



12. Wahlperiode

Drucksache **12/7186**

# HESSISCHER LANDTAG

22. 08. 90

## **Vorlage der Landesregierung**

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

Vorgelegt mit der Stellungnahme zum Achtzehnten Tätigkeitsbericht des  
Hessischen Datenschutzbeauftragten - Drucks. 12/4040 - gemäß § 30 Abs. 2  
Satz 2 des Hessischen Datenschutzgesetzes vom 11. November 1986.

Eingegangen am 22. August 1990 · Ausgegeben am 3. September 1990

Druck und Auslieferung: Kanzlei des Hessischen Landtags · Postfach 32 40 · 6200 Wiesbaden 1

KKD12/7186

S.2

**Inhaltsverzeichnis**

1. Vorbemerkung	5
2. Bearbeitung von Beschwerden gegen datenverarbeitende Stellen des 3. Abschnitts des Bundesdatenschutzgesetzes	5
3. Bearbeitung von Beschwerden gegen datenverarbeitende Stellen des 4. Abschnitts des Bundesdatenschutzgesetzes	6
4. Prüfung datenverarbeitender Stellen des 4. Abschnitts des Bundesdatenschutzgesetzes von Amts wegen	6
4.1 Meldepflicht gemäß § 39 Abs. 1 i.V.m. § 31 Abs. 1 Nr. 1 - 3 Bundesdatenschutzgesetz	6
4.2 Register	7
4.3 Prüfungsübersicht	7
5. Kreditkartenunternehmen	8
5.1 Datenverarbeitungsermächtigungsklausel	8
5.2 Kreditkarten als Marketinginstrument (Co-Branding)	8
5.3 Auswertung der Rechnungszusammenstellungen	8
5.4 Weitergabe von Leistungsbelegen	9
6. Wirtschaftsauskunfteien	9
6.1 Benachrichtigung	9
6.2 SCHUFA	9
6.3 Wechselprotestlisten	9
7. Zentrales Handelsregister	10
8. Anbieten von Datenbanken auf CD-ROM	10
9. Warndienste	12
10. Markt- und Meinungsforscher	13
10.1 Quittungslisten	13
10.2 Weitergabe von Adressen aus Befragungen	13
11. Datenvernichtung	13
12. Versandhandel	14
13. Datensicherung	14
14. Bildschirmtext	14
14.1 Dialogdienste	15
14.2 Geschlossene Teilnehmergruppen	15
15. Ordnungswidrigkeiten	15

KKD12/7186

S. 4

## 1. Vorbemerkung

Die Erfahrungen der Aufsichtsbehörden haben auch in diesem Berichtszeitraum gezeigt, daß ihre Tätigkeit vor allem deshalb eingeschränkt ist, weil im geltenden Bundesdatenschutzgesetz eine unterschiedliche Kontrollbefugnis besteht, je nachdem, ob ein Unternehmen unter den Dritten oder den Vierten Abschnitt des Gesetzes fällt. Nach dem Vierten Abschnitt (§ 40) des Bundesdatenschutzgesetzes kann die Aufsichtsbehörde von Amts wegen Prüfungen vornehmen, wenn Unternehmen geschützte personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung speichern und übermitteln oder anonymisieren oder im Auftrag als Dienstleistungsunternehmen verarbeiten. Dazu gehören Auskunftsteien, Detekteien, Adressverlage, Markt-, Meinungs- und Sozialforschungsinstitute sowie Service-Rechenzentren, Software-Unternehmen und Datenerfassungsbüros. Dagegen darf die Aufsichtsbehörde bei allen Unternehmen, die Daten für ihre eigenen Zwecke verarbeiten, nach dem Dritten Abschnitt (§ 30 Abs. 1 BDSG) nur tätig werden, wenn ein Betroffener begründet darlegt, daß er bei der Verarbeitung seiner personenbezogenen Daten in seinen Rechten verletzt worden ist. Zu diesem Bereich gehören der gesamte Handel, die Banken, Versicherungen, Kreditkarten-Unternehmen, Inkasso-Unternehmen, Vermieter und Ärzte. Hier kann die Aufsichtsbehörde weder eingreifen, wenn sie durch die Medien von Mißständen erfährt, noch wenn sie bei Prüfungen von Unternehmen des Vierten Abschnitts auf eine unzulässige Datenverarbeitung von Unternehmen des Dritten Abschnitts stößt.

Es ist deshalb mit Nachdruck zu begrüßen, daß der Entwurf der Bundesregierung zur Novellierung des Bundesdatenschutzgesetzes Abhilfe schaffen will, indem er Prüfungen der Aufsichtsbehörden grundsätzlich zuläßt, wenn hinreichende Anhaltspunkte für eine Rechtsverletzung vorliegen. Diese entscheidende Änderung sowie die erstmalige Schaffung von Eingriffsbefugnissen bringen für die Aufsichtsbehörden eine so wesentliche Ausweitung und Verstärkung ihrer Kontrollmöglichkeiten, daß die Beschränkung des Gesetzes auf Dateien im nicht-öffentlichen Bereich in den Hintergrund tritt.

## 2. Bearbeitung von Beschwerden gegen datenverarbeitende Stellen des 3. Abschnitts des Bundesdatenschutzgesetzes

Gegen Stellen, die Datenverarbeitung als Hilfsmittel für die Erfüllung ihrer Geschäftszwecke oder -ziele verarbeiten, gingen im Berichtsjahr 94 Beschwerden ein, die zu einer Überprüfung gem. § 30 Bundesdatenschutzgesetz führten.

Die Beschwerden betrafen

- den Handel (Versand sowie Einzelhandel)	in 16 Fällen,
- Versicherungen und Versicherungsagenturen	in 15 Fällen,
- Kreditinstitute	in 9 Fällen,
- Kreditkarten-Unternehmen	in 4 Fällen,
- das Gesundheitswesen (Ärzte und Krankenhäuser)	in 5 Fällen,
- Inkasso-Unternehmen	in 2 Fällen,
- Vermieter	in 2 Fällen,
- Verlage	in 3 Fällen,
- sonstige Unternehmen	in 38 Fällen.
	94

In 23 Fällen waren die Beschwerden begründet, davon sechs gegen den Handel, fünf gegen Versicherungen und Versicherungsagenturen, drei gegen Kreditinstitute, eine gegen eine Stelle des Gesundheitswesens, eine gegen einen Autovermieter sowie sieben gegen sonstige Unternehmen.

Bei fünf Beschwerden konnte nicht mehr abschließend festgestellt werden, ob die Datenverarbeitung in zulässiger oder unzulässiger Art und Weise erfolgte. In zwei Fällen sind die Ermittlungen der Aufsichtsbehörde noch nicht abgeschlossen.

Von den genannten Beschwerden abgesehen, sind in diesem Bereich zahlreiche schriftliche und mündliche Anfragen von Bürgern, Betriebsräten, Datenschutzbeauftragten und Unternehmen zu Fragen des Datenschutzes beantwortet worden.

### **3. Bearbeitung von Beschwerden gegen datenverarbeitende Stellen des 4. Abschnitts des Bundesdatenschutzgesetzes**

Im Berichtsjahr gingen 28 Beschwerden betroffener Bürger gegen Unternehmen ein, die geschäftsmäßige Datenverarbeitung für fremde Zwecke betreiben. Alle diese Beschwerden führten zu einer Überprüfung durch die Aufsichtsbehörde.

Die Beschwerden betrafen

- Kreditinformationsdienste  
(Wirtschaftsauskunfteien und SCHUFA) in 26 Fällen,
- Markt- und Meinungsforschungsinstitute in 2 Fällen.

In drei Fällen (Kreditinformationsdienste) waren die Beschwerden begründet.

Auch im Bereich des 4. Abschnittes des Bundesdatenschutzgesetzes wurden zahlreiche schriftliche und mündliche Anfragen betroffener Bürger beantwortet.

Darüber hinaus wandten sich im Berichtsjahr vier Betroffene an die Aufsichtsbehörde mit Beschwerden gegen datenverarbeitende Stellen sowohl des 3. wie des 4. Abschnitts. Sie befürchteten, ihre personenbezogenen Daten seien bei Kreditinstituten bzw. Kreditinformationsdiensten in unzulässiger Art und Weise gespeichert und darüber hinaus unzulässigerweise an Kreditinformationsdienste bzw. Kreditinstitute übermittelt worden. Alle diese Beschwerden waren begründet.

### **4. Prüfung datenverarbeitender Stellen des 4. Abschnitts des Bundesdatenschutzgesetzes von Amts wegen**

#### **4.1 Meldepflicht gemäß § 39 Abs. 1 i.V.m. § 31 Abs. 1 Nr. 1 - 3 Bundesdatenschutzgesetz**

Gemäß § 39 Abs. 1 BDSG haben die in § 31 Abs. 1 Nr. 1 - 3 BDSG genannten Personen und Gesellschaften, die Datenverarbeitung für fremde Zwecke betreiben, die Aufnahme der meldepflichtigen Tätigkeit der zuständigen Aufsichtsbehörde binnen eines Monats zur Aufnahme in das bei ihr geführte Register (siehe Punkt 4.2) anzuzeigen. Dennoch ist immer wieder festzustellen, daß sich zahlreiche meldepflichtige Unternehmen durch Nichtabgabe entsprechender Meldungen der Kontrolle der Aufsichtsbehörde entziehen. Teilweise in Unkenntnis der Tatsache, daß auf die geschäftsmäßige Verarbeitung personenbezogener Daten die Vorschriften des Bundesdatenschutzgesetzes anzuwenden sind, geben gerade kleinere meldepflichtige Unternehmen, z.B. aus der Dienstleistungsdatenverarbeitungs-Branche, keine Meldungen ab, oder melden sich erst dann verspätet an, wenn sie durch die Aufsichtsbehörde oder durch andere meldepflichtige Unternehmen auf die gesetzlichen Bestimmungen hingewiesen wurden.

Wenn gegen die Verantwortlichen dieser Unternehmen gemäß § 42 Abs. 1 Nr. 4 BDSG Ordnungswidrigkeitenverfahren wegen Nichtabgabe der Meldung bzw. verspäteter Meldung eingeleitet werden, führen diese immer wieder an, sie seien davon ausgegangen, daß durch die erfolgte Gewerbe- oder -ummeldung bei dem zuständigen Gewerbeamt alle bestehenden Meldepflichten erfüllt seien bzw. durch den jeweiligen Magistrat/Gemeindevorstand - etwa analog der Mitteilung an das zuständige Finanzamt - erledigt würden. Darüber hinaus macht anscheinend nur eine geringe Zahl der Industrie- und Handelskammern ihre Mitglieder auf die Bestimmungen des Bundesdatenschutzgesetzes aufmerksam.

Eine Verbesserung könnte deshalb möglicherweise dadurch erreicht werden, daß bei der Gewerbean- oder -ummeldung neben den gewerberechtlichen Hinweisen formularmäßig auch auf andere gesetzliche Meldepflichten, z.B. nach dem Bundesdatenschutzgesetz, hingewiesen wird.

#### 4.2 Register

Bisher sind zu dem gem. § 40 Abs. 1 Satz 2 Bundesdatenschutzgesetz bei den Aufsichtsbehörden geführten Register 498 Unternehmen gemeldet, die Datenverarbeitung für fremde Zwecke betreiben. Der Rückgang gegenüber dem vorangegangenen Bericht (514) beruht auf Abmeldungen, die vor allem auf eine Konzentrierung der Datenverarbeitung auf weniger Stellen zurückzuführen sind.

#### 4.3 Prüfungsübersicht

Im Berichtsjahr 1989 wurden 37 Prüfungen durchgeführt.

Davon betrafen:

1. Datenverarbeiter nach § 31 Abs. 1 Ziffer 3 BDSG	
1.1 Service-Rechenzentren	9
1.2 Konzerndatenverarbeiter	6
1.3 Datenerfasser	3
1.4 Mikroverfilmer	1
1.5 Datenträgervernichter	3
1.6 Tele-Marketing	3
1.7 Sonstige	1
2. Datenspeichernde Stellen/Übermittler nach § 31 Abs. 1 Ziffer 1 BDSG	
2.1 Kreditinformationsdienste	5
2.2 Brancheninformationsdienste	2
3. Markt- und Meinungsforscher nach § 31 Abs. 1 Ziffer 2 BDSG	4

Die Prüfungen brachten folgendes Ergebnis:

- Beanstandungen	14
- Empfehlungen	9
- ohne wesentliche Beanstandungen	14

Folgende wesentlichen Mängel wurden am häufigsten festgestellt:

1. Keine bzw. verspätete Registermeldung nach § 39 Bundesdatenschutzgesetz
2. Unzureichende Zugangssicherung (Zugangskontrolle)
3. Mängel in der Tätigkeit des Datenschutzbeauftragten (geringe Aktivität, mangelnde Beteiligung durch das Unternehmen, insbesondere mangelnde Mitwirkung bei der Personalauswahl)
4. Unzureichende Auftragskontrolle
5. Unzureichende Zugriffskontrolle (kein Passwort, seltener Wechsel des Passwortes, zu weit gehende bzw. zu viele Zugriffsberechtigungen)
6. Fehlende Benachrichtigung nach § 34 Abs. 1 Bundesdatenschutzgesetz
7. Mangelhafte Datenträgerverwaltung
8. Unzureichende Verfahrensdokumentation

## **5. Kreditkartenunternehmen**

### **5.1 Datenverarbeitungsermächtigungsklausel**

Bereits im Ersten Tätigkeitsbericht (S. 21) wurde geschildert, daß und welche datenschutzrechtlichen Probleme hinsichtlich der zum damaligen Zeitpunkt von den vier Kreditkartenunternehmen verwandten Datenverarbeitungsermächtigungsklauseln bestanden.

Nachdem es dann gelungen war, diese Unternehmen von der Notwendigkeit einer neuen Klausel zu überzeugen, haben mittlerweile drei der Unternehmen in ihren Kartenanträgen eine den gesetzlichen Anforderungen an eine Einwilligung entsprechende Klausel aufgenommen. Auch das vierte Unternehmen wollte neue Kartenanträge mit einer gesetzeskonformen Klausel aufliegen, hat dies aber zurückgestellt, weil aufgrund einer möglichen Vertragsänderung mit der SCHUFA eine noch ausführlichere SCHUFA-Klausel in die Kartenanträge eingearbeitet werden soll. Da auch bei den anderen Kreditkartenorganisationen eine Vertragsänderung möglich ist, werden die Datenverarbeitungsermächtigungsklauseln im Hinblick auf die Teilnahme am SCHUFA-Verfahren aller Voraussicht nach in absehbarer Zeit erneut geändert.

### **5.2 Kreditkarten als Marketinginstrument (Co-Branding)**

Die Kreditkarten werden von den unterschiedlichsten Unternehmen auch für eigene Marketing-Zwecke eingesetzt. In diesen Fällen firmiert neben dem Kreditkartenunternehmen bzw. der ausstellenden Bank noch mindestens ein weiteres Unternehmen zumeist mit seinem Firmenzeichen auf der Kreditkarte. Dieses Unternehmen erwartet hiervon weitere Informationen über seine Kunden und damit eine bessere Ausgangsbasis für sein Marketing und seine Werbung. Ebenso erhofft man sich hiervon eine stärkere Markenbindung. Kreditkarten-Vertragspartner bleibt das Kreditkartenunternehmen bzw. die ausstellende Bank.

Problematisch ist aus datenschutzrechtlicher Sicht die Weitergabe von Daten des Kreditkartenkunden an den Co-Branding-Partner sowie die Erhebung einer Vielzahl von für das Kreditkartenunternehmen nicht nötigen Kundendaten. Denkbar ist im Extremfall, daß sich aus dem Zusammenspiel von Kreditkartenunternehmen und Co-Branding-Partner ein Informationspool ergibt, der in bestimmten Bereichen wirtschaftlich interessante, sehr differenzierte Datenprofile von Kartenbenutzern ermöglicht. Die vom Kreditkartenunternehmen um Beratung gebetene Aufsichtsbehörde regte deshalb an, die Menge der vom Kunden im Kartenantrag abgefragten Daten möglichst zu begrenzen und durch entsprechende Formulierung der Datenverarbeitungsermächtigungsklausel sicherzustellen, daß der Kunde über Umfang und Zweck der Datenflüsse zwischen Kreditkartenunternehmen und Co-Branding-Partner Klarheit bekommt. Da die Kreditkartenunternehmen unter den 3. Abschnitt des Bundesdatenschutzgesetzes fallen, kann die Aufsichtsbehörde nach § 30 BDSG nur tätig werden, wenn das Kreditkartenunternehmen selbst an sie herantritt oder die Beschwerde eines persönlich Betroffenen vorliegt.

### **5.3 Auswertung der Rechnungszusammenstellungen**

In einem Fall hat ein Kreditkartenunternehmen die krankheitsbedingten Fehltagel einer seiner Arbeitnehmerinnen, die gleichzeitig Kreditkartenkundin bei diesem Unternehmen war, mit den Rechnungszusammenstellungen aus den Kreditkartenumsätzen verglichen. Ihre Arbeitsunfähigkeit wurde in Zweifel gezogen, da sie an Krankheitstagen auch Kartenleistungen in Anspruch genommen hatte. Ihr Arbeitsverhältnis wurde deswegen gekündigt. Die Recherchen der Aufsichtsbehörde ergaben, daß sich die ausgewerteten Rechnungszusammenstellungen nur noch auf Mikrofiches befanden, die den Dateibegriff des § 2 Abs. 3 Ziff. 3 Bundesdatenschutzgesetz nicht erfüllten. Die ursprüngliche EDV-Datei war gelöscht worden.

Die Aufsichtsbehörde mußte daher ihre Überprüfung abbrechen, obwohl aus der Sicht des Persönlichkeitsschutzes eine in dieser Weise gezielte Verknüpfung beider Datenbestände sehr bedenklich erscheint. Hier zeigt sich wieder



einmal, daß der Anwendungsbereich des Bundesdatenschutzgesetzes mit der Beschränkung auf Daten, die in Dateien gespeichert sind oder aus Dateien an Dritte übermittelt werden, zu kurz greift, um das Persönlichkeitsrecht umfassend zu schützen.

#### **5.4 Weitergabe von Leistungsbelegen**

In einem Fall hat ein Kreditkartenunternehmen Leistungsbelege eines Kreditkartenkunden, die bei unterschiedlichen Vertragsunternehmen angefallen waren, fotokopiert und einem Vertragsunternehmen übersandt, das hiermit die Echtheit der Unterschrift eines Kunden in anderer Sache überprüfen wollte. Das Vertragsunternehmen hatte hier ein berechtigtes Interesse an der Kenntnisnahme verschiedener echter Unterschriftsausführungen. Schutzwürdige Belange des betroffenen Kreditkartenkunden wurden jedoch dadurch verletzt, daß nicht nur Kopien von Unterschriftsproben, sondern die vollständig kopierten Leistungsbelege von unterschiedlichen Vertragsunternehmen mit allen Daten - Vertragsunternehmen, Ort, Datum, Betrag, Unterschrift - übersandt wurden. Die Aufsichtsbehörde hat aus den genannten Gründen die Übermittlung der Daten auf den Leistungsbelegen außer dem Namen und der Unterschrift des Kunden vom Kreditkartenunternehmen an das betroffene Vertragsunternehmen beanstandet.

### **6. Wirtschaftsauskunfteien**

#### **6.1 Benachrichtigung**

In mehreren Fällen mußte die Aufsichtsbehörde feststellen, daß Auskunfteien, die in § 34 Abs. 1 BDSG geforderte Benachrichtigung überhaupt nicht oder nicht in ausreichendem Maße durchgeführt haben. Sie verschaffen sich durch den Verzicht auf die schriftliche Benachrichtigung erhebliche Wettbewerbsvorteile (Kostensparnisse) gegenüber ihren korrekt schriftlich benachrichtigenden Wettbewerbern. Eine telefonische Benachrichtigung - in der Regel verbunden mit einer Befragung des Betroffenen - wird als nicht ausreichend angesehen, weil bei einem überraschenden Anruf der Betroffene in der Regel weder die Bedeutung des Anrufs noch Namen und Adresse der Auskunftei sofort richtig einschätzen und registrieren kann. Kenntnis des Namens und der Adresse der Auskunftei sind aber für den Betroffenen Voraussetzung, um sein Recht auf Selbstauskunft wahrzunehmen.

Bei den beanstandeten Auskunfteien bestand im übrigen der Verdacht, daß die behauptete telefonische Benachrichtigung eine reine Schutzbehauptung war, weil über die Telefongespräche keinerlei schriftliche Aufzeichnungen vorlagen. Im Falle der Nichtbenachrichtigung und im Falle der behaupteten telefonischen Benachrichtigung sind Bußgeldverfahren anhängig.

#### **6.2 SCHUFA**

Die Zahl der begründeten Beschwerden gegen die Schutzgemeinschaft für Allgemeine Kreditsicherung (SCHUFA) ist zurückgegangen.

Zu beanstanden war in einem Fall die Speicherung von Daten eines deutschen Ehepaares, das einen Kredit im Ausland aufgrund der Zusicherung der ausländischen Bank aufgenommen hatte, daß keine Weitergabe der Daten an die SCHUFA erfolge.

#### **6.3 Wechselprotestlisten**

Die Banken haben eine Arbeitsgemeinschaft mit der Aufgabe betraut, sämtliche bekanntgewordenen Wechselproteste zu sammeln und als Listen herauszugeben. Für diese Vorgänge ist das Bundesdatenschutzgesetz nicht anwendbar, weil der in § 2 Abs. 3 Ziffer 3 definierte Dateibegriff nicht erfüllt ist. Der persönlich Betroffene kann bei der genannten Arbeitsgemeinschaft deshalb auch keine Auskunftsrechte nach § 34 BDSG geltend machen. Die Situation wird lediglich dadurch etwas gemildert, daß man dem Betroffenen auch ohne den gesetzlichen Anspruch Auskünfte erteilt und erforderliche Korrekturen veranlaßt.

Diese Wechselprotestlisten wurden bei einer Auskunft auf Magnetband erfaßt. Damit war zumindest in diesem Fall der Datei-Begriff erfüllt und das Bundesdatenschutzgesetz anwendbar. Inzwischen werden dort diese Daten direkt in die vorhandene Auskunftsdatenbank eingegeben. Dadurch kann dann der Betroffene im Wege der Selbstauskunft nach § 26 Abs. 2 BDSG alle ihn betreffenden Daten erfahren.

Über die Herkunft eines möglicherweise fälschlich gespeicherten Wechselprotestes erfährt der Betroffene in der Regel jedoch nichts. Die unterschiedlichen rechtlichen Möglichkeiten für den Betroffenen je nachdem, ob die Wechselproteste in einer Liste oder einer sortierbaren Auskunftsdatenbank gespeichert sind, machen einmal mehr die Mängel des geltenden Datenschutzgesetzes anschaulich.

## **7. Zentrales Handelsregister**

Ein Wirtschaftsinformationsdienst übernimmt u.a. die Veröffentlichungen aus dem Handelsregister im Bundesanzeiger, um Firmendaten bundesweit zugänglich zu machen.

Der Bundesbeauftragte für den Datenschutz ist der Auffassung, daß die Registergerichte einem privaten Unternehmen nicht gestatten dürften, die Handelsregistereintragungen auf Mikrofilm aufzuzeichnen, weil er Bedenken gegen die Zulässigkeit eines privaten zentralen Handelsregisters hat (11. Tätigkeitsbericht, S. 22).

Zwar kommt die Tätigkeit des Unternehmers dem Betrieb eines zentralen Zweitregisters nahe, doch gibt es auch Unterschiede zum Handelsregister. Es sollen nämlich nicht sämtliche Firmen in die Datenbank aufgenommen werden und es sollen nur aktuelle Daten gespeichert werden. Eine mit den dezentralen Handelsregistern vergleichbare vollständige und lückenlose Dokumentation aller Firmen sei nicht beabsichtigt. Davon abgesehen teilte das Unternehmen mit, daß unter Beachtung des Beschlusses des Bundesgerichtshofes vom 12. Juli 1989 (Az.: IV a ARZ (VZ) 9/88 - NJW 1989, 2818), wonach § 9 HGB (Einsichtsrecht) kein Recht auf Gestattung der Mikroverfilmung des gesamten Handelsregisters gewähre, nicht mehr an die Registergerichte herangetreten werde. Es würden überwiegend die Veröffentlichungen des Bundesanzeigers und zur Ergänzung andere öffentlich zugängliche Quellen genutzt.

Es ist wünschenswert, daß der Gesetzgeber eine Entscheidung trifft, ob solche zentralen Datenbanken mit Daten aus allgemein zugänglichen Quellen zur kommerziellen Nutzung errichtet werden dürfen oder nicht.

## **8. Anbieten von Datenbanken auf CD-ROM**

Seit einiger Zeit bieten Unternehmen Daten nicht nur in on-line-Datenbanken, sondern auch auf einem neuen Speichermedium, der sogenannten CD-ROM (compact disk - read only memory), an. Hierbei handelt es sich um einen optisch lesbaren Datenträger mit extrem hoher Speicherkapazität und kurzer Zugriffszeit, der bereits bei der Herstellung mit Daten versehen wird. Die enthaltenen Daten lassen sich nicht mehr ändern oder löschen, sondern nur mittels besonderer Laufwerke lesen.

Datenschutzrechtlich relevant ist die Speicherung auf CD-ROM dann, wenn - wie in wissenschaftlichen oder wirtschaftlichen Datenbanken - unter anderem personenbezogene Daten, z.B. von Geschäftsführern, Ansprechpartnern oder Autoren, gespeichert sind.

Es stellt sich die Frage nach der Anwendbarkeit des Bundesdatenschutzgesetzes und - bei uneingeschränkter Anwendbarkeit - nach der Glaubhaftmachung und Aufzeichnung des berechtigten Interesses (§ 32 Abs. 2 BDSG) und der Benachrichtigungspflicht (§ 34 Abs. 1 BDSG). Ursprünglich lagen die mit dieser neuen Technik verbreiteten Daten in gedruckter Form vor. Das Bundesdatenschutzgesetz fand keine Anwendung, weil bereits die Datei-Eigenschaft fehlte. Auch die CD selbst kann nicht nach bestimmten Merkmalen umgeordnet werden. Sie enthält aber eine nach bestimmten Ordnungsmerk-

malen strukturierte Datensammlung und bietet zumindest die Möglichkeit, ihren Inhalt z.B. durch zwischengeschaltete Kopier- und Sortierläufe auf einem zweiten Datenträger nach anderen Merkmalen umzuordnen und auszuwerten. Nur bei einem wirksamen Kopierschutz würde eine Sortiermöglichkeit entfallen. Ein solcher Kopierschutz wäre aber mit der Art des Einsatzes einer solchen CD-ROM unvereinbar, weil auf eine Anzeige der Daten am Bildschirm bzw. einen Ausdruck zur Nutzung der CD nicht verzichtet werden kann. Die Bildschirmhalte bzw. die Druckdateien lassen sich dann wieder aufbereiten und sortieren.

Oft werden aber auch bereits fertige Auswertungsprogramme angeboten, die mittels eines PC (Personalcomputer) eine freie Auswertung erlauben.

Eine CD-ROM erfüllt also den Dateibegriff des Bundesdatenschutzgesetzes, so daß dies uneingeschränkt anwendbar ist.

In zwei Fällen berufen sich Unternehmen, die kommerziell Wirtschaftsdatenbanken auf CD-ROM anbieten, auf das Medienprivileg des § 1 Abs. 3 BDSG und wollen der Aufforderung der Aufsichtsbehörde zur Abgabe der Meldung nach § 39 BDSG nicht nachkommen. Die Berufung auf das Medienprivileg ist nicht überzeugend, weil mit der Verwertung nicht nur ausschließlich eigene publizistische Zwecke verfolgt werden, die Daten nicht nur gelegentlich an andere weitergegeben werden (S. VV zum BDSG B 2.1 - StAnz. 1981, S. 426) und die Dateien aus kommerziellen Gründen betrieben werden, die Daten also verkauft werden. Da die Tätigkeit eines solchen Unternehmens mit der Tätigkeit von Auskunftsteilen und Informationsdiensten vergleichbar ist, weil die Datenspeicherung geschäftsmäßig zum Zwecke der Übermittlung und somit für fremde Zwecke geschieht, sind die Vorschriften des 4. Abschnitts des Bundesdatenschutzgesetzes anzuwenden.

In der Praxis ist dies insofern weniger problematisch, soweit von den Unternehmen Datensicherungsmaßnahmen verlangt werden müssen. Problematisch erscheinen jedoch die Forderungen des Bundesdatenschutzgesetzes nach glaubhafter Darlegung des berechtigten Interesses bei jeder Übermittlung personenbezogener Daten und dessen Aufzeichnung. Fraglich erscheint bereits, ob ein berechtigtes Interesse an dem Inhalt einer vollständigen Datenbank und zugleich an jedem einzelnen darin enthaltenen personenbezogenen Datum dargelegt werden kann. § 32 BDSG sieht jedoch keine Ausnahme von der Darlegungs- und Aufzeichnungspflicht vor.

Hinsichtlich der Benachrichtigungspflicht gilt, daß in der Regel nicht davon ausgegangen werden kann, daß der Betroffene dem Unternehmen die Daten selbst zur Verfügung gestellt hat oder er in anderer Form ausreichend konkrete Kenntnis über die verarbeitende Stelle erlangt hat; er ist daher nach der ersten Übermittlung (Verkauf der CD-ROM oder Ermöglichen des online-Zugriffs, § 2 Abs. 2 Nr. 2, 2. Alt. BDSG) von der Speicherung zu benachrichtigen. Die Verpflichtung zur Benachrichtigung entfällt auch nicht nach §§ 34 Abs. 1 Satz 1, 32 Abs. 3 BDSG, weil keine "sonst zusammengefaßten" Daten (die sonstige Zusammenfassung muß mit der Form einer Liste vergleichbar sein) und außerdem mehr als nur ein zusätzliches Merkmal übermittelt werden. Eine Ausnahmeregelung wie § 26 Abs. 4 Nr. 4 BDSG besteht nicht.

Die Überlegungen zur Benachrichtigungspflicht dürfen aber nicht bei den Betreibern der Datenbanken oder den Firmen enden, die die CD-ROM erstellen und vermarkten, sondern es ist auch daran zu denken, daß Empfänger einer CD-ROM nach § 26 Abs. 1 BDSG ebenfalls zu benachrichtigen hätten, wenn man die CD-ROM nicht als allgemein zugängliche Quelle i.S. des § 26 Abs. 4 Nr. 4 BDSG ansieht.

Wenn man allerdings die praktischen und rechtlichen Probleme bei der Durchführung der Benachrichtigung betrachtet, die sich wiederum daraus ergeben, daß in zusammengefaßten Firmendaten auf der CD-ROM oder in übernommenen Handelsregistereintragungen personenbezogene Daten unstrukturiert "verborgen" sind, erscheint auch in diesem Zusammenhang eine Novellierung des Bundesdatenschutzgesetzes erforderlich. Da eine programmgesteuerte Suche personenbezogener Daten bei nur nach Firmen geordneten, ansonsten aber unstrukturierten Texten nach dem derzeitigen

Stand der Technik kaum möglich ist - und entsprechende Weiterentwicklungen im Hinblick auf dann immer leichter zu erstellende Persönlichkeitsprofile auch nicht erstrebenswert erscheinen - müßten diese Daten zur Erfüllung der Benachrichtigungspflicht mit sehr großem manuellem Aufwand durch Lesen aufgefunden und firmenübergreifend gesondert gespeichert werden. Weiterer fast unzumutbarer Aufwand entstünde durch die für die Zustellung der Benachrichtigung erforderliche Ermittlung der Anschriften der betroffenen Personen. Nicht selten dürfte dann eine Benachrichtigung eines Betroffenen mit verbreitetem Nachnamen wegen Identitätsverwechslung zu unzulässigen Datenübermittlungen führen.

Es wird jedoch nicht verkannt, daß ein vollständiger Verzicht auf eine Benachrichtigung zugunsten der angesprochenen Unternehmen nicht unproblematisch erscheint, weil die technischen Möglichkeiten es solchen Unternehmen im Prinzip erlauben, ohne Kenntnis des Betroffenen recht präzise Persönlichkeitsprofile, z.B. hinsichtlich seiner Tätigkeit im Wirtschaftsleben, zu erstellen, was dem Grundanliegen des Datenschutzes zuwiderliefe. Es müßten daher Regelungen geschaffen werden, die unter Abwägung der verschiedenen Interessen den veränderten technischen Verfahren bei der Datenverbreitung und den veränderten Informationsinteressen insbesondere im Hinblick auf Datenbanken in ausreichendem Maß Rechnung tragen. Zumindest sind bereichsspezifische Regelungen anzustreben. Daß Regelungsbedarf auch wegen der zunehmend internationalen Verbreitung von Datenträgern wie der CD-ROM und des grenzüberschreitenden Zugriffs auf on-line-Datenbanken besteht, kann hier nur angemerkt werden.

## 9. Warndienste

Im Berichtsjahr ist die Datenschutzaufsicht aufgrund von Eingaben oder Anfragen auf mehrere brancheninterne Warndienste aufmerksam geworden. In Verfahren und Aufbau unterscheiden sie sich nur unwesentlich voneinander. In der Regel werden sie von einer Stelle des entsprechenden Verbandes geführt und dienen den angeschlossenen bzw. den Verbandsunternehmen zur Beurteilung der Kreditfähigkeit ihrer Kunden z.B. bei Warenlieferungen auf Ziel. Ein Teil dieser Stellen ist der behördlichen Kontrolle bereits dadurch entzogen, daß jeweils aktuell monatlich oder vierteljährlich Listen zur Versendung an die angeschlossenen Unternehmen erstellt werden, die nicht dem Dateibegriff unterfallen und deshalb auch nicht nach den Vorschriften des Bundesdatenschutzgesetzes zu bewerten sind. In den Fällen, in denen die Datensammlungen den Dateibegriff erfüllen, unterliegen die Unternehmen der Meldepflicht gem. § 31 Abs. 1 Nr. 1 in Verbindung mit § 39 BDSG, da geschützte personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert werden. In mehreren Fällen wurde dieser Meldepflicht zum Teil jahrelang nicht nachgekommen.

Auch der Umfang der Datensammlungen war in einigen Fällen zu beanstanden. Insbesondere die Übermittlung und Speicherung von Negativ-Daten war mit dem Ziel der Objektivierung und Nachprüfbarkeit zu begrenzen. So kommt bei Merkmalen wie "Einleitung der Zwangsvollstreckung", "Eröffnung des Konkursverfahrens" oder "Abgabe der eidesstattlichen Versicherung nach § 807 ZPO" den berechtigten Interessen ein solches Gewicht zu, daß die schutzwürdigen Belange des Betroffenen demgegenüber in der Regel zurücktreten müssen. Problematisch wird die Übermittlung solcher Daten, die ohne gerichtliches Verfahren anfallen, wie z.B. "Mahnbescheid" oder gar "Mahnung bei Verzug des Schuldners".

Um das Risiko einer unerlaubten Datenverarbeitung auszuschalten, wurde den Mitgliedsunternehmen von den Warndiensten häufig bereits vertraglich zur Auflage gemacht, eine schriftliche Einwilligung zur Datenspeicherung und -übermittlung beim Betroffenen einzuholen. Hierbei waren jedoch in der Regel Verbesserungen hinsichtlich der Klarheit und Ausführlichkeit der Klauseln angebracht.

## 10. Markt- und Meinungsforscher

### 10.1 Quittungslisten

In einzelnen Fällen erhalten die Befragten Geld für die Teilnahme an bestimmten Veranstaltungen (z.B. Gruppendiskussionen) der Markt- und Meinungsforscher. Die bezahlten Beträge können von den Unternehmen nur steuerlich geltend gemacht werden, wenn die Empfänger den Erhalt des Geldes quittieren. In den meisten Fällen wurden bisher Quittungslisten angelegt, in denen nur der Name, der Betrag und die Unterschrift festgehalten wurde. Jetzt ist nach einer Steuerprüfung ein Markt- und Meinungsforschungsunternehmen veranlaßt worden, neben dem Namen auch noch die volle Adresse aufzuzeichnen. Es entstehen so personenbezogene Aufzeichnungen, die sonst nicht entstanden wären.

Hier steht die Forderung, möglichst wenig personenbezogene Daten aufzuzeichnen, gegen die Forderung der Finanzverwaltung nach nachprüfbaren Belegen über getätigte Ausgaben. Möglichkeiten, hier einzuschreiten, hat die Aufsichtsbehörde jedoch zur Zeit nicht, da die Quittungslisten in der Regel nicht den Dateibegriff des § 2 Abs. 3 Ziff. 3 BDSG erfüllen und damit das Bundesdatenschutzgesetz in diesem Zusammenhang nicht anwendbar ist.

### 10.2 Weitergabe von Adressen aus Befragungen

An Markt- und Meinungsforschungsunternehmen treten immer wieder deren Kunden mit der Bitte heran, die Adressen der Befragten herauszugeben. Als Begründung hierfür wird beispielsweise genannt, daß man bestimmte Geschenke dem Befragten selbst übersenden möchte.

Derartige Datenübermittlungen sind unzulässig. Selbst wenn nur die isolierten Adressen übermittelt werden, wird in unzulässiger Weise das Vertrauen des Befragten in das Markt- und Meinungsforschungsunternehmen auf ein dem Befragten häufig unbekanntes Unternehmen übertragen. Jedenfalls ist nicht auszuschließen, daß durch die Verbindung informatischer Zwecke mit wirtschaftlichen Interessen schutzwürdige Belange der Betroffenen beeinträchtigt werden (§ 32 Abs. 2 und 3 BDSG).

Erfreulicherweise geben die Markt- und Meinungsforschungsunternehmen in der Praxis dann auch keinerlei Adressen heraus. In Einzelfällen müssen sie sich lediglich mit Hilfe der Aufsichtsbehörde den weitergehenden Wünschen ihrer Kunden erwehren. Die Auffassungen der Markt- und Meinungsforscher und der Aufsichtsbehörde stimmen in diesem Punkt überein.

## 11. Datenvernichtung

Bei der Überprüfung mehrerer Unternehmen, die Datenvernichtung anbieten, war ein sehr unterschiedlicher Leistungsstandard festzustellen. Ein größerer Automatisierungsgrad der Datenvernichtung ist insgesamt vorteilhaft, weil manuelle Eingriffe von Mitarbeitern und die damit verbundenen Mißbrauchsmöglichkeiten verringert werden.

Der Verzicht auf jegliche manuelle Vorsortierung des angelieferten Materials erhöht ebenfalls die Sicherheit der Datenvernichtung. Auch hierbei verhindert die sofortige Beschickung der Maschinen mißbräuchliche Eingriffe des Personals. Diese Vorgehensweise gefährdet allerdings die Maschinen (z.B. Schäden durch größere Hartmetallgegenstände) und die Qualität der erzeugten Papierballen sinkt erheblich. Es muß deshalb schon mit konsequentem getrennten Sammeln beim Kunden des Datenvernichters begonnen werden.

Einige Kunden von Datenvernichtern lieferten besonders sensitive Daten in einfachen Plastiksäcken an. Diese nicht sehr zuverlässige Transportsicherung war zu beanstanden. Da hierfür jedoch noch nicht der Datenvernichter die Verantwortung trägt, hat die Aufsichtsbehörde in diesen Fällen in der Regel erst Eingriffsbefugnisse, wenn sich der persönlich Betroffene bei ihr beschwert, weil er sich in seinen schutzwürdigen Belangen beeinträchtigt sieht. Die Kunden von Datenvernichtern verarbeiten nämlich zum größten Teil nur Daten für eigene Zwecke, so daß die Aufsichtsbehörde nach den Bestimmungen des § 30 BDSG auf die Anlaßkontrolle beschränkt ist.

## 12. Versandhandel

Auch im Berichtsjahr 1989 gingen wiederum eine Vielzahl von Anfragen und Beschwerden bezüglich des Versandhandels ein. In diesem Bereich ist auf Seiten der Betroffenen ein geschärftes Datenschutzbewußtsein zu bemerken.

In mehreren Fällen wurde die Behörde um Unterstützung bei der Wahrnehmung von Auskunfts- und Löschungsansprüchen gebeten. Ebenfalls in mehreren Fällen wurde die Anbringung der Telefonnummer des Kunden deutlich sichtbar auf der Postsendung kritisiert. In diesen Fällen erklärte sich das betroffene Versandhaus lediglich bereit, bei einzelnen Beschwerden die Telefonnummer in Zukunft aus dem Anschriften- und Datenfeld auf der Sendung wegzulassen. Eine generelle Änderung des Versandverfahrens wurde abgelehnt.

## 13. Datensicherung

Im Berichtsjahr konnte bei Überprüfungen gem. § 40 BDSG bei einer Reihe von Unternehmen festgestellt werden, daß die Vorschriften zur Datensicherung weitgehend in die Praxis umgesetzt worden sind. War jedoch der Trend bis Ende der 80er Jahre hinsichtlich der Maßnahmen insgesamt als positiv zu bewerten, so nahm im letzten Jahr die Ratlosigkeit der Datenverarbeiter wieder in dem Maße zu, in dem die Arbeitsplatzrechner (PC) und on-line-Anschlüsse zunahmen.

Die verteilte Datenverarbeitung hat hier neue Risiken in zunehmender Größenordnung geschaffen, zu deren Eindämmung bzw. Beherrschung noch keine allgemein gültigen Regeln gefunden wurden.

Die verbesserten Arbeitstechniken führen auch dazu, daß der Sachbearbeiter weitere Aufgabengebiete zugewiesen bekommt, dadurch mehr Daten verarbeiten muß als zuvor und entsprechend auch weitere Zugriffsmöglichkeiten auf personenbezogene Daten erhalten muß.

Die Entwicklung im Bereich der PC- und On-line-Anwendungen hat weiter dazu geführt, daß die zu fordernde Funktionstrennung zwischen Entwickler- und Anwenderseite oft nicht mehr eingehalten werden kann, weil z.B. der Entwickler bei einem Fehler, der im on-line-Bereich aufgetreten ist, unter Umständen an diesem bestimmten Terminal die Verarbeitungsfolge mit Originaldaten nachvollziehen muß, um den Fehler lokalisieren zu können. Es führte dennoch zu einer Beanstandung durch die Aufsichtsbehörde, wenn Mitarbeitern aus dem Entwicklungsbereich bereits vorsorglich umfassende Berechtigungen auch für Originaldatenbestände gegeben worden waren.

Beanstandungen erfolgten häufig auch im Bereich der Zugangskontrolle. Es war festzustellen, daß Zugangsberechtigungen oftmals zu großzügig und vor allem in nicht jederzeit überschau- und überprüfbarem Umfang ausgegeben wurden. Das gleiche gilt für die Vergabe von Passwörtern. Auch hier werden lieber zu weit gehende Berechtigungen eingeräumt, als daß Berechtigungen eingeschränkt werden. Teilweise war zu beanstanden, daß die automatisierte Verarbeitung nicht nachvollziehbar war. Es war im nachhinein nicht mehr festzustellen, wer für eine bestimmte Dateneingabe bzw. Datenveränderung verantwortlich war. Kontrollen im Bereich der Dateneingabe werden zum Teil von den Unternehmen als unzumutbar bezeichnet. Es bleibt jedoch festzuhalten, daß mit den heutigen technischen Möglichkeiten eine ausreichende Eingabekontrolle in zumutbarer Weise zu erfüllen ist.

## 14. Bildschirmtext

Die hessischen Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich sind auch zuständige Verwaltungsbehörden für den Vollzug des Bildschirmtext-Staatsvertrages (Btx-StV) bei nicht-öffentlichen Stellen. Beim Betrieb des Bildschirmtextsystems treten infolge der Verarbeitung personenbezogener Daten Datenschutzprobleme auf, die nach den Regelungen des Bildschirmtext-Staatsvertrages oder kraft Verweisung (Artikel 9 Abs. 1 Btx-StV) nach den Vorschriften des Bundesdatenschutzgesetzes zu beurteilen sind.

### 14.1 Dialogdienste

Die Problematik der elektronischen "Pin-Wand" wurde bereits im letzten Jahresbericht (Drucks. 12/5153, S. 15) dargestellt.

In dem konkret bekannt gewordenen Fall wurde die Möglichkeit des Mißbrauchs durch Angabe einer fremden Telefonnummer dadurch abgestellt, daß die Inhalte der "Pin-Wand" mehrfach am Tag überprüft und eingegebene Telefonnummern grundsätzlich gelöscht werden.

Weitere Fälle von Mißbrauch sind bisher nicht bekannt geworden.

### 14.2 Geschlossene Teilnehmergruppen

Zur Überprüfung sowohl der Einhaltung datenschutzrechtlicher Bestimmungen (hier gelten wie oben ausgeführt kraft Verweisung das Bundesdatenschutzgesetz sowie die speziellen Datenschutzregelungen des Art. 9 Abs. 2 - 8 Btx-StV) als auch der speziellen Vorschriften des Btx-Staatsvertrages wäre es, wie es sich gezeigt hat, angebracht, die Praktiken der Anbieter auch insoweit kontrollieren zu können, als Angebote an bestimmte Teilnehmer gerichtet werden, die durch gemeinsame berufliche, ideelle oder vergleichbare persönliche Merkmale untereinander und durch vertragliche, mitgliedschaftliche oder öffentlich-rechtliche Beziehungen mit dem jeweiligen Anbieter verbunden sind (geschlossene Teilnehmergruppen gem. Artikel 3 Abs. 1 Satz 2 Btx-StV).

Der Zugang zu solchen geschlossenen Teilnehmergruppen wird jedoch erst durch den Anbieter eröffnet, der im konkreten Fall diesen auf freiwilliger Basis der Aufsichtsbehörde nicht gewährte. Es ist bisher nicht geklärt, ob und in welcher Weise der Zugang von der Aufsichtsbehörde erzwungen werden kann. Die deutsche Bundespost interpretiert die Befugnisse der Aufsichtsbehörde nach Artikel 12 Btx-Staatsvertrag dahingehend, daß eine richterliche Durchsuchungsanordnung für die im Postrechner gespeicherten Daten aus dem Angebot für die geschlossene Teilnehmergruppe erforderlich ist.

In einem Fall wurde deshalb Strafanzeige bei der Staatsanwaltschaft erstattet, da sie erweiterte Ermittlungsmöglichkeiten hat. Dieses Verfahren ist noch nicht abgeschlossen. Im genannten Fall muß die Aufsichtsbehörde davon ausgehen, daß fingierte Partnerschaftsangebote Btx-Teilnehmer zur Offenlegung ihres Namens, ihrer Adresse, ihres Btx-Anschlusses und ihrer speziellen Sexwünsche gegenüber dem Btx-Anbieter veranlassen. Darüber hinaus geht der neue Teilnehmer an der geschlossenen Teilnehmergruppe erhebliche finanzielle Verpflichtungen gegenüber dem Anbieter ein, deren Angemessenheit und rechtliche Begründetheit sehr zweifelhaft erscheinen. Unklar ist weiter, wie der Btx-Anbieter all diese Daten verwendet.

Beschwerden Betroffener werden, wie der Zusammenhang mit sexuellen Angeboten vermuten läßt, an die Aufsichtsbehörde aus datenschutzrechtlicher Sicht kaum herangetragen. Die betroffenen Teilnehmer bzw. Interessenten an den geschlossenen Teilnehmergruppen versuchen lediglich, von den eingegangenen, anfangs in ihrer Höhe jedoch nicht durchschauten finanziellen Verpflichtungen freizukommen.

## 15. Ordnungswidrigkeiten

Im Berichtsjahr wurden 14 Bußgeldverfahren eingeleitet, die in sieben Fällen mit einem Bußgeldbescheid, und in fünf Fällen mit einer Einstellung des Verfahrens abgeschlossen wurden. Ein Bußgeldbescheid ist noch nicht rechtskräftig, da Einspruch eingelegt wurde. Zwei Verfahren sind noch nicht abgeschlossen.

Die Mehrzahl der Bußgeldverfahren (sieben Fälle) betraf die verspätete Abgabe der nach § 39 BDSG erforderlichen Meldungen an die Aufsichtsbehörde (Ordnungswidrigkeit nach § 42 Abs. 1 Nr. 4 BDSG). In zwei dieser Fälle kam hinzu, daß entgegen § 38 i.V.m. § 28 Abs. 1 BDSG ein Beauftragter für den Datenschutz nicht rechtzeitig bestellt wurde (Ordnungswidrigkeit nach § 42 Abs. 1 Nr. 2 BDSG).

In einem weiteren Fall hatte ein brancheninterner Warndienst neben der Nichtabgabe der erforderlichen Meldung und der Nichtbestellung eines Datenschutzbeauftragten die Betroffenen weder nach § 34 Abs. 1 BDSG von der erfolgten Datenspeicherung benachrichtigt (Ordnungswidrigkeit nach § 42 Abs. 1 Nr. 1 BDSG), noch das berechnigte Interesse gem. § 32 Abs. 2 Satz 2 BDSG aufgezeichnet (Ordnungswidrigkeit nach § 42 Abs. 1 Nr. 3 BDSG). In diesem Fall wurde die Aufsichtsbehörde erst aufgrund der Beschwerde eines persönlich Betroffenen auf die Existenz des seit Jahrzehnten bestehenden Warndienstes aufmerksam.

Bei einem weiteren Schwerpunkt der Verfahren (sechs Fälle) waren die Betroffenen ihrer Auskunftspflicht gegenüber der Aufsichtsbehörde nach §§ 30 Abs. 2 bzw. 40 Abs. 2 i.V.m. § 30 Abs. 2 BDSG nicht rechtzeitig nachgekommen (Ordnungswidrigkeiten nach § 42 Abs. 1 Nr. 5 BDSG).

Ein weiteres Verfahren wurde gegen eine Auskunftfei aufgrund der nicht erfolgten Benachrichtigung der Betroffenen über die Speicherung ihrer personenbezogenen Daten entgegen § 34 Abs. 1 Satz 1 BDSG eingeleitet (Ordnungswidrigkeit nach § 42 Abs. 1 Nr. 1 BDSG). Da Einspruch eingelegt wurde, ist der hier ergangene Bußgeldbescheid noch nicht rechtskräftig.

Wiesbaden, den 20. August 1990

Der Hessische Ministerpräsident  
Dr. Wallmann

Der Hessische Minister des Innern  
In Vertretung:  
Stanitzek



- 1 - 13



12. Wahlperiode

zu Drucksache **12/7186**

# HESSISCHER LANDTAG

22. 08. 90

**Berichtigung  
zu Drucksache 12/7186**

**Vorlage  
der Landesregierung**

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

Im Vorspann muß es richtig lauten:

Vorgelegt mit der Stellungnahme zum Achtzehnten Tätigkeitsbericht des  
Hessischen Datenschutzbeauftragten - Drucks. 12/6126 - gemäß § 30 Abs. 2  
Satz 2 des Hessischen Datenschutzgesetzes vom 11. November 1986.

Wiesbaden, den 22. November 1990

**Kanzlei des Landtags**