14. Wahlperiode

Drucksache **14/3086**

HESSISCHER LANDTAG

01. 08. 97

Vorlage der Landesregierung

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

Vorgelegt mit der Stellungnahme zum Fünfundzwanzigsten Tätigkeitsbericht des Hessischen Datenschutzbeauftragten - Drucks. 14/2701 - nach § 30 Abs. 2 des Hessischen Datenschutzgesetzes vom 11. November 1986.

Eingegangen am 1. August 1997 · Ausgegeben am 19. August 1997

Druck und Auslieferung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden

Inhaltsverzeichnis

1. Bearbeitung von an die Behörde herangetragenen Datenschutzbeschwerden nach § 38 Abs. 1 BDSG

Die Aufsichtsbehörden überprüfen nach § 38 Abs. 1 BDSG im Einzelfall die Ausführung des Bundesdatenschutzgesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die Verarbeitung oder Nutzung personenbezogener Daten in oder aus Dateien regeln, wenn ihnen hinreichende Anhaltspunkte dafür vorliegen, daß eine dieser Vorschriften durch eine nichtöffentliche Stelle verletzt ist, insbesondere wenn es Betroffene selbst begründet darlegen.

Im Berichtsjahr gingen bei den Aufsichtsbehörden 149 Beschwerden gegen Stellen ein, die Datenverarbeitung nach § 28 BDSG für die Erfüllung eigener Geschäftszwecke betreiben oder personenbezogene Daten nach §§ 29, 30 BDSG zur personenbezogenen oder anonymisierten Übermittlung speichern und nutzen.

Alle Beschwerden führten zur Überprüfung der datenverarbeitenden Stellen durch die Aufsichtsbehörde.

Die Beschwerden betrafen:

- Kreditinformationsdienste
  (Handels- und Wirtschaftsauskunfteien, SCHUFA) in 27 Fällen,
- Versicherungen in 24 Fällen,
- Kreditinstitute und Banken in 13 Fällen,
- den Handel und Einzelhandel in 10 Fällen,
- Verbände und eingetragene Vereine in 9 Fällen,
- das Gesundheitswesen (Kliniken, Heime, Ärzte) in 5 Fällen,
- Paket- und Kurierdienste in 4 Fällen,
- den Versandhandel in 4 Fällen,
- Adreßverlage in 4 Fällen,
- Vermögens- und Finanzberater in 3 Fällen,
- Vermieter und Hausverwaltungen in 3 Fällen,
- Kreditkartenunternehmen in 2 Fällen,
- Touristikbüros und Reiseveranstalter in 2 Fällen,
- Anbieter von Telekommunikationsdiensten in 2 Fällen,
- sonstige Unternehmen unterschiedlicher Branchen (z.B. Autovermietung, Sicherheitsdienst, Softwarebranche, Partnervermittlung, Personenbeförderung, Immobilienmakler, Markt- und Meinungsforschung, Glaubensgemeinschaft, Anwaltskanzlei) in 37 Fällen.

In 35 Fällen waren die Beschwerden wegen unzulässiger Datenverarbeitung begründet, davon in 11 Fällen gegen Versicherungsgesellschaften, wobei acht dieser Beschwerden gegen eine Krankenversicherung lediglich teilweise begründet waren. Weitere durch Verstöße gegen Datenschutzbestimmungen begründete Eingaben richteten sich in fünf Fällen gegen Banken, in fünf Fällen gegen Kreditinformationsdienste, sowie in je einem Fall gegen ein Einzelhandelsunternehmen, zwei Vereine, einen Reiseveranstalter, sowie einen Finanzmakler. Acht weitere begründete Beschwerden richteten sich gegen sonstige Unternehmen.

Bei elf Beschwerden konnte der zugrunde liegende Sachverhalt nicht mehr vollständig aufgeklärt werden, so daß eine abschließende Beurteilung, ob die Datenverarbeitung in zulässiger oder in unzulässiger Weise erfolgt war, nicht getroffen werden konnte. In 22 Fällen sind die Ermittlungen der Aufsichtsbehörde noch nicht abgeschlossen.

Aus den Vorjahren wurden 64 Beschwerdefälle abgeschlossen. Diese Fälle waren in der Regel nur mit hohem Ermittlungsaufwand aufklärbar. Die Beurteilung der Aufsichtsbehörde ergab, daß davon 25 Beschwerden begründet waren. Dabei hatten in fünf Fällen Kreditinstitute, in jeweils drei Fällen Wirtschaftsauskunfteien und Versandhandelsunternehmen, in jeweils zwei

Fällen Versicherungsgesellschaften, Vereine, Fluglinien und Verlage, sowie in je einem Fall ein Reisebüro, ein Kreditkartenunternehmen, ein Einzelhändler und drei sonstige Unternehmen personenbezogene Daten unzulässig verarbeitet oder genutzt.

In zwölf bereits in den Vorjahren eingereichten Fällen konnte eine abschließende Beurteilung, ob die Datenverarbeitung in zulässiger oder in unzulässiger Weise erfolgt war, mangels eindeutigen Sachverhaltes nicht getroffen werden.

Weiterhin erhielt die Aufsichtsbehörde in fünf Fällen durch Artikel in der lokalen und überregionalen Presse Anhaltspunkte für Verstöße gegen datenschutzrechtliche Vorschriften. Die vier betroffenen Banken und das Kreditkartenunternehmen wurden durch die Aufsichtsbehörde überprüft. Gegenüber zwei Banken wurden Beanstandungen ausgesprochen. Die anschließende Beratung durch die Aufsichtsbehörde führte zu geeigneten Maßnahmen, mit denen die Mängel beseitigt wurden. Ein Fall im Bankbereich konnte mangels eindeutigen Sachverhalts nicht aufgeklärt werden, ein weiterer Fall wird noch bearbeitet.

2. Von Amts wegen durchgeführte Überprüfungen von Stellen, die nach § 32 Abs. 1 Ziff. 1 bis 3 BDSG geschäftsmäßig personenbezogene Daten verarbeiten oder nutzen

2.1 Register

Die Aufsichtsbehörde führt nach § 38 Abs. 2 BDSG das Register der Stellen, die personenbezogene Daten geschäftsmäßig zum Zweck der personenbezogenen oder der anonymisierten Übermittlung speichern oder im Auftrag als Dienstleistungsunternehmen verarbeiten oder nutzen. Diese Stellen unterliegen nach § 32 BDSG der Meldepflicht.

Am 1. Februar 1997 waren im Register der meldepflichtigen Stellen bei den Aufsichtsbehörden 682 Unternehmen eingetragen. Die nach § 32 Abs. 1 Ziff. 1 BDSG meldepflichtigen Unternehmen haben daran den geringsten Anteil, gefolgt von den nach § 32 Abs. 1 Ziff. 2 BDSG gemeldeten Markt- und Meinungsforschungsunternehmen. Die nach § 32 Abs. 1 Ziff. 3 BDSG meldepflichtigen Unternehmen, die im Auftrag Dritter Datenverarbeitung als Dienstleistung betreiben, stellen mit 500 gemeldeten Stellen den Hauptanteil des Meldebestandes bei den Aufsichtsbehörden dar.

Innerhalb dieser Gruppe von Dienstleistungsunternehmen sind die Dienstleistungsrechenzentren am stärksten vertreten, was auch der auf dem Markt zu beobachtenden Outsourcingtendenz im Datenverarbeitungsbereich entspricht. Als weitere relevante Branchen sind die Schreibservices und Datenerfasser zu verzeichnen, gefolgt von Konzernrechenzentren, Adreßbrokern/Lettershop-Unternehmen und Datenträgervernichtern.

2.2 Prüfungsübersicht

Im Berichtsjahr wurden 46 Prüfungen nach § 38 Abs. 2 BDSG durchgeführt. Davon betrafen Datenverarbeiter nach § 32 Abs. 1 Ziff. 3 BDSG insgesamt 36, nämlich

- Servicerechenzentren 10
- Konzerndatenverarbeiter 2
- Datenerfasser und Schreibbüros 7
- Adreßhändler 5
- Mikroverfilmer 1
- Datenträgervernichter 6
- Telemarketingunternehmen 1
- Sonstige 4

Desweiteren wurden 4 Kreditinformationsdienste und 6 Unternehmen aus dem Bereich der Markt- und Meinungsforschung geprüft.

Die Prüfungen brachten folgendes Ergebnis:

- Beanstandungen 15
- Empfehlungen 23
- ohne wesentliche Beanstandungen 8

Folgende wesentliche Mängel wurden am häufigsten festgestellt:

1. keine bzw. verspätete oder unvollständige Registermeldung nach § 32 BDSG
2. keine bzw. unvollständige Weisungen des Auftraggebers nach § 11 BDSG
3. kein Datenschutzbeauftragter, Mängel in der Aus- und Fortbildung, Mängel in der Tätigkeit
4. fehlende bzw. unvollständige Dokumentation
5. unvollständige Zugangskontrolle, mangelhafte Datenträgerverwaltung
6. mangelhafte Zugriffskontrolle, unzureichende Paßwortverwendung
7. fehlende Verpflichtung auf das Datengeheimnis (§ 5 BDSG)

2.3 Meldepflichten

Die Meldepflichten werden von zahlreichen - in der Regel mittleren und kleineren - Unternehmen überhaupt nicht oder in nicht ausreichendem Umfang beachtet.

Bei gezielten Rückfragen nach Veränderungen konnte mehrmals festgestellt werden, daß die Unternehmen bereits ihren Standort gewechselt hatten, ohne dies zu melden. Gegen Unternehmen, die sich ohne besondere Aufforderung - wenn auch verspätet - melden, wird gegenwärtig kein Ordnungswidrigkeitsverfahren eingeleitet.

2.3.1 Meldepflicht von Konzerndatenverarbeitern

Einige Konzerndatenverarbeiter wickeln große Teile der Datenverarbeitung zentral für ihre Tochterunternehmen ab. Zusätzlich wird die Datenverarbeitung als Kontrollinstrument zur Überwachung der verbundenen Unternehmen genutzt. Nach Auffassung dieser Konzerndatenverarbeiter - hier vor allem Großbanken - begründet die Überwachungstätigkeit eine Funktionsübernahme. Demnach wäre der Datenverarbeiter nicht mehr Auftragnehmer, sondern selbst speichernde Stelle und eine Meldepflicht nach § 32 BDSG würde entfallen. In diesen Fällen wäre die Datenweitergabe im Konzern als Übermittlung zu werten. Die Aufsichtsbehörde teilt diese Auffassung jedoch nicht uneingeschränkt. Wie weitgehend die Kontrollen über das auftraggebende Tochterunternehmen auch immer sein mögen, in der Regel wird die Durchführung der Datenverarbeitung im zentralen Konzernrechenzentrum im Vordergrund stehen. In konkreten Einzelfällen wird nachzuprüfen sein, wo der Schwerpunkt der Datenverarbeitung für die Tochterunternehmen liegt. Wenn das Unternehmen die Datenverarbeitung des Konzerns wie bei einem Outsourcing-Unternehmen nutzt, ist von einer Meldepflicht nach § 32 Bundesdatenschutzgesetz auszugehen.

So wurde im Fall einer Frankfurter Großbank Übereinstimmung im Hinblick auf deren Meldepflicht erzielt.

2.3.2 Meldepflicht von Nachrichtenagenturen

Die Überprüfung einer Nachrichtenagentur ergab, daß es sich um ein Hilfsunternehmen der Presse handelte. Der Abruf von Nachrichten aus den Datenbanken des Unternehmens ist zwar in vielen Fällen personenbezogen, die Nutzung bleibt jedoch journalistischen Zwecken vorbehalten. Eine Meldepflicht des Unternehmens ist daher zu verneinen; lediglich die §§ 5 (Datengeheimnis) und 9 (technische und organisatorische Maßnahmen) BDSG sind zu beachten.

2.3.3 Meldepflicht von Telekommunikationsunternehmen

Telekommunikationsunternehmen, deren Tätigkeit vor allem darin besteht, ein Kommunikationsnetz zur Verfügung zu stellen, betreiben keine meldepflichtige Tätigkeit nach § 32 BDSG. Aus technischen Gründen werden Daten für sehr kurze Zeiträume gespeichert, die Anwendung des Bundesdatenschutzgesetzes bleibt nach § 1 Abs. 3 Ziff. 1 BDSG auf die §§ 5 und 9 BDSG (Datengeheimnis bzw. technische organisatorische Maßnahmen) beschränkt.

Im Rhein-/Main-Gebiet befinden sich einige große Netzanbieter, die mit modernster Technik Telekommunikationsdienstleistungen anbieten. Teilweise werden eigene Netze, unter anderem Glasfasernetze, teilweise die Netze der Telekom AG genutzt. Die Einhaltung der Datenschutzbestimmungen überwacht in diesem Fall der Bundesbeauftragte für den Datenschutz nach § 91 Abs. 4 Telekommunikationsgesetz (TKG).

Bei der Aufsichtsbehörde laufende Verfahren aus diesem Bereich werden zukünftig an den Bundesbeauftragten abgegeben.

3. Bearbeitung von Anfragen zu Datenschutzproblemen

Im Berichtsjahr wurden an die Aufsichtsbehörden zahlreiche schriftliche und telefonische Anfragen von betroffenen Bürgern, Arbeitnehmern, Datenschutzbeauftragten und Unternehmen zu unterschiedlichsten Fragestellungen des Datenschutzes herangetragen.

Einen Schwerpunkt bildeten dabei die zahlreichen Fragen zur Position und Funktion des betrieblichen Datenschutzbeauftragten im Unternehmen nach §§ 36, 37 BDSG. Dies kann als Ergebnis der verstärkten Pressearbeit der Aufsichtsbehörde verstanden werden und zeigt erneut, daß an diesem sensiblen Punkt des institutionalisierten Datenschutzes im Betrieb noch erheblicher Nachholbedarf, aber gleichzeitig auch großes Interesse bei den Wirtschaftsunternehmen besteht.

Oftmals stand bei den Eingaben durch Datenschutzbeauftragte, Unternehmen und deren Rechtsvertreter auch die Frage nach der Zulässigkeit geplanter Datenverarbeitungsvorhaben im Vordergrund. Dieses Vorgehen soll regelmäßig sicherstellen, daß geplante Systeme den Datenschutzbestimmungen entsprechen. Datenschutzrechtliche Einwände und kostspielige Fehlinvestitionen der Unternehmen können so durch die rechtzeitige Einbindung der Aufsichtsbehörde bereits im Planungsstadium vermieden werden.

Hervorzuheben ist das verstärkte Engagement von Fach- und Dachverbänden oder als eingetragene Vereine organisierter Interessengruppen, deren Datenschutzbeauftragte für ihre Mitglieder den Kontakt zur Aufsichtsbehörde suchen, um Probleme zu analysieren und Lösungen zu erarbeiten.

Inhaltlich richteten sich die Anfragen auf die verschiedensten von automatisierten Datenverarbeitungsprozessen durchdrungenen Lebensbereiche der Bürgerinnen und Bürger. Das Themenspektrum reichte von Sicherheitsproblemen beim Telebanking bis zu Anfragen nach der Zulässigkeit der Verarbeitung personenbezogener Daten zu historisch-archivarischen Zwecken. Weitere Fragen betrafen den Adreßhandel, Banken, Auskunfteien, Vermieter und Eigentümergemeinschaften, Wohnen, Verkehr, Touristik, Arbeitsverhältnis und Datenverarbeitung im Verein.

Die Aktivitäten eines Internet-Hackers, dem es von einem privaten Netz-Provider im Rhein-Main Gebiet aus gelungen war, sogar bis in die Rechner ausländischer Militäreinheiten zu gelangen, führten ebenfalls zu Anfragen betroffener Stellen bei der Aufsichtsbehörde. Der Hacker, der weltweit vollautomatisiert zahlreiche Fremdsysteme attackierte und dabei versuchte, an deren Paßwortdateien zu gelangen, benutzte zur Täuschung über seine Identität unter anderem auch fremde Zugangsberechtigungen zum Rechnernetz einer hessischen Hochschule, über die er seine unzulässigen Aktivitäten abwickelte. Die folgende Zusammenarbeit mit dem für den öffentlichen Bereich zuständigen Hessischen Datenschutzbeauftragten gestaltete sich positiv und führte schnell zu einem Ergebnis.

Die breite Streuung der Themengebiete veranschaulicht die beherrschende Position der Datenverarbeitung als Querschnittstechnologie in der Alltagskultur. Es wird gleichzeitig deutlich, daß der Schutz personenbezogener Daten in der modernen Informationsgesellschaft beständig weiterentwickelt und verfeinert werden muß, um den neuen Anforderungen und Herausforderungen, die in fast allen Lebenssphären durch den Einsatz moderner Kommunikations- und Informationstechnologien gestellt werden, gerecht werden zu können.

4. Wirtschaftsauskunfteien

Beschwerden gegen Wirtschaftsauskunfteien sowie Anfragen über deren Tätigkeit nehmen einen wesentlichen Raum ein.

In diesem Zusammenhang wäre in manchen Fällen eine offenere Informationspolitik der Auskunfteien wünschenswert. Ein informierter Bürger wird nachvollziehen können, daß ein Geschäftspartner - Kreditgeber, Warenlieferant etc. - sichergehen möchte, daß der Betroffene seinen finanziellen Verpflichtungen auch nachkommen kann.

Die häufig gestellte Frage, ob die Auskunftei über den Betroffenen Daten speichern und übermitteln darf, ist in den vorgenannten Fällen in der Regel zu bejahen, wenn die Daten zutreffend sind und sich auf die wirtschaftlichen Verhältnisse beschränken. Dem von Betroffenen gelegentlich vorgebrachten Wunsch, die Aktivitäten der Auskunftei zu untersagen, kann bei Beachtung der Erlaubnistatbestände des § 29 BDSG (geschäftsmäßige Datenverarbeitung zum Zweck der Übermittlung) nicht entsprochen werden.

4.1 Testanfragen

Nur in Einzelfällen konnte festgestellt werden, daß die Anfragen bei einer Auskunftei und die damit verbundene Datenverarbeitung datenschutzrechtlich problematisch waren.

So wollte eine Auskunftei einen neuen Kunden werben und führte für diesen Kunden Testanfragen an der Originalauskunftsdatenbank durch. Bei Anfragen über personenbezogene Daten ist die Übermittlung jedoch nur zulässig, wenn nach § 29 Abs. 2 Ziff. 1 a BDSG das berechtigte Interesse an den Daten glaubhaft dargelegt wird und dem keine schutzwürdigen Interessen der Betroffenen entgegenstehen.

Eine Testanfrage erhielt als berechtigtes Interesse das unzutreffende Merkmal "Kreditanfrage". Zufällig führte der Test dann nicht zu einer Anfrage über eine gewünschte Firmengruppe sondern zu Recherchen über eine natürliche Person (inklusive Nachbarschaftsbefragungen). Die Auskunftei konnte den Eingriff in die Privatsphäre des Betroffenen begrenzen, weil Sie rechtzeitig erkannte, daß die betroffene Einzelperson in keinerlei Verbindung mit der angefragten Firmengruppe stand. Die Auskunft wurde nicht herausgegeben.

Der Fall zeigt einen grundsätzlichen Mangel auf. Bei Kundenvorführungen, Messen etc. dürfen keinesfalls Daten über die wirtschaftlichen Verhältnisse von Einzelpersonen zu Demonstrationszwecken abgefragt und übermittelt werden.
Es besteht Bedarf an derartigen Vorführungen - hier auch zu Schulungszwecken für künftige Direktabfrager -; es sollten jedoch Testdaten bzw. Daten von juristischen Personen (Ausnahme: Ein-Personen-Gesellschaft) für diese Zwecke benutzt werden. Das berechtigte Interesse muß darüber hinaus zutreffend aufgezeichnet werden, wenn auch bei der Nennung eines Geschäftsführers/Gesellschafters einer juristischen Person in der Regel keine Beeinträchtigung schutzwürdiger Belange zu befürchten ist.

4.2 Ehegattendaten

Bei Anfragen über eine Person, wird nur in Ausnahmefällen eine Auskunft über den Ehepartner erforderlich sein (z.B. Strohmann-Situation). In einem Beschwerdefall waren die schutzwürdigen Belange der Ehefrau beeinträchtigt, weil sich das berechtigte Interesse eindeutig nur auf den Ehemann bezog. Die Ehefrau hatte Anspruch darauf, daß sie nicht ohne ein besonderes

Erfordernis gemeinsam mit den (negativen) Daten des Ehemannes genannt wurde, umso mehr als das Ehepaar getrennt lebte. In der Auskunft über den Ehemann hätte es völlig ausgereicht, den Familienstand "verheiratet" zu benennen. Insgesamt entstand bei der erteilten Auskunft der Eindruck, daß die Ehefrau genannt wurde, um die im übrigen wenig aufschlußreichen Auskünfte optisch anzureichern. Eine derartige Auskunfts-"Kosmetik" kann aus datenschutzrechtlichen Gründen nicht akzeptiert werden.

5. SCHUFA

Die SCHUFA (Schutzgemeinschaft für allgemeine Kreditsicherung) speichert und übermittelt personenbezogene Daten zur Kreditwürdigkeit. Vertragspartner der SCHUFA sind Banken, Versandhäuser, Leasingunternehmen und Telekommunikationsanbieter.

Der Umfang der eingegangenen Beschwerden war - in Anbetracht des Massengeschäfts - gering. Die Zusammenarbeit mit der SCHUFA gestaltete sich in diesem Bereich weiterhin erfreulich. Berechtigten Beschwerden wurde sofort nachgegangen; Mängel wurden umgehend beseitigt.

Ein grundsätzliches Problem der SCHUFA ist, daß sie als speichernde Stelle verantwortlich für die Daten ist, den Nachweis der Richtigkeit von Daten aber nur mit Hilfe der einmeldenden Stelle - in der Regel einer Bank - führen kann. Den Betroffenen entstehen dadurch jedoch keine Benachteiligungen, weil die SCHUFA die Daten zunächst sperrt und erst wieder freigibt, wenn sie nachweisen kann, daß die Daten zutreffend sind.

Bedauerlicherweise kommt es in diesem Zusammenhang immer wieder vor, daß Betroffene zum Sachverhalt unrichtige bzw. unvollständige Informationen geben, vor allem indem sie negative Daten verschweigen. Ein derartiges Verhalten führt zu einem erheblichen Verwaltungsaufwand, weil erst langwierig der tatsächliche Sachverhalt ermittelt werden muß. Häufig stellt sich heraus, daß die angebliche Verletzung der schutzwürdigen Belange nicht vorliegt. Insoweit muß Privatpersonen immer wieder verdeutlicht werden, daß Datenschutz nicht zur Abwehr berechtigter finanzieller Forderungen mißbraucht werden kann.

In einer steigenden Zahl von Fällen ist es erforderlich, die Betroffenen an die Schuldnerberatung zu verweisen. Bei Überschuldung können die datenschutzrechtlichen Bestimmungen nicht weiterhelfen.

5.1 Auskunft über Verwandte

Es gelingt leider immer wieder einzelnen Personen, unter der Nennung eines falschen berechtigten Interesses, Schufa-Auskünfte zu erlangen. Die Strafandrohungen des § 43 BDSG (Freiheitsstrafe bis zu einem Jahr oder Geldstrafe) sind offensichtlich zu wenig bekannt oder entfalten keine Abschreckungswirkung.

Im konkreten Fall hatte ein Hauseigentümer unter dem Vorwand, einen Mietvertrag abschließen zu wollen, über seine Hausbank pauschale Schufa-Auskünfte über einen Verwandten erlangt. Es war zu beanstanden, daß die Bank ohne die Genehmigung der betroffenen Privatperson Auskünfte erteilt hatte und darüber hinaus ein berechtigtes Interesse nicht existent war. Dem Betroffenen wurde der Sachverhalt - der ihm durch familiäre Auseinandersetzungen schon dem Grunde nach bekannt war - nochmals mitgeteilt und er wurde auf sein Recht nach § 43 Abs. 4 BDSG, Strafanzeige zu erstatten, verwiesen. Ob die Strafanzeige - zumindest im familiären Bereich - das geeignete Mittel ist, mußte der Betroffene selbst entscheiden. Die Behörde hat insoweit kein Antragsrecht. Die Auskünfte erteilende Bank wurde jedoch aufgefordert, zukünftig derartige Informationen nicht mehr weiterzugeben. Es kann davon ausgegangen werden, daß in dieser Bank Schufa-Auskünfte künftig vertraulicher gehandhabt werden.

5.2. Scheinbare Negativdaten

Ein Betroffener beschwerte sich darüber, daß seine Hausbank ihn über einen negativen Schufa-Eintrag in Kenntnis setzte, obwohl gegen ihn keinerlei Verbindlichkeiten bestünden. Überprüfungen bei der Schufa bestätigten dies,

wobei zu einer Forderung auch die Zahlung eingetragen war. Es stellte sich heraus, daß die beteiligte Banksachbearbeiterin auf der ersten Bildschirmseite die Forderung dargestellt bekam, und es lediglich versäumt hatte, eine Seite weiterzublättern und sich die zugehörige Zahlung anzeigen zu lassen. Obwohl dies der erste derartige Fall war, ist es für potentielle Kreditnehmer empfehlenswert, die vollständigen Daten bei der SCHUFA mit einer Selbstauskunft zu erfragen.

6. Kreditkartenunternehmen

6.1 Adreßvermietung

Ein Kreditkartenunternehmen wollte wissen, ob es unter Einhaltung der Datenschutzbestimmungen seine Kundenadressen unter dem Merkmal "Kreditkarteninhaber" z.B. an Mailingunternehmen vermieten könne. Da in solchen Fällen jedoch die werbenden Unternehmen den Werbeerfolg anhand der Adreßnummern im Rücklauf kontrollieren, ist für sie dann nachvollziehbar, daß eine Werbeantwort aus der Mailing-Aktion "Kreditkarteninhaber" kommt. Bei diesem Vorgang werden schutzwürdige Belange i.S.d. § 28 Abs. 2 Ziff. 1 BDSG verletzt, weil der Betroffene selbst, ohne dies zu erkennen, mit der Werbeantwort die Merkmale "Kreditkarteninhaber", "bonitätsgeprüft" und unter Umständen "Mindesteinkommen" übermittelt.

Eine Möglichkeit, der zulässigen Gestaltung solcher Werbemaßnahmen, wäre die Information auf dem Werbeschreiben, daß die Adresse des Empfängers aus dem Bestand des Kreditkartenunternehmens stammt und der Empfänger mit der Rücksendung der Werbeantwort diesen Umstand dem werbenden Unternehmen zur Kenntnis gibt. Darüber hinaus wäre noch in Betracht zu ziehen, daß das werbende Unternehmen auf Adreßnummern und damit auf die Rücklaufkontrolle verzichtet und die Werbemaßnahme so gestaltet, daß die Rückläufe zeitlich nicht auf den Adreßbestand des Kreditkartenunternehmens zurückzuführen sind; z.B. durch parallele Werbemaßnahmen in der Presse oder mittels Postwurfsendungen.

6.2 Datenerhebung mit einem Kreditkartenantrag

Bei Datenerhebungen auf Kreditkartenanträgen wird teilweise großzügig verfahren, und alles, was von Nutzen sein könnte, erfragt und gespeichert. Die Fragen betreffen oft auch den Partner, selbst wenn dieser keine Zweitkarte beantragt hat. Der Partner ist nicht Vertragspartner des Unternehmens und eine gesonderte Einwilligung liegt nicht vor. Die Datenerhebung sowie die darauffolgende Datenspeicherung - lediglich auf Vorrat - sind deshalb grundsätzlich datenschutzrechtlich unzulässig. Allgemeine Fragen nach der Berufstätigkeit des Partners und nach dem Familienstatus können wegen des zu beurteilenden Kreditrisikos von Bedeutung sein und beeinträchtigen in der Regel keine schutzwürdigen Belange des Betroffenen. Die konkrete Erhebung und Speicherung des Arbeitsverhältnisses des Partners ist aber nur akzeptabel, wenn der Betroffene Mitantragsteller ist.

Ein konkret geprüftes Kreditkartenunternehmen wird seine Antragsformulare dahingehend ändern, daß die Partnerfragen nur im Falle der Mitantragstellung auszufüllen sind.

7. Versicherungen

7.1 Register von Versicherungs- und Finanzdienstleistungsvermittlern

Mehrere konkurrierende Unternehmen speichern die Daten von Versicherungs- und Finanzdienstleistungsvermittlern und übermitteln diese Daten an den interessierten Versicherungskunden. Ziel ist es, im Vorgriff auf eine europäische Regelung, einen Qualitätsstandard zu erstellen und dem Kunden nur qualifizierte Vermittler zu benennen. Insgesamt spielt eine Rolle, daß der Status des Vermittlers - selbständig, abhängig beschäftigt, vertriebsgebunden, Nebenbeschäftigung - eindeutig dokumentiert wird. Die widerstreitenden wirtschaftlichen Interessen haben es bisher jedoch nicht zugelassen, daß ein einheitliches Register für die gesamte Branche aufgestellt wurde. Entsprechende Empfehlungen der Europäischen Union hat der Bundesgesetzgeber noch nicht aufgegriffen und in nationales Recht umgesetzt.

Ein geprüftes Unternehmen verarbeitete die Daten im Auftrag für ein derartiges Register. Die Datenverarbeitung war nicht zu beanstanden. Die Verarbeitungsinhalte wurden dahingehend geprüft, ob es sich um allgemein zulässige Verarbeitungszwecke handelte. Die Abläufe waren eindeutig dokumentiert; die Datenspeicherung und Übermittlung erfolgte im Auftrag der gespeicherten Versicherungsvermittler. Dem betroffenen Versicherungsvermittler wurde unmißverständlich beschrieben, welche seiner Daten zur Übermittlung bestimmt sind. Seine Interessen bleiben damit gewahrt.

7.2 Stellungnahmen der Versicherungen in Beschwerdefällen beim Bundesaufsichtsamt

Das Bundesaufsichtsamt für das Versicherungswesen fordert im Rahmen der Bearbeitung von Beschwerden der Versicherten Stellungnahmen von den betroffenen Versicherungsunternehmen an. Es hat hierzu Hinweise herausgegeben, welche Informationen im konkreten Beschwerdefall in der Stellungnahme der Versicherung enthalten sein müssen.

Dazu gehören regelmäßig die wesentlichen Vertragsdaten wie Vertragsbeginn, Laufzeit, Beitragshöhe, Versicherungsumfang, Tarif. Die Mitteilungspflicht im Hinblick auf sonstige Details aus der Vertragsabwicklung wird jedoch darauf beschränkt, welche Informationen für die Beurteilung der Sach- und Rechtslage durch das Bundesaufsichtsamt erforderlich sind. Insbesondere im Hinblick auf medizinische Daten der Versicherten bedeutet dies, daß deren Übermittlung an das Bundesaufsichtsamt nur dann zulässig ist, wenn der Betroffene es entweder ausdrücklich erlaubt hat oder sich eindeutig eine Einwilligung aus seinem Beschwerdeschreiben an das Bundesaufsichtsamt ergibt.

In einem konkreten Fall hatte ein Versicherungsunternehmen vorsorglich neben sämtlichen Vertragsdaten auch alle Einzeldaten aus der aktuellen Vertragsabwicklung des Krankenversicherungsverhältnisses übermittelt, obwohl dies für die Beurteilung der Sach- und Rechtslage nicht erforderlich war. Es wurde darauf hingewirkt, daß derartige Verstöße gegen datenschutzrechtliche Bestimmungen zukünftig unterbleiben.

7.3 Auskunftsrecht ist nicht gleich Einsichtnahmerecht

Das Recht auf Auskunft nach § 34 BDSG über die bei einer Versicherung gespeicherten personenbezogenen Daten ist nicht gleichzusetzen mit einem Recht auf Akteneinsicht bei derselben. Diese Erfahrung mußte ein Beschwerdeführer machen, der mit Hilfe datenschutzrechtlicher Bestimmungen die Einsicht in die Unfallakte bei der gegnerischen Versicherung erzwingen wollte.

8. Datenverarbeitung im medizinischen Bereich

8.1 Auswertung von Rezeptdaten

Ein Apothekenrechenzentrum erhält die Rezeptdaten der Kassenpatienten und Sozialhilfeempfänger von den angeschlossenen Apotheken zur Abrechnung mit den Kostenträgern und verwaltet die hierfür geleisteten Zahlungen. Der Auftrag der Apotheken umfaßt darüber hinaus die Erstellung von Verbandsstatistiken. Zusätzlich werden für ein Marketingunternehmen Auswertungen erstellt, die nicht als Verbandsstatistiken bezeichnet werden können und deshalb vom Auftrag der Apotheken nicht gedeckt sind.

Die Marketingauswertungen/-statistiken lassen keine Rückschlüsse auf den Patienten zu. Zielperson ist der behandelnde Arzt. Die Ärzte werden ohne personenbezogene Arztnummer in Gruppen zusammengefaßt. Nach Facharztgruppen gegliedert, lassen sich die Aktivitäten der Ärzte in den Postleitzahlbereichen feststellen. Die Arzneimitteldaten sind jedoch in der Regel einem einzelnen Arzt nicht direkt zurechenbar.
Allgemeine Rückschlüsse über den Erfolg einer Besuchsserie eines Pharmavertreters werden sich aber hieraus ziehen lassen. Zur Zeit wird vom Rechenzentrum versucht, durch unterschiedliche Sortierungsläufe herauszufinden, ob bei besonderen Verschreibungsgewohnheiten nicht doch einzelne Ärzte zu identifizieren sind. Bei einem großen Datenvolumen bietet es sich

an, das Rechenzentrum als verantwortliche Stelle mit derartigen Untersuchungen zu beauftragen. Ein endgültiges Ergebnis steht hierzu noch aus.

Sollten Ärzte mit ihren Verschreibungsgewohnheiten identifizierbar sein, beeinträchtigen die Auswertungen ihre schutzwürdigen Belange. Die Methode eines Marktforschungswettbewerbers, derartige Auswertungen nur mit dem Einverständnis des Arztes vorzunehmen, ist in jedem Fall vorzuziehen.

8.2 Die Abrechnung durch privatärztliche Verrechnungsstellen

Privatärztliche Verrechnungsstellen sind aufgrund ihrer Tätigkeit der Abrechnung und Einziehung von Arzthonorarforderungen nicht bloß Auftragsdatenverarbeiter und werden daher allgemein auch nicht als meldepflichtig i.S.d. § 32 BDSG angesehen.

Werden demnach aber Abrechnungsdaten aus dem Arzt-Patienten-Verhältnis an Abrechnungsstellen weitergegeben, liegt eine Übermittlung vor, die der Einwilligung des Patienten bedarf.

Erbringt ein Arzt gegenüber dem Patienten Laborleistungen, Röntgenleistungen o.ä. für den primär behandelnden Arzt, so kann er seine Leistungen gegenüber dem Patienten nicht ohne weiteres durch seine Verrechnungsstelle abrechnen lassen, wenn etwa eine Einwilligung des Patienten sich nicht auf alle an der Behandlung beteiligten Ärzte erstreckt oder gar keine Einwilligung vorliegt, weil etwa der primär behandelnde Arzt seinerseits nicht Mitglied der Verrechnungsstelle ist. Tut er dies doch, so liegt keine rechtmäßige Übermittlung vor.

Die Aufsichtsbehörde wies insoweit eine privatärztliche Verrechnungsstelle darauf hin, daß Ärzte und Krankenhausträger diese spezielle Problematik berücksichtigen und auf die vorherige Einwilligung der Patienten achten müssen.

9. Arbeitnehmerdatenschutz

9.1 Fehlende Betriebsvereinbarung und leichtfertiger Umgang mit E-Mails

Sein freizügiger und sorgloser Umgang mit dem innerbetrieblichen E-Mail-System hat einen Arbeitnehmer seinen Arbeitsplatz gekostet. Er hatte das System auch zur privaten Kommunikation mit Kolleginnen und Kollegen genutzt. Dabei wurden neben privaten und teilweise intimen Angaben auch geschäftsschädigende Äußerungen des Arbeitnehmers im E-Mail-System des Arbeitgebers gespeichert. Eine Auswertung der E-Mails durch das Unternehmen führte zur fristlosen Kündigung des Betroffenen, der sich mit der Bitte um Überprüfung der Zulässigkeit der E-Mail-Auswertung an die Datenschutzaufsichtsbehörde wandte.

In dem betroffenen Unternehmen existierte keine Betriebsvereinbarung zwischen Arbeitgeber und Betriebsrat über die Nutzungsbedingungen sowie die Kontroll- und Auswertungsmöglichkeiten des betrieblichen E-Mail-Systems. Gegenstand der Kontrolle und Analyse der E-Mails war somit die betriebliche und nicht eine ausdrücklich erlaubte, private und als solche gekennzeichnete Kommunikation. Im Rahmen seiner Organisationsbefugnis und seines Aufsichtsrechts ist die Einsichtnahme und Auswertung der im betrieblichen Mail-Rechner gespeicherten Daten durch den Arbeitgeber allgemein zulässig. Bei der Anwendung von Überwachungsprogrammen sind allerdings die Mitbestimmungsrechte des Betriebsrates nach § 87 Abs. 1 Ziff. 6 BetrVG zu berücksichtigen.

Arbeitnehmer sollten sich vergegenwärtigen, daß die Nutzung neuer technischer Möglichkeiten oft auch Gefahren für das informationelle Selbstbestimmungsrecht mit sich bringt. Die neuen Risiken liegen vor allem in der mangelnden Transparenz der Kommunikationssituation. Wie auch schon bei Einführung und Nutzung betrieblicher ISDN-Anlagen empfiehlt die Aufsichtsbehörde hier dringend, geeignete Betriebsvereinbarungen abzuschließen, um die datenschutzverträgliche Nutzung firmeninterner E-Mail-Systeme gewährleisten zu können. Die Beachtung von Mitbestimmungsrechten sowie Offenheit und Klarheit bei datenschutzrelevanten Aspekten des Systems kön-

nen auch bei dieser Kommunikationstechnologie entscheidend dazu beitragen, betriebliche Konfliktsituationen zu vermeiden und die Rechte auf informationelle und kommunikative Selbstbestimmung am Arbeitsplatz zu wahren.

9.2 Arbeitnehmeranfragen

Darf der Arbeitgeber anläßlich des Dienstjubiläums persönliche Daten des Arbeitnehmers über dessen schulischen und beruflichen Werdegang in einer Festrede oder anderweitig im Betrieb bekannt machen? Dürfen Vermerke in der Personalakte darüber enthalten sein, ob der Arbeitnehmer privat eine Waffe besitzt, welcher Religion, welcher Partei oder welchem Verein er angehört? Dürfen firmeninterne Mitarbeiter-Adreßdateien mit privaten Adressen und Telefonnummern erstellt und von den Firmenmitarbeitern genutzt werden? Solche und ähnliche Fragestellungen wurden auch im vergangenen Berichtsjahr immer wieder an die Aufsichtsbehörde herangetragen.

Soweit derartige personenbezogene Daten von Arbeitnehmern in oder aus Personaldatensammlungen verarbeitet oder genutzt werden, gelten die Vorschriften des BDSG.

Danach ist die Erhebung, Verarbeitung und Nutzung von Arbeitnehmerdaten durch den Arbeitgeber nur erlaubt, wenn die Daten im Rahmen des konkreten Arbeitsverhältnisses erforderlich sind; also für den konkreten Zweck der Durchführung des Arbeitsverhältnisses benötigt werden. Daneben kann im Einzelfall eine Einwilligung des Arbeitnehmers genügen. Berücksichtigt man jedoch, daß eine Verweigerung möglicherweise negative Auswirkungen im Arbeitsverhältnis nach sich ziehen kann, wird man in vielen Fällen nicht zweifelsfrei von einer freiwilligen Einwilligung ausgehen können.

Für den Fall des Dienstjubiläums bedeutet dies, der Arbeitnehmer muß vor der Veröffentlichung seiner privaten Daten um Einwilligung gebeten werden. Der Vermerk des Waffenbesitzes ist nur zulässig, wenn dieser Umstand berufliche Relevanz besitzt, z.B. für Tätigkeiten in Sicherheitsunternehmen. Ebenso selten besteht das berechtigte Interesse des Arbeitgebers im Regelfall an der Kenntnis der Religions-, Partei- oder Vereinszugehörigkeit, wenn nicht steuerliche Aspekte oder die Tätigkeit in einem Tendenzbetrieb im konkreten Fall eine Rolle spielen. Mitarbeiter-Adreßdateien dürfen nicht allgemein im Betrieb, sondern lediglich den mit der Verarbeitung von Personaldaten befaßten Mitarbeitern zugänglich sein. Private Telefonnummern der Mitarbeiter sind in der Regel für das Arbeitsverhältnis nicht relevant und daher nur in solchen Fällen zu speichern, in denen dienstliche Interessen bestehen; z.B. bei Rufbereitschaftsdienst.

10. Erfassung von Kfz-Daten

Datenschutzrechtliche Bedenken gegen die Erfassung von Kfz-Kennzeichen am Frankfurter Flughafen konnte die Aufsichtsbehörde ausräumen. Ein Betroffener befürchtete, daß auf diese Weise Bewegungsprofile von den Parkhausbenutzern erstellt und weitergegeben werden könnten.

Die regelmäßige, inzwischen automatisierte Kennzeichenerfassung in den öffentlichen Parkboxen der Flughafen Frankfurt Main AG soll jedoch dem Kunden beim Wiederauffinden seines Fahrzeuges nach längerer Abwesenheit oder nach dem Verlust des Parktickets dienen.

Darüber hinaus werden die Daten zur Entfernung von Schrottwagen und herrenlosen Fahrzeugen verwandt. Die Halter werden nach längerer Verweildauer ermittelt und aufgefordert, ihre Fahrzeuge abzuholen und die Parkgebühr zu begleichen. Die erfaßten Kfz-Kennzeichendaten werden nur so lange gespeichert, wie es für die genannten Zwecke erforderlich ist. Auch werden die Daten nicht zur Erstellung von Bewegungsprofilen oder zu statistischen Zwecken verwandt, ebenso wenig werden sie an Dritte weitergegeben.

11. Unsicherheit bei Kontoauszugsdruckern

Kontoauszugsdrucker nutzen nur die auf dem Magnetstreifen gespeicherten Informationen.

Wie Presseveröffentlichungen zu entnehmen war, genügte bereits die Kenntnis der Kontonummer und der Bankleitzahl, um mit einem (leicht zu beschaffenden) Kartenrohling Duplikate zu erstellen, die einen Kontoabruf ermöglichten. In einigen Fällen führte dies trotzdem zu keiner Ausspähung, weil der Drucker lediglich mitteilte "keine Veränderung seit dem letzten Ausdruck". Waren dann doch Veränderungen eingetreten, konnten diese jedoch gemeinsam mit dem Saldo ausgedruckt werden. Andere Kreditinstitute drucken in jedem Fall den Kontosaldo aus. Es bot sich insgesamt ein sehr uneinheitliches Bild vom multifunktionalen Terminal mit Paßwortabfrage bis zum "dummen" Kontoauszugsdrucker, der entweder alle aktuellen Informationen ausdruckte oder das unvollständige Duplikat - hier nur Kontonummer und Bankleitzahl - nicht akzeptierte.

Die betroffenen Großbanken haben sofort reagiert und zusätzliche Sicherungen vorgesehen, die das Problem im Rahmen des mit der vorhandenen Technik Möglichen begrenzten.

Eine gleichfalls angeforderte Stellungnahme des Bundesverbandes der Banken zur Datensicherheit bei Kontoauszugsdruckern steht noch aus.

12. Forderungsaufkauf im Telekommunikationsbereich

Ein englisches Unternehmen kauft in größerem Umfang Forderungen aus dem Telekommunikationsbereich. Es versucht - vergleichbar einem Inkassounternehmen -, die Forderungen einzutreiben. Nach erfolglosen Mahnungen wird der Inkassoauftrag an kooperierende Rechtsanwälte weitergegeben.

Da das Unternehmen - im Gegensatz zu Werbeaussagen bzw. Mahnbriefen - keinerlei Daten an Dritte liefert, ist die Datenverarbeitung für eigene Zwecke nicht zu beanstanden. Das Unternehmen wird jedoch weiterhin beobachtet werden, da die Herausgabe - z.B. von Negativlisten an Telekommunikationsanbieter - nicht gänzlich auszuschließen ist. Bemerkenswert war in diesem Zusammenhang, daß der englische Registrar (engl. Datenschutzaufsichtsbehörde) das Mutterunternehmen in seinem Aufsichtsbereich nicht ermitteln konnte.

13. Mißbräuchliche Nutzung von Schuldnerdaten

Ein Bürger wandte sich an die Aufsichtsbehörde, mit der Bitte festzustellen, ob ein Unternehmen ihn aufgrund der im Schuldnerregister eingetragenen eidesstattlichen Versicherung angeschrieben habe. Bei der Werbung handelte es sich um das Angebot eines Kreditvermittlers. Dem Werbeschreiben war ein Kreditantrag beigefügt.

An der angegebenen Geschäftsadresse wurden mehrere Unternehmen vorgefunden. Es stellte sich heraus, daß diese Unternehmen gemeinsam mit dem Kreditvermittler die Geschäftsräume nutzten. Eine der Firmen war als Direktmarketingunternehmen im Gewerberegister eingetragen. Dieses Unternehmen hatte bundesweit Abdrucke aus den Schuldnerverzeichnissen der Amtsgerichte bezogen. Die Daten der Schuldner wurden in einer Datenbank gespeichert, entsprechend aufbereitet und mit dem Werbematerial des Kreditvermittlers an die in den Schuldnerverzeichnissen eingetragenen Personen versandt. Die Rückläufe und die zugesandten Kreditanträge wurden vom Kreditvermittler verarbeitet. Die betroffenen Antragsteller erhielten allerdings keinen Kredit. Ihnen wurden lediglich wertlose Unterlagen gegen eine hohe Nachnahmegebühr zugesandt.

Die Angaben aus den Kreditanträgen wurden in eine Datenbank eingegeben und an ein Unternehmen mit Sitz in Panama übermittelt. Darüber hinaus wurden die Daten einem Adreßvermieter für seine Adreßkollektion zur Verfügung gestellt. Diese Adreßkollektion war bereits an Lotterie-Anbieter vermietet worden. Außerdem bestanden bundesweit Beziehungen zwischen verschiedenen Unternehmen, die Kredite über Zeitungsanzeigen anbieten. Diese Firmen tauschten auch ihre Datenbestände untereinander aus. Bei der zuständigen Staatsanwaltschaft ist ein Ermittlungsverfahren wegen Betruges anhängig.

Die Nutzung der Daten aus Schuldnerverzeichnissen ist in der Schuldnerverzeichnisverordnung geregelt. Danach dürfen personenbezogene Daten aus

privatrechtlichen Vertragsfreiheit. In diesen Fällen ist der einzelne betroffene Bürger gefordert, genau zu überlegen, ob er bereit ist, für den Besuch einer solchen Großveranstaltung personenbezogene Daten weiterzugeben oder ob er in derartigen Fällen auf den Besuch der Veranstaltung verzichten will.

15. Dezentralisierung der Personaldatenverarbeitung

Im Bereich der Verarbeitung von Personaldaten hat sich im Berichtszeitraum ein Trend herausgestellt, der erhöhte Beachtung erfordert. Bisher zentral geführte Personalstammdateien und zentral vorgehaltene Personalakten werden verstärkt dezentralisiert. So entstehen zunächst einmal redundante Datenbestände. Die Pflege dieser Datenbestände sowie deren Absicherung erfordert von den speichernden Stellen einen doppelten Aufwand.

In Frage zu stellen ist eine Dezentralisierung der Personalverwaltung nicht nur aus Sicherheitsgründen, sondern durchaus auch aus Gründen der Wirtschaftlichkeit. Wirtschaftlich erscheint zunächst, daß vor Ort bereits vorhandene DV-Systeme mit ausreichenden Speicherkapazitäten auch für die Personalverwaltung zusätzlich genutzt werden. Die eingesetzte Standardsoftware ermöglicht es, schnell einfache Auswertungen zu erstellen. Der Einsatz der allgemein genutzten PC-Standardsoftware ist mit erheblichen Sicherheitsrisiken verbunden. Zwangsläufig erhöht sich mit der Dezentralisierung der Überwachungsaufwand für den Datenschutzbeauftragten.

Anders als bei traditionellen zentralen Systemen ist eine ordnungsgemäße und nachvollziehbare Datenverarbeitung nicht ausreichend gewährleistet. Maßnahmen z.B. zur Eingabekontrolle werden nicht durchgeführt, weil das System die notwendige Protokollierung nicht unterstützt.

Flexibilität, Zeitvorteil und Entlastung der zentralen Datenverarbeitung stehen aber in keinem Verhältnis zu den neu geschaffenen Gefahren der Dezentralisierung. Die speichernde Stelle, die Dezentralisierungsmaßnahmen durchführt, sollte angemessene Voraussetzungen für die Datensicherheit schaffen. Außerdem ist zu gewährleisten, daß Veränderungen weitgehend simultan in den redundanten Datenbeständen vorgenommen werden.

16. Der betriebliche Datenschutzbeauftragte

Zu beanstanden war häufig, daß in kleinen und mittleren Unternehmen überhaupt kein Datenschutzbeauftragter bestellt wurde. Bei Unternehmen, die einen Datenschutzbeauftragten bestellt haben, gelangen diese aus Kostengründen zunehmend unter Druck. Die Aus- und Fortbildung des Datenschutzbeauftragten mußte teilweise von der Aufsichtsbehörde eingefordert werden. Mit der Bestellung eines Datenschutzbeauftragten allein ist es nicht getan. Zeit und finanzielle Mittel werden nämlich in vielen Fällen von der Geschäftsführung nicht ausreichend zur Verfügung gestellt.

Die betriebliche Eigenkontrolle, wie sie der Gesetzgeber durch das Amt des Datenschutzbeauftragten vorgesehen hat - d.h. die Kontroll-, Aus- und Fortbildungstätigkeit des Datenschutzbeauftragten im Betrieb - funktioniert nicht ohne Zeitaufwand und finanzielle Mittel.

Der Datenschutzbeauftragte ist aus den verschiedensten Gründen nicht in allen Fällen in der Lage, eine ausreichende Ausstattung einzufordern. Ebensowenig hat die Aufsichtsbehörde umfassende Kenntnis vom Bedarf und der gesamten Arbeitsbelastung des einzelnen Datenschutzbeauftragten. In dieser Hinsicht sind offene Auskünfte wünschenswert. Verstärkt wird die Aufsichtsbehörde jedoch auch Informationen aus den Tätigkeitsnachweisen der Datenschutzbeauftragten heranziehen, um zusätzlich Maßnahmen anzumahnen.

17. Datensicherheit

17.1 Benutzerkennung und Paßwort

Soweit dies möglich ist, muß der einzelne Benutzer sich gegenüber dem Computersystem persönlich ausweisen. Die Vertraulichkeit des Paßwortes und der regelmäßige Wechsel des Paßwortes werden nach wie vor zu wenig

Schuldnerverzeichnissen bzw. Abdrucken derselben nur zu den in § 19 Abs. 2 ZPO aufgeführten Zwecken wie Zwangsvollstreckung, Prüfung der wirtschaftlichen Zuverlässigkeit und ähnliches, nicht aber zu Werbezwecken verwandt werden. Die betroffenen Schuldner müssen entsprechend § 19 Abs. 2 ZPO lediglich solche Eingriffe in ihr grundgesetzlich geschütztes Recht auf informationelle Selbstbestimmung hinnehmen, die nach der oben genannten Vorschrift dem Schutz von Rechtsgütern Dritter oder der Vermeidung wirtschaftlicher Schäden bei Dritten dienen. Eine Nutzung der in den Verzeichnissen abgedruckten personenbezogenen Daten durch Dritte zu deren eigenen Geschäftszwecken ist nicht zulässig. Eine Übermittlung der gespeicherten Daten an andere Unternehmen ist ebenfalls nicht zulässig, da diese Übermittlungen gegen die schutzwürdigen Interessen der Betroffenen verstoßen. Eine Übermittlung ins Ausland sowie die Adreßvermittlung über einen Adreßvermieter entbehren ebenfalls jeglicher Rechtsgrundlage.

Alle Versender von Abdrucken aus den Schuldnerverzeichnissen, von denen das Unternehmen Schuldnerlisten bezogen hatte, wurden auf die mißbräuchliche Verwendung hingewiesen. Diese schlossen das Unternehmen sofort vom Bezug der Schuldnerlisten aus. Der Adreßvermieter hat ebenfalls sofort die Weitervermietung gestoppt, wie auch den Vertrag mit dem Unternehmen gekündigt.

Das Unternehmen nutzte personenbezogene Daten gesetzeswidrig. Es verstieß somit gegen grundrechtlich geschützte Rechtspositionen und zwar nicht nur einmalig, sondern fortlaufend seit etwa Mitte 1995. Ohne die Anordnung sofortiger Maßnahmen mit Zwangsgeldandrohung hätten die Grundrechtsverstöße bis zum Abschluß des Rechtsmittelverfahrens weitergehen können. Gleichwohl mußte nach Rechtskraft der ersten Anordnung festgestellt werden, daß das Unternehmen noch nicht umworbene eingetragene Personen wie bisher anschrieb. Daraufhin wurde eine zweite Anordnung mit der Androhung eines wesentlich höheren Zwangsgeldes erlassen. Das Unternehmen hat nunmehr seine Tätigkeit eingestellt. Der geschilderte Sachverhalt gibt Anlaß, über den Versand von Abdrucken aus Schuldnerverzeichnissen nachzudenken.

Im Gegensatz zu einem Versandhändler, der die Zahlungsfähigkeit seiner Kunden überprüfen muß, besteht für ein Direktmarketing-Unternehmen nur im Einzelfall - z.B. bei einer neuen Geschäftsverbindung - die Notwendigkeit, Einblick in Schuldnerlisten zu nehmen.

14. Datenerhebung auf Vorrat

Im Rahmen einer Europameisterschaft 1996 hat ein Verband Richtlinien für den Verkauf von Eintrittskarten an die Vorverkaufsstellen herausgegeben. Unter anderem enthielten diese Richtlinien den Hinweis, daß jedem Besteller nur Karten zugeteilt werden könnten, wenn vorher Namen, Geburtsdaten und Anschriften der Personen, die die Karten erhalten, mitgeteilt worden sind. Auch Reiseveranstalter waren verpflichtet, unverzüglich die Personalien der Personen, an die sie die Karten weitergeben, mitzuteilen. Der Verband verlangte darüber hinaus, daß der Besteller die geforderten Angaben und zusätzlich auch die Paßnummer auf dem Vordruck für die Eintrittskartenbestellung einzutragen habe. Mit der Bestellung sollte der Besteller verpflichtet werden, sich mit der Weitergabe seiner persönlichen Daten einverstanden zu erklären. Diese Daten sollten vom Verband aufbewahrt werden und auf Anforderung dem Europäischen Verband bzw. Sicherheitsorganen zur Verfügung gestellt werden.

Begründet wurde diese Datenerhebung mit dem Hinweis, daß damit Randalierer und Betrüger von vornherein ausgeschlossen werden sollten. Zusätzlich problematisch war der Vorgang auch deshalb, weil der Kartenvorverkauf bereits begonnen hatte, bevor die Richtlinien für den Vorverkauf ergingen.

Aus Sicht der Aufsichtsbehörde haben sich einige Kartenbesteller verständlicherweise gegen diese Vorratsspeicherung ihrer personenbezogenen Daten gewandt. Auch bei anderen Großveranstaltungen wird versucht, Daten zu erheben und auf Vorrat zu speichern. Wenn der Veranstalter der Meinung ist, daß er einen Betroffenen ausschließen möchte, so ist ihm dies nicht abzusprechen. Die diesbezügliche Datenspeicherung liegt im Rahmen seiner

beachtet. In diesem Zusammenhang ist zu berücksichtigen, daß nicht nur das Paßwort, sondern auch die Benutzerkennung (User-Id) weitgehend vertraulich gehalten werden sollte. Kritisch ist nicht nur die Weitergabe einer einzelnen Benutzerkennung, sondern vor allem die unbefugte Kenntnis einer größeren Zahl von Benutzerkennungen. Im Besitz aller Benutzerkennungen eines Computersystems ist es für einen unbefugten Dritten erheblich leichter, fremde Zugriffsberechtigungen zu erlangen. Auf die Darstellung, wie ein "Hacker" in einem solchen Fall vorgehen könnte, wird in diesem Zusammenhang bewußt verzichtet.

17.2 Sicherheit für Internet-Neulinge

Wie bereits bei T-Online wollen einige Firmen ihre Chancen im neuen Medium zunächst testen und auch gegenüber ihren Kunden Präsenz dokumentieren. Für den Anfang kann - bei in der Regel begrenztem finanziellen Einsatz - empfohlen werden, einen völlig von den übrigen Computersystemen isolierten Personal-Computer (PC) für die Nutzung des Internets zu verwenden. Sicherheitsbedenkliche Zwischenfälle beschränken sich dann auf diesen einzelnen PC. Das Unternehmen kann zunächst Erfahrungen bei der Nutzung der Internet-Dienste sammeln und in einem zweiten Schritt das Internet nach Einrichtung entsprechender zusätzlicher Sicherheitsvorkehrungen für weitere Benutzer freigeben. Die Sicherheitsvorkehrungen müssen dann jedoch den Erfordernissen des technischen Wandels angepaßt werden.

18. Ordnungswidrigkeitenverfahren

Von den bereits in den letzten Berichten der Landesregierung über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden aufgeführten Bußgeldverfahren konnte im Berichtsjahr 1996 ein weiteres Verfahren nach § 44 Abs. 1 Ziff. 2 BDSG gegen ein Marktforschungsunternehmen mit einer Bußgeldsumme in Höhe von 3000,-- DM rechtskräftig abgeschlossen werden. Das Unternehmen hatte bereits mehrere Jahre lang personenbezogene Daten geschäftsmäßig zum Zwecke der anonymisierten Übermittlung im Bereich der Marktforschung gespeichert, ohne seiner Meldepflicht nach § 32 Abs. 1 Ziff. 2 BDSG gegenüber der Aufsichtsbehörde nachgekommen zu sein.

Im Berichtsjahr 1996 wurden von der Aufsichtsbehörde gegen 3 Unternehmen Ordnungswidrigkeitenverfahren nach dem BDSG eingeleitet.

So hat die Aufsichtsbehörde gegen ein Finanzdienstleistungsunternehmen ein Ordnungswidrigkeitenverfahren wegen der trotz mehrfacher Aufforderung unvollständigen Erteilung von Auskünften entgegen § 38 Abs. 3 Satz 1 BDSG eingeleitet (Ordnungswidrigkeit nach § 44 Abs. 1 Ziff. 6, 1. Alternative BDSG). Gegen jeweils ein Marktforschungsunternehmen und eine Direktmarketinggesellschaft wurden Ordnungswidrigkeitenverfahren nach § 44 Abs. 1 Ziff. 2 BDSG wegen der entgegen § 32 Abs. 1 BDSG nicht erfolgten Mitteilung über die Aufnahme einer meldepflichtigen Tätigkeit eingeleitet.

In den drei im Berichtsjahr eingeleiteten Verfahren hat die Aufsichtsbehörde Bußgeldbescheide mit einer Bußgeldsumme in Höhe von 11.000,-- DM erlassen. Zwei dieser Bußgeldbescheide haben im Berichtsjahr Rechtskraft erlangt.

Wiesbaden, den 29. Juli 1997

Der Hessische Ministerpräsident
Eichel

Der Hessische Minister des Innern
und für Landwirtschaft, Forsten
und Naturschutz
Bökel