscheidung. Nachdem eine Auskunft erteilt war, führte die Auskunftei selbst in diesen Fall eine Stichprobe durch und fragte einige Zeit später nochmals nach den – genaueren – Gründen für die Anfrage. Als Antwort erhielt sie die Mitteilung, bei dem Betroffenen habe es sich um einen „Bewerber für eine Verkäufertätigkeit" gehandelt. Die Auskunftei nahm dies zur Kenntnis, ohne aus den unterschiedlichen Begründungen Konsequenzen zu ziehen und ihren Kunden zu korrekten Angaben anzuhalten. Außerdem ist es zweifelhaft, ob die Einstellung eines Immobilienverkäufers ein wirtschaftliches Risiko darstellt, das zur Einschaltung einer Wirtschaftsauskunftei berechtigt.

Mittlerweile haben zwei große Wirtschaftsauskunfteien ihr Angebot erweitert und bieten ihren Kunden die Möglichkeit, on-line direkt auf die bei der Auskunftei gespeicherten personenbezogenen Daten zuzugreifen. Auch hier wird nur noch die Plausibilität des Anfragegrundes geprüft. Allerdings mit dem Nachteil, daß diese Prüfung maschinengestützt erfolgt und nicht mehr durch Mitarbeiter der Auskunftei. Von einer glaubhaften Darlegung der Gründe für ein im Sinne des § 32 Abs. 2 BDSG berechtigtes Interesse der anfragenden Stelle kann hier keine Rede sein.

7.2
SCHUFA

Die Schutzgemeinschaft für allgemeine Kreditsicherung, besser bekannt unter der Kurzbezeichnung SCHUFA, ist eine Gemeinschaftseinrichtung der kreditgebenden Wirtschaft. Es gibt in der Bundesrepublik insgesamt 13 regionale, rechtlich und wirtschaftlich selbständige Schufa-Gesellschaften in der Rechtsform der GmbH, die der Bundes-Schufa, Vereinigung der deutschen Schutzgemeinschaften für allgemeine Kreditsicherung e. V., angehören. Gesellschafter der regionalen SCHUFA-Gesellschaften sind Sparkassen, Banken, Volksbanken, Raiffeisenbanken, Teilzahlungsbanken sowie Einzel- und Versandhandelsunternehmen.

7.2.1
Aufgabe der SCHUFA

Aufgabe der SCHUFA ist es, ihren Vertragspartnern Informationen zu geben, um sie vor Verlust im Konsumentenkreditgeschäft zu schützen und ihnen damit gleichzeitig die Möglichkeit zu eröffnen, die Kreditnehmer durch Beratung vor einer übermäßigen Verschuldung zu bewahren. Zu diesem Zweck übermitteln zum Beispiel Kreditinstitute der SCHUFA bestimmte Daten aus der Geschäftsverbindung mit ihren Privatkunden. Die SCHUFA speichert diese Daten, um daraus ihren Vertragspartnern Informationen zur Beurteilung der Kreditwürdigkeit von Kunden geben zu können.

Vertragspartner der SCHUFA können Kreditinstitute, Leasinggesellschaften, Einzelhandelsunternehmen einschließlich des Versandhandels, Kreditkartengesellschaften und sonstige Unternehmen sein, die gewerbsmäßig Geld oder Warenkredite an Konsumenten geben. Konsumenten in diesem Sinne sind natürliche Personen, die Kredite für private, nicht aber für berufliche oder gewerbliche Zwecke aufnehmen. Warenkredite sind auch Lieferungen gegen Rechnung oder unter Einräumung von Zahlungszielen.

7.2.2
SCHUFA-Verfahren

Die SCHUFA arbeitet nach dem Prinzip der Gegenseitigkeit. Danach kann nur selbst Auskunft von der Schufa erhalten, wer der Schufa auch Informationen gibt. Die Auskünfte, die ein Vertragspartner erhält, beruhen auf den Informationen, die andere Vertragspartner zuvor der SCHUFA gegeben haben oder die diese aus öffentlichen Verzeichnissen (z. B. Schuldnerverzeichnis) entnommen hat. Die Vertragspartner erhalten nur dann Daten von der SCHUFA, wenn sie ein berechtigtes Interesse an der Datenübermittlung glaubhaft darlegen. Ein Vertragspartner der SCHUFA darf daher nur über Personen eine Auskunft einholen, die einen Geld- oder Warenkredit aufnehmen oder eine Bürgschaftsverpflichtung eingehen wollen. Kreditinstitute dürfen außerdem vor der Eröffnung eines Giro-

kontos eine SCHUFA-Auskunft einholen, weil den Kunden allgemein nach relativ kurzer Zeit ein Dispositionskredit und die Teilnahme am Eurocheque-Verfahren angeboten wird. Anfragen zu anderen Zwecken, zum Beispiel Personalanfragen, sind unzulässig und führen in letzter Konsequenz zum Ausschluß des Vertragspartners aus der SCHUFA.

Neben den Auskünften aufgrund von Anfragen erhalten Vertragspartner, wenn das berechtigte Interesse fortbesteht (beispielsweise bei einem noch bestehenden Kredit), von der SCHUFA auch nachträglich bekanntgewordene Informationen, die die ursprüngliche Auskunft ergänzen (Nachmeldungen). Der Vertragspartner wird zum Beispiel informiert, wenn sich Unregelmäßigkeiten bei der Abwicklung eines Kredits ergeben, den der Kunde bei einem anderen Vertragspartner der SCHUFA aufgenommen hat.

Der Informationsbedarf der einzelnen Gruppen von Vertragspartnern der SCHUFA ist nicht einheitlich. Deshalb haben sie auch verschiedene SCHUFA-Anschlußverträge mit unterschiedlichen Informationsrechten und Meldepflichten.

7.2.3
Schufa-Klausel

Mit Wirkung vom 1. Juli 1986 ist das Schufa-Verfahren verbessert und insbesondere die Schufa-Klausel neu gefaßt worden. Ausgelöst wurde diese Neufassung durch ein Urteil des Bundesgerichtshofs vom 19. September 1985 (BGHZE 95, 362), in dem der BGH festgestellt hatte, daß die bis dahin geltende Schufa-Klausel gegen § 9 AGB-Gesetz verstieß. Damit bestätigte der BGH die schon früher geäußerten Bedenken der Datenschutzaufsichtsbehörden.

Durch diese Veränderungen ist das Schufa-Verfahren in einigen Bereichen verbessert worden. Für den Betroffenen ist es transparenter geworden, da ihm die neuen Klauseln, mit denen er einwilligt, daß die Schufa über ihn Daten speichern und verbreiten darf, bessere Informationen über den wesentlichen Umfang der beabsichtigten Verarbeitung geben. Außerdem erhält er auf Wunsch von seinem Kreditinstitut eine ausführliche schriftliche Verfahrensbeschreibung. Der Kreis der Schufa-Vertragspartner wurde reduziert. Die für eine Schufa-Auskunft erforderlichen Kriterien wurden teils eingeschränkt, teils genauer formuliert.

Durch diese Neugestaltung wurden jedoch nicht alle aus dem Schufa-Verfahren resultierenden Probleme gelöst.

So versuchen einige Betroffenen bei der Neueröffnung eines Girokontos oder der Beantragung eines Kredits die Schufa-Klausel aus den Vertragsbedingungen des Kreditinstituts zu streichen. In solchen Fällen bestehen die Kreditinstitute in der Regel darauf, daß das Girokonto ausschließlich auf Guthabenbasis geführt wird oder sie vergeben den beantragten Kredit nur, wenn der Kunde über ausreichende – z. B. dingliche – Sicherheiten verfügt. In allen übrigen Fällen wird ein Vertragsabschluß zumeist abgelehnt. In derartigen Fällen haben sich Betroffene mit dem Argument an die Aufsichtsbehörde gewandt, daß sie ihre Rechte nach dem BDSG gar nicht wahrnehmen könnten, wenn sie letztlich gezwungen würden, in die Schufa-Klausel und damit die weitere Verarbeitung ihrer Daten durch die Schufa einzuwilligen.

Den Betroffenen mußte die Aufsichtsbehörde in diesen Fällen mitteilen, daß hier ein grundsätzliches Problem der Vertragsfreiheit angesprochen ist, weil der Kunde eines Kreditinstituts kaum mehr in der Lage ist, die Vertragsbedingungen auszuhandeln. Das Datenschutzrecht bietet dem Betroffenen keine Möglichkeit, ein Kreditinstitut z. B. zur Vergabe eines Kredits zu zwingen bei gleichzeitigem Verzicht auf weitere Informationen über den Antragsteller bzw. Einschaltung der Schufa.

Viele der Betroffenen gaben sich mit dieser Mitteilung nicht zufrieden, sondern wiesen darauf hin, daß ihnen die gesetzlich eingeräumten Rechte dann nichts nützten, wenn sie nicht in der Lage seien, diese gegen einen wirtschaftlich stärkeren Vertragspartner durchzusetzen.

7.2.4
Identitätsprüfung bei Datenübermittlungen der Schufa an ihre Vertragspartner

Es kommt immer wieder vor, daß Personen mit dem selben Vor- und Familiennamen und/oder dem selben Geburtsdatum verwechselt werden. Zustande kommen solche Verwechslungen, weil die Identität der Betroffenen nicht sorgfältig geprüft wird, was die folgenden Beispiele, denen Eingaben Betroffener zugrunde liegen, verdeutlichen:

Der in Hessen wohnende Beschwerdeführer wurde mit einer Person gleichen Vor- und Familiennamens – jedoch mit abweichendem zweiten Vornamen – und dem selben Geburtsdatum, die ihren letzten Wohnsitz in einem anderen Bundesland hatte, verwechselt. Letztere hatte unter Hinterlassung von Schulden ihren Wohnsitz aufgegeben und die Zahlungen eingestellt. Daraufhin hatte die Gläubigerin der Schufa einen Suchauftrag gemeldet. Suchaufträge werden bei allen Schufa-Geschäftsstellen durchgeführt, um sicherzustellen, daß ein säumiger Schuldner, der ohne Bekanntgabe seiner neuen Anschrift verzogen ist, evtl. aufgefunden wird.

Die Verwechslung der namensgleichen Personen kam zustande, als der Beschwerdeführer ein Girokonto eröffnen wollte. Das Kreditinstitut fragte, wie in solchen Fällen üblich, bei der Schufa an. Diese gab danach ihrem Vertragspartner, der den Suchauftrag erteilt hatte, einen Hinweis, daß in Hessen eine Person gleichen Namens und mit dem selben Geburtsdatum aufgetreten sei, wobei sie darauf hinwies, daß sie die Identität nicht geprüft habe. Kurze Zeit später erhielt der Beschwerdeführer von den Gläubigern des Gesuchten Zahlungsaufforderungen.

In einem anderen Fall wollte der Beschwerdeführer einen PKW leasen. Er reichte einen Kreditantrag bei der finanzierenden Bank ein, die ihrerseits eine Anfrage an die Schufa richtete. Nach Erhalt der Schufa-Auskunft lehnte die Bank die Finanzierung ab. In der Schufa-Auskunft wurde auf eine Person gleichen Namens, allerdings mit anderer Anschrift, hingewiesen, die mit einer eidesstattlichen Versicherung im Schuldnerverzeichnis eingetragen war. Die Schufa-Auskunft enthielt außerdem folgenden Vermerk: „Identität nicht feststellbar, ohne Geburtsdatum".

Die Schufa weist zwar ihre Vertragspartner darauf hin, daß mit der Schufa-Auskunft „Existenz oder Identität der angefragten Personen nicht bestätigt" werden. Darum obliege die Identitätsprüfung bei jeder Auskunft dem Empfänger.

Die Schufa übermittelt somit ihren Vertragspartnern Daten Betroffener auch dann, wenn die Identität nicht zweifelsfrei geklärt ist. Zwar verbietet sie vertraglich den Empfängern die Nutzung einer Auskunft, wenn diese die Identität des Betroffenen nicht eindeutig feststellen können. Die Schufa ist jedoch als speichernde Stelle im Sinne des BDSG selbst gesetzlich verpflichtet, nur richtige personenbezogene Daten zu speichern und zu übermitteln. Wenn durch das Kreditinformationssystem Schufa Daten verbreitet werden, deren Richtigkeit nicht eindeutig geklärt ist, so können dadurch für die Betroffenen erhebliche Nachteile, ja sogar wirtschaftliche Schäden entstehen. Die Erfahrungen der Aufsichtsbehörden zeigen, daß die Schufa-Vertragspartner bei Zweifeln an der Identität des Betroffenen nicht immer mit der nötigen Sorgfalt vorgehen, das heißt, sie gehen oft ohne weiteres davon aus, daß z. B. eine von der Schufa gemeldete Eintragung im Schuldnerverzeichnis sich tatsächlich auf den Betroffenen, über den nachgefragt wurde, bezieht. Da die Schufa die bei ihr gesammelten Daten weiterverbreitet, und, wie in den Beispielsfällen, den Anschein eines möglichen Zusammenhangs erweckt, ist sie selbst verpflichtet, sich zu vergewissern, daß die weitergegebenen Daten sich tatsächlich auf die angefragte Person beziehen, also Personenidentität gegeben ist.

Der lapidare Hinweis einer Schufa-Gesellschaft, da sie keine originären Kenntnisse über einen Betroffenen besitze, sondern diese immer nur von ihren Vertragspartnern erhalte, könne sie selbst keine Ermittlungen zur Identitätsfeststellung betreiben, kann jedenfalls nicht akzeptiert werden.

Die Aufsichtsbehörde hatte daher von der Schufa verlangt, daß sie ihre Vertragspartner ausdrücklich verpflichtet, nach Erhalt einer Auskunft, bei der die Identität nicht eindeutig gegeben ist, an die Schufa zurückzumel-

den, ob und gegebenenfalls wie der Vertragspartner die Zuordnung der Daten vorgenommen hat. Die Erfüllung dieser Rückmeldepflicht müßte bei der Schufa gesondert überwacht werden. Die Schufa war jedoch bisher nicht bereit, entsprechende Maßnahmen zu ergreifen.

7.2.5
Anforderungen zur Identitätsfeststellung bei Schufa-Selbstauskünften

Wenn ein Betroffener von der Schufa gemäß § 34 Abs. 2 BDSG Auskunft über die zu seiner Person gespeicherten Daten verlangt, so stellt eine in Hessen ansässige Schufa-Gesellschaft wesentlich höhere Anforderungen an die Feststellung der Identität des Betroffenen als in den unter 7.2.4 geschilderten Fällen.

Diese Schufa-Gesellschaft schickt Betroffenen, die Auskunft gemäß § 34 Abs. 2 BDSG verlangen, ein Formschreiben mit der Aufforderung, Name, Vorname, Geburtsdatum und Anschrift anzugeben. Außerdem wurden sie um eine Ablichtung ihres Personalausweises gebeten.

Durch eine Eingabe wurde der Aufsichtsbehörde bekannt, daß dieses Formschreiben selbst dann verschickt wurde, wenn der Betroffene mit seinem Auskunftsverlangen bereits sein Geburtsdatum mitgeteilt hatte.

In zahlreichen Fällen ist zur eindeutigen Identifizierung eines Auskunftsersuchenden sicherlich auch die Angabe des Geburtsdatums erforderlich. Die generelle Forderung nach einer Kopie des Personalausweises findet jedoch keine Rechtfertigung im BDSG. Wenn ein Betroffener in einem Auskunftsersuchen gemäß § 34 Abs. 2 BDSG neben Name und Anschrift bereits das Geburtsdatum angibt, besteht in der Regel auch kein Grund, von ihm noch weitere Angaben zu verlangen.

Auf die Intervention der Aufsichtsbehörde hin hat die Schufa ihr Verfahren teilweise geändert und verlangt bei schriftlichen Auskunftsersuchen nur noch in begründeten Einzelfällen eine Kopie des Personalausweises.

Festzuhalten bleibt, daß die Schufa bei der Identitätsfeststellung wesentlich strengere Maßstäbe anlegt, wenn ein Bürger von ihr eine Auskunft über seine eigenen Daten haben will, als wenn ein Schufa-Vertragspartner eine Auskunft über diesen Bürger einholt.

7.2.6
Fehlerhafte Datenverarbeitung

Über die oben geschilderten Personenverwechslungen wegen unzureichender Identitätsprüfung hinaus gibt es immer wieder andere Fälle fehlerhafter Datenverarbeitung mit oft unangenehmen Folgen, ja sogar wirtschaftlichen Schäden für die Betroffenen.

Dies soll am folgenden Beispiel deutlich werden:

Ein selbständiger EDV-Berater beantragte bei seiner Bank einen Kredit über 30 000,– DM. Die Bank fragte bei der Schufa an; die Anfrage wurde dort gespeichert. Obwohl der Kredit später nicht zustandekam und die Bank behauptete, dies der Schufa gemeldet zu haben, wurde bei der Schufa zu Lasten des Betroffenen ein entsprechender Kredit eingetragen. Im Wege der Nachmeldung informierte die Schufa auch andere Anschlußfirmen über den Kredit. Ein anderes Kreditinstitut, das dem Betroffenen einen Dispositionskredit eingeräumt hatte, reduzierte das Kreditlimit in erheblichem Maße. Der Betroffene erfuhr erst 9 Monate später von der fehlerhaften Datenverarbeitung und schaltete die Aufsichtsbehörde ein. Ein Kreditinstitut beantragte gegen eine Kundin einen Mahnbescheid über 2600,– DM und meldete diesen der Schufa. Die Schufa speicherte diesen Mahnbescheid und informierte die betreffenden Anschlußfirmen. Einen Monat später bezahlte die Betroffene die Schuld.

Als sie zweieinviertel Jahr später bei einer Teilzahlungsbank einen Kredit beantragte, erfuhr sie, daß der Mahnbescheid bei der Schufa immer noch als unerledigt eingetragen war. Im Laufe der Überprüfung durch die Aufsichtsbehörde stellte sich heraus, daß die Schufa zwischenzeitlich mehreren Kreditinstituten den Mahnbescheid als unerledigt gemeldet hatte.

In beiden Fällen konnte die Aufsichtsbehörde zwar den Sachverhalt ermitteln und eine entsprechende Berichtigung durch die Schufa auch bei denjenigen Vertragspartnern veranlassen, denen sie die falschen Daten

übermittelt hatte. Es war jedoch nicht feststellbar, ob der Fehler von der Schufa oder der einmeldenden Anschlußfirma verursacht worden war. Eine Aufklärung war deshalb nicht möglich, weil die entsprechenden schriftlichen Meldungen der Schufa-Anschlußfirmen bei der Schufa aus Kapazitätsgründen nur kurze Zeit aufbewahrt werden. Die Betroffenen sind daher kaum in der Lage, der Schufa bzw. ihren Anschlußfirmen das für die Durchsetzung eines Schadensersatzanspruches erforderliche Verschulden nachzuweisen.

Die Schufa verweist immer wieder darauf, daß es sich bei diesen ebenso wie bei den unter 7.2.4 geschilderten Vorkommnissen um Einzelfälle handele, die gemessen an ihrem Auskunftsvolumen – bundesweit weit über 20 Mio Auskünfte pro Jahr – kaum ins Gewicht fielen und daher als entschuldbares „menschliches Versagen" von Mitarbeitern hinzunehmen seien.

Hinsichtlich der falschen Zuordnung von Daten (7.2.4) wird dabei jedoch übersehen, daß es sich um strukturbedingte Fehler handelt, die auf ein unzureichendes Verarbeitungsverfahren mit zurückzuführen sind, da die Schufa bei der Einarbeitung der gemeldeten Daten in ihren Bestand keine Kontrollerfassung vorsieht. Die zweimalige Erfassung (Erst- und Kontrollerfassung) gehört jedoch in vielen Branchen, insbesondere in der Kreditwirtschaft, schon seit langem zum Verarbeitungsstandard.

Es ist schon bemerkenswert, wenn die Kreditwirtschaft bei der Verarbeitung ihrer „eigenen" Daten strenge – aber auch notwendige – Kontrollen durchführt, die von ihr getragene Schufa aber bei der Verarbeitung von personenbezogenen Daten der Betroffenen, deren Kreditruf letztlich davon abhängt, noch nicht einmal bei der Speicherung von Negativmerkmalen eine Kontrollerfassung vorsieht.

7.2.7
Datenübermittlung an die Schufa

Der folgende Fall verdeutlicht, wie ein auf den ersten Blick eindeutiger Sachverhalt, nämlich die Kündigung eines Kredits durch eine Bank zu einer unzulässigen Meldung dieser Kreditkündigung an die Schufa führte.

Die Beschwerdeführer unterhielten bei der Bank ein gemeinsames Girokonto, auf dem ihre Gehaltszahlungen eingingen. Nach Meinungsverschiedenheiten mit der Bank über die Kontoführung lösten die Beschwerdeführer das Girokonto auf. Daraufhin kündigte die Bank einen noch laufenden Kredit und stellte die gesamte Restschuld fällig. Außerdem meldete sie die Kreditkündigung der Schufa. Kurz danach erklärte sich die Bank einverstanden, daß die Beschwerdeführer die Restschuld ratenweise in der ursprünglich vereinbarten Höhe zurückzahlen.

Als die Beschwerdeführer ca. fünf Monate später einen Finanzkauf tätigen wollten, wurde dieser abgelehnt, weil die vorher eingeholte Schufa-Auskunft einen Hinweis auf die Kreditkündigung enthielt.

Nach vergeblichen Bemühungen bei der Schufa und der Bank um Löschung der „Kreditkündigung" wandten sich die Beschwerdeführer an die Aufsichtsbehörde. Außerdem stellten sie Strafantrag.

Im Zuge der Anhörung der Bank und der Schufa wurde das Merkmal Kreditkündigung bei der Schufa gelöscht, noch bevor die Aufsichtsbehörde eine abschließende Stellungnahme abgegeben hatte; außerdem informierte die Schufa die Auskunftsempfänger im Wege der Nachmeldung über die Löschung.

Nach den Feststellungen der Aufsichtsbehörde verstieß die geschilderte Meldung der Kreditkündigung durch die Bank an die Schufa gegen die §§ 3, 24 BDSG, da sie nicht zur Wahrung berechtigter Interessen erforderlich war. Die Beschwerdeführer waren mit ihren Ratenzahlungen unstreitig nicht in Verzug. Das Merkmal „Kreditkündigung" signalisiert aber in der Regel gerade die Zahlungsunfähigkeit oder -unwilligkeit des Kreditnehmers. Hier war der Kredit aber gekündigt worden, weil ihn die Bank wegen der Auflösung des Girokontos als nicht mehr ausreichend abgesichert beurteilte. Derartige einschränkende Erläuterungen sind jedoch im Informationssystem der Schufa nicht vorgesehen.

Weil das Merkmal keine eindeutige Aussage über die Gründe für die Kreditkündigung zuließ, es mangels Kenntnis der näheren Umstände bei dem Auskunftsempfänger aber zu der Annahme führen mußte, daß die

Betroffenen mit Ratenzahlungen in Verzug waren, verstieß seine Übermittlung wegen fehlender Eindeutigkeit gegen die §§ 3, 24 BDSG. Die Staatsanwaltschaft kam dagegen zu dem Ergebnis, daß die Meldung an die Schufa berechtigt gewesen sei, weil auch die Kreditkündigung berechtigt gewesen sei. Auf die Beschwerde der Betroffenen hin bestätigte der Generalstaatsanwalt diese Auffassung und verwarf die Beschwerde.

Auch wenn man der Ansicht der Staatsanwaltschaft folgen will, bestehen Zweifel, ob die Aufrechterhaltung der Meldung an die Schufa dann noch gerechtfertigt war, als die Bank sich auf weitere Ratenzahlungen einließ.

Zwischenzeitlich hat die Schufa ihr Verfahren verbessert. Nach den neuen Richtlinien für das Schufa-Verfahren (Technische Abwicklung des SCHUFA-Verfahrens, Stand 1987) darf die Kündigung eines Kredits nur noch dann der Schufa mitgeteilt werden, wenn Ursache für die Beendigung der Geschäftsbeziehung die Zahlungsunfähigkeit des Kunden ist oder seine Unwilligkeit, eine unstreitige Forderung zu begleichen. Dies ist bei Ratenzahlungen im allgemeinen dann anzunehmen, wenn der Kunde mit einem Betrag in Verzug ist, der mindestens zwei vollen Raten entspricht, bei Kreditverhältnissen ohne Ratenvereinbarung nach zwei vorausgegangenen fruchtlosen schriftlichen Zahlungsaufforderungen.

7.3
Kreditkartenorganisationen

Wer mit Kreditkarte einkauft, nimmt einen von dem Kreditkartenunternehmen eingeräumten Kredit in Anspruch, da die Kartenorganisation dem jeweiligen Vertragsunternehmen die Begleichung der Rechnung garantiert. Um bei der Ausstellung einer Kreditkarte und damit der Vergabe entsprechender – teilweise sogar unbeschränkter – Kredite eventuelle Risiken erkennen zu können, prüfen die Kreditkartenorganisationen zunächst die Bonität eines Antragstellers, bevor sie diesem die beantragte Kreditkarte ausstellen. Hierzu holen sie bei dem Kreditinstitut und oft auch bei dem Arbeitgeber des Betroffenen Auskünfte ein, außerdem wird bei der Schufa sowie bei Wirtschaftsauskunfteien nachgefragt.

Die Unternehmen lassen sich von den Antragstellern auf den Kartenanträgen ausdrücklich dazu ermächtigen, entsprechende Auskünfte einzuholen. Diese sogenannte Ermächtigungsklausel entspricht jedoch nicht den Anforderungen des BDSG, da sie zu allgemein gefaßt ist.

Für die Nachfrage beim Kreditinstitut, beim Arbeitgeber sowie bei einer Wirtschaftsauskunftei benötigt das Kreditkartenunternehmen die schriftliche Einwilligung des Betroffenen gemäß § 3 BDSG in die Verarbeitung seiner personenbezogenen Daten. Rechtswirksam einwilligen kann jedoch nur jemand, der hinreichend darüber informiert ist, welche Daten über ihn an welche Stellen übermittelt und welche Auskünfte dabei eingeholt und bei dem Kreditkartenunternehmen gespeichert werden.

Von der Schufa erhält die Kreditkartenorganisation nur eingeschränkte Auskünfte, die sich auf sogenannte Negativmerkmale beschränken (z. B. Kreditkündigung wegen zweimaligen Zahlungsrückstandes bei unbestrittener Forderung, Zwangsvollstreckung usw.). Die Übermittlung solcher Negativmerkmale ist in der Regel durch §§ 24 Abs. 1, 32 Abs. 2 BDSG gedeckt, so daß insoweit eine ausdrückliche Einwilligung des Betroffenen entbehrlich ist. Allerdings muß dieser über die Einschaltung der Schufa sowie den Umfang des entsprechenden Datenaustauschs hinreichend informiert werden.

Im Zusammenhang mit der Bearbeitung von Beschwerden hat die Aufsichtsbehörde die Ermächtigungsklauseln von vier Kreditkartenorganisationen geprüft und die Unternehmen über die datenschutzrechtlichen Bedenken informiert. Obwohl sie sich teilweise bereits seit Anfang 1986 um eine gesetzeskonforme Änderung der Klauseln bemüht, haben ihr die Unternehmen – mit einer Ausnahme – bisher keine bzw. keine akzeptablen Änderungsvorschläge unterbreitet.

Lediglich ein Unternehmen zeigte von Anfang an Bereitschaft zur Zusammenarbeit und hat mittlerweile eine den Anforderungen des § 3 BDSG entsprechende Klausel vorgelegt. Die Haltung der übrigen Unternehmen ist um so unverständlicher, als der Bundesgerichtshof mit Urteil vom 19. September 1985 (BGHZE 95, 362) zur Schufa-Klausel grund-

sätzliche Ausführungen zur Einwilligungsproblematik gemacht hat, die hier größtenteils heranzuziehen sind.

Da das BDSG den Aufsichtsbehörden keine Eingriffsbefugnisse gibt, kann die Aufsichtsbehörde weiterhin nur auf dem Verhandlungsweg – wenn auch mit großem Nachdruck – auf die erforderlichen Änderungen dringen. Die Beschwerdeführer hat die Aufsichtsbehörde über diese Bemühungen sowie ihre eingeschränkten Möglichkeiten informiert.

7.4
Adressenhandel und Werbung

Viele Bürger beschweren sich bei der Aufsichtsbehörde über unverlangt zugesandte Werbebriefe. Wenn auch zunächst der Ärger über verstopfte Briefkästen im Vordergrund stehen mag (in erster Line werden die Briefkästen allerdings durch nicht adressierte Hauswurfsendungen verstopft), fragen sich die Betroffenen, woher das werbende Unternehmen oder die um Spenden bittende Hilfsorganisation ihre Anschrift hat. Hinzu kommt die Befürchtung, daß die werbende Stelle über Name und Anschrift hinaus weitere Informationen über den Betroffenen haben könnte. Diese Sorge wird durch die Aufmachung mancher Werbebriefe ausgelöst, in denen die Umworbenen sehr direkt und „persönlich" angesprochen werden, z. B. als Bezieher eines höheren Einkommens. Häufig beruhen solche Einschätzungen nicht auf detaillierten Angaben über die Betroffenen, sondern man versucht, z. B. aus Berufsangaben Schlüsse auf die Kaufkraft zu ziehen. Außerdem beschweren sich Bürger, wenn sie im Wahlkampf den Werbebrief einer politischen Partei erhalten, der an sie persönlich unter Angabe ihrer Firmenanschrift (Arbeitgeber) gerichtet ist.

Bei diesen Beschwerden handelt es sich um Fälle, in denen der Betroffene keine Kontakte zu der werbenden Stelle hatte, indem er z. B. etwas bestellt oder gespendet hatte.

Die Betroffenen mußte die Aufsichtsbehörde immer wieder über den Ablauf solcher Werbemaßnahmen informieren. Für die Werbung werden sogenannte Adreßverlage oder Direktwerbeunternehmen eingeschaltet. Diese geben die von ihnen gesammelten Anschriften häufig nicht aus der Hand, sondern fertigen Adressenaufkleber an oder bringen die Anschrift direkt auf dem Werbebrief an und geben diese Briefe direkt bei der Post auf. Die werbende Stelle, die als Absender angegeben wird, erfährt von den Umworbenen erst dann etwas, wenn diese auf die Werbung reagieren und z. B. etwas bestellen.

Die Adreßverlage selbst erhalten die Anschriften auf verschiedenen Wegen, durch Auswertung allgemein zugänglicher Quellen (Telefon- und Adreßbücher), durch Auswertung der Teilnehmerlisten von Tagungen und ähnlichen Veranstaltungen. Häufig stellen ihnen Firmen Kundenanschriften zur Verfügung.

Wenn die Betroffenen – in Unkenntnis der Abläufe – von dem werbenden Unternehmen die Löschung ihrer Anschrift verlangen, ist deren Reaktion unterschiedlich. Manche verweisen den Betroffenen direkt an den Adreßverlag, von dem sie für die betreffende Werbeaktion die Anschrift bezogen haben, so daß der Betroffene sein Recht auf Löschung seiner Daten direkt gegenüber dem Adreßverlag geltend machen kann. Andere wiederum teilen lediglich mit, daß sie die Adressen für die Werbeaktion angemietet haben, ohne die Quelle zu nennen. Einige können trotz Bemühens die Quelle nicht nennen, weil sie von verschiedenen Adreßverlagen Anschriften beziehen und der Umworbene den Briefumschlag mit dem Adreßaufkleber, der häufig in verschlüsselter Form einen Hinweis auf die Herkunft der Anschrift enthält, bereits weggeworfen hat.

Die Aufsichtsbehörde kann Beschwerdeführer oft nur auf die sogenannte Robinson-Liste hinweisen, die vom Deutschen Direktmarketing Verband e. V., Schiersteiner Str. 29, 6200 Wiesbaden geführt wird. Durch Eintragung in diese Liste erreicht man, daß die dem Verband angeschlossenen Unternehmen die Anschrift nicht mehr für Werbezwecke nutzen. Da jedoch bei weitem nicht alle Adreßverlage und Direkt-Werbeunternehmen diesem Verband angeschlossen sind, die Liste außerdem nur zweimal jährlich aktualisiert wird, bietet eine Eintragung nur einen lückenhaften Schutz.

Unter Ziffer 7.4.2ff. werden einzelne Werbemaßnahmen geschildert, die die Aufsichtsbehörde aufgrund von Beschwerden Betroffener überprüft hat.

7.4.1
Adressen der Telefonteilnehmer

Sehr begehrt in der Werbebranche sind die Anschriften von Telefonteilnehmern, die die Deutsche Postreklame GmbH, eine Tochter der Deutschen Bundespost, vertreibt. Diese Anschriften sind auf dem neuesten Stand, da das Fernmeldeamt frühzeitig vom Umzug eines Telefonteilnehmers erfährt. Die Gefahr des Rücklaufs eines Werbeschreibens, weil die Anschrift veraltet ist, ist bei dieser Adressenkollektion sehr gering. Die Postreklame erhält die Anschriften von den Fernmeldeämtern. Dies ist jedoch nur dann zulässig, wenn der betroffene Telefonteilnehmer gemäß § 3 BDSG ausdrücklich schriftlich darin eingewilligt hat, daß die Post der Postreklame Name, Anschrift und gegebenenfalls Berufsgruppe für Werbezwecke Dritter zur Verfügung stellt.

Diese Einwilligung wird mit den Antragsformularen für die Einrichtung bzw. Änderung eines Telefonhauptanschlusses eingeholt. Die Bundespost hat vor einiger Zeit diese Formulare geändert. Das Regierungspräsidium in Darmstadt ist zwar für die Deutsche Bundespost nicht zuständig, da aber die privatrechtlich organisierte Deutsche Postreklame GmbH in Frankfurt, die seiner Zuständigkeit unterliegt, als Rechtsgrundlage ihres Adressenhandels die von den Betroffenen erteilte Einwilligung ansieht, ist seine Zuständigkeit zumindest berührt.

Die auf dem Antragsformular neugefaßte Einwilligungsklausel lautet nunmehr: „Ich bin widerruflich damit einverstanden, daß meine Anschrift und gegebenenfalls die Berufsgruppe der Deutschen Postreklame GmbH für Werbezwecke übermittel wird". Daneben steht: „Wenn Sie damit nicht einverstanden sind, streichen Sie bitte diese Erklärung".

Hier wird die Einwilligung bereits vorgegeben. Unternimmt der Betroffene nichts, gilt sie als erteilt, auch wenn der Betroffene die Erklärung nicht gelesen hat. § 3 BDSG verlangt aber die bewußte Einwilligung.

Es fragt sich, warum die Bundespost nicht die Regelung gewählt hat, die zum Beispiel von hessischen Behörden zu beachten ist, wenn Daten zu Werbezwecken herausgegeben werden. Danach muß die Einwilligung eindeutig erklärt werden. Im Zweifelsfall ist davon auszugehen, daß die Einwilligung nicht erteilt wurde (s. Erlaß des HMdI vom 15. August 1979, StAnz.S. 1800).

7.4.2
Werbung für Kreditkarten

Eine Kreditkartenorganisation verschickte an einen bestimmten Personenkreis Werbebriefe, die u. a. folgende Formulierungen enthielten:

„Ich möchte Sie einladen, ohne die ansonsten erforderlichen zeitraubenden Formalitäten, die ....-Karte zum persönlichen 3-Monats-Test anzufordern. Ihre ....-Karte liegt abrufbereit, denn Ihr beiliegender, vorbereiteter Antrag ist bereits vorgeprüft. Daher garantiere ich Ihnen bevorzugte Bearbeitung. Ihre Anforderung genügt und die Karte wird Ihnen umgehend zugeschickt."

Bei mehreren Empfängern solcher Werbeschreiben entstand aufgrund der Formulierung „vorgeprüfter" Antrag der Eindruck, das betreffende Unternehmen habe bereits ohne ihr Wissen kreditrelevante Informationen bei Dritten, z. B. der Schufa oder anderen Stellen, über sie eingeholt.

Wie die Überprüfung ergab, war diese verständliche Befürchtung jedoch unbegründet.

Das Kreditkartenunternehmen hatte für diese Werbeaktion von einem Adressenverlag die Anschriften bestimmter Berufsgruppen wie Ärzte, Rechtsanwälte, Ingenieure usw. angemietet. Dabei wurden solche Berufsgruppen ausgewählt, bei denen man ein bestimmtes Mindesteinkommen und damit ein möglichst geringes Kreditrisiko unterstellen konnte. Lediglich diese Vorauswahl war mit dem Ausdruck „vorgeprüft" gemeint. Weder die Kreditkartenorganisation noch der Adreßverlag hatten außer

Name, Anschrift und Berufsgruppe zusätzliche Informationen über die in der Adressenkollektion enthaltenen Personen.

Ein anderes Kreditkartenunternehmen übersandte den umworbenen Personen per Einschreiben Werbebriefe, denen eine gebrauchsfertige Kreditkarte beigefügt war. Der Empfänger mußte die Karte nur noch unterschreiben. Außerdem wurde er gebeten, dem Kreditkartenunternehmen innerhalb von 8 Tagen eine persönliche Bestätigung zurückzuschikken. Er konnte die unterschriebene Kreditkarte jedoch bereits unabhängig von dieser Bestätigung benutzen. Das Kreditkartenunternehmen erläuterte diese überraschende Werbemaßnahme u. a. mit folgenden Worten: „Wir erlauben uns jedoch, besonders vertrauenswürdigen Kunden die ....-Karte auf diese recht ungewöhnliche Weise vorzustellen. In diesem ausgesuchten Kreis möchten wir auch Sie begrüßen und Sie zu einem dreimonatigen Test der ....-Karte einladen....“

Auch hier befürchteten Empfänger solcher Werbeschreiben, daß das Kreditkartenunternehmen Informationen über ihre finanziellen Verhältnisse habe, da sich die Betroffenen – wiederum verständlicherweise – nicht vorstellen konnten, daß eine gebrauchsfertige Kreditkarte ohne vorherige Bonitätsprüfung übersandt wird. Außerdem waren sie wegen der Versendungsart verärgert, weil sie die eingeschriebenen Werbeschreiben beim Postamt abholen mußten, wenn sie der Briefträger nicht zu Hause angetroffen hatte.

Die Überprüfung ergab auch in diesem Falle, daß das Kreditkartenunternehmen auf die Adressenkollektion eines Adreßverlages zurückgegriffen hatte, in der lediglich Name, Anschrift und Berufsgruppe enthalten waren. Die Kreditkartenorganisation verfügte über keine darüber hinausgehenden Informationen.

7.4.3
Bereitstellung der Kundenadressen für Werbezwecke Dritter

Mehrere Petenten, die Kreditkarten besaßen, erhielten Werbeschreiben ihnen unbekannter Firmen, zu denen sie keine Kontakte hatten. Aufgrund besonderer Umstände vermuteten sie, daß ihre Anschrift nur von ihrem Kreditkartenunternehmen stammen könne. Die Überprüfung der Aufsichtsbehörde ergab bisher folgendes:

Eine Kreditkartenorganisation gestattet geschäftlich verbundenen Unternehmen, gelegentlich Kreditkarteninhaber zu Werbezwecken anzuschreiben. Die Adressen der Kreditkarteninhaber werden nicht unmittelbar Dritten zugänglich gemacht, sondern lediglich als Band einer Agentur zur Verfügung gestellt. Diese schickt dann die Werbeschreiben ohne weiteres Zutun des werbenden Unternehmens ab. Erst durch die Antwort des Kreditkarteninhabers und das damit zum Ausdruck gebrachte Interesse erfährt das werbende Unternehmen die Adresse des Kreditkarteninhabers.

Die Überprüfung gemäß § 30 BDSG ist noch nicht abgeschlossen. Schon jetzt ist aber darauf hinzuweisen, daß eine evtl. Übermittlung der Adressen der Kreditkarteninhaber an interessierte Dritte gegen § 24 BDSG verstoßen würde. Neben Name und Anschrift würden dabei folgende Angaben übermittelt: Kunde der betreffenden Kreditkartenorganisation, bestimmtes Mindesteinkommen (nur dann erhält man eine Kreditkarte), einwandfreies Zahlungsverhalten (anderenfalls wird die Karte gekündigt). Die Kreditkarteninhaber wissen und erwarten auch nicht, daß das Kreditkartenunternehmen ihre Anschriften Dritten für Werbezwecke zur Verfügung stellt. Eine Datenübermittlung für Werbezwecke ginge über den Vertragszweck weit hinaus. Durch eine derartige, unzulässige Zweckänderung würden daher die schutzwürdigen Belange der Betroffenen erheblich beeinträchtigt.

7.4.4
Werbung bei verschuldeten Personen

Betroffene, die im Schuldnerverzeichnis nach § 915 Zivilprozeßordnung eingetragen waren, erhielten Werbeschreiben von Kreditvermittlern, in denen Kredite, Schuldenregulierungen, Umschuldungsprogramme u. ä. angeboten wurden. In einem Fall erhielt der Betroffene in einem relativ kurzen Zeitraum Werbebriefe von 13 verschiedenen Kreditvermittlern aus dem gesamten Bundesgebiet.

Bisher ließ sich nicht genau aufklären, woher die Kreditvermittler die Anschriften sowie die Information bezogen hatten, da es sich um hoch verschuldete Personen handelte. Es ist zu vermuten, daß das Schuldnerverzeichnis für Werbezwecke genutzt wird. In den überprüften Beschwerdefällen ließ sich das jedoch nicht nachweisen.

Durch die Veröffentlichung von Schuldnern im Schuldnerverzeichnis soll die Allgemeinheit davon Kennntnis nehmen können, daß bestimmte Personen „wegen ihrer Mittellosigkeit zur Anknüpfung von Geschäftsbeziehungen nicht geeignet erscheinen". Jedermann kann gemäß § 915 Abs. 3 ZPO auf Antrag Auskunft über das Bestehen oder Nichtbestehen einer bestimmten Eintragung erhalten.

Abschriften aus dem Schuldnerverzeichnis dürfen gemäß§ 915 Abs. 4 ZPO nur einem begrenzten Empfängerkreis zugänglich gemacht werden. Das nähere Verfahren regeln „Allgemeine Vorschriften über die Erteilung und die Entnahme von Abschriften oder Auszügen aus den Schuldnerverzeichnissen" des Bundesministers der Justiz aus dem Jahre 1955. Danach erhalten u. a. die Industrie- und Handelskammern regelmäßig Abschriften. Die Industrie- und Handelskammern des Landes Hessen haben einen Verlag mit der Veröffentlichung der Schuldnerlisten der hessischen Amtsgerichte beauftragt. In anderen Bundesländern wird ähnlich verfahren. Der Verlag gibt diese Abschriften in „Vertraulichen Mitteilungen" an Mitglieder der IHK heraus. Problematisch an diesem Verfahren ist der unüberschaubar gewordene Personenkreis, der Kenntnis von allen Eintragungen nehmen kann und sie für beliebige, nicht vom Schutzzweck des § 915 ZPO umfaßte Zwecke nutzt. Die zwischen dem Verlag und den Beziehern der „Vertraulichen Mitteilungen" getroffenen vertraglichen Regelungen hinsichtlich der Verpflichtung zur Nichtweitergabe sowie des Verbots der zweckwidrigen Nutzung können eine mißbräuchliche Nutzung nicht verhindern.

Außerdem ist nicht sichergestellt, daß die Löschungsregelung des § 915 Abs. 2 ZPO auf der Empfängerseite eingehalten wird.

7.5
Personaldaten

7.5.1
Verarbeitung von personenbezogenen Daten erfolgloser Bewerber

Aufgrund mehrerer Anfragen hatte sich die Aufsichtsbehörde mit der Frage zu befassen, ob und wie lange ein Arbeitgeber Personalfragebogen erfolgloser Bewerber aufbewahren darf. Ein datenschutzrechtlicher Ansatz für die Antwort ist nur dann gegeben, wenn die formatisierten Personalfragebogen in einer Datei geführt werden, was zumeist nicht der Fall ist, da die Unterlagen des Bewerbers in einer Akte aufbewahrt werden.

Das Bundesarbeitsgericht hat in einer Grundsatzentscheidung vom 6. 6. 84, 5 AZR 286/81 (DB 1984, S. 2626) festgestellt, daß die dauerhafte Aufbewahrung eines Personalfragebogens, der von einem erfolglos gebliebenen Stellenbewerber auf Verlangen der Firma ausgefüllt worden ist und der unter anderem auch Angaben über die Privat- und Intimsphäre enthält, das verfassungsrechtlich geprägte Persönlichkeitsrecht des Bewerbers verletzen kann. In einem solchen Fall hat der Bewerber daher, unabhängig von den Schutzvorschriften des BDSG, einen Anspruch auf Vernichtung des Fragebogens, analog § 1004 BGB. Das Gericht betonte, die Absicht, den Fragebogen bei einer nochmaligen Bewerbung zu einem Datenvergleich heranzuziehen oder den Bewerber später zu einer nochmaligen Bewerbung anzuhalten, begründe kein berechtigtes Interesse des Arbeitgebers an der Aufbewahrung des Fragebogens.

Der Beschwerdeführer wurde entsprechend informiert.

7.5.2
Nutzung von Privatanschriften der Arbeitnehmer für die Zusendung von Arbeitgeberinformationen

In mehreren Beschwerden wandten sich Arbeitnehmer der metallverarbeitenden Industrie dagegen, daß ihr Arbeitgeber ihnen eine von den Arbeitgeberverbänden finanzierte Zeitschrift, die allgemeinwirtschaftliche, sozial- und gesellschaftspolitische Themen aus Sicht der Arbeitgeber behandelt, zuschicken ließ. Der Arbeitgeber übersandte dem Verlag, der

die Zeitschrift kostenlos im Auftrag der Verbände verteilte, Adreßlisten mit den Privatanschriften seiner Beschäftigten zum Zwecke des Postversands. Eine Gruppe von Beschwerdeführern schaltete die Datenschutzaufsichtsbehörde ein, nachdem sie beim Arbeitgeber vergeblich der weiteren Zusendung der Zeitschrift und der damit verbundenen Nutzung ihrer Adresse widersprochen hatte. In anderen Fällen wandten sich die Arbeitnehmer unmittelbar an die Aufsichtsbehörde, ohne vorher der Zusendung widersprochen zu haben. In allen Fällen war die Zeitschrift zum Zeitpunkt der Beschwerde bereits über einen längeren Zeitraum zugeschickt worden.

Die Nutzung der Privatanschrift für die Zusendung von Arbeitgeberinformationen ist sowohl in der datenschutzrechtlichen Literatur wie auch zwischen den obersten Länderaufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich in der Vergangenheit kontrovers diskutiert worden.

In den geschilderten Fällen lag keine Datenübermittlung vom Arbeitgeber an den Verlag im Sinne des § 2 Abs. 2 Nr. 2 BDSG, sondern ein Auftragsverhältnis vor. Zu prüfen war daher, ob der Arbeitgeber die Anschriften der Beschäftigten zum Zwecke der Versendung der Zeitschrift gemäß § 23 HDSG speichern und verwenden durfte.

Die entsprechende Datenverarbeitung bewegt sich nicht im Rahmen der Zweckbestimmung des Arbeitsverhältnisses (§ 23 Satz 1, 1. Alternative BDSG). Der Arbeitnehmer stellt dem Betrieb seine Daten lediglich zur Erfüllung des Arbeitsverhältnisses und der sich daraus ergebenden Rechte und Pflichten zur Verfügung.

Der Arbeitgeber kann sich allenfalls auf die Wahrung seiner berechtigten Interessen berufen, (§ 23 Satz 1, 2. Alternative BDSG). Dazu muß allerdings die Verarbeitung der Privatanschriften erforderlich sein. Außerdem darf kein Grund zu der Annahme bestehen, daß schutzwürdige Belange des Arbeitnehmers beeinträchtigt werden.

Dem Arbeitgeber ist zuzugestehen, daß auf seiner Seite ein berechtigtes Interesse vorhanden ist, den Arbeitnehmern die Zeitschrift zukommen zu lassen und damit für seinen Standpunkt zu werben. Schwieriger zu beantworten ist allerdings die Frage, ob es für die Wahrung der Arbeitgeberinteressen auch erforderlich ist, die Zeitschrift an die Privatadresse zu schicken oder ob es nicht ausreicht, die Zeitschrift im Unternehmen bzw. direkt am Arbeitsplatz auszulegen. Letzterem wird entgegengehalten, daß man mit der Zusendung auf dem Postweg den Mitarbeiter direkt ansprechen und ihm vor allem die Zeitschrift unbeobachtet von Kollegen oder dem Betriebsrat zukommen lassen möchte.

Es ist zweifelhaft, ob eine strikte Beachtung des Grundsatzes der Erforderlichkeit bei der Nutzung von Adressen für Werbezwecke zu einer sachgerechten Lösung führt, wenn man auch hier Erforderlichkeit in dem Sinne interpretiert, daß keine andere Methode zur Wahrung der Interessen möglich sein darf. Dabei wird nicht verkannt, daß die Adressen ursprünglich für einen anderen Zweck überlassen wurden. Mit der Zusendung der Zeitschrift wird für einen bestimmten arbeitspolitischen Standpunkt geworben. Zwar kann man dies nicht mit der Werbung für ein bestimmtes Produkt oder eine Dienstleistung gleichsetzen. Einige Parallelen sind jedoch vorhanden.

Personenbezogene Daten ihrer Kunden erhalten Unternehmen zur Abwicklung des jeweiligen Vertragsverhältnisses, z. B. Kaufvertrag, Reisevertrag usw. Wenn das Unternehmen später dem Kunden einen Werbebrief zuschickt, so ist die Zulässigkeit der Briefwerbung bisher nicht in Frage gestellt worden, weil man etwa diese Methode für nicht erforderlich hielt, da das Unternehmen andere Werbemaßnahmen hätte durchführen können, ohne auf personenbezogene Daten zurückgreifen zu müssen.

Insoweit ist die Werbung für Arbeitgeberstandpunkte durch Zusendung einer Zeitschrift mit der Direktwerbung für Waren oder Dienstleistungen durchaus vergleichbar.

Entscheidend ist daher, ob Grund zu der Annahme besteht, daß schutzwürdige Belange der Betroffenen beeinträchtigt werden, d. h., durch die Zusendung der Zeitschrift deren Privatsphäre in unzumutbarer Weise berührt wird.

Dies ist grundsätzlich nicht der Fall, da es dem Arbeitnehmer wie bei der Produktwerbung überlassen bleibt, ob er die Zeitschrift lesen will oder nicht. Lehnt er diese Art von Werbung ab, so entsteht ihm allein durch die Zusendung der Zeitschrift noch keine unzumutbare Belastung.

Anders verhält es sich dagegen, wenn er der weiteren Zusendung widerspricht. Hier muß der Arbeitgeber den Wunsch des Betroffenen respektieren und eine weitere Zusendung unterbinden (vgl. BGHZ 60, 296).

Die Aufsichtsbehörde hat die Beteiligten über diese Auffassung informiert.

7.5.3
Übermittlung von Personaldaten ins Ausland

In den letzten zwei Jahren gab es mehrere Anfragen von Unternehmen, aber auch Eingaben Betroffener, die den grenzüberschreitenden Datenverkehr zum Gegenstand hatten. Zumeist ging es dabei um die Übermittlung von Arbeitnehmerdaten ins Ausland. Zweck derartiger Übermittlungen ist vornehmlich die Sicherung einer einheitlichen und unternehmensübergreifenden Personalplanung internationaler Konzerne bzw. international tätiger Unternehmen.

Das Problem liegt vor allem darin, daß es infolge der Datenübermittlung in das Ausland und der dort stattfindenden weiteren Datenverarbeitung für den Betroffenen wesentlich schwieriger sein kann, die sich aus dem BDSG ergebenden Auskunfts-, Berichtigungs- und Löschungsansprüche durchzusetzen. Von der Ausnahme der Auftragsdatenverarbeitung durch ausländische Firmen abgesehen, fehlen im BDSG Regelungen für den grenzüberschreitenden Datenverkehr.

7.5
Vorrang des Sozialgesetzbuches

Ein Träger der gesetzlichen Unfallversicherung fragte bei dem Arbeitgeber des Beschwerdeführenden unter Berufung auf § 99 SGB X nach der Höhe seines Nettolohnes im Halbjahr 1987. Als Begründung führte die gesetzliche Unfallversicherung folgendes an: die geschiedene Ehefrau des Beschwerdeführers beziehe wiederauflebende Witwenrente von ihrem ersten Mann. Da die Rentenhöhe von dem Unterhaltsanspruch gegenüber ihrem geschiedenen Mann abhängig sei, müßten dessen Einkommensverhältnisse regelmäßig überprüft werden.

Der Arbeitgeber kam diesem Begehren nach, obwohl der Betroffene weder bei der anfragenden Unfallversicherung versichert war, noch eine Auskunftspflicht nach § 99 SGB X bestand. Denn aufgrund dieser Bestimmung ist allein der Betroffene als Unterhaltspflichtiger zur Auskunft verpflichtet, nicht dagegen sein Arbeitgeber. Auch in § 24 BDSG ist keine Rechtsgrundlage für die Datenübermittlung zusehen. Denn diese Datenübermittlung erfolgte nicht im Rahmen der Zweckbindung des Vertragsverhältnisses (§ 24 Abs. 1 S. 1 BDSG) zwischen dem Beschwerdeführer und seinem Arbeitgeber, da der Anfrage kein Sozialversicherungsverhältnis des Beschwerdeführers zugrunde lag.

Darüber hinaus konnte die Erforderlichkeit der Datenübermittlung auch nicht auf die Wahrung berechtigter Interessen eines Dritten oder der Allgemeinheit gemäß § 24 Abs. 1 S. 1 2. Alt. BDSG gestützt werden. Die allgemeine Regelung des BDSG wird von der spezielleren Vorschrift des § 99 SGB X verdrängt, der allein auf den Unterhaltspflichtigen und nicht auf dessen Arbeitgeber abzielt.

7.6
Patientendaten

7.6.1
Aufbewahrung von Patientendaten außerhalb der Arztpraxis

Ein Arzt und ein Betriebswirt beabsichtigen, ein Unternehmen zu gründen, das Ärzten die Aufbewahrung verwahrungspflichtiger Unterlagen anbieten soll. Sie wandten sich an die Aufsichtsbehörde mit der Bitte um datenschutzrechtliche Beratung.

Der beabsichtigte Unternehmenszweck stellt ein Novum dar und berührt grundsätzliche Fragen des Arztgeheimnisses und des Datenschutzes in einem Bereich äußerst sensibler personenbezogener Daten. Eine Weitergabe von ärztlichen Unterlagen aus laufenden Praxen macht im Hinblick auf § 203 StGB die Einwilligung des betroffenen Patienten erforderlich.

Eine konkludente oder stillschweigende Einwilligung aufgrund mangelnden Widerspruchs ist nur ausreichend, wenn der Patient ausdrücklich und nicht durch kleingedruckte Vertragsbedingungen über die vorgesehene externe Aufbewahrung unterrichtet worden ist.

Weitere gesetzliche Bestimmungen für die externe Aufbewahrung der ärztlichen Unterlagen aus laufenden Praxen sind nicht gegeben. Lediglich für die Unterlagen aus aufgegebenen Praxen besagt § 11 Abs. 4 der Berufsordnung für die deutschen Ärzte, daß der Arzt dafür Sorge tragen soll, daß seine ärztlichen Aufzeichnungen und Untersuchungsbefunde in gehörige Obhut gegeben werden.

7.6.2
Übermittlung zwischen Kurklinik und Krankenkassen

Von einer Kurklinik wurde berichtet, daß die Krankenkassen vollständige Entlassungsberichte und Aufzeichnungen über den Krankheitsverlauf von Patienten angefordert hatten. Die Bedenken wegen des Schutzes des besonderen Vertrauensverhältnisses Arzt-Patient wurden von der Aufsichtsbehörde geteilt. Unter Hinweis auf den 8. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz (Bundestags-Drucks. 10/4690 S. 34) wurde die Klinik über eine spezielle Vereinbarung zwischen der Bundesversicherungsanstalt für Angestellte und dem Verband der Angestelltenkrankenkassen unterrichtet, nach der lediglich das 1. Blatt des Entlassungsberichts nach ausdrücklichem Hinweis an den Patienten über sein Weigerungsrecht übersandt werden darf.

7.6.3
Speicherung von Mütterdaten; Verletzung der ärztlichen Schweigepflicht

Ein Unternehmen erbat von Krankenhäusern die Namen und Anschriften von Müttern, die dort entbunden hatten. Bei diesen Müttern wollte es für seine Produkte werben. Vertreter der Firma legten den Krankenhausverwaltungen ein von zwei Rechtsanwälten verfaßtes Schreiben vor, mit dem die „datenschutzrechtliche Unbedenklichkeit" der Weitergabe der gewünschten Daten bescheinigt wurde. Die Verfasser vertraten die Auffassung, daß die Weitergabe der gewünschten Adressen durch die Krankenhäuser an das betreffende Unternehmen auch ohne Einwilligung der betroffenen Mütter zulässig sei. Ein Krankenhaus wandte sich an den Hessischen Datenschutzbeauftragten, der die Aufsichtsbehörde über den Vorgang informierte. Kurze Zeit später beschwerte sich dort eine betroffene Mutter, weil sie nach der Entbindung unerwünschte Werbung des Unternehmens erhalten hatte. Durch diese Werbung fühlte sie sich besonders verletzt, da das Baby wenige Tage nach der Entbindung verstorben war. Ohne die Beschwerden betroffener Mütter hätte die Aufsichtsbehörde die Datenbeschaffungsmethoden der Firma nicht überprüfen können – obwohl der Verstoß gegen §§ 203 StGB, 3, 23 BDSG offensichtlich war –, da es sich um eine datenverarbeitende Stelle des 3. Abschnitts handelte und ein Anlaß im Sinne des § 30 BDSG für eine Überprüfung vorher nicht gegeben war.

Die Weitergabe von Daten über Mütter, die in einer Klinik entbunden haben, ohne deren Einverständnis verletzt die ärztliche Schweigepflicht, die auch für ärztliches Hilfspersonal einschließlich der Krankenhausverwaltung gilt, (§ 203 Abs. 1 Nr. 1 in Verbindung mit Abs. 3 StGB).

Die Speicherung derart erlangter Daten ist nicht durch § 23 BDSG gedeckt.

Im Rahmen ihrer Überprüfung konnte die Aufsichtsbehörde erreichen, daß die Firma ihr Verfahren änderte. Sie läßt seitdem in den Krankenhäusern Listen auslegen, in die sich interessierte Mütter eintragen können. Die Mütter sollen ihren Namen, ihre Anschrift und den Geburtstermin angegeben. Auf dem Vordruck werden die Mütter über die weiter

beabsichtigte Verarbeitung ihrer Daten mit folgendem Hinweis informiert: „Der.... möchte Ihnen interessante Informationen und kostenlose Proben nach Hause senden. Geben Sie uns bitte nachstehend Ihre Adresse an. Ihre Angaben sind freiwillig....“ „(Die Firma) verpflichtet sich, die erhaltenen Adressen nur für die Übersendung von kostenlosen Informationen und Proben zu verwenden. Die Daten werden nicht an Dritte weitergegeben.“ Sodann wird die Mutter gebeten, ihr Einverständnis durch ihre Unterschrift zu erklären. Eine Übersetzung in fünf Sprachen für ausländische Mütter befindet sich auf der Rückseite.

Dieser Fall liegt zwar vor dem Berichtszeitraum, das zugrundeliegende Problem ist jedoch nach wie vor aktuell. So erhielt die Aufsichtsbehörde Hinweise, daß Mitarbeiter eines Unternehmens, das sich ebenfalls an Mütter kurz nach deren Entbindung wendet, versuchen sollen, vom Personal der Kliniken wie z. B. Stationsschwestern Anschriften von Müttern zu erhalten, die dort entbunden haben. Die Überprüfung ist jedoch noch nicht abgeschlossen.

7.7
Kundendaten

7.7.1
Auskünfte über Fluggastdaten

Durch Eingaben sowie die Anfrage einer deutschen Luftverkehrsgesellschaft wurde die Aufsichtsbehörde mit einem Problem befaßt, in dem eine sachgerechte Abwägung der Interessen der Beteiligten besonders schwierig ist. Täglich werden Luftverkehrsgesellschaften mit zahlreichen Auskunftsersuchen über Flugpassagiere konfrontiert. Solche Auskünfte sind nur unter den Voraussetzungen der §§ 3, 24 BDSG zulässig. Die Gesellschaften müssen sorgfältig abwägen zwischen dem berechtigten Interesse des Dritten an einer Auskunft, wobei Servicegesichtspunkte mit einfließen, und den schutzwürdigen Belangen des Fluggastes, der vielleicht gar nicht daran interessiert ist, daß andere von seinem Flug oder seiner Begleitung erfahren. Die Mitarbeiter der Fluggesellschaften sind in besonderem Maße gefordert, weil sie einerseits rasch entscheiden müssen, ob die gewünschte Auskunft gegeben werden kann, andererseits aber nicht genau abschätzen können, inwieweit sie dem Auskunftsersuchenden glauben können.

Für das Problem wurde eine zufriedenstellende Lösung gefunden. Sie ist von der Fluggesellschaft in einer Entscheidungshilfe für ihre Mitarbeiter niedergelegt worden, aus der die folgenden Auszüge entnommen sind. Außer Betracht bleiben dabei Auskünfte, für die eine Rechtspflicht besteht:

„Die der ... im Zusammenhang mit dem Abschluß eines Beförderungsvertrages von dem Fluggast oder einem von ihm Beauftragten bekanntgegebenen personenbezogenen Daten wie Flugbuchung, Hotel-/Mietwagenreservierung, spezielle Serviceinformationen u. ä. werden mit Hilfe der EDV im Reservierungssystem gespeichert. Bei der Verarbeitung dieser Daten ist das Bundesdatenschutzgesetz (BDSG) zu beachten. Danach dürfen Auskünfte über diese Daten grundsätzlich nur an den betroffenen Fluggast selbst gegeben werden. Abweichend von dieser Regel ist eine Übermittlung an Dritte dagegen nur zulässig, wenn

- der Fluggast seine Einwilligung dazu gegeben hat oder
- dies zur Durchführung des Beförderungsvertrages (z. B. bei Flugunregelmäßigkeiten) oder zur Wahrung der berechtigten Interessen der ... oder eines Dritten erforderlich ist und schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden.

Ein berechtigtes Interesse des Dritten kann angenommen werden, wenn der Auskunftsersuchende unter Hinweis auf sein Beziehungsverhältnis zu der Person des betroffenen Fluggastes (Verwandter, Mitarbeiter, Vorgesetzter) darlegt,

- zu welchem Zweck er die Auskunft benötigt,
- das Erreichen dieses Zwecks allgemeinen Rechtsgrundsätzen nicht offensichtlich widerspricht,
- keine zumutbare Alternative zur Erlangung der Auskunft besteht, d. h. nur ... kann Auskunft geben.

Beispiele: Sicherstellung eines Pick-up am Flughafen, Weiterleitung einer wichtigen Nachricht, Änderung des Reiseweges und gleichgelagerte Fälle.

... selbst als speichernde Stelle hat aus Servicegesichtspunkten in der Regel ein berechtigtes Interesse an der Erteilung der Auskunft in solchen Fällen. Nicht zulässig wäre dagegen die Weitergabe von Reservierungsdaten einer Persönlichkeit des Öffentlichen Lebens an eine Zeitungsredaktion.

Die Beeinträchtigung schutzwürdiger Belange kann in der Regel als ausgeschlossen angesehen werden, wenn der Auskunftsersuchende wesentliche Einzelheiten der Reise kennt (Flugdaten, Reiseweg, Name), die er entweder nur vom Fluggast selbst erfahren haben kann bzw. dadurch, daß er diese Reise bezahlt oder in irgendeiner Weise vorbereitet hat.

Zur Vermeidung von Unklarheiten bei der Auskunftserteilung hat der Fluggast jedoch die Möglichkeit, bei seiner Buchung einen Sperrvermerk aufnehmen zu lassen mit der Maßgabe, daß im Rahmen des BDSG seine Reservierungsdaten nicht an Dritte zu Auskunftszwecken weitergegeben werden dürfen. Auf diese Möglichkeit werden die Fluggäste durch einen Hinweis im Taschenflugplan aufmerksam gemacht.

Vor Erteilen einer Auskunft ist daher in jedem Fall zu prüfen, ob ein Sperrvermerk vorliegt oder nicht. Dieser Sperrvermerk gilt nur für Auskünfte durch... Dienststellen. Werden im Rahmen eines Beförderungsvertrages Reservierungsdaten z. B. an andere Luftverkehrsgesellschaften übermittelt, so kann... keine Zusicherung abgeben, daß ein ihr gegenüber ausgesprochener Sperrvermerk dort auch beachtet wird.

Auskünfte sollten also nicht grundsätzlich (z. B. unter Verweis auf Datenschutzregelungen) abgelehnt werden; in Zweifelsfällen ist vielmehr der Vorgesetzte einzuschalten. Diese Zweifelsfälle sind – soweit möglich – durch Festhalten der Identifikationsmerkmale des Auskunftsersuchenden (Namen, Anschrift und z. B. Nummer des Identifikationspapieres und der ausstellenden Behörde) zu dokumentieren.

"Es wäre zu begrüßen, wenn der Fluggast auf die Möglichkeit, eine Auskunftssperre vornehmen zu lassen, nicht nur im Taschenflugplan hingewiesen würde.

7.7.2
Kopieren des Personalausweises bei Zahlung mit Scheck

Einige Großmarktketten notieren sich bei Abzahlungskäufen bzw. der Annahme von Euroschecks, die den Garantiebetrag von DM 400,– übersteigen, nicht nur Anschrift und Personalausweisnummer des Kunden, sondern fertigen Kopien des vollständigen Personalausweises an und bewahren sie auf. Im Rahmen der durch entsprechende Beschwerden veranlaßten Überprüfungen gaben die Unternehmen im wesentlichen folgende Begründung für diese Verfahrensweise:

Eine Fotokopie des vollständigen Personalausweises sei erforderlich, um evtl. Übertragungs- und Schreibfehler zu verhindern und später möglicherweise auftretende Beweisschwierigkeiten über die Identität eines Kunden zu vermeiden. Durch Aushändigung des Ausweises erkläre der Kunde außerdem sein Einverständnis mit dieser Art der Datenverarbeitung.

Dem ist zunächst entgegenzuhalten, daß in den Beschwerdefällen die Kunden zwar ihre Personalsweise vorlegten, ihre ausdrückliche Einwilligung zum Kopieren wurde jedoch nicht eingeholt, vielmehr wurden Sie vor vollendete Tatsachen gestellt.

Die Speicherung der Ausweiskopien verstößt gegen § 23 Satz 1 BDSG. Zwar sind zur Abwicklung des Kaufvertrages einige im Personalausweis enthaltene Daten (Namen, Anschrift, Ausweisnummer) erforderlich, nicht jedoch die übrigen personenbezogenen Daten im Ausweis. Auf die Wahrung berechtigter Interessen bei der Speicherung der weiteren Daten können sich die Unternehmen auch nicht berufen, da Fehler bei der Übertragung der wenigen Daten durch entsprechende Sorgfalt – z. B. Gegenkontrolle – weitgehend ausgeschlossen werden, so daß die Anfertigung von Kopien der Personalausweise nicht zwingend erforderlich ist.

Auf die Aufforderung der Aufsichtsbehörde zu einer Verfahrensänderung hatte eine Firma schriftlich zugesichert, sie wolle zukünftig das Kopieren der Ausweise in derartigen Fällen unterlassen. Durch telefonische Hinweise, die aber nicht zu konkreten Beschwerden führten, wurde jedoch bekannt, daß das Unternehmen entgegen dieser Zusage in einer neu eröffneten Filiale weiterhin Ausweise kopieren läßt. Hinsichtlich einer anderen Firma ist die Überprüfung noch nicht abgeschlossen.

7.7.3
Zweckwidriger Umgang mit Kundendaten im Kreditgewerbe

7.7.3.1
Ermittlung der Anschriften von Kindergeldempfängern für Werbezwecke

Ein Kreditinstitut wollte zur Unterstützung einer Marketing-Aktion die Adressen derjenigen Kunden, die Kindergeldzahlungen erhalten, zusammenstellen.

Das Kindergeld wird von den Arbeitsämtern berechnet und mit entsprechendem Hinweis in der Rubrik „Verwendungszweck" an das Kreditinstitut des Empfängers weitergeleitet. Aus den von den Landeszentralbanken übersandten Gutschriftsbändern wollte das Kreditinstitut eine Datei mit Kontonummern der Kindergeldempfänger erstellen, um letzteren dann ein bestimmtes Werbeprogramm anzubieten. Der Verwendungszweck „Kindergeld" muß dem Kontoinhaber mitgeteilt werden, da er wissen muß, wofür die Überweisung bestimmt ist. Das Kreditinstitut des Empfängers erhält ein Exemplar des Überweisungsformulars ausschließlich zu dem Zweck, dem Kontoinhaber das Kindergeld gutzuschreiben. Die Angabe des Verwendungszweckes ist ausschließlich als Mitteilung für den Kontoinhaber gedacht.

Die beabsichtigte Marketing-Aktion hätte damit gegen § 78 Sozialgesetzbuch X verstoßen, da diese Daten zu einem anderen Zweck als zur Information des Kontoinhabers genutzt worden wären. Aufgrund der von der Aufsichtsbehörde geäußerten Bedenken hat das betreffende Kreditinstitut die Auswertung der Daten der Kindergeldempfänger gestoppt.

7.7.3.2
Verletzung des Bankgeheimnisses

Die Beschwerdeführerin unterhielt mit ihrem Ehemann ein gemeinsames Girokonto. Nachdem sich die Eheleute getrennt hatten, wurde das Konto allein für die Beschwerdeführerin weitergeführt; sie allein war auch verfügungsberechtigt. Einige Monate später gab das Kreditinstitut dem Ehemann auf dessen Wunsch Auskunft über das Konto seiner Ehefrau, und zwar über eine monatlich eingehende Zahlung (Dauerauftrag der Mutter der Beschwerdeführerin).

Die zunächst mündlich erteilte Auskunft wurde außerdem noch schriftlich bestätigt; dies geschah ca. elf Monate, nachdem die Verfügungsberechtigung des Ehemannes über das Konto erloschen war. Im Rahmen der Unterhaltsstreitigkeiten zwischen den Eheleuten legte der Ehemann die schriftliche Auskunft des Kreditinstitutes vor.

Die Überprüfung der Aufsichtsbehörde ergab, daß die dem Ehemann erteilte Auskunft gegen §§ 3, 24 BDSG verstieß und das Kreditinstitut damit gleichzeitig das Bankgeheimnis verletzte. Die Auskunft an den Ehemann hätte hier nur mit ausdrücklicher Einwilligung der alleinverfügungsbefugten Kontoinhaberin gegeben werden dürfen.

Das Kreditinstitut hat sein Verhalten damit gerechtfertigt, daß der Ehemann selbst Adressat des Dauerauftrages gewesen sei, weil der Dauerauftrag auf „Eheleute X" lautete. Die Verfügungsberechtigung über das Konto habe in diesem Zusammenhang allenfalls eine untergeordnete Rolle gespielt. Der Dauerauftrag war jedoch erst zu einer Zeit eingerichtet worden, als der Ehemann kein Kontomitinhaber und damit nicht mehr verfügungsberechtigt gewesen war. Wenn man wie das Kreditinstitut davon ausginge, daß der Ehemann Mitinhaber des materiellen Anspruches gewesen sei, hätte der Dauerauftrag in Ermangelung der Verfügungsbefugnis des Ehemannes dann von Anfang an nicht ausgeführt werden dürfen.

Die Bank wie auch der von ihr eingeschaltete zuständige Verband haben sowohl eine Verletzung des Bankgeheimnisses als auch eine Verletzung der

Datenschutzvorschriften mit Nachdruck bestritten. Der von der Beschwerdeführerin gestellte Strafverfolgungsantrag wurde von der Staatsanwaltschaft im wesentlichen mit folgender Begründung zurückgewiesen:

„Ein strafrechtlich geschütztes Bankgeheimnis gibt es in der Bundesrepublik Deutschland nicht.... Darüber hinaus ist festzustellen, daß an den Ehemann Auskunft über einen Dauerauftrag erteilt wurde, zu dessen Begünstigten er gehört. Die Verfügungsberechtigung über das Konto spielt in diesem Zusammenhang allenfalls eine untergeordnete Rolle. Eine solche Auskunft an unmittelbar Beteiligte wird man bei vernünftiger Betrachtungsweise nicht unterbinden können".

7.7.4
Telefondatenerfassung in Hotels und Behörden

Mehrere Eingaben richteten sich gegen die Erfassung von Telefondaten in Hotels. Dabei werden in Telefoncomputern Daten über die von den Hotelgästen vom Zimmer aus geführten Telefongespräche für Abrechnungszwecke gespeichert und ausgedruckt. Folgende Daten werden in der Regel gespeichert: Datum, Uhrzeit, Zimmernummer, Telefonnummer des angerufenen Teilnehmers und der zu zahlende Betrag. Die Beschwerdeführer wandten sich dagegen, daß die Telefonnummer des Angerufenen gespeichert wurde und man auf diese Weise feststellen könne, wen der Gast angerufen habe.

Bei den in einem Telefoncomputer erfaßten Gesprächsdaten handelt es sich um personenbezogene Daten im Sinne des § 2 Abs. 1 BDSG, wobei man zwischen den Daten, die sich auf den Hotelgast beziehen und den Daten des Angerufenen (Telefonnummer) unterscheiden muß. Die Speicherung dieser Daten ist nur unter den Voraussetzungen der §§ 3, 23 BDSG zulässig. Sofern sie sich auf Zeitpunkt, Dauer und Anzahl der Gebühreneinheiten (Gesamtbetrag) beschränkt, bestehen keine datenschutzrechtlichen Bedenken. Darüber hinaus ist bei Ferngesprächen die Speicherung der Vorwahlnummer zulässig. Für die Kontrolle der Telefonrechnung ist es dagegen nicht erforderlich, die gesamte Zielnummer zu speichern. Hinsichtlich dieses Datums sind die Voraussetzungen des § 23 BDSG nicht erfüllt. Andererseits liegt die dann gemäß § 3 BDSG erforderliche Einwilligung des angerufenen Betroffenen in die Speicherung seines Datums nicht vor und kann auch nicht eingeholt werden.

Die Aufzeichnung der gesamten Telefonnummer des Angerufenen ist daher unzulässig.

Eine vergleichbare Problematik ergibt sich bei der mitbestimmungspflichtigen Aufzeichnung von Telefongesprächsdaten in Betrieben. Im Verhältnis Arbeitgeber, Arbeitnehmer wird diese Telefondatenerfassung meist durch Betriebsvereinbarung geregelt, die eine „andere Rechtsvorschrift" i. S. von § 3 S. 1 Nr. 1 BDSG darstellt, aus der sich die Zulässigkeit der Datenverarbeitung ergibt. Davon unabhängig bleibt das Verhältnis zum Angerufenen. Wenn die volle Zielnummer gespeichert wird, liegt darin auch eine Verarbeitung seiner personenbezogenen Daten (so BAG, NJW 1987 S. 674). Deren Zulässigkeit richtet sich allein nach dem Erforderlichkeitsgrundsatz des BDSG, der wie bereits dargelegt die Speicherung der vollständigen Zielnummern nicht rechtfertigt.

7.7.5
Heiratsvermittler-Fall

Ein Heiratsvermittler, der darauf spezialisiert ist, südostasiatische Frauen „an den deutschen Mann zu bringen", verschickte an Interessenten, die sich auf Zeitungsanzeigen hin meldeten, ein Werbeschreiben. Darin warb er mit „voller Vermittlungsgarantie bis zur standesamtlichen Trauung". Weiter schrieb er: „Unser Vertrag ist erst erfüllt, wenn auch Sie eine solche Heiratsurkunde in Ihren Händen halten". Beigefügt waren nämlich verkleinerte Fotokopien von vierzehn Heiratsurkunden von Kunden des Vermittlers. Die Kunden hatten, um das erfolgreiche Ende der Vermittlung zu dokumentieren, dem Heiratsvermittler Kopien ihrer Heiratsurkunden übersandt. Die dem Werbeschreiben beigefügten Kopien enthielten deutlich lesbar alle auf der Heiratsurkunde vermerkten Daten der Eheleute, nämlich Name, Geburtsdatum, -ort, Religionszugehörigkeit, Wohnort, Ort und Datum der Eheschließung sowie teilweise personenbezogene Daten der Eltern der Eheleute.

Ein betroffener Ehemann wandte sich beschwerdeführend an die Aufsichtsbehörde. Er war zusätzlich verärgert, weil auf der beglaubigten Fotokopie seiner Heiratsurkunde der Dienststempel seines Arbeitgebers, einer Behörde, zu erkennen war.

Die Versendung der Kopien der Heiratsurkunden verstieß gegen §§ 3, 24 BDSG. Nur mit ausdrücklicher Einwilligung der betroffenen Eheleute hätte er deren Daten Dritten bekanntgeben dürfen. Eine derartige Einwilligung war nicht eingeholt worden. Aus der Tatsache, daß die betroffenen Kunden ihm Kopien der Heiratsurkunden als Nachweis für den Erfolg der Ehevermittlung zugesandt hatten, konnte er nicht auf eine Einwilligung in die Weitergabe der Heiratsurkunden an Dritte schließen.

Aufgrund des sofortigen Eingreifens der Aufsichtsbehörde hin stellte der Heiratsvermittler die Versendung des Werbeschreibens mit den kopierten Heiratsurkunden ein. Es konnte jedoch nicht mehr festgestellt werden, wie oft bereits die Fotokopien versandt worden waren.

Den Beschwerdeführer wies die Aufsichtsbehörde auch auf die Strafvorschrift des § 41 BDSG sowie die Möglichkeit hin, einen Strafantrag zu stellen. Die Tat wird nämlich nur auf Antrag des Betroffenen selbst verfolgt.

7.8
Mieterdaten

7.8.1
Bekanntgabe von Mieterdaten bei der Heizkostenabrechnung

Auf Anfrage eines Unternehmens, das im Auftrag von Vermietern Heizkostenabrechnungen erstellt, hatte die Aufsichtsbehörde die Frage zu prüfen, ob personenbezogene Abrechnungsdaten eines Mieters anderen Hausbewohnern bekanntgegeben werden dürfen. Die Antwort ergibt sich aus § 24 Abs. 1 BDSG. Die Bekanntgabe könnte bereits aufgrund der sich aus dem Mietvertrag ergebenden Rechte und Pflichten (§ 24 Abs. 1, 1. Alternative), zulässig sein, da einerseits der Vermieter zu einer verbrauchsabhängigen Heizkostenabrechnung verpflichtet und andererseits der Mieter berechtigt ist, die Richtigkeit der Abrechnung zu überprüfen, wozu ihm die Kenntnis der Verbrauchsanteile der anderen Wohnungen hilfreich ist.

Folgt man dieser Begründung nicht, so ist die Übermittlung jedenfalls nach der 2. Alternative des § 24 Abs. 1 zulässig, soweit die Daten zur Wahrung berechtigter Interessen der anderen Mieter erforderlich sind und dabei schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. Das Gesetz verlangt also eine am Einzelfall orientierte Abwägung zwischen dem Interesse an der Bekanntgabe der Ableseergebnisse und dem Interesse des Betroffenen, dessen Daten den anderen Mietern zugänglich gemacht werden.

Angaben zum Gesamtverbrauch pro Wohnung können anderen Mietern bekanntgegeben werden. Ein berechtigtes Interesse eines Mieters, ohne weitere Voraussetzungen sämtliche Einzelableseergebnisse aller anderen Mieter eines Hauses zu erhalten, ist demgegenüber nicht anzuerkennen.

7.8.2
Veröffentlichung von Mieterdaten durch Immobilienmakler

Eine Immobilienfirma erwarb mehrere Hochhäuser, wandelte die Wohnungen in Wohnungseigentum um und bot sie zum Verkauf an. Dazu erstellte sie Verkaufsbroschüren, die neben einer allgemeinen Beschreibung der Wohnlage Verkaufspreislisten enthielten. Auf diesen Verkaufspreislisten waren neben Lage, Größe und Verkaufspreis der Wohnungen auch die Namen der Mieter sowie die Höhe des jeweiligen Mietzinses angegeben. Diese Broschüre verschickte die Firma auf Anfrage an Interessenten. Außerdem wurden ca. 1000 Exemplare in dem Ort über die Briefkästen verteilt, u. a. auch bei den betroffenen Mietern.

Mit der Verteilung der Broschüren wurden personenbezogene Daten der Mieter, die bei der Immobilienfirma in einer Datei gespeichert waren, an Dritte übermittelt. Diese Übermittlung verstieß gegen § 24 BDSG, da zum Zeitpunkt der Verteilung der Broschüren weder ein berechtigtes Interesse

der Immobilienfirma an der Bekanntgabe der Daten noch ein berechtigtes Interesse der Umworbenen an deren Kenntnis vorlag.

Zwar ist es für Kaufinteressenten wichtig, z. B. Lage, Größe und Kaufpreis der angebotenen Wohnungen sowie die Höhe der zu erzielenden Miete zu wissen. Insoweit konnte sich die Firma auch darauf berufen, daß ihr Geschäftsinteresse die Bekanntgabe dieser Daten bereits in den Broschüren erforderte, mit denen sie die Wohnungen zum Kauf anbot. Es war jedoch nicht erforderlich, daß die Namen der Mieter in Verkaufsbroschüren genannt wurden.

Außerdem wurden durch die Verteilung der Verkaufslisten die schutzwürdigen Belange der Mieter beeinträchtigt, da ein Teil ihrer Lebensumstände nahezu öffentlich bekannt gemacht wurde.

Der weitaus größte Teil der Broschüren war bereits verteilt. Auf Intervention der Aufsichtsbehörde stellte die Firma die weitere Verteilung ein und erklärte sich bereit, zukünftig in derartigen Verkaufsbroschüren die Namen der Mieter nicht mehr zu nennen.

8.
Datensicherung

8.1
Äußere und innere Sicherheitsmaßnahmen

Datensicherung sind die technischen und organisatorischen Maßnahmen, die erforderlich sind, um die Ausführungen der Vorschriften des BDSG zu gewährleisten.

Beschrieben sind diese Maßnahmen in § 6 BDSG und in der Anlage zu dieser Vorschrift. Jede Datenverarbeitung muß technisch und organisatorisch so ausgelegt sein, daß der Schutz entsprechend der Sensibilität der Daten gewährleistet ist.

Zu schützen sind alle personenbezogenen Daten in allen in § 2 BDSG genannten Phasen der Datenverarbeitung. Der für die Datenverarbeitung Verantwortliche sowie alle Mitarbeiter, die Daten verarbeiten, haben sich bestimmten Regeln zu unterwerfen und sind so in ihrer Gestaltungsfreiheit eingeschränkt.

Die erforderlichen Sicherungsmaßnahmen sind in 2 Bereiche zu gliedern:

1. Die Absicherung der gesamten Datenverarbeitung nach Außen – der Schutz gegen Betriebsfremde.
2. Die innere Sicherheit, zu der die Isolierung der Datenverarbeitung innerhalb des Betriebes gehört, aber auch die Absicherung im internen Datenverarbeitungsbereich.

8.1.1
Maßnahmen zur äußeren Sicherheit

Seit Inkrafttreten des BDSG am 1. Januar 1978 hat sich das Erscheinungsbild der Datenverarbeitung erheblich verändert. Die Abhängigkeit des Unternehmens von einer funktionierenden Datenverarbeitung ist um ein Vielfaches größer geworden. Auch die terroristischen und vom Vandalismus geprägten Zerstörungen von Rechenzentren haben dazu beigetragen, daß man heutzutage nur noch sehr selten bei einem Unternehmen als Betriebsfremder weiß, wo die Datenverarbeitungsanlagen zu finden sind. Vor einigen Jahren noch wurde das betriebliche Rechenzentrum als gläsernes, von jedem einsehbares (nach Möglichkeit Straßenfront) Aushängeschild des Unternehmens präsentiert.

Große Schilder wiesen jedem Fremden den Weg direkt zum Rechenzentrum.

Heute dagegen wird dieser wichtige Bereich, von dessen Funktionsfähigkeit die Existenz eines Unternehmens im besonderen Maße abhängt, in Gebäuden oder Räumen untergebracht, die von außen nicht einsehbar oder als Rechenzentrum nicht identifizierbar sind. Es wurden bauliche Maßnahmen getroffen, die vielfach auch als Schutzmaßnahmen im Sinne der Datensicherung nach dem BDSG anzusehen sind. Häufig mußte die Aufsichtsbehörde in den ersten Jahren ihrer Tätigkeit z. B. große, offene Glasfenster zur Straßenseite beanstanden und fordern, daß das Rechen-

zentrum verlagert wurde, oder die einsehbaren Bereiche besonders abgesichert wurden (z. B. Panzerglas). Im Einklang damit steht auch die Forderung auf Verzicht von Hinweisschildern wie „Rechenzentrum oder Datenverarbeitungsabteilung".

Viele Unternehmen haben die Gelegenheit, neue Räumlichkeiten für die Datenverarbeitung zu finden, dazu genutzt, gleichzeitig einen höheren Schutz gegen die Zerstörung durch Brand oder Löschwasser zu erreichen – und dies nicht nur aufgrund der Beanstandungen durch die Aufsichtsbehörde, sondern auch aufgrund eigener schmerzlicher Erfahrungen.

Durch Verlagerung des Rechenzentrums in nicht einsehbare Bereiche der Gebäude, z. B. den Innenbereich, ins Tiefgeschoß oder aber in ein höher gelegenes Stockwerk usw. wird die Möglichkeit, durch Vandalismus eine Zerstörung von Daten herbeizuführen, stark vermindert. Um Einwirkungen von außen abzuhalten, gibt es sehr vielseitige und weitgehende Maßnahmen. Dies ermöglicht eine Abschottung der sensiblen Bereiche auf mehreren Ebenen. Der äußerste Schutz ist die Einzäunung des Betriebsgeländes. Der nächste ist die Überwachung mit Perimeter-Überwachungssystemen, wie z. B. Infrarot-Barrieren oder Video-Kameras usw.

Das Gebäude selbst ist entsprechend seiner Beschaffenheit mit Schutzeinrichtungen zu versehen. Besonders zu beachten sind Maßnahmen bei Fenstern, Lüftungsöffnungen und Türen. Geeignet sind unter anderem Glasbruchmelder, Bewegungsmelder, Verriegelungssysteme und vieles mehr. Bei der Verglasung ist nach der Gefahrenabwägung zwischen verschiedenen Widerstandsklassen zu wählen (von der Durchwurf- oder Einbruch-Hemmung bis hin zur Sprengstoff-Hemmung). Bei den von der Aufsichtsbehörde bisher überprüften Unternehmen werden alle denkbaren Schutzeinrichtungen unterschiedlich miteinander kombiniert, so daß sie abzuwägen hat, ob bei der Art personenbezogener Daten und der Verarbeitung, der sie unterliegen, die getroffenen Maßnahmen in ihrer Gesamtheit ausreichend sind. Beanstandungen sind z. B. bei Auskunfteien ausgesprochen worden, wenn die Eingangstüren noch nicht einmal mit einem von den kriminalpolizeilichen Beratungsstellen empfohlenen Sicherheitsschloß versehen waren. Bei kleineren und mittleren Rechenzentren, die ihre Einrichtungen im Erdgeschoß installiert haben, mußte beanstandet werden, daß z. B. keine gegen Hochschieben gesicherten Rollos an den Fenstern angebracht waren. Insbesondere auch dann, wenn die Fenster zur Straßenseite lagen und freien Einblick in das Rechenzentrum gewährten.

Bei einem größeren Rechenzentrum mußte festgestellt werden, daß keinerlei Außenabsicherungen vorhanden waren. Erschwerend kam noch hinzu, daß die Luftgitter für die Klimaanlage im Bereich der Fenster des Rechenzentrums aus einer Gartenanlage von der Straße gut einsehbar herausragten. Bei einer solchen Sorglosigkeit sind Gefährdungen von außen Tür und Tor geöffnet.

Bei einem Rechenzentrum, das in einem eigenen Gebäude untergebracht ist, kann Unbefugten recht einfach das Betreten des Gebäudes verwehrt werden.

Liegt das Rechenzentrum innerhalb eines auch anderweitig genutzten (z. B. Besucherräume) Gebäudes, dann müssen Unbefugte durch besondere Maßnahmen vom Rechenzentrums-Bereich ferngehalten werden.

8.1.2
Maßnahmen innerhalb des Gebäudes

Häufig befindet sich die Datenverarbeitung als Abteilung im Bürogebäude der Hauptverwaltung, die täglich Besucher – vom Kunden über Seminarteilnehmer bis hin zu Schulklassen – empfängt. Die Unterschiede hinsichtlich der Maßnahmen zur Sicherheit des Gebäudeinneren zeigen sich schon beim Empfang/Pförtner. Bei einem Unternehmen ist der Eingang generell verschlossen. Will der Besucher eintreten, so muß von innen die Tür durch Personal entriegelt werden. Beim anderen Unternehmen dagegen ist das Gebäude frei betretbar. Dann geht es weiter über das Ausfüllen eines Besucherzettels, eine Identifizierungskarte, die den Besucher als Betriebsfremden kenntlich macht, über das Abholen durch den Besuchten bis dahin, daß der Besucher ohne die Überwindung einer Hürde bis hin zu einzelnen Büroräumen gelangen kann, die allerdings noch außerhalb der verschiedenen Sicherheitszonen liegen.

Beanstandungen hinsichtlich der Vorschriften zur Zugangskontrolle noch außerhalb der Sicherheitszonen des Rechenzentrums, aber bereits in Bereichen, in denen personenbezogene Daten einzusehen waren, mußten bisher häufig ausgesprochen werden. Dazu gehören z. B. der offene Zugang zur Poststelle, unbesetzte Schreibtische in Fachabteilungen, teilweise unbesetzte, aber angemeldete Bildschirmsichtgeräte.

8.1.3
Sicherheit intern; Sicherheit unter Schwester-Unternehmen

Häufig sind mehrere Unternehmen, die zu einem Konzern gehören, oder Unternehmen, die einem Inhaber gehören, in einem Bürogebäude zusammen untergebracht. In diesen Fällen wird nicht selten übersehen, daß die einzelnen Unternehmen, wenn sie eine eigene Rechtsperson sind, gegenseitig als Dritte im Sinne des BDSG anzusehen sind. So mußte die Aufsichtsbehörde bei Kontrollbesuchen mehrmals feststellen, daß zwei oder mehrere Unternehmen sich ein Gebäude teilten, das zwar nach außen genügend abgesichert war, intern aber überhaupt keine Abgrenzungen aufwies.

In einem bestimmten Fall betätigte sich eins der Unternehmen als Dienstleistungsbetrieb gemäß § 31 Abs. 1 Nr. 3 BDSG. Hier mußte beanstandet werden, daß keine Regelungen hinsichtlich des gegenseitigen Zugangs durch Mitarbeiter beider Unternehmen getroffen worden waren. So gelangten Mitarbeiter des Schwesternunternehmens in den Bereich, in dem im Auftrag für dritte Auftraggeber Daten verarbeitet wurden. Die Aufsichtsbehörde konnte erreichen, daß die Räume, die vom Dienstleistungsunternehmen benutzt werden, mit einem Zugangskontroll-System ausgestattet wurden und nunmehr nur noch von berechtigtem Personal (mit Erkennungskarte) betreten werden.

Zugangskontrollsysteme gibt es in sehr unterschiedlicher Qualität. Sie reichen vom einfachen Zahlensystem oder Magnetstreifenkarten bis hin zur Einzelpersonenschleuse mit Kameraüberwachung und Gesichtskontrolle.

Welches System zur Anwendung gelangt, hängt auch hier letztendlich von der Sensibilität der Daten ab. Ein häufiger Mangel liegt darin, daß zwar mehrere Sicherheitszonen einschließlich eines besonderen innerer Sicherheitsbereichs geschaffen sind, zu denen in der Regel das eigentliche Rechenzentrum (also der Maschinenraum) gehört, sowie das Datenträgerarchiv und die Steuerung der Datenfernübertragungseinrichtungen, aber nicht verhindert wird, daß Daten auf Datenträgern außerhalb dieser Sicherheitsbereiche weiterverarbeitet werden, ohne weiterhin geschützt zu sein. Vergessen wird dabei auch, daß Terminals mit zum Teil hoher Berechtigungsstufe außerhalb jeder Sicherheitszone aufgestellt sind und so fast frei zugänglich sind. Das gleiche gilt natürlich für Ausdrucke und Micro-fiches.

Hier werden Regelungen erforderlich, die eine besondere Absicherung des Terminals beinhalten, oder die Terminals mit hohen Berechtigungen müssen in einer eigenen Sicherheitszone installiert werden. Der Bereich, in dem Micro-fiches aufbewahrt werden, muß ebenfalls besonders abgesichert werden.

Wichtig für hohe Sicherheitsanforderungen ist auch, daran zu denken, daß das System nicht nur die Zugänge protokolliert, sondern auch die Ausgänge, und automatisch jede weitere Zugangsberechtigung von Personen sperrt, für die zuvor zwar ein Zugang aber kein ordnungsgemäßer Ausgang registriert wurde. Angemessen können auch Systeme sein, die nicht nur die Berechtigung prüfen, sondern eine zeitliche Einschränkung beinhalten, so daß z. B. ein Mitarbeiter der Frühschicht während der Nachtschicht nicht zugangsberechtigt ist.

Weiterhin ist es bei sehr sensiblen Daten erforderlich, daß neben jeder technischen Zugangsregelung das vier-Augen-Prinzip gewährleistet bleibt. So sollte demjenigen, der mit Datenträgern arbeitet die Berechtigung zum Betreten des Datenträger-Archivs fehlen.

Alle Datenträger, auf denen personenbezogene Daten gespeichert sind, erfordern eine Datenträgerverwaltung, unabhängig von der Größe oder der Speicherkapazität. Hierzu gibt es wiederum verschiedene Möglichkeiten: Manuelle Systeme, wie z. B. fortlaufende Listen, Karteien, oder

maschinelle Systeme, die so weit gehen, daß sie von der Namensgebung bis zur Löschung nach dem Verfallsdatum und zur Freigabe der Datenträger automatisch arbeiten.

Nicht zu vergessen sind auch die Datenträger, deren Sicherung häufig von den Datenverarbeitern vernachlässigt wird, wie z. B. Papier, und Microfiche. Hierbei sollte festgelegt sein, wer z. B. welche Auswertungen erhält, was nach der Nutzung mit dem Datenträger zu geschehen hat usw. (Vernichtung von Altpapier z. B.).

Immer wieder mußte beanstandet werden, daß Magnetbänder – besonders häufig aber Disketten – überhaupt nicht verwaltet werden. Häufig löst die Frage nach Anzahl und Belegung der Datenträger nur Schweigen aus. Bei einer ordnungsgemäßen Datenträgerverwaltung ist ohne Aufwand festzustellen, mit welchen Daten dieser Datenträger belegt ist, welches Programm verantwortlich war und welche Auswertungen aus ihm vorgenommen werden, ebenfalls, was mit ihm nach dem Freigabedatum zu geschehen hat. In einer gut organisierten Datenverarbeitung ist darüber hinaus jederzeit feststellbar, wieviele Datenträger belegt sind, wie viele frei sind und welche fehlen. Weiterhin gehört zur Abgangskontrolle das Festlegen der Bereiche, in denen sich Datenträger befinden dürfen. Hierzu waren ebenfalls viele Beanstandungen auszusprechen. Außerhalb des Archivs dürfen nur ganz wenige Bereiche bestimmt sein, in denen Datenträger aufbewahrt werden. Diese Bereiche können nur der Platz am Gerät, an dem sie gelesen und beschrieben werden und das Archiv sein. Dazu zählt auch ein bestimmter Bereich für die Auslagerung.

Besonderes Augenmerk ist auch auf die in § 2 Abs. 1 Nr. 4 BDSG definierte vierte Phase der Datenverarbeitung zu legen, nämlich auf das Löschen von Daten. Sollen und dürfen Daten gelöscht werden, dann ist sicherzustellen, daß sie nicht nur logisch sondern auch physisch gelöscht sind. Besonders wichtig ist dieser Punkt bei jeder Form des Datenträgeraustauschverfahrens.

8.2
Zugriffssicherheit

8.2.1
Begriffsbestimmung

Unter Zugriffssicherheit kann man vereinfachend Benutzer-, Eingabe-, Speicher- und Zugriffskontrolle gemäß der Anlage zu § 6 BDSG zusammenfassen. Mit dieser Zusammenfassung vermeidet man die Überschneidungen der Begriffe und orientiert sich stärker an den Arbeitsabläufen. Bei der Zugriffssicherheit muß man aber eindeutig unterscheiden zwischen Zugriffen, die nur das Lesen ermöglichen und solchen, die Datenbestände erstellen (schreiben) bzw. verändern sollen.

8.2.2
Sicherung mit Benutzerkennung (Passwort/password)

Obwohl das Passwort seit langem als Sicherungsmittel eingesetzt wird, ist sein Einsatz häufig unbefriedigend. Das Passwort ist immer noch die häufigste und in vielen Fällen die alleinige Sicherung, so daß es erforderlich ist, darauf einzugehen.

Häufig ist das Passwort im Klartext in der EDV-Anlage gespeichert. System dumps (vormals Kernspeicherausdrucke) ermöglichen es eigenen Mitarbeitern und Service-Technikern, sämtliche Passwörter festzustellen. Daher sollte zumindest in den Fällen, in denen das Betriebssystem eine Verschlüsselung der Passwörter vorsieht, diese Möglichkeit auch genutzt werden.

Seit die PCs auch gleichzeitig als Arbeitsstationen an den Zentralrechner (host) angeschlossen werden, greift die Unsitte um sich, das Passwort und die ganze Anmeldeprozedur im PC einzuprogrammieren und nur noch über eine Funktionstaste aufzurufen. In diesen Fällen hat eine aufwendige Anmeldeprozedur keinerlei Schutzwirkung, sie könnte deshalb ebenso entfallen.

Die Vergabepraxis für die Passwörter ist ein weiterer Unsicherheitsfaktor. Im Idealfall wird ein Passwort einmal vergeben und ein neuer Benutzer muß es sofort bei seiner ersten Tätigkeit am Bildschirm und dann erneut in

festgelegten Zeitabständen selbst ändern. Ein Musterbeispiel hierfür ist die bekannte Passwortvergabe beim Bildschirm-Text-System.

In der Praxis ist diese für den Änderungsdienst vorteilhafte Lösung leider selten anzutreffen. Einige Sicherungssysteme gestatten zumindest eine dezentrale Passwortvergabe. Sie ermöglichen vor allem in Großbetrieben einen schnellen Änderungsdienst und bewirken damit mehr Sicherheit. Trotz vielfachen Hinweisen wird das Passwort häufig noch mit wenig Bedacht gewählt. Der Eigenname oder der Geburtstag ist z. B. sicher nicht die richtige Passwortwahl.

Die Zuteilung von Berechtigungen für die einzelnen Passwörter erfordert teilweise einen erheblichen Arbeitsaufwand. Hierbei bestehen die beiden entgegengesetzten Ansatzpunkte,

1. alles zu verbieten, was nicht ausdrücklich erlaubt oder
2. alles zu erlauben, was nicht verboten wurde.

Die letztere Vorgehensweise hat den Nachteil, daß bei Einführung schutzwürdiger neuer EDV-Verfahren und Dateien vergessen werden kann, erforderliche Verbote zu veranlassen. In der Folge haben dann auch unberechtigte Personen Zugriff auf schützenswerte Dateien. Prinzipiell ist es deshalb sicherer nach der ersten Methode erst einmal sämtliche Zugriffe, bis auf die erlaubten Ausnahmen, für unzulässig zu erklären.

Nach dem Prinzip der Verhältnismäßigkeit kann es aber, bei einer sehr geringen Anzahl schützenswerter Daten, auch sinnvoll sein, nach der zweiten Methode alles zu erlauben und nur einzelne Zugriffe zu verbieten. Der Verwaltungsaufwand wird in diesem Fall beträchtlich gesenkt. Im Idealfall würden, je nach generellem Bedarf, beide Möglichkeiten der Berechtigungsvergabe wahlweise genutzt. Dies könnte durch einen Schalter in der Systemgenerierung einheitlich ermöglicht werden.

8.2.3
Sicherung der Systemberechtigung

Die Personen, die das System generieren und die Sicherungs-Software installieren, entziehen sich bei dem heutigen Stand der Technik einer vollständigen Kontrolle. Das gleiche gilt für die Systemtechniker, die mit dem technischen Service an den EDV-Anlagen betraut sind.

Zu beobachten ist eine starke Spezialisierung im Systembereich, wobei der Einzelne in seinem Bereich als einziger Experte häufig noch nicht einmal nach dem Vier-Augen-Prinzip kontrolliert werden kann.

Es muß deshalb oberstes Gebot sein, daß möglichst alle Aktivitäten protokolliert und damit zumindest nachträglich auch geprüft werden können. Die Vollständigkeit der Protokollierung und die Sicherung der erstellten Protokolle sind hierfür die Grundvoraussetzung. Gerade diese vollständige Protokollierung wird aber bei Überprüfungen nicht in allen Fällen angetroffen. Bei der besonderen Schutzwürdigkeit des Systembereichs ist in jedem Fall, soweit das irgendmöglich ist, das Vier-Augen-Prinzip anzustreben. Dies bringt dem Unternehmen auch zusätzliche Vorteile für die personelle Verfügbarkeit bei Ausfallsituationen, wie Urlaub, Krankheit oder Kündigung.

Es versteht sich von selbst, daß der Systembereich insgesamt und auch seine Teilbereiche (z. B. Datenfernverarbeitungssteuerung, Datenbanken) durch besondere Maßnahmen gesichert werden muß. Dies geschieht in aller Regel durch die besondere Berechtigung einzelner Terminals und die Vergabe besonderer Berechtigungscodes – Benutzerkennung (User-Id), Passwort –.

8.2.4
Sicherung der Schreib-/Leseberechtigung

In vielen Fällen wird überhaupt keine differenzierte Berechtigung vergeben. Insbesondere im Falle der Schreibberechtigung kann das eigentlich nicht im jeweiligen Unternehmensinteresse liegen, da durch Unachtsamkeit sehr schnell wertvolle Datenbestände verlorengehen können. Das Interesse des Unternehmens deckt sich hier – Kleinstbetriebe ausgenommen – vollkommen mit der datenschutzrechtlichen Forderung, daß Berechtigungen nur insoweit vergeben werden dürfen, wie sie für die Aufgabenerfüllung benötigt werden.

Man scheut aber häufig den dafür nötigen hohen Verwaltungsaufwand. Im Großbetrieb läßt sich mit einer Dezentralisierung der Berechtigungsvergabe sehr viel erreichen, denn wer „seine" Daten unbedingt für die tägliche Arbeit benötigt, hat auch ein ganz persönliches Interesse an deren Schutz. Versehentliche Pannen, bei denen Daten verlorengehen und den betroffenen Mitarbeitern erhebliche Mehrarbeit verursachen, haben dann gelegentlich eine größere Wirkung als die Forderungen des betrieblichen Datenschutzbeauftragten.

8.2.5
Eingabekontrolle

Wenn wie vorstehend ausgeführt, nur ein ausdrücklich Berechtigter Daten eingeben darf, so muß diese Eingabe auch nachträglich kontrollierbar sein. Dies kann im eingegebenen Datensatz oder in einer separaten log-Datei geschehen.

Der Eingabe-Nachweis im Datensatz ist insgesamt vorteilhaft, weil ohne Zugriff auf log-Dateien oder Listen sofort festgestellt werden kann, wer was wann eingegeben hat. Bei Änderungen dieses Datensatzes wird es jedoch problematisch, weil dann die Eingabe für jedes einzelne Datenfeld festgehalten werden müßte. Dies führt dazu, daß bei Stammdaten, die öfter einer Änderung unterworfen sind, die Eingabe in der Regel nicht im Datensatz dokumentiert ist. In vielen Fällen – insbesondere in der Lohn/Gehalts-Datenverarbeitung – werden bei allen Daten die Eingaben und die Bedienerkennung in einer Liste ausgedruckt.

Die Änderung ist häufig nur im Vergleich mit dem ursprünglichen Datensatz erkennbar. Wünschenswert wäre, wenn beispielsweise in vorhandenen Kontrollausdrucken das einzelne geänderte Datenfeld kenntlich gemacht würde. Bei Prüfungen wird von der Aufsichtsbehörde eine derartige Änderungsdokumentation positiv bewertet, weil schneller feststellbar ist, wann ein gegebenenfalls falsches Datum übernommen wurde. Für die Arbeitsabläufe bieten solche detaillierten Änderungsdokumentationen ebenfalls Erleichterungen, weil Suchvorgänge entfallen bzw. verkürzt werden können.

In einem geprüften Fall – in dem ausschließlich sensible Schuldnerdaten gespeichert waren – wurde die Eingabebekennung des Bedieners gelöscht, wenn eine Änderung vorgenommen wurde. Der Bediener für die Ersteingabe war dann nur feststellbar, wenn der Datensatz vorher ausgedruckt wurde. Dies ist auch aus betrieblichem Interesse nicht akzeptabel, da sich niemand für die Daten verantwortlich fühlt. Die Aufsichtsbehörde hat diese Form der Dokumentation beanstandet, weil die Eingabekontrolle nicht lückenlos gewährleistet war.

8.2.6
Kontrollen der Arbeitsvorbereitung

Positiv bewertet wird die Trennung von Arbeitsvor- und Arbeitsnachbereitung, weil hierdurch das Vier-Augen-Prinzip gewährleistet wird.

Die Arbeitsvorbereitung kann Verarbeitungsaufträge von Unberechtigten abweisen.

Ebenso kann sie die problematische Verwendung von Passwörtern in Stapel-(batch) Verarbeitungsaufträgen überwachen. Hierbei ist ein hohes Maß an Vertraulichkeit geboten, da bereits aus dem Verarbeitungsauftrag (Job-Control) das Passwort ersichtlich ist.

Soweit es die Arbeitsvorbereitung selbst betrifft, ist wünschenswert, daß diese keinen direkten Zugang zu dem Datenträgerlager und dem Rechenzentrum hat. Bei den Datenträgern würde auch ausreichen, wenn diese von der Datenträgerverwaltung direkt in das Rechenzentrum geliefert werden. Wenn statt dessen in vielen Fällen die aktuell zu bearbeitenden Datenträger über die Arbeitsvorbereitung in das Rechenzentrum gelangen, ist dies eine zusätzliche Kontrolle. Damit läßt sich z. B. verhindern, daß Datenträger-Verwalter und Konsoloperater im Rechenzentrum gemeinsam nicht autorisierte Verarbeitungen durchführen.

In den geprüften Unternehmen kontrollierte dann auch häufig die Arbeitsvorbereitung die Art und Menge der zu verarbeitenden Datenträger. Man wollte verhindern, daß batch-Arbeitsabläufe gestartet werden, ohne

daß das erforderliche Band zur Verarbeitung beim Band-Operator zur Verfügung steht.

In einigen Betrieben werden die Arbeitsabläufe von der Arbeitsvorbereitung für einen ganzen Arbeitstag fest vorgegeben und dann von einer speziellen Software automatisch gestartet. Menschliche Eingriffe sind dann nur in den Änderungsfällen nötig. Diese Vorgehensweise wird bei einer Überprüfung positiv bewertet, weil hierbei zwangsläufig planvoll und sehr übersichtlich gearbeitet wird und man damit über besser kontrollierbare Abläufe verfügt.

8.2.7
Protokollierung der Systemaktivitäten

Im Regelfall sollte ein unberechtigter Zugriff auf personenbezogene Daten schon vorher abgewehrt werden. Kennern gelingt es trotzdem immer wieder, aufgebaute Sicherheitsschranken zu überwinden. Dies mag in Einzelfällen relativ spielerisch beginnen. So versuchte während einer von der Aufsichtsbehörde durchgeführten Prüfung offensichtlich ein anderes Unternehmen, das möglicherweise seine Datenverarbeitungsanlage gerade neu erworben hatte, in die gerade geprüfte Datenverarbeitungsanlage einzudringen. Die Kenntnis des „Eindringlings" über den Datenverarbeitungs-Partner mit gleicher Technik stammte dabei nach Ansicht des geprüften Unternehmens von der Kundenreferenzliste, die als Empfehlung beim Kauf vorgelegt worden war. Im konkreten Fall wurde der Versuch, sich in das geprüfte Unternehmen einzuwählen und einzudringen, automatisch abgewiesen. Gelingen derartige unberechtigte Zugriffe auch auf personenbezogene Daten, läßt sich das nur aufklären, wenn die gesamten Systemaktivitäten vollständig protokolliert werden.

Im Regelfall sind diese Protokolle und darüber hinaus log-Dateien, für den Wiederanlauf bei einer technischen Störung gedacht. Selbst für eine reine batch Datenverarbeitung ohne Datenfernverarbeitung sind diese Aufzeichnungen erforderlich, obwohl hier die Gefährdungslage erheblich geringer ist, weil der Kreis der Berechtigten besser überschaubar und kontrollierbar ist.

Negativ aufgefallen ist bei den vorgefundenen Protokollen, daß zwar das gestartete Programm oder die Transaktion in aller Regel erkennbar war, nicht jedoch welche Dateien eröffnet, geschlossen, gelesen oder beschrieben wurden. Dies ließ sich erst dann feststellen, wenn man in das jeweilige Programm und die zugehörigen Prozeduren und Ablaufbeschreibungen einsah. Eine direkt zusammenhängende Protokollierung (mindestens open und close) der jeweils verarbeiteten Dateien ist aber in jedem Fall vorzuziehen, weil

- je nach Parameter-Steuerung eine Einzelverarbeitung unterschiedlich ablaufen kann,
- die Aktualität und damit die richtige Aussagefähigkeit nur dann in jedem Fall gegeben ist.

Widerstände gegen diese Protokollierung bestehen vor allem deshalb, weil hierdurch die Verarbeitungsabläufe verlangsamt werden. Je nach Betriebssystem wird ein nicht unerheblicher Teil der Datenverarbeitungskapazität für die Protokollierung benötigt. Deshalb hatten dann auch einige geprüfte Rechenzentren die Protokollierung der Dateizugriffe bei der Systemgenerierung ausgeschlossen.

8.2.8
Prüfung der Systemaufzeichnungen

Kontrollaufzeichnungen sind nur dann sinnvoll, wenn sie auch systematisch – und sei es auch stichprobenweise – ausgewertet werden. In einem Fall hatte ein Rechenzentrumsleiter ein sehr umfangreiches Konsolprotokoll „vollständig" geprüft und das letzte Blatt zum Nachweis der Kontrolle unterschrieben. Eine derartige Kontrolle war von vornherein wenig glaubhaft, weil es kaum möglich ist, das Konsolprotokoll eines großen Rechenzentrums in angemessener Zeit „vollständig" zu prüfen. Auch im geschilderten Fall handelte es sich ausschließlich um die Prüfung entstandener Fehlersituationen. Darüber hinaus sollten aber aussagefähige, gründliche Stichproben vorgenommen werden. Die Stichprobe garantiert durch ihre Zufälligkeit, daß kein geschlossenes Bild über die

Arbeitsleistung einzelner Mitarbeiter ohne deren Einwilligung oder die Beteiligung des Betriebsrats entsteht. Wenn allerdings ein einzelner Mitarbeiter auch bei Stichproben immer wieder auffällig wird, muß sich die Geschäftsleitung die Frage der datenschutzrechtlichen Zuverlässigkeit des Mitarbeiters stellen und ihm gegebenenfalls andere Aufgaben zuweisen.

Eine systematische maschinelle Auswertung von Kontrollaufzeichnungen ist ebenfalls wünschenswert, dies sollte aber auf die Situation und nicht auf den Mitarbeiter bezogen geschehen. Bei zahlreichen Fehlersituationen (z. B. Systemabbrüche) wird man allerdings zwangsläufig auch auf den Mitarbeiter zukommen, wenn er als Einzelperson häufig der Verursacher war. Beispiele für Auswertungen sind:

- Prüfung der zeitlichen Folge und deren Unterbrechungen in den Aufzeichnungen,
- die Auflistung der Systemabbrüche und der Verarbeitungszustände, die zum Abbruch führten,
- Liste der Fälle, in denen eine Schreibsperre übergangen wurde,
- Liste der falschen Passwort-Eingaben,
- Liste der produktiven Datenverarbeitung mit Testdateien/Testbibliotheken usw.

Derartige Kontrollauswertungen bieten, vergleichbar einem Sicherheitsnetz, die Möglichkeit, unberechtigte Zugriffe auf das Datenverarbeitungs-System, die vom System nicht automatisch als unberechtigt erkannt wurden, festzuhalten und zu bewerten. In Einzelfällen offenbart dann beispielsweise der Abgleich der Urlaubsliste mit den Systemaktivitäten der Mitarbeiter, daß Mitarbeiter, die gar nicht anwesend sind, trotzdem noch mit Aktivitäten ausgewiesen werden. Bei einer unbefugten Verarbeitung personenbezogener Daten ist es der Urlauber dann in keinem Fall gewesen.

Dieses einfache Beispiel legt sehr schnell Schwachstellen offen. Die beispielhaft angeführte Überprüfung sollte andererseits nicht dazu führen, umgekehrt zu kontrollieren, wer alles am Arbeitsplatz war und Systemaktivitäten hätte verursachen müssen.

Die Auswertung von Systemaktivitäten wird immer in Grenzbereiche stoßen, in denen der Mitarbeiter sich persönlich betroffen fühlt. Solange man aber eine systematische Auswertung vermeidet, die sich auf die gesamte Arbeitszeit eines Mitarbeiters erstreckt, läßt sich eine derartige Datensicherungsmaßnahme im Interesse eines wirksamen Datenschutzes vertreten.

8.3
Übermittlungssicherheit

8.3.1
Wählleitungen/Standleitungen

Bei den Prüfungen konnte von Jahr zu Jahr ein verstärkter Einsatz der Datenfernübertragung festgestellt werden. Anfangs beschränkte sich dieser Einsatz auf den reinen Dateitransfer. Mittlerweile wird in vielen Fällen der on-line Dialog über Wähl- bzw. Standleitungen verwirklicht.

Es würde den Rahmen dieses Berichts überschreiten, eine ausführliche Stellungnahme über die Sicherheitsaspekte der verschiedenen DFÜ-Verbindungen abzugeben. Insgesamt erscheinen die Standleitungen mit ihren fest definierten Endpunkten und den damit eindeutig identifizierbaren Dialogpartnern sicherer zu sein. Eine Wählleitung ist demgegenüber immer für denjenigen am sichersten, der diese Verbindung mit der Anwahl des Partners aufbaut. Ebenso sicher sind Wählverbindungen mit automatischem Rückruf. Letzteres fiel positiv bei einer technischen Wartungsfirma auf, die damit ihrem Kunden garantierte, daß kein Unbefugter die Fernwartung durchführte.

Größere Serviceunternehmen bieten ihren Kunden das gesamte Spektrum von Datenfernübertragungs-Verbindungen an. Ausschlaggebend für die jeweilige Leitungswahl sind dann in der Regel die Wünsche des Kunden und die Kosten-Nutzen-Aspekte für das jeweilige Anforderungsprofil. Eine Auswahl unter Datenschutzgesichtspunkten fand nach den Feststellungen der Aufsichtsbehörde nicht statt.

8.3.2
Sicherheit durch Datenverschlüsselung

Bisher wurde nur ein konkreter Fall von Datenverschlüsselung bekannt. Die Daten werden aber offensichtlich weniger wegen ihrer datenschutzrechtlichen Schutzwürdigkeit verschlüsselt, sondern weil es sich um finanzielle Transaktionsdaten handelt und bei unbefugten Zugriffen große Geldbeträge weltweit verloren gingen.

Beim dem heutigen technischen Standard und den heutigen Kosten kann eine Datenverschlüsselung sicher noch nicht allgemein gefordert werden. Es wäre jedoch durchaus möglich, nur die Anmeldeprozedur oder das Passwort bereits verschlüsselt zu senden, ohne daß damit ein größerer Zeit- und Kostenaufwand verbunden wäre. Wenn dann in diese Verschlüsselung variable Teile des Dialogs eingearbeitet würden, wäre es für einen unbefugten Dritten sehr schwer, u. U. sogar unmöglich, das Passwort in einer abgehörten Nachricht zu erkennen. Hierzu liegen bisher aber aus der Prüfungspraxis keine praktischen Erfahrungen vor.

8.4
Ferndiagnose und Fernwartung

Eine Ferndiagnose eröffnet die Möglichkeit, über eine Datenleitung mit Hilfe eines Service-Computers direkt in das System des Anwenders einzugreifen und z. B. Fehler zu erkennen.

Der „Diagnose-Computer" kann auf verschiedene Art und Weise tätig werden:

- Er ist mit Daten gespeichert, die eine Interpretation der Fehlermeldung ermöglichen und diese einem befugten Personenkreis sichtbar macht.
- Der Service-Computer enthält bestimmte Daten, mit deren Hilfe er den angewählten Anwender-Computer überprüfen kann. Dabei werden evtl. vorhandene Fehler angezeigt.

Beide Möglichkeiten werden in der Praxis angewendet. Sie richten sich nach Hersteller und Art der Anlage. In beiden gezeigten Fällen besteht die Möglichkeit, daß entweder

a) die Behebung des Fehlers durch den Service-Computer vorgenommen wird (1. durch den Techniker, 2. durch den Computer), oder

b) die Behebung vor Ort beim Anwender-Computer durch den Techniker durchgeführt wird.

Fernwartung geht darüber hinaus einen Schritt weiter und bietet die Möglichkeit, Daten oder Befehle über eine Datenleitung direkt im Anwender-Computer auszutauschen.

Dabei ergeben sich ebenfalls verschiedene Möglichkeiten der Ausführung:

- Der fernwartende Computer erzeugt Meldungen an den Techniker und läßt diese vom Anwender-Computer in dessen Technik-Bereich einspeichern; dieser Bereich wird dann vom Techniker vor Ort gelesen.
- Der fernwartende Computer erneuert Teile im Anwender-Computer; d. h., es können natürlich nur Daten bzw. Adressen, Weichen oder Programmteile ausgetauscht werden.
- Es besteht auch die Möglichkeit, Programmteile auf der Ebene des Anwenders auszutauschen, wie z. B. der Austausch einer Steuerberechnungsformel im Programm Gehaltsabrechnung. Hierbei wird der in der Programmbibliothek vorhandene Teil der Steuerberechnung über eine Datenfernverarbeitungsverbindung mit dem neuen Teil ausgewechselt.

Die häufig noch anzutreffende herkömmliche Methode der Wartung oder Fehlerdiagnose bei Computern ist im Gegensatz zu den oben beschriebenen Formen folgende:

Der Techniker arbeitet mit speziellen Programmen, die wie im Beispiel der Diagnose oben beschrieben, Fehlermeldungen des Computers, hier allerdings vor Ort, interpretieren.

Die Fernwartung ist heute noch so organisiert, daß der Anwender tätig werden muß, um die Verbindung herzustellen. In der Regel wählt er über seine Telefonanlage den Service-Computer an und verbindet dann den Service-Computer mit seinem Computer. Dann erst kann der Service-Computer seine Arbeit beginnen. Um das Eindringen unberechtigter Datenverarbeitungssysteme in die so entstehenden Verbindungen zu verhindern, wird mit sogenannten Security-Modems gearbeitet. Diese Geräte, die für jede Leistungsverbindung erforderlich sind, bieten nach den heutigen Erkenntnissen eine ausreichende Sicherheit.

Neben allgemeinen Anfragen zur Problematik der Fernwartung und den Erkenntnissen bei durchgeführten Regelüberprüfungen, mußte die Aufsichtsbehörde in diesem Bereich dem System eines Unternehmens besondere Aufmerksamkeit zukommen lassen, das sich auf die Automatisierung der Verwaltungstätigkeiten in Arztpraxen spezialisiert hat. In diesem speziellen Fall vertreibt das Unternehmen sowohl die Hardware wie auch die Software und bietet gleichzeitig hierzu die Wartung an.

Dabei wird sowohl die Ferndiagnose wie auch die Fernwartung durchgeführt. Das umfassende Angebot zur Pflege des Systems bietet sich auch deshalb an, weil in Arztpraxen in der Regel kein spezialisiertes Datenverarbeitungspersonal vorhanden ist. So werden Veränderungen in Programmen hinsichtlich der Verarbeitung vom Hersteller erstellt, ausgetestet und im Zuge der Wartung dem Anwender zur Verfügung gestellt. Andererseits kann der Anwender bei auftretenden Problemen jederzeit über sein Telefon eine Verbindung von seiner Computer-Anlage zu dem Service-Rechner des Herstellers herstellen. Bei dieser Verbindung hat das Wartungsunternehmen u. a. auch die Möglichkeit, personenbezogene Daten oder Daten, die der ärztlichen Schweigepflicht unterliegen, zur Kenntnis zu nehmen. Dabei gibt es eigentlich keinen gravierenden Unterschied, ob der Techniker vor Ort diese Daten zur Kenntnis nimmt oder ob die Daten erst einmal über die Datenleitung zu dem Techniker gelangen.

Aber gerade der Weg über die Datenleitung zum Techniker wird von einigen Datenschutzaufsichtsbehörden als besonders problematisch bezeichnet. Es mag die Vermutung dahinterstehen, daß der Techniker vor Ort durch den Anwender besser kontrollierbar ist.

Dieser Auffassung ist jedoch entgegen zu halten, daß kein Anwender heutzutage mehr in der Lage ist, die besonderen Verfahren zur Wartung, die jeder Techniker benutzen muß, zu kennen. Dadurch, daß die Wartung nicht vor Ort, sondern entfernt stattfindet, ergeben sich nicht mehr Möglichkeiten im Hinblick auf die Kenntnisnahme von Daten.

Festzustellen bleibt, daß die Möglichkeit, einen Fehler zu diagnostizieren sowohl vor Ort als auch im Rahmen der Fernwartung vorhanden sein muß. Daraus ergibt sich zwangsläufig, daß ein Wartungsunternehmen in beiden Fällen uneingeschränkte Zugriffsmöglichkeiten haben muß. Hinzu kommt, daß nicht nur die Software gewartet wird, sondern auch die Hardware und daß in dem Augenblick, wo ein Techniker in den Hardware-Bereich eindringt, jede Absicherung des Software-Bereichs unwirksam wird.

Daraus entsteht das Problem, daß besonders im geschilderten Beispiel, aber auch bei allen Rechenzentren, die mit medizinischen Daten arbeiten, die gemäß § 203 StGB der ärztlichen Schweigepflicht unterliegen, bei Eintritt des Wartungsfalles diese Daten möglicherweise Dritten (Techniker) offenbart werden, also Personen, die nicht der ärztlichen Schweigepflicht unterliegen.

Da ein Verbot der Vornahme von Wartungstätigkeiten nicht realisierbar ist, bietet eine ansatzweise Lösung dieses Problems nur die Möglichkeit, die Wartung in eine feste Organisation einzuschließen und besondere Kontrollmöglichkeiten zu schaffen, die einen Mißbrauch verhindern helfen.

Kontrollmöglichkeiten sind:

a) Eine vollständige Protokollierung aller Aktivitäten des Systems während der Fernwartung (wobei es keine Möglichkeit zur Unterbindung bzw. zum Eingriff in das Protokoll geben darf),

b) Beginn der Wartungstätigkeit nur auf Antrag des „Herrn der Daten"

c) Sicherheit der Verbindungsleitungen z. B. durch Security-Modems.

Es muß allerdings betont werden, daß die Untersuchungen der Aufsichtsbehörde noch nicht beendet sind und daß gerade in diesem sensiblen Bereich noch weitergehende Erfahrungen zu sammeln sind.

8.5
Programmsicherheit

8.5.1
Programmentwicklung

In vielen Fällen wird der sogenannte Organisationsprogrammierer eingesetzt. Da dieser ein weites Tätigkeitsspektrum abdeckt, ist dann nicht exakt feststellbar, zu welchem Zeitpunkt die Analyse und Programmvorgabe erstellt wurde. Lediglich in einigen Großbetrieben wurden die einzelnen Programm-Entwicklungsstadien kontrolliert und dokumentiert.

Allgemein war die Programmdokumentation sowohl im Programm selbst als auch in den entsprechenden Programmakten unbefriedigend.

In vielen Fällen wurden bei der Programmentwicklung Strukturen vorgegeben, die das jeweilige Programm übersichtlich und einheitlich gestalten sollten. Es wurden hierbei die unterschiedlichsten Lösungsansätze vorgefunden, wobei die Nutz-Effekte – mehr Übersichtlichkeit, bessere Revisionsfähigkeit, Wartungsfreundlichkeit usw. – sich nicht so sehr aus der einzelnen Methode als aus der einheitlichen und konsequenten Anwendung eines Strukturierungs- und Standardisierungs-Verfahrens ergaben.

Unverständlich ist, daß noch immer völlig unübersichtliche und unstrukturierte Programme geschrieben werden. Bei Assembler-Programmen (Assembler = maschinenorientierte Programmiersprache) hat man inzwischen hinzugelernt und dokumentiert die einzelnen Arbeitsschritte im Programm selbst. Bei älteren, schlechter dokumentierten Assembler-Programmen konnte dagegen in einigen Fällen - auch im Eigeninteresse des geprüften Betriebes - nur eine völlige Neuerstellung des jeweiligen Programmes empfohlen werden.

Es ist zu wünschen, daß sich die Ansicht durchsetzt, daß mit einem übersichtlich entwickelten und geschriebenen Programm nicht nur die datenschutzrechtliche Sicherheit, sondern auch die Verarbeitungssicherheit erhöht wird und sich damit die ständige Datenverarbeitungsverfügbarkeit verbessert.

8.5.2
Programmänderung

Ein neu geschriebenes Programm kann kurz nach seiner Entstehung noch unbedenklich sein. Durch später vorgenommene Änderungen verliert es dann u. U. diesen Charakter sehr schnell.

Es wurde bei den Prüfungen häufig festgestellt, daß die Dokumentation der Programmänderungen mangelhaft war. Dies ist um so unverständlicher, weil gerade hier viele Fehler passieren, die häufig in der mangelnden Dokumentation ihre Ursache haben.

Selbst ein guter Programmierer weiß nach einigen Jahren nicht mehr, warum er an einigen Stellen im Programm beispielsweise einen Schalter eingesetzt hat. Möglicherweise glaubt er es noch genau zu wissen und führt dann die Änderung falsch durch.

Eine gute Dokumentation ist also sowohl für den ursprünglichen Autor als auch für einen späteren fremden Programmierer wichtig.

Die unzulänglichste Änderungsdokumentation, die bei einer Prüfung angetroffen wurde, betraf ein bereits mehrfach geändertes großes Gehaltsprogramm, dessen letzte Änderung man nur durch einen losen Schmierzettel in der Programmliste dokumentiert hatte. Mangels Dokumentation konnte nicht festgestellt werden, ob vielleicht noch ohne Test das geänderte Programm für die Produktion verwendet (Compile, Link und Go) wurde. Ausschließen ließ sich das in diesem Fall nicht.

Aufgrund des Hinweises, daß außer der Datenschutzaufsichtsbehörde weder der Auftraggeber noch das Finanzamt dieses Verhalten billigen dürften, ist dann für zukünftige Änderungen eine andere Arbeitsweise in Aussicht gestellt worden. Allein mit datenschutzrechtlichen Argumenten

wäre eine Einflußnahme bei der derzeitigen Gesetzeslage, die der Aufsichtsbehörde keine Eingriffsbefugnis gibt, noch schwerer gewesen.

Datenschutzrechtliche Forderungen würde es durchaus unterstützen, wenn zukünftig auch der Auftraggeber eines derartigen Service-Unternehmens sich einmal stichprobenweise von für ihn wichtigen Programmen – z. B. Gehalt/Lohn – die Änderungsdokumentation vorlegen ließe. Nach den Feststellungen der Aufsichtsbehörde sind durch solche Einblicke durchaus auch Rückschlüsse auf die Qualität der Datenverarbeitungs-Dienstleistung insgesamt möglich.

8.5.3
Programmendabnahme

Bevor ein neues bzw. geändertes Programm in die Produktion übernommen wird, sollten sowohl das Programm als auch die zugehörigen vollständigen Testunterlagen nochmals von mindestens einer zweiten Person (4-Augen-Prinzip) kontrolliert werden. Neben dem datenschutzrechtlichen Sicherheitsgewinn kann dadurch gewährleistet werden, daß der Programmauftrag/Änderungsauftrag erfüllt wurde, die Tests umfassend waren und die Testunterlagen vollständig sind. Ebenso läßt sich gewährleisten, daß die Dokumentation der Programmbeschreibung und die Dokumentationen für Arbeitsvorbereitung, Arbeitsnachbereitung, Operating und Benutzer vollständig sind.

Möglichst ein weiterer Mitarbeiter sollte die vorgelegten Programme nochmals übersetzen (Compile und Link) und dieses Programm dann in die Produktionsbibliothek übernehmen. Die Schreibberechtigung für die Produktionsbibliothek sollte hierbei sehr eng ausgelegt werden, weil sonst überhaupt nicht sicher feststellbar ist, welches Programm bzw. welche Programmversion sich in der Produktionsbibliothek befindet. Ein Schutz ausschließlich der Produktionsbibliothek ist allerdings dann hinfällig, wenn nicht gleichzeitig verhindert wird, daß Testbibliotheken für Produktionsarbeiten genutzt werden.

Der hieraus abzuleitende Grundsatz, daß die Daten nur so sicher sein können wie die Programme, die sie verarbeiten, wird zwar anerkannt, entsprechende Maßnahmen und Kontrollen hatten aber nur einige geprüfte Betriebe verwirklicht. Günstig wirkte sich aus, wenn für Test und Produktion getrennte EDV-Anlagen und Dateien benutzt wurden. Man konnte in diesem Fall die Autorisierung des Programmierers auf die Testanlage begrenzen. Selbst einige Kleinbetriebe hatten sich so geschützt, weil sie keinesfalls ihre Produktion gefährden wollten.

8.5.4
Sonderbehandlung von Berichts- und Datei-Generatoren sowie Dienstprogrammen (Utilities)

Problematisch ist, daß jede Anwendung dieser Programme ein neues Programm darstellt, wenn die ursprünglich gewählten Parameter verändert werden.
Im einfachsten Anwendungsfall wäre das Erstellen eigener Programme überflüssig und man würde nur die genannten Programme mit den unterschiedlichsten Parametern einsetzen.

Man kann beispielsweise aus einer Lohndatei mit einem Berichtsgenerator eine Kostenstellen-/Kostenträgerrechnung erstellen. Ebenso läßt sich jedoch mit dem gleichen Programm, aber anderen Parametern, eine Akkord-Leistungsstatistik aufbauen, die nach dem Betriebsverfassungsgesetz mitbestimmungspflichtig wäre. Diese Auswertungen haben datenschutzrechtlich eine völlig unterschiedliche Qualität.

Hier kann man den Betrieb nur verpflichten, zu jeder Auswertung auch die Parameter zu protokollieren. Letzteres wird in der Regel auch durchgeführt, weil nur so Verarbeitungsfehler nachträglich analysiert werden können.

Einige Dienstprogramme (Utilities) und vom Hersteller nicht freigegebene Programme, die ähnlichen Charakter haben, sollten sich möglichst erst gar nicht auf der Produktionsanlage befinden. Läßt sich dies nicht von vornherein vermeiden, so sollten diese Programme besonders geschützt werden und nur einem kleinen Kreis z. B. von Systemprogrammierern zur Nutzung überlassen werden.

Insgesamt bleiben die genannten Programme problematisch, weil insbesondere durch die Verknüpfung mehrerer Dateien neue schutzwürdige Zusammenhänge entstehen können, die vorher nicht näher bedacht wurden.

Genaue Stichprobenkontrollen des Arbeitsergebnisses sind deshalb dringend zu empfehlen. Gerade diese wurden aber in den seltensten Fällen angetroffen.

8.6
Organisationssicherheit

8.6.1
Beschreibung der Verantwortungsbereiche

In vielen Betrieben kleiner und mittlerer Größen wird noch ohne eine genaue Arbeitsplatzbeschreibung gearbeitet. Ein Organigramm, welches die Struktur der Organisation aufzeigt, war ebenfalls nicht sehr verbreitet.

Aus Sicht der Aufsichtsbehörde ist sowohl zur Erreichung des Geschäftszweckes als auch für die datenschutzrechtliche Verantwortung des einzelnen eine übersichtlich beschriebene Arbeitsplatzorganisation erforderlich. Lediglich im Kleinbetrieb kann man teilweise noch ohne eine genaue Arbeitsteilung und Arbeitsbeschreibung auskommen. Je größer dann der Betrieb wird, um so dringlicher wird eine straffe Organisation. Letztlich sollte jeder einzelne Mitarbeiter an seinem Arbeitsplatz in seinem Verantwortungsbewußtsein für datenschutzrechtliche Fragen gestärkt werden. Die einmalige Unterschrift unter die nach § 5 Abs. 2 BDSG abzugebende Verpflichtungserklärung hätte sonst keine länger anhaltende Wirkung auf das Verantwortungsbewußtsein des einzelnen.

8.6.2
Kontrollen des täglichen Arbeitsablaufes

Teilweise wurde dieses Thema schon unter dem Begriff Zugriffssicherheit (8.2) behandelt. Auch hier ist vor allem das Vier-Augen-Prinzip als Maßstab anzusetzen.

Bei der Datenerfassung wurde mehrfach festgestellt, daß keine Kontrollerfassung vorgenommen wurde. Bei sensiblen Daten sollte aber mindestens eine Sichtkontrolle vorgenommen werden.

Die Arbeitsnachbereitung kontrollierte häufig nur, ob eine Arbeit ohne Fehlermeldung abgelaufen war, das eigentliche Arbeitsergebnis wurde aber nur in vereinzelten Fällen stichprobenweise kontrolliert.

In fast allen geprüften Fällen hat man die genauen Endkontrollen dem Datenempfänger überlassen.

In einem Fall hatte noch nicht einmal der Kunde kontrolliert, was er an Daten erhielt, sondern die erstellten Lastschriftbelege einfach an seine Bank weitergegeben. Dort hielt man Kontrollen auch nicht für nötig und erst, als das Geld auf dem Bankkonto des EDV-Servicekunden fehlte, stellte man fest, daß man auch noch die Mitarbeiter einer zweiten Firma – die ebenfalls Servicekunde beim gleichen Service-Rechenzentrum war – mitbezahlt hatte.

In diesem Fall brauchte dann nicht verdeutlicht zu werden, daß fehlender Datenschutz – hier fehlende Endkontrollen – sehr teuer werden kann.

So etwas geschieht auch sehr schnell, wenn keine geeignete Drucksoftware vorhanden ist, die es erlaubt, beim Druck die Papiertrennkanten durch besonderen Aufdruck zu markieren. Der in diesem Fall betroffene Hersteller bietet aber neuerdings gegen Aufpreis die Möglichkeit, die Papiertrennkanten bei Listenende zu bedrucken. Diese Möglichkeiten sind aber seit langem technischer Standard.

8.6.3
Kontrollen der internen Revision

In vielen positiv bewerteten Fällen hat die interne Revision die Fragen des Datenschutzes in ihren Prüfungskatalog mit übernommen.

Die Aufsichtsbehörde hat dann bei ihren Prüfungen die entsprechenden Revisionsberichte eingesehen. Erfreulicherweise greift auch zunehmend

die externe Revision die Datenschutzproblematik auf und führt diesbezügliche Kontrollen durch.

8.6.4
Rolle des betrieblichen Datenschutzbeauftragten bei der Organisationssicherheit

Die Tätigkeit des betrieblichen Datenschutzbeauftragten stellt sich in der Praxis als schwierig dar. In einigen Fällen war er von dem Informationsfluß innerhalb des Betriebes abgeschnitten und konnte deshalb auch nicht effektiv arbeiten.

Seine Dateiübersicht war, ebenso wie die Zusammenstellung der eingesetzten automatisierten Anlagen, häufig unvollständig. Dies beruhte dann in der Regel nicht auf mangelndem gutem Willen, sondern lag wiederum an seiner teilweise isolierten Stellung innerhalb des Betriebes.

Das Fehlen von Übersichten wurde immer dann beanstandet, wenn der Datenschutzbeauftragte noch nicht einmal Zugriff auf entsprechende Unterlagen in der EDV-Organisation und der Programmierung hatte.

Mit der Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungs-Programme ist der Datenschutzbeauftragte im Arbeitsalltag, vor allem im Großbetrieb, überfordert. In positiven Fällen verbesserte der Datenschutzbeauftragte das Kontrollgefüge der täglichen Arbeitsabläufe und führte selbst Stichproben durch. Häufig war er aber bei den Einzelkontrollen auf die Unterstützung anderer Mitarbeiter angewiesen.

Die Schulung der Mitarbeiter fand in vielen Fällen überhaupt nicht statt. Die Aufsichtsbehörde hat dann auf regelmäßigen Schulungen bestanden. Einige Datenschutzbeauftragte haben hierfür auch sehr übersichtliche Schulungsunterlagen ausgearbeitet.

Die Mitwirkung des Datenschutzbeauftragten bei der Personalauswahl ist bei den geprüften Unternehmen umstritten. Hauptargument war, daß man wohl kaum bereit sei, schon aus eigenem Interesse einen als unzuverlässig erkannten neuen Mitarbeiter einzustellen. Als Kompromiß, vor allem für Großbetriebe, hat die Aufsichtsbehörde vorgeschlagen, daß der Datenschutzbeauftragte zumindest kurze Richtlinien für die Einstellung neuer Mitarbeiter ausarbeitet, die dann bei der Prüfung der Bewerber mit berücksichtigt werden sollen.

8.7
Personal-Computer

Immer wieder, sowohl bei Einzelanfragen von betrieblichen Datenschutzbeauftragten als auch auf deren Tagungen wurde die Datenschutzaufsicht mit dem Problem von Datenschutz und Datensicherung bei der Benutzung von Personal-Computern (PC's) konfrontiert.

Am häufigsten wird die Frage nach der Kontrollierbarkeit gestellt. Nach vielen Jahren der fast unkontrollierten Arbeit mit Groß-Rechnern begrüßen die betrieblichen Datenschutzbeauftragten heute die endlich zeitgemäße Dokumentation oder das kontrollierbare Vorhandensein bestimmter organisatorischer Abläufe in diesem Bereich der Datenverarbeitung.

Dagegen entstehen bei der zunehmenden Verwendung von PC's neue Unsicherheiten. PC ist der Computer am Arbeitsplatz. Er kann überall installiert werden, wo eine Steckdose ist, er braucht keine klimatisierten Räume, er benötigt keine besondere Eröffnungseingabe (d. h., er kann auch ohne Spezialwissen benutzt werden), um arbeiten zu können, er arbeitet mit besonders kleinen Datenträgern (z. B. kleine Disketten).

Es gibt keine vom Betriebssystem unterstützte Protokollierung der Aktivitäten an diesem Arbeitsgerät.

Die entscheidenden Stichworte sind demzufolge Dezentralisierung, kleine Datenträger und keine Protokollierung.

8.7.1
Dezentralisierung

Bei einigen Unternehmen ist aufgrund fehlender Organisationsstrukturen eine ausreichende Kontrolle kaum oder nur unter großen Schwierigkeiten

möglich. Andere haben von vornherein eine zentrale Stelle geschaffen, die für die Beschaffung der Geräte und der Software verantwortlich ist. Gleichzeitig werden alle Anwendungen zentral festgelegt. Ebenfalls entscheidet diese zentrale Stelle über die zu benutzende Software, die Betriebssysteme, Programme und Dateien.

Unter Datenschutzgesichtspunkten ist zu fordern, daß an jedem PC-Arbeitsplatz Dateiennachweise, kurze Anwendungsbeschreibungen und ein Datenträgerverzeichnis zu führen sind. Dazu gehört ein vernünftiger Zugriffsschutz (Passworte).

Je nach Größe des Unternehmens ist die Zugangssicherung zu beachten. Natürlich müssen hier für den PC angemessene Verfahren eingerichtet werden.

Einfache Maßnahmen sind u. a. das Abstellen des PC, sobald eine Arbeitssitzung beendet ist oder Besucher den Raum betreten, das Unterverschlußhalten der externen Datenträger (evtl. auch das Wegschließen des gesammten Geräts) und das Verschließen des Raumes bei Verlassen desselben.

Solche Regelungen sind allerdings nur sinnvoll, wenn sie auch vom betrieblichen Datenschutzbeauftragten auf ihre Einhaltung überwacht und wenn Verfahren überprüft werden.

Andere Möglichkeiten zur Regelung der ordnungsgemäßen Verarbeitung personenbezogener Daten mit dem PC ergeben sich, wenn der PC mit dem Hauptrechner verbunden ist.

Oberstes Gebot bei einer Verbindung zwischen PC und Hauptrechner ist die Protokollierung aller Aktivitäten vom und zum PC. Weiterhin ist festzulegen, welche Daten bearbeitet werden und ob Daten aus dem Hauptrechner in den PC übertragen werden dürfen. Auch hierzu gehört eine intensive Kontrolle durch den betrieblichen Datenschutzbeauftragten.

8.7.2
Kleine Datenträger

Zu den Disketten ist anzumerken, daß diese, wie alle anderen externen Datenträger (z. B. Magnetbänder) zu behandeln sind. Daß gerade hierbei viele, insbesondere langjährige, Datenverarbeitungsmitarbeiter eine kleine Diskette nicht als vollwertigen Datenträger ansehen, liegt nicht zuletzt daran, daß immer noch davon ausgegangen wird, bei einem PC handele es sich hauptsächlich um einen Spielcomputer.

Disketten sind Datenträger, auf denen sich eine Vielzahl von personenbezogenen Daten befinden kann. Sie sind deshalb zu inventarisieren, vor Verlust zu sichern, und sie sind vor unberechtigtem Zugriff zu sichern. Es sollte also eine Datenträgerverwaltung auch für Disketten vorhanden sein, aus der z. B. hervorgeht, wie viele Disketten mit welchen Daten belegt sind.

Das Verschließen der Datenträger und das Aufbewahren von Sicherungskopien an einem sicheren Ort sollte als selbstverständlich angesehen werden.

8.7.3
Protokollierung

Eine Protokollierung in Form eines Logs (automatisches Aufschreiben aller vom Computer durchgeführten Arbeiten) oder eines sogenannten Konsolprotokolls gibt es bedauerlicherweise noch zu keinem Gerät, während es diese Protokollierungen in vergleichbarer Form bei allen Groß-Rechnern gibt.

Selbst Systeme, die mittlerweile mit bis zu 64 Bildschirmarbeitsplätzen in lokalen oder in öffentlichen Netzen einsetzbar sind, verfügen über keine zwangsweise Protokollierung. Das bedeutet, daß nicht nachvollziehbar ist, von wem das Gerät benutzt worden ist, wann Daten in welchen Bereichen (z. B. in einer Datenbank) verändert worden sind.

Hier kann nur an alle Hersteller solcher Geräte appelliert werden, endlich eine zwangsweise, lückenlose Protokollierung aller Aktivitäten an dem System zu schaffen. Daß darunter die Wirtschaftlichkeit dieser Geräte leiden sollte, ist nicht mehr nachvollziehbar, weil mittlerweile sowohl die

Speicherkapazitäten wie auch die Geschwindigkeiten so hoch sind, daß eine Protokollierung nicht mehr zu einem erkennbaren Verlust führen kann.

9.
Ordnungswidrigkeiten

Im Berichtsjahr wurden 15 Bußgeldverfahren eingeleitet, die in 13 Fällen mit einem Bußgeldbescheid und in 2 Fällen mit einer Einstellung des Verfahrens abgeschlossen wurden. Drei Bußgeldbescheide sind noch nicht rechtskräftig, da Einspruch eingelegt wurde.

Die Mehrzahl der Bußgeldverfahren (10) betraf die verspätete Abgabe der nach § 39 BDSG erforderlichen Meldungen an die Aufsichtsbehörde (Ordnungswidrigkeit nach § 42 Abs. 1 Nr. 4 BDSG). In zwei Fällen wurde entgegen §§ 28, 38 BDSG ein Beauftragter für den Datenschutz nicht rechtzeitig bestellt (Ordnungswidrigkeit nach § 42 Abs. 1 Nr. 2 BDSG). In weiteren zwei Fällen waren die Betroffenen im Rahmen von Überprüfungen ihrer Auskunftspflicht gegenüber der Aufsichtsbehörde nach §§ 30 Abs. 2, 40 Abs. 2 BDSG, nicht rechtzeitig nachgekommen (Ordnungswidrigkeit nach § 42 Abs. 1 Nr. 5 BDSG). Ein anderer Fall betraf die nicht rechtzeitige Benachrichtigung eines Betroffenen (Ordnungswidrigkeit nach § 42 Abs. 1 Nr. 1 BDSG).

Anhang

Berichtsantrag der Abg. Posch, Hahn (F.D.P.) und Fraktion (Drucks. 12/2377)

Von einer Einarbeitung der im Berichtsantrag gestellten Fragen in den Tätigkeitsbericht wurde abgesehen, da eine getrennte Behandlung das Auffinden der Antworten erleichert.

1. Wie viele Beschwerden – aufgegliedert nach Branchen unter besonderer Berücksichtigung von Handel, Banken und Versicherungen – hat es in den letzten drei Jahren in den Fällen gegeben, wo lediglich eine Anlaßaufsicht besteht?

In den Jahren 1985–1987 sind gegen private datenverarbeitende Stellen, für die gemäß §§ 22 ff. BDSG nur die sogenannte Anlaßaufsicht besteht, insgesamt 240 Beschwerden eingegangen. Von diesen Eingaben betrafen

Handel (Versand-, Einzel-, Großhandel)	75
Kreditinstitute	42
Versicherungen	28
Kreditkartenunternehmen	30
Inkassounternehmen	7
Übrige	58
	240

2. Wie viele dieser Beschwerden – aufgegliedert wie zu Ziff. 1 – waren
   a) begründet,
   b) unbegründet?

Von diesen Beschwerden waren insgesamt 76 (= 31,6 v. H.) begründet und 161 unbegründet. Davon betrafen

	begründete	unbegründete
Handel	20	54
Kreditinstitute	17	25
Versicherungen	5	21
Kreditkartenunternehmen	12	16
Inkassounternehmen	2	5
Übrige	20	40

Die Überprüfung von 3 Beschwerden ist noch nicht abgeschlossen (davon Handel: 1, Kreditkartenunternehmen: 2).

3. Welche Fälle haben die begründeten Beschwerden betroffen?

Die begründeten Beschwerden ergaben folgende Verstöße:

25 Fälle unzulässiger Datenspeicherung
(Verstoß gegen §§ 3, 23 BDSG),

31 Fälle unzulässiger Datenübermittlung
(Verstoß gegen §§ 3, 24 BDSG),

17 Fälle unzureichender Auskunftserteilung an den Betroffenen bzw. unbegründeter Auskunftsverweigerung
(Verstoß gegen § 26 Abs. 2 BDSG),

3 Fälle unzureichender Datensicherung
(Verstoß gegen § 6 Abs. 1 Satz in Verbindung mit der Anlage zu § 6 Abs. 1 Satz 1.)

4. Konnte gewährleistet werden, daß den Beschwerden wirksam abgeholfen wurde und es zu keinen Folgewirkungen für die jeweils betroffenen Bürger gekommen ist?

Zunächst ist hervorzuheben, daß das BDSG der Aufsichtsbehörde keine Möglichkeit gibt, eine datenverarbeitende Stelle zu zwingen, von ihr für erforderlich gehaltene Maßnahmen zu ergreifen. Sie kann daher bei Verstößen – von den wenigen in § 42 aufgezählten Ordnungswidrigkeitstatbeständen abgesehen – nur auf dem Verhandlungsweg auf Abhilfe dringen. Außerdem werden die betroffenen Beschwerdeführer gegebenenfalls auf die Strafvorschriften des § 41 BDSG hingewiesen, wonach die unbefugte Übermittlung geschützter personenbezogener Daten mit Strafe bedroht ist. Die Tat wird jedoch nur auf Strafantrag des Betroffenen verfolgt; die Datenschutzaufsichtsbehörden haben keine Antragsbefugnis.

Die durch eine konkrete Beschwerde ausgelöste Überprüfung hat zunächst das Ziel, den zugrundeliegenden Sachverhalt aufzuklären. Dabei sind zwei Fallgestaltungen zu unterscheiden:

- Der vom Beschwerdeführer beanstandete Verarbeitungsvorgang ist bereits abgeschlossen,
- die Verarbeitung personenbezogener Daten dauert noch an oder es ist eine Wiederholung des Verarbeitungsvorgangs zu befürchten.

In beiden Fällen ist die Aufsichtsbehörde im Rahmen ihrer Überprüfung bemüht, durch Überzeugung zu erreichen, daß negative Folgen einer nicht datenschutzgerechten Datenverarbeitung vermieden werden oder zu befürchtende Verstöße gegen die Datenschutzvorschriften in der Zukunft unterbleiben. In der überwiegenden Zahl der Fälle hat diese häufig sehr langwierige Überzeugungstätigkeit Erfolg. Die datenverarbeitende Stelle wird erforderlichenfalls zur Berichtigung oder Löschung von personenbezogenen Daten aufgefordert. Dabei wird auch geprüft, ob sie dieser Forderung nachkommt.

Wurden über einen Beschwerdeführer falsche Daten an Dritte übermittelt, wird die übermittelnde Stelle auch zur Berichtigung gegenüber den Datenempfängern aufgefordert. Es wird jedoch zumeist nicht bekannt, welche Konsequenzen der Datenempfänger beispielsweise aus der Berichtigung ihm übermittelter Daten zieht.

5. Wie viele Stellen gibt es in Hessen, die der Kontrolle nach dem 4. Abschnitt des Bundesdatenschutzgesetzes unterliegen?

Derzeit sind 491 datenverarbeitende Stellen gemeldet, die einer regelmäßigen Kontrolle gemäß § 40 BDSG unterliegen.

6. a) Wie viele Überprüfungen vor Ort wurden jeweils
   aa) im Rahmen der Anlaßaufsicht,
   bb) im Rahmen der Kontrolle nach dem 4. Abschnitt des Bundesdatenschutzgesetzes in den letzten drei Jahren durchgeführt?
   b) In welchen zeitlichen Abständen muß ein der Kontrolle nach dem 4. Abschnitt des Bundesdatenschutzgesetzes unterliegender Betrieb mit einer Überprüfung seiner Datenverarbeitung rechnen?

a) In den Jahren 1985 – 1987 wurden folgende Überprüfungen vor Ort durchgeführt:

aa) im Rahmen der Anlaßaufsicht: 11

bb) im Rahmen der Kontrolle nach dem 4. Abschnitt des BDSG: 73

Im Rahmen der Anlaßaufsicht werden in der Regel nur dann Überprüfungen vor Ort durchgeführt, wenn entweder die schriftliche Anhörung der datenverarbeitenden Stelle nicht zu der erforderlichen Sachverhaltsaufklärung führt oder besondere Umstände des Einzelfalles dies erfordern.

b) Für die zeitlichen Abstände, in denen eine datenverarbeitende Stelle des 4. Abschnitts des BDSG mit einer Überprüfung gemäß § 40 BDSG rechnen muß, gibt es keine feste Regel. Die Auswahl der für eine Prüfung vorgesehenen Unternehmen richtet sich zunächst nach der Art der verarbeiteten personenbezogenen Daten. Begründete Beschwerden gegen datenverarbeitende Unternehmen des 4. Abschnitts können ebenfalls zu einer Regelprüfung führen, z. B. wenn Mängel in der Organisation oder der Datensicherung erkennbar wurden. Führt eine Überprüfung zu Beanstandungen, so muß das betroffene Unternehmen eher mit einer weiteren Prüfung rechnen als andere. Im Hinblick auf die unter 12. geschilderte Personalsituation war es bisher nicht möglich, häufig Wiederholungsprüfungen durchzuführen.

7. In wie vielen Fällen wurde bei den Überprüfungen gemäß Ziff. 6 ein Verstoß gegen das Bundesdatenschutzgesetz oder andere Datenschutzbestimmungen festgestellt?

Bei den 11 Überprüfungen vor Ort im Rahmen der Anlaßaufsicht wurden in 3 Fällen Verstöße gegen Datenschutzvorschriften festgestellt. Bei den 56 Prüfungen nach dem 4. Abschnitt des BDSG wurden in 33 Fällen Verstöße gegen Datenschutzvorschriften festgestellt.

8. In wie vielen Fällen hat der Verstoß eine Geldbuße zur Folge gehabt?

In insgesamt 19 Fällen wurden Geldbußen gemäß § 42 BDSG verhängt. Dabei ist zu betonen, daß wesentliche Verstöße gegen Datenschutzvorschriften wie z. B. unzulässige Datenspeicherung, Verletzung der Datensicherungs- und Verletzung der Auskunftspflicht weder Straf- noch Bußgeldbewehrt sind.

9. Um welche nicht-öffentlichen Stellen, aufgegliedert wie zu Frage 1, und um welche Verstöße hat es sich hierbei gehandelt?

Diejenigen Verstöße, die zu Geldbußen führten, betrafen Unternehmen des 3. Abschnitts:

– Kreditkartenunternehmen	1
Unternehmen des 4. Abschnitts:	18
davon	
– Kreditinformationsdienste	2
– Service-Rechenzentren	11
– Datenerfasser	5
Art der Verstöße:	
Verspätete Meldung zum Register gemäß § 39, Ordnungswidrigkeit gemäß § 42 Abs. 1 Nr. 4:	12
Verspätete Bestellung eines Beauftragten für den Datenschutz, Ordnungswidrigkeit gemäß § 42 Abs. 1 Nr. 2:	4
Verspätete bzw. falsche Auskunftserteilung gegenüber der Aufsichtsbehörde, Ordnungswidrigkeit gemäß § 42 Abs. 1 Nr. 5:	3

10. Welche Stellung bezieht die Landesregierung zu der in der Literatur und von einigen Datenschutzbeauftragten geäußerten Auffassung, daß für eine wirksame Datenschutzkontrolle im nicht-öffentlichen Bereich die Anlaßaufsicht nicht ausreichend sei?

Im Gegensatz zur Regelaufsicht bei Stellen, die Daten für fremde Zwecke verarbeiten, kann es bei Stellen, die Daten für eigene Zwecke verarbeiten, grundsätzlich bei der Anlaßaufsicht bleiben. Allerdings sollte der Anlaß weiter gefaßt werden, als im geltenden § 30 Abs. 1 BDSG, wonach die Aufsichtsbehörde nur tätig werden darf, wenn ein Betroffener begründet darlegt, daß er bei der Verarbeitung seiner personenbezogenen Daten in seinen Rechten verletzt worden ist. Die Aufsichtsbehörde sollte vielmehr auch dann zur Prüfung berechtigt sein, wenn andere Anlässe dies nahelegen. Ein solcher Anlaß könnte z. B. vorliegen, wenn von dem Unternehmen besonders sensible Daten verarbeitet werden oder wenn es

ein größeres Rechenzentrum betreibt. Es ist nämlich anzunehmen, daß in den Rechenzentren der Unternehmen des 3. Abschnitts des BDSG mindestens ebenso viele Verstöße gegen die Datensicherungspflichten vorliegen, wie bei den Regelprüfungen nach dem 4. Abschnitt des BDSG festgestellt wurden. Auch Presseveröffentlichungen könnten Anlaß für eine Überprüfung bieten.

11. Inwieweit hält die Landesregierung besondere Schutzbestimmungen für die Erhebung und Verarbeitung von personenbezogenen Daten durch Detekteien und Auskunfteien über die Vorschriften des 4. Abschnitts des Bundesdatenschutzgesetzes hinaus für erforderlich?

Zumindest für Wirtschaftsauskunfteien sollte die Datei als Anwendungsvoraussetzung für das BDSG entfallen. Diese Auskunfteien handeln im großen Umfang mit besonders zu schützenden Kreditinformationen. Soweit sie diese Informationen in Akten und auf nicht formalisierten Einzelblättern aufbewahren, ist der Dateibegriff nicht erfüllt und damit das BDSG nicht anwendbar, obwohl der Gesetzgeber bei der Einführung des BDSG auch den Umgang mit Kreditinformationen regeln wollte.

Es kommt immer wieder zu Beschwerden gegen die Recherchemethoden der Wirtschaftsauskunfteien, weil sie Nachbarn und Arbeitgeber der Betroffenen über deren persönliche Verhältnisse befragen. Diese Datenerhebung, die mit schwerwiegenden Eingriffen in die Privatsphäre der Betroffenen verbunden ist, ist im BDSG nicht geregelt. Gegen die Ansicht, die Umstände solcher Befragungen als Maßstab für die Zulässigkeit der anschließenden Speicherung zu betrachten, wenden sich die Auskunfteien mit dem Argument, daß die Datenerhebung nicht im BDSG geregelt sei und daher bei der Beurteilung der Zulässigkeit der Speicherung nicht berücksichtigt werden dürfe.

12. Wie sind die mit der Datenschutzkontrolle bei nicht-öffentlichen Stellen beauftragten Behörden personell und sachlich ausgestattet (aufgegliedert nach einzelnen Behörden und nach Qualifikationen)?

Regierungspräsidium in Darmstadt:

Zwei Juristen

Zwei EDV-Fachleute (davon ein Betriebswirt)

Eine Sachbearbeiterstelle ist seit dem 1. Oktober 1986 bis voraussichtlich 30. September 1988 wegen personeller Engpässe vorübergehend nicht besetzt.

Der Leiter des Dezernats nimmt außerdem die Aufgaben des behördlichen Beauftragten für den Datenschutz gemäß § 5 Abs. 2 HDSG wahr.

Die EDV-Fachleute (techn. Dezernenten) führen seit dem 15. Januar 1987 zugleich im Auftrag der Regierungspräsidien in Kassel und Gießen die technischen Prüfungen gemäß § 40 BDSG durch.

Regierungspräsidium in Gießen:

Eine Juristin mit der Hälfte ihrer Arbeitszeit

Regierungspräsidium in Kassel:

Ein Jurist, der die Aufgaben als Leiter des Datenschutzdezernates anteilig neben seinen Aufgaben im Baurechtsdezernat wahrnimmt.

Ein Mitarbeiter des gehobenen Dienstes (Sachbearbeiter), der alle nachgeordneten Aufgaben im Datenschutzdezernat anteilig neben Tätigkeiten im Verkehrsdezernat wahrnimmt.

Wiesbaden, den 21. September 1988

Der Hessische Ministerpräsident
Dr. Wallmann

Der Hessische Minister des Innern
Milde