



15. Wahlperiode

Drucksache **15/23**

HESSISCHER LANDTAG

08. 04. 99

Siebenundzwanzigster Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

vorgelegt am 31. Dezember 1998
nach § 30 des Hessischen Datenschutzgesetzes vom 11. November 1986

Eingegangen am 8. April 1999 · Ausgegeben am 6. Mai 1999

Druck: Wiesbadener Graphische Betriebe GmbH · 65199 Wiesbaden · Auslieferung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden

Inhaltsverzeichnis 27. Tätigkeitsbericht

- 1. Vorwort**
- 2. Die Umsetzung der EG-Datenschutzrichtlinie in Hessen**
 - 2.1 Einleitung
 - 2.2 Einzelfragen
 - 2.2.1 Stellung und Aufgaben der behördlichen Datenschutzbeauftragten
 - 2.2.2 Register und Benachrichtigungspflicht
 - 2.2.2.1 Dateienregister
 - 2.2.2.2 Benachrichtigungspflicht
 - 2.2.3 Durch Technikentwicklung bedingte Änderungen
 - 2.2.3.1 Technische und organisatorische Maßnahmen
 - 2.2.3.2 Vorabkontrolle
 - 2.2.3.3 Regelungen für gemeinsame Verfahren
 - 2.2.3.4 Besonderheiten bei Chipkarten und ähnlichen Technologien
 - 2.2.3.5 Besonderheiten bei der Videoüberwachung
 - 2.2.4 Landesübergreifende Datenverarbeitung, insbesondere Übermittlung von Daten
 - 2.2.5 Stellung des Hessischen Datenschutzbeauftragten
 - 2.3 Fazit und Ausblick
- 3. Europa**
 - Schengener Durchführungsübereinkommen
 - 3.1 Auskunftsrecht
 - 3.2 Sicherheit der SIRENE-Büros
 - 3.3 Zugriff von Verwaltungsbehörden auf das Schengener Informationssystem
 - 3.4 Mißbräuchliche Verwendung von Alias-Personalien
 - 3.5 Weitere Stellungnahmen der Gemeinsamen Kontrollinstanz
 - 3.6 Kontrolle des Zentralen Schengener Informationssystems (CSIS)
- 4. Banken**
 - Geldkarte
 - 4.1 Kontroverse
 - 4.2 Elektronische Geldbörse
 - 4.3 Vertragliche Grundlagen
 - 4.4 GeldKarte-System
 - 4.4.1 Infrastruktur
 - 4.4.2 Abläufe
 - 4.4.2.1 Vorbereitung
 - 4.4.2.2 Händlerinnen und Händler
 - 4.4.2.3 Kundin und Kunde
 - 4.4.2.4 Laden der GeldKarte
 - 4.4.2.5 Zahlung bei der Händlerin und dem Händler
 - 4.4.2.6 Datenflüsse
 - 4.5 Abgleichsmöglichkeiten
 - 4.6 Auftragsdatenverarbeitung oder Funktionsübertragung
 - 4.7 Personenbezogene oder anonyme Daten
 - 4.8 Erfahrungen
 - 4.9 Fazit und Empfehlungen
- 5. Polizei- und Strafverfolgungsbehörden**

- 5.1 DNA-Dateien
- 5.2 HSOG-Novelle
 - 5.2.1 Wohnraumüberwachung
 - 5.2.2 Verdachtsunabhängige Kontrollen
 - 5.2.3 Kontrollstellen
 - 5.2.4 Vorsorge zur Verfolgung künftiger Straftaten
 - 5.2.5 Datenspeicherung durch die Polizei
- 5.3. INPOL-neu
 - 5.3.1 Kriterien für die Speicherung in INPOL
 - 5.3.2 Protokollierung
 - 5.3.3 Anzuwendendes Recht für Speicherungen von Länderpolizeien in INPOL-Verbunddateien
- 5.4 Schutz privater Rechte
 - 5.4.1 Der Parkverstoß
 - 5.4.2 Das Hausverbot
 - 5.4.3 Der nachträglich aufgenommene Verkehrsunfall

6. Justiz und Strafvollstreckung

- 6.1 Datenverarbeitung bei der Justiz
 - 6.1.1 Bereichsspezifische Rechtsgrundlagen für alle Bereiche der Justiz
 - 6.1.2 Prüfungskompetenz der Datenschutzbeauftragten bei den Gerichten
 - 6.1.3 Entwicklungen im Sicherheitsbereich
- 6.2 Strafvollzug – Weihnachtspaketmarken
- 6.3 Staatsanwaltschaften – Das Verfahren MESTA

7. Gesundheit

- 7.1 Krebsregister für Hessen
 - 7.1.1 Das Krebsregistergesetz des Bundes von 1994
 - 7.1.2 Das hessische Ausführungsgesetz
 - 7.1.2.1 Meldepflicht statt Melderecht der Ärztinnen und Ärzte
 - 7.1.2.2 Ausgestaltung der anonymen Meldungen
 - 7.1.2.3 Speicherung von Gauß-Krüger-Koordinaten in der Registerstelle
 - 7.1.3 Zur Umsetzung des hessischen Ausführungsgesetzes
- 7.2 Umsetzung des Psychotherapeutengesetzes
- 7.3 Prüfung des Rechenzentrums der AOK ARGE-Mitte
 - 7.3.1 Technisches Umfeld
 - 7.3.1.1 Das Betriebssystem MVS
 - 7.3.1.2 Schutzfunktionen von MVS
 - 7.3.1.3 Grenzen der Schutzfunktionen von MVS
 - 7.3.2 Konzeptioneller Rahmen
 - 7.3.2.1 DV-Konzept
 - 7.3.2.2 RACF-Konzept
 - 7.3.3 Feststellungen
 - 7.3.3.1 Räumliche Sicherungsmaßnahmen
 - 7.3.3.2 Benutzerkennungen mit besonderen Zugriffsrechten
 - 7.3.3.3 RACF
 - 7.3.3.3.1 Anmeldung am Rechner
 - 7.3.3.3.2 Zugriffskontrolle

- 7.3.3.3 RACF-Parameter und DES-EXIT
- 7.3.3.4 Kontrolle
- 7.3.3.4 Einzelprobleme
- 7.3.4 Fazit
- 7.4 Mitarbeiterdatenschutz bei der AOK Hessen
- 7.5 Feststellung der sachlichen Zuständigkeit des überörtlichen Sozialhilfeträgers nach dem Bundessozialhilfegesetz bei stationärer Krankenhausbehandlung
- 7.6 EDV- und Softwareausstattung hessischer Gesundheitsämter

8. Internet

- 8.1 Datenschutzrechtliche Verantwortlichkeit für Internet-Links
 - 8.1.1 Teledienstegesetz oder Mediendienste-Staatsvertrag
 - 8.1.2 Vermittlung fremder Inhalte
 - 8.1.3 Link als Teil des eigenen Informationsangebots
 - 8.1.4 Unterlassungspflicht
- 8.2 Orientierungshilfe Internet

9. Entwicklungen im Bereich der Technik

- PERKEO - Programm zur Identifizierung strafrechtlich relevanter Darstellungen
- 9.1 Funktionsweise des Programms
- 9.2 Keine Kontrollpflicht der Betreiber von Rechnernetzen
- 9.3 Das Fernmeldegeheimnis als Grenze der Kontrollmöglichkeit
- 9.4 Kontrollmöglichkeiten bei dienstlich genutzten Rechnern

10. Forschung

- Datenschutz und Forschung - kontroverse Diskussionen
- 10.1 Kritik am Datenschutz und ihr Hintergrund
- 10.2 Gemeinsame Diskussionen von Forscherinnen und Forschern und Datenschutzbeauftragten
- 10.3 Neufassung des § 33 HDSG

11. Ausländer

- 11.1 Gesetz zur Änderung des Ausländerzentralregisters und zur Errichtung einer Warndatei
- 11.2 Verpflichtungserklärung von Gastgebern ausländischer Bürgerinnen und Bürger
- 11.3 Medizinische Unterlagen in Ausländerakten
- 11.4 Anmeldung von Ausländervereinen
- 11.5 Gemeinsame Arbeitsgruppe der Polizei und Ausländerbehörde in Frankfurt zur Bekämpfung von ausländischen Intensivstraftätern
- 11.6 Inaktuelle Ausschreibungen in polizeilichen Fahndungsdateien
 - 11.6.1 Die Beschwerde
 - 11.6.2 Prüfungen
 - 11.6.2.1 Ausländerbehörde des Landkreises Groß-Gerau
 - 11.6.2.2 Ausländerbehörde des Main-Taunus-Kreises
 - 11.6.3 Konsequenzen

12. Kommunen

- 12.1 Pressemitteilung über die Höhe eines beantragten Verdienstausfalls für die Teilnahme an Sitzungen kommunaler Gremien
- 12.2 Öffentliche Bekanntgabe des Wasserverbrauchs eines Gemeindevertreters
- 12.3 Prüfung und Beratung hessischer Kommunen
- 12.4 Parallele Führung eines landwirtschaftlichen Unternehmerverzeichnisses bei Kommunen und der Land- und forstwirtschaftlichen Berufsgenossenschaft

13. Landwirtschaft und Umwelt

- 13.1 Gesamtnovelle Hessisches Wassergesetz
- 13.2 Errichtung eines Herkunftssicherungs- und Informationssystems für Tiere
 - 13.2.1 Zweck der Datenbank
 - 13.2.2 Datenschutzrechtliche Defizite der Vereinbarung

14. Soziales

- 14.1 Automatisierte Datenabgleiche im Zusammenhang mit Sozialhilfe
- 14.2 Zusammenarbeit des Jugendamtes mit anderen Behörden und freien Trägern der Kinder- und Jugendhilfe
- 14.3 Bekämpfung von Sozialhilfemißbrauch mit falschen Mitteln
- 14.4 Verdeckte Ermittlungen durch eine vom Sozialamt beauftragte Detektei

15. Personalwesen

- 15.1 Kontrollrecht des behördlichen Datenschutzbeauftragten
- 15.2 Personaldatenverarbeitung

16. Verfassungsschutz

- 16.1 Untergesetzliche Vorschriften des Landesamtes für Verfassungsschutz
- 16.2 System LARGO beim Verfassungsschutz

17. Schulen

- 17.1 Die Verschwiegenheitspflicht der Schülerversretung
- 17.2 Internet-Nutzung im Schulunterricht

18. Hochschulen

- Prüfung der Gesamthochschule Kassel
- 18.1 Aufbewahrungsfrist für Altakten
- 18.2 Personalakten
- 18.3 Studentensekretariat

19. Statistik

- Prüfung von kommunalen Statistikstellen
- 19.1 Vorgaben aus dem Landesstatistikgesetz
- 19.2 Prüfkriterien
- 19.3 Prüfergebnisse
 - 19.3.1 Statistikstelle der Stadt Darmstadt
 - 19.3.2 Statistikstelle der Stadt Kassel

19.3.3 Statistikstelle der Stadt Fulda

20. Straßenverkehr

Name und Adresse im Autofenster

20.1 Stadtverwaltung Flörsheim

20.2 Stadtverwaltung Frankfurt

21. Kammern

Akteneinsicht in Vorgänge der Industrie- und Handelskammer

22. Wohnungswesen

22.1 Zweckentfremdung von Wohnraum

22.2 Fehlbelegung

23. Finanzwesen

23.1 Neue DV-Entwicklung in der Finanzverwaltung

23.1.1 FISKUS (Förderales integriertes standardisiertes computerunterstütztes Steuersystem)

23.1.2 GÜP (Unterstützung der Veranlagungstätigkeiten für Gewerbetreibende, Bezieher von Überschufeinkünften und für die Gewinn-/Verlustfeststellung bei Personengesellschaften)

23.2 Bestandsaufnahme zur Hundesteuer in Friedrichsdorf

24. Ordnungswidrigkeiten

Der Flughafenschutzdienst leistet keine Amtshilfe

25. Bilanz

25.1 Ökologischer Landbau / Umsetzung der EWG-Verordnung Nr. 2092/91 (24. Tätigkeitsbericht, Ziff. 10 und 25. Tätigkeitsbericht, Ziff. 21.6)

25.2 Europol nimmt die Arbeit auf (25. Tätigkeitsbericht, Ziff. 2.2)

25.3 HEPOLAS (25. Tätigkeitsbericht, Ziff. 21.7)

25.4 Verwaltungsvorschriften zum Ausländergesetz (25. Tätigkeitsbericht, Ziff. 13.1)

25.5 Smart-Card im Asylverfahren (26. Tätigkeitsbericht, Ziff. 24.4)

25.6 Entwurf eines Gesetzes über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Landes Hessen (26. Tätigkeitsbericht, Ziff. 24.5)

26. Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

26.1 Datenschutz beim digitalen Fernsehen

26.2 Datenschutzprobleme der Geldkarte

- 26.3 Fehlende bereichsspezifische Regelungen bei der Justiz
- 26.4 Dringlichkeit der Datenschutzmodernisierung
- 26.5 Entwicklungen im Sicherheitsbereich
- 26.6 Verweigerung der Auskunft durch das Bundesamt für Finanzen auf Anfragen Betroffener über Freistellungsaufträge
- 26.7 Weitergabe von Meldedaten an Adreßbuchverlage und Parteien
- 26.8 Prüfungskompetenz der Datenschutzbeauftragten bei den Gerichten

Anhang 1 Hessisches Datenschutzgesetz (Fassung vom Februar 1999)

Anhang 2 Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet

Anhang 3 Epidemiologie und Datenschutz

Deutsche Arbeitsgemeinschaft für Epidemiologie
Arbeitskreis Wissenschaft der Datenschutzbeauftragten des Bundes und der Länder

Anhang 4 Beschlüsse des 62. Deutschen Juristentages Bremen 1998

Organisationsplan des Hessischen Datenschutzbeauftragten

Abkürzungsverzeichnis

Sachwortverzeichnis zum 27. Tätigkeitsbericht

Kernpunkte des 27. Tätigkeitsberichts

1. Hessen hat als erstes Bundesland die EG-Datenschutzrichtlinie mit einer Änderung des Hessischen Datenschutzgesetzes umgesetzt. Hierbei hat das zuständige Hessische Ministerium des Innern und für Landwirtschaft, Forsten und Naturschutz mich umfassend beteiligt (Ziff. 2).
2. Mit der von der deutschen Kreditwirtschaft angebotenen Geldkarte kann anonym bezahlt werden. Bei kontogebundenen Geldkarten könnten allerdings die Zahlungsvorgänge einer bestimmten Person zugeordnet werden, wenn mehrere an dem Zahlungsverkehr beteiligte Stellen zu diesem Zweck in einer vom System nicht vorgesehenen Weise zusammenwirken (Ziff. 4).
3. Beim Bundeskriminalamt wurde eine Datei zur Speicherung von DNA-Analysen eingerichtet. Einzelheiten der gesetzlichen Regelung, die die Voraussetzungen einer Speicherung festlegt, sind mangelhaft (Ziff. 5.1).
4. Wer seinem in einer Justizvollzugsanstalt einsitzenden Angehörigen zu Weihnachten ein Paket schicken will, darf nicht zur Verwendung von Paketmarken verpflichtet werden, die Außenstehenden offenbaren, daß der Adressat im Gefängnis sitzt (Ziff. 6.2).
5. Der Hessische Landtag hat 1998 ein Gesetz zur Ausführung des Krebsregistergesetzes verabschiedet. Die von mir geforderten datenschutzrechtlichen Verbesserungen sind in das Gesetz aufgenommen worden (Ziff. 7.1).
6. Stellen, die auf ihrer Internet-Homepage einen Link auf fremde Dokumente einrichten, sind für den Inhalt der Dokumente, auf

die der Link verweist, datenschutzrechtlich nicht verantwortlich (Ziff. 8.1).

7. Inaktuelle Fahndungsausschreibungen der Ausländerbehörden können für die Betroffenen erhebliche Belastungen verursachen. Vom Innenministerium muß ein Verfahren entwickelt werden, das künftig inaktuelle Fahndungsausschreibungen verhindert (Ziff. 11.6).
8. Datenschutz kann zum Infragestellen langjähriger Verwaltungspraxis und damit zur Verwaltungsvereinfachung führen. Die parallele Führung eines landwirtschaftlichen Unternehmerverzeichnisses sowohl bei den Kommunen als auch bei der Land- und forstwirtschaftlichen Berufsgenossenschaft wurde beendet (Ziff. 12.4).
9. Verkehrsteilnehmer dürfen nicht verpflichtet werden, eine Genehmigung der Straßenverkehrsbehörde, die Name und Anschrift des Inhabers enthält, im Fahrzeug offen auszulegen (Ziff. 20).
10. Dem Betroffenen darf die Einsicht in die zu seiner Person bei der Industrie- und Handelskammer gespeicherten Daten nicht mit der Begründung verweigert werden, daß die Unterlagen lediglich interne Bedeutung haben (Ziff. 21).

1. Vorwort

Das Berichtsjahr war für uns neben der stets vielfältigen Alltagsarbeit durch vier datenschutzrechtliche „Großereignisse“ geprägt, die das mir anvertraute Verfassungsanliegen insgesamt ein gutes Stück vorangebracht haben:

- Die Verabschiedung des Änderungsgesetzes zum Hessischen Datenschutzgesetz, mit dem für unser Bundesland die Europäische Datenschutzrichtlinie fristgerecht umgesetzt wurde;
- der 62. Deutschen Juristentag in Bremen, dessen öffentlich-rechtliche Abteilung sich mit den neuen Herausforderungen des Datenschutzrechts befaßte;
- die unter meinem turnusmäßigen Vorsitz in Wiesbaden durchgeführten Konferenzen der Datenschutzbeauftragten des Bundes und der Länder;
- das 7. Wiesbadener Forum Datenschutz, das sich mit der Vereinbarkeit des Grundrechts auf Forschungsfreiheit mit dem Recht auf informationelle Selbstbestimmung befaßte.

Daß es dem hessischen Gesetzgeber gelungen ist, die Dreijahresfrist einzuhalten, innerhalb derer alle Mitgliedsstaaten der Europäischen Union ihr Datenschutzrecht an die Anforderungen der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutze natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 24. Oktober 1995 anzupassen hatten, ist das Ergebnis einer vorbildlich überparteilichen und fachlich-sachlichen Zusammenarbeit des Parlaments und der Landesregierung unter der Federführung des Innenministeriums. In die Beratungen war mein Haus von Anfang an intensiv eingebunden. Der Erfolg dieser Kooperation ist um so bemerkenswerter, als kein anderes Bundesland und auch nicht der Bundesgesetzgeber dieser Pflicht rechtzeitig nachgekommen ist. Dieses Versäumnis hat für Hessen insofern Bedeutung, als das Datenschutzrecht und die

Datenschutzkontrolle in der Privatwirtschaft noch nicht richtlinienkonform geregelt sind. Da die Regelungskompetenz für den Datenschutz im nicht-öffentlichen Bereich allein beim Bund liegt und die von den Ländern zu organisierende Kontrolle der privaten datenverarbeitenden Stellen der Vorgaben durch ein modernisiertes Bundesdatenschutzgesetz bedarf, war es vertretbar, die in meinen früheren Tätigkeitsberichten angesprochene Frage der Verselbständigung und Zusammenlegung der zur Zeit noch bei den Regierungspräsidien angesiedelten Datenschutzkontrollstellen einer späteren gesetzlichen Regelung vorzubehalten.

Die Gespräche darüber, aber auch die förmlichen Stellungnahmen zu diesem Thema während des Berichtszeitraums haben gezeigt, daß meine Auslegung der Richtlinie, wonach die Datenschutzkontrollstellen für alle Bereiche funktional und institutionell unabhängig anzusiedeln sind, in allen Fraktionen des Landtages immer mehr Anhänger hat, während die Landesregierung und einzelne Abgeordnete gegen die Konstruktion völlig unabhängiger, d.h. auch von einem Ministerium weisungsfreien Aufsichtsbehörden, noch verfassungsrechtliche Bedenken geltend machen.

Es ist zu hoffen, daß diese anhaltende Diskussion durch die Beschlüsse des 62. Deutschen Juristentages aus dem September 1998 positiv befruchtet wird. Unter dem Vorsitz des Bundesverfassungsrichters Prof. Kirchhoff hat die öffentlich-rechtliche Abteilung des Juristentages auf meinen durch ein eigenes Referat begründeten Antrag u.a. mehrheitlich beschlossen, daß das materielle Datenschutzrecht für den öffentlichen und den privaten Bereich einander anzugleichen ist. Außerdem hat sich der Juristentag dafür ausgesprochen, die Kontrollstellen für die privatwirtschaftliche Datenverarbeitung „verselbständigt und weisungsfrei“ zu institutionalisieren und das Datenschutzrecht in eine allgemeine „Informationsverkehrsordnung“ einzupassen (Beschlüsse im Anhang 4). Dabei ist mittel- oder langfristig an ein

„Bundesinformationsgesetz“ gedacht, das auch das Recht des Zugangs zu Daten der öffentlichen Verwaltung und seine Grenzen regelt. Mein Amt wird dafür eintreten, daß das Land Hessen im Rahmen seiner föderativ-verfassungsrechtlichen Möglichkeiten eine solche Entwicklung aufgeschlossen und konstruktiv begleitet.

Der einjährige Vorsitz in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat mir besonders eindrucksvoll vor Augen geführt, wie wichtig und wertvoll die Bemühungen um gemeinsame Standards zum Schutz des Rechts der Bürgerinnen und Bürger auf informationelle Selbstbestimmung sind und welchen Wert der ständige Austausch zwischen allen mit dieser Aufgabe betrauten Stellen und Personen hat. Neben den intensiven Sachdiskussionen, deren Ergebnisse nur insoweit, als sie in förmliche Entschlüsseungen eingeflossen sind, unter Ziff. 26 zu diesem Bericht abgedruckt sind, hat sich die Konferenz jeweils auch in einem Informationsprogramm von der Praxis der Datenverarbeitung in spezifischen Zusammenhängen vertraut gemacht. Die Frühjahrskonferenz konnte sich einen halben Tag lang bei der Frankfurter Flughafen AG von dem hohen technischen Aufwand überzeugen, mit dem die komplexen Datenbewegungen teils durch öffentliche Stellen (Bundesgrenzschutz), teils durch nicht-öffentliche Unternehmungen (Airlines, FAG) mit ausgeprägtem Sinn für den Datenschutz organisiert werden. Anlässlich der Herbstkonferenz hat uns der Präsident des Bundeskriminalamtes in seiner Behörde empfangen und u.a. durch die auf diesem Gebiet tätigen Spezialisten eine praktische Anschauung von den Recherchen nach strafbaren Inhalten im Internet ermöglicht. Der bei diesen Anlässen geführte konstruktive Gedanken-, Erfahrungs- und Meinungsaustausch mit unseren kompetenten Gesprächspartnern hat erneut gezeigt, wie wichtig es ist, bei unserer täglichen Arbeit sowohl die Praxisrelevanz unserer normativen Anforderungen als aber auch die Vernetzungen informationeller Einzelvorgänge im Blick zu behalten. Dabei war in beiden Fällen wiederum die

Sinnwidrigkeit einer Unterscheidung zwischen öffentlicher und nicht-öffentlicher Datenverarbeitung augenfällig.

Einen Beitrag zur Vereinheitlichung der Praxis beim Zugang von personenbezogenen Daten auf einem besonders sensiblen Gebiet haben wir bei dem 7. Wiesbadener Forum Datenschutz zu leisten versucht. Das seit 1992 jährlich vom Präsidenten des Hessischen Landtages und vom Hessischen Datenschutzbeauftragten veranstaltete Forum hat sich von Anfang an zum Ziel gesetzt, Reichweite und Grenzen des Grundrechts auf informationelle Selbstbestimmung auf ihre Vereinbarkeit mit anderen wichtigen Anliegen der Rechtsordnung zu überprüfen. Ein Spannungsverhältnis besteht überall dort, wo eine grundrechtsverankerte und damit ebenfalls verfassungsgetragene Freiheitsgarantie mit dem Recht auf informationelle Selbstbestimmung zusammentrifft. Das durch die Wissenschaftsfreiheit (Art. 5 Abs. 3 GG) geschützte Interesse der Forschung an der Erhebung, Verarbeitung und der weiteren Verwertbarkeit möglichst vieler personenbezogener Daten muß mit den Grundsätzen des Datenschutzrechts so in Einklang gebracht werden, daß weder verfassungswidrige Forschungshemmnisse auf Seiten der Wissenschaft noch ein Verlust an Selbstbestimmung auf Seiten der Betroffenen entstehen. Auf dem Forum diskutierten Medizininformatiker, Epidemiologen, Kriminologen, Wirtschaftsforschung und Datenschutzexperten über die Frage, wie die beiden Grundrechtsfelder in eine praktische Konkordanz gebracht werden können. Der Tagungsband unter dem Titel des Forums „Datenschutz und Forschung“ ist bereits (1999) im NOMOS-Verlag erschienen. Er dokumentiert den gesamten Wortlaut der Referate und der Diskussionen sowie das bei dem Forum vorgestellte und auch im Anhang 3 zum vorliegenden Bericht abgedruckte gemeinsam mit Forschern erarbeitete Papier zur Vereinbarkeit von Datenschutz und epidemiologischer Forschung.

Die von meinen Mitarbeiterinnen und Mitarbeitern verfaßten Einzelbeiträge des Berichts legen nicht nur ein Zeugnis davon ab, was wir im Jahr 1998 getan haben. Es wird daraus auch deutlich, daß wir uns weiterhin nicht als Gegner der hessischen Staatsverwaltung, sondern als Gesprächspartner verstehen, die beratend, objektiv prüfend und gelegentlich auch deutlich kritisierend den unserer Kontrolle unterstehenden Adressaten des Hessischen Datenschutzgesetzes gegenübertreten. Dabei zeigt sich häufig, daß erst die genauere Befassung mit der Technik eines Prüfungsgegenstandes eine zutreffende Beurteilung des Gefährdungspotentials und die rechtliche Bewertung ermöglicht. Hierfür kann die ausführliche Darstellung des in der Öffentlichkeit viel beachteten Themas der sogenannten Geldkarte („elektronischen Geldbörse“) als Beispiel dienen. Die Konferenzentschließung dazu (Ziff. 26.2) konnte nach der Überprüfung der komplizierten rechtlichen und informationstechnischen Zusammenhänge durch eine differenzierte Bewertung mit praktischen Empfehlungen ergänzt werden (Ziff. 4).

Dieses und eine Reihe anderer Themen des Berichts haben zwar jeweils einen hessischen Anlaß, reichen aber in ihrer Bedeutung weit über unser Bundesland hinaus. Das gilt z.B. auch für die Probleme der Justizverwaltungen bei der Datenerhebung und Datenübermittlung im Zusammenhang mit der neuen beim Bundeskriminalamt errichteten DNA-Analyse-Zentraldatei (Ziff. 5.1) und mit der weiterhin fehlenden Rechtsgrundlage für eine Reihe anderer datenschutzrelevanter Vorgänge bei den Gerichten und Staatsanwaltschaften (Ziff. 6.1.1).

Das Hessische Ausführungsgesetz zum Bundeskrebsregistergesetz schreibt meiner Behörde zwei neue Aufgaben zu: Der Hessische Datenschutzbeauftragte ist Entschlüsselungsstelle für die Identitätsdaten der Patienten und in bestimmten Fällen sogar selbst speichernde Stelle für die Referenzlisten von einzelnen Arztpraxen (siehe Ziff. 7.1). Die personellen und sachlichen Voraussetzungen

für diese völlig neuen Aufgaben müssen erst noch geschaffen werden.

Dieses Erfordernis ist eine weitere Bestätigung der schon in meinen vorangegangenen Tätigkeitsberichten beschriebenen Tendenz, die es dringend erforderlich erscheinen läßt, meine Behörde ausreichend mit Technik und informationstechnisch geschultem Personal auszustatten, weil das datenschutzrechtliche Know-how nur in enger Zusammenarbeit mit Informatikern einen Sinn macht, deren Kenntnisse und Fertigkeiten in den sich immer schneller ändernden Hard- und Softwarestandards zu den Bedingungen eines effektiven Datenschutzes gehören. Die Gruppe der in meinem Hause tätigen Informatikerinnen und Informatiker bedarf dringend einer Verstärkung. Dabei ist es nicht mit Erhaltung oder Schaffung von Planstellen und deren Besetzung getan. Unverzichtbar ist auch die Bereitstellung von Arbeits- und finanziellen Mitteln, um durch ständige Weiter- und Fortbildung den Anschluß an die rasante Entwicklung nicht zu verlieren.

Ich danke allen meinen Mitarbeiterinnen und Mitarbeitern für die im Berichtszeitraum geleistete Arbeit, die sich nur insoweit in dem Bericht niederschlägt, als es um nicht „alltägliche“ Tätigkeiten geht. Würden wir auch diese im Bericht festhalten, wäre er zu umfangreich. Ich bin aber zuversichtlich, daß den Leserinnen und Lesern auch so unsere Pflichterfüllung deutlich wird.

R.H.

2. Die Umsetzung der EG-Datenschutzrichtlinie in Hessen

Hessen hat als erstes Bundesland die EG-Datenschutzrichtlinie mit einer Änderung des Hessischen Datenschutzgesetzes umgesetzt. Hierbei hat das zuständige Hessische Ministerium des Innern und für Landwirtschaft, Forsten und Naturschutz mich umfassend beteiligt.

2.1

Einleitung

Die EG-Datenschutzrichtlinie vom 24. Oktober 1995 „zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ (Amtsblatt der EG Nr. L 281/31 vom 23. November 1995) verpflichtet die Mitgliedstaaten, die Regelungen innerhalb von drei Jahren in nationales Recht umzusetzen. Änderungen zum Hessischen Datenschutzgesetz (HDSG) sind mit dem Regierungsentwurf vom 27. April 1998 im Landtag eingebracht worden. Der zuständige Ausschuß hat am 24. Juni 1998 die kommunalen Spitzenverbände, einen von den Vertretern der CDU benannten Sachverständigen und mich angehört. Das auf dieser Basis vom Parlament am 28. Oktober 1998 verabschiedete Änderungsgesetz beruht auf einem breiten Konsens aller vier im Hessischen Landtag vertretenen Parteien mit der Regierung, der auch meine Unterstützung gefunden hat.

Die hessische Landesregierung hat die notwendige Überarbeitung des Hessischen Datenschutzgesetzes zum Anlaß genommen, nicht nur die Vorschriften der EG-Datenschutzrichtlinie umzusetzen, sondern in ihrem Entwurf auch Anpassungen an die fortgeschrittene technologische Entwicklung vorzunehmen und Regelungslücken zu schließen. Damit hat sie einer Forderung der Datenschutzbeauftragten des Bundes und der Länder Rechnung

getragen, die die Bundes- und Landesgesetzgeber bereits im März 1996 aufgefordert hatten, die zur Umsetzung der EG-Datenschutzrichtlinie erforderliche Überarbeitung der Datenschutzgesetze auch dazu zu nutzen, neuere Entwicklungen der Informationstechnologie in die Gesetze einzuarbeiten (s. Entschließung der 51. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Modernisierung und zur europäischen Harmonisierung des Datenschutzrechts, 25. Tätigkeitsbericht, Ziff. 24.1).

In den Referentenentwurf in Hessen sind bereits im Entstehungsstadium Anregungen aus der Praxis, d.h. aus einer Arbeitsgruppe, in der behördliche Datenschutzbeauftragte der verschiedensten öffentlichen Stellen und mein Haus vertreten waren, eingeflossen.

Grundprinzip bei der Novellierung war es, nur dort die Regelungen zu ändern oder zu ergänzen, wo entweder die EG-Datenschutzrichtlinie eine Änderung erfordert oder die gesetzlichen Regelungen nicht (mehr) ausreichen, z.B. infolge der Technikentwicklung. Ziel war es, die Regelungen möglichst wenig kompliziert und praxisgerecht zu gestalten.

Im Zuge dieser Novellierung ist die Frage der Organisation der Kontrollstellen im öffentlichen und nicht-öffentlichen Bereich und deren Zusammenlegung in einer Stelle nicht behandelt worden. Dies haben die Parlamentarier ausdrücklich einer Diskussion nach der Umsetzung der EG-Datenschutzrichtlinie im Bundesdatenschutzgesetz vorbehalten, das die Datenschutzvorschriften im nicht-öffentlichen Bereich erheblich ändern muß.

2.2

Einzelfragen

Nachfolgend sollen nur die wesentlichen Neuerungen herausgestellt werden. Der interessierte Leser kann dabei auf den im Anhang 1 abgedruckten Wortlaut des neuen Gesetzes zurückgreifen, wie es nach Einarbeitung des Änderungsgesetzes voraussichtlich bereits bei Erscheinen dieses Tätigkeitsberichts vorliegt. Bei Redaktionsschluß war die Neufassung des Gesetzes noch nicht veröffentlicht. Die Änderungen sind im Anhang 1 durch Fettdruck kenntlich gemacht.

2.2.1

Stellung und Aufgaben der behördlichen Datenschutzbeauftragten

Die bisherige Regelung zu den behördlichen Datenschutzbeauftragten in Hessen war wenig aussagekräftig. Meine Querschnittsprüfung bei ca. 300 hessischen Dienststellen hatte erhebliche Defizite in diesem Bereich ergeben (s. 26. Tätigkeitsbericht, Ziff. 4). Deshalb wurden Stellung und Aufgaben des behördlichen Datenschutzbeauftragten konkreter und deutlicher gefaßt.

Kernstück der Neuregelung ist die detaillierte Aufgabenaufzählung. Neu sind auch die Weisungsfreiheit, das Benachteiligungsverbot, die Regelungen zur Freistellung von sonstigen Aufgaben und zur Ausstattung sowie das Recht aller Beschäftigten, sich ohne Einhaltung des Dienstweges an den behördlichen Datenschutzbeauftragten zu wenden (§ 5 Abs. 1). Auch die Pflicht zur rechtzeitigen und umfassenden Information ist jetzt ausdrücklich vorgeschrieben. Durch die Unterstellung unter die Leitung der Dienststelle bzw. in großen Kommunen unter fachlich zuständige hauptamtliche Beigeordnete soll die Stellung der behördlichen Datenschutzbeauftragten aufgewertet werden.

2.2.2

Register und Benachrichtigungspflicht

2.2.2.1

Dateienregister

Bislang führte meine Dienststelle ein Dateienregister und die datenverarbeitenden Stellen waren verpflichtet, mir ihre Dateien sowie jede Änderung zu melden. Aufwand und Nutzen standen in einem Mißverhältnis. In der langen Zeit, in der in Hessen das Dateienregister geführt wird, gab es nur vereinzelt Auskunftersuchen von Bürgerinnen und Bürgern aus diesem Register.

Die EG-Datenschutzrichtlinie schreibt die Meldung von Datenverarbeitungen zu einem Verzeichnis vor, allerdings nicht mehr auf Basis von Dateien, sondern für Verfahren. Das Verzeichnis soll die Transparenz automatisierter Datenverarbeitung erhöhen und die Kontrollinstanzen dadurch unterstützen, daß auf Grund der Beschreibung beurteilt werden kann, ob die vorgesehenen Maßnahmen zur Sicherheit der Verarbeitung angemessen sind.

In Hessen werden die behördlichen Datenschutzbeauftragten dezentral das Verzeichnis führen. Durch diese neue Regelung ist eine Reduzierung des Aufwandes zu erwarten. Die nach der EG-Datenschutzrichtlinie in das Verzeichnis aufzunehmenden Daten zu Rechtsgrundlagen, Aufgabenstellung und Struktur der automatisierten Datenverarbeitung sind ohnehin bei den datenverarbeitenden Stellen vorhanden; das erfordert schon die Revisionsfähigkeit von DV-Verfahren. Mit der neuen Regelung werden zwei Fliegen mit einer Klappe geschlagen: zum einen erhält der interne Datenschutzbeauftragte zwangsläufig Kenntnis von den Verfahren und kann deren datenschutzrechtliche Aspekte

besser beurteilen. Zum anderen kann er wegen der größeren Nähe mit sehr viel weniger Aufwand als eine zentrale Stelle Unklarheiten beseitigen, fehlende Angaben nachfragen und die Plausibilität der Angaben prüfen. Für meine Kontrollmaßnahmen wird eine Vereinfachung dadurch erreicht, daß ich mir durch Einsicht in das bei der geprüften Stelle geführte Verzeichnis ohne großen Aufwand einen Überblick über die dort eingesetzten Verfahren verschaffen kann. Da im Verzeichnis nicht mehr Dateien, sondern Verfahren zu beschreiben sind und ein Verfahren eine Vielzahl von Dateien enthalten kann, entfallen in solchen Fällen auch die bislang erforderlichen wiederkehrenden Angaben. Außerdem läßt die Verfahrensbeschreibung ein besseres Gesamtverständnis zu und die Sicherheit des Verfahrens kann nicht auf Datei-, sondern nur auf Verfahrensbasis beurteilt werden.

Damit genügend Zeit für die Umstellung von Datei- auf Verfahrensverzeichnisse besteht, tritt diese Vorschrift erst am 1. Juni 1999 in Kraft.

2.2.2.2

Benachrichtigungspflicht

In der Praxis immer wieder angegriffen und als generelle Regelung von zweifelhaftem Wert ist die im bisherigen Hessischen Datenschutzgesetz festgelegte Pflicht zur schriftlichen Benachrichtigung über eine automatisierte Datenverarbeitung. Aus Datenschutzsicht erscheint eine umfassende Information des Betroffenen vor oder bei der Datenerhebung viel wichtiger als eine Benachrichtigung von einer Datenverarbeitung. Eine Reduzierung der Benachrichtigungen hilft auch unnötigen und vom Betroffenen mit Unverständnis quittierten Verwaltungsaufwand zu vermeiden. Auch die EG-Datenschutzrichtlinie geht von einer Information des Betroffenen im Zusammenhang mit der Datenerhebung aus. Sie sieht für Betroffene vor, sie von einer Datenverarbeitung zu

benachrichtigen, wenn die Daten nicht bei ihnen erhoben wurden, sie keine Kenntnis von der Verarbeitung haben, die Vereinbarung nicht gesetzlich vorgesehen ist und die Benachrichtigung keinen unverhältnismäßigen Aufwand erfordert. Die Neuregelung der Benachrichtigungspflicht hat diese Ausnahmen übernommen. Dadurch werden Benachrichtigungen fast völlig entfallen.

2.2.3

Durch Technikentwicklung bedingte Änderungen

Der Fortschritt der Datenverarbeitungstechnik hat einige Neuerungen erforderlich gemacht, die nachfolgend dargelegt werden.

2.2.3.1

Technische und organisatorische Maßnahmen

Die bisher einheitlich in allen Datenschutzgesetzen des Bundes und der Länder geregelten zehn Maßnahmen (die „Zehn Gebote“ des Datenschutzes) waren überarbeitungsbedürftig, weil sie sich teilweise überschneiden, angesichts der neuen Entwicklungen teilweise aber auch Lücken aufwiesen. Forderungen aus der EG-Datenschutzrichtlinie wie die Sicherstellung der Integrität und Verfügbarkeit von Daten und die Berücksichtigung besonderer Sicherheitsanforderungen in Netzen fanden sich in den alten Regelungen nicht wieder. Deshalb ist § 10 Abs. 2 völlig neu formuliert. Dabei ist die Einbindung einer speziellen Technik oder spezieller Verfahren bewußt vermieden worden, um die Vorschrift zukunfts offen zu halten. Ohnehin sind ja die zu ergreifenden Maßnahmen nicht nur an die Verhältnismäßigkeit, sondern auch an den jeweiligen Stand der Technik gekoppelt.

Statt der bisher zehn werden acht Begriffe eingeführt:

- Zutrittskontrolle
- Benutzerkontrolle
- Zugriffskontrolle
- Datenverarbeitungskontrolle
- Verantwortlichkeitskontrolle
- Auftragskontrolle
- Dokumentationskontrolle
- Organisationskontrolle.

Im wesentlichen sind dabei die ehemalige Übermittlungs- und Eingabekontrolle in eine umfassendere Verantwortlichkeitskontrolle und die ehemalige Datenträger-, Speicher-, Benutzer- und Transportkontrolle in eine umfassendere Definition der Benutzer- und Datenverarbeitungskontrolle eingeflossen. Neu ist dafür die Dokumentationskontrolle, die auch die Forderung nach Revisionsfähigkeit von Datenverarbeitungsverfahren beinhaltet.

Obwohl eigentlich im Erforderlichkeitsgrundsatz enthalten, ist in § 10 Abs. 2 HDSG der Grundsatz der „**Datensparsamkeit**“ bei der Auswahl von automatisierten Verfahren konkretisiert. Hintergrund dieser Klarstellung war, daß ich bei meinen Prüfungen immer häufiger auf Verfahren stieß, die - meist nicht für den Einsatz in öffentlichen Stellen, sondern in Privatunternehmen entwickelt - einen umfassenden Datenkatalog erforderten und ebenso umfassende Auswertungen ermöglichten. Bei der Auswahl wurde häufig nicht darauf geachtet, daß die Verfahren nur eingesetzt werden dürfen, wenn sie so geändert sind, daß eine unzulässige Datenverarbeitung ausgeschlossen ist, insbesondere auch die Speicherung und Verarbeitung von mehr Daten, als sie Rechtsgrundlage und Zweck erfordern. Deshalb ist nun klargestellt, was auch bisher schon galt: Sind „maßgeschneiderte“ Verfahren am Markt nicht zu erhalten und die vorhandenen nicht so zu ändern, daß mit ihnen eine zulässige Datenverarbeitung möglich ist, muß die Stelle ein eigenes Verfahren entwickeln (lassen).

Andere Umformulierungen in § 10 Abs. 1 HDSG wurden vorgenommen, um den Verhältnismäßigkeitsgrundsatz klarer zu fassen und auch darauf zu verweisen, daß Maßstab für die Maßnahmen auch die Art der zu verarbeitenden Daten, also deren Sensitivität ist.

2.2.3.2

Vorabkontrolle

Die EG-Datenschutzrichtlinie sieht vor, daß bei „Verarbeitungen, die spezifische Risiken für die Rechte und Freiheiten der Personen beinhalten können“, eine Vorabkontrolle erfolgen soll. Die Diskussion zur Umsetzung dieser Vorschrift machte deutlich, daß sich im voraus selten abschätzen läßt, welche Verarbeitungen solche Risiken enthalten. Es kommt nämlich einerseits auf die Art der Daten und andererseits auf die Art der Verarbeitung an. Eigentlich läßt sich die Frage nach dem Risiko erst als Ergebnis einer Vorabkontrolle beantworten.

Deshalb ist die Pflicht zur Vorabkontrolle als generelle Pflicht in § 7 Abs. 6 HDSG postuliert, also Voraussetzung für die Zulässigkeit jeder automatisierten Datenverarbeitung. Die Vorabkontrolle obliegt dem für Einsatz oder Änderung des Datenverarbeitungsverfahrens Zuständigen. Der behördliche Datenschutzbeauftragte prüft das Ergebnis. In Zweifelsfällen ist meine Dienststelle einzuschalten. Ein hoher Aufwand muß dadurch nicht entstehen: Zum einen setzt die Verwaltung inzwischen eine Vielzahl von Standard-Verfahren ein, für die natürlich das Ergebnis einer einmal durchgeführten Vorabkontrolle bei gleicher Sachlage übernommen werden kann. Bei einfachen und wenig sensiblen Verfahren wird sich die Vorabkontrolle in der kurzen Darlegung und Begründung dieses Sachverhaltes erschöpfen. Bei Verfahren, die tatsächlich Risiken enthalten, ist sie Kernstück der

Datenschutzprüfung und soll gerade die verantwortlichen Stellen dazu anhalten, Risiken zu erkennen und abzusichern. Denkt man an Verfahren mit sensitiven Daten (z.B. im Gesundheitsbereich), an die Probleme von Vernetzung und Internetanschlüssen und an Probleme, die die künftige Entwicklung von gemeinsam von verschiedenen Stellen genutzten Verfahren und Datenbasen stellen, so erscheint hier eine Verdeutlichung der Risiken und die Entwicklung von Maßnahmen zur Vermeidung dieser Risiken unverzichtbar. Das Hessische Modell zur generellen Einführung einer Vorabkontrolle kann daher zu einer echten Qualitätssteigerung im Datenschutz führen.

2.2.3.3

Regelung für gemeinsame Verfahren

Bislang enthielt das Hessische Datenschutzgesetz – wie viele andere auch – nur eine Regelung für „Abrufverfahren“. Verfahren mit gemeinsamem Datenbestand und verteilter Verantwortung waren nicht vorgesehen. Die Regelung für Abrufverfahren erschöpfte sich im wesentlichen darin, daß diese als Grundlage einer Rechtsverordnung bedurften. Darin waren die wesentlichen Verfahrensfestlegungen zu treffen. Außerdem war vorher meine Dienststelle anzuhören.

Die neue Vorschrift des § 15 trägt der Tatsache Rechnung, daß in einigen Bereichen eine ressortübergreifende Bearbeitung von Vorgängen erforderlich ist, die automationsgestützt nicht zu Abrufverfahren, sondern zu gemeinsamen Verfahren auch in der Form führt, daß die Verantwortung für die Datenbasis und ggf. auch für verschiedene Datenverarbeitungsteile eines Gesamtverfahrens geteilt ist. Ein striktes Verbot solcher Ansätze – wie es manchmal verfochten wird – erscheint wenig hilfreich. Datenschutz sollte nicht den Fortschritt hindern, sondern ihn in die richtigen Bahnen lenken.

Angesichts der dynamischen Entwicklung von Datenverarbeitungsverfahren erschien auch das in der alten Vorschrift gesetzte Erfordernis, eine Rechtsverordnung müsse die Einzelheiten der Datenverarbeitung regeln, nicht mehr sinnvoll. Wesentlich für die Rechtmäßigkeit solcher Verfahren unter dem Aspekt des Grundrechtsschutzes ist, daß Datenschutzrisiken vermieden werden.

Die Verarbeitung von personenbezogenen Daten in gemeinsamen Verfahren birgt besondere Risiken. Deshalb war auch hier das Kernstück die Vorabkontrolle, auf die § 15 HDSG ausdrücklich verweist. Außerdem ist festgelegt, daß meine Dienststelle in jedem Fall vor Einrichtung oder Änderung eines solchen Verfahrens anzuhören und ihr dazu auch das Ergebnis der Vorabkontrolle vorzulegen ist (§ 15 Abs. 1 Satz 3 und 4 HDSG).

Wesentlich bei gemeinsamen Verfahren ist die Festlegung der Verantwortung, der Zuständigkeiten und im Hinblick z.B. auf die Sicherheit des Verfahrens insgesamt und die Abschottung einzelner Bereiche voneinander auch die Festlegung der technischen und organisatorischen Maßnahmen, insbesondere eine klare Regelung der Zugriffsrechte (Lese- und Schreibrechte).

Wegen der geteilten Verantwortlichkeit waren besondere Regelungen erforderlich, die auch die Führung und Einsicht in das Verfahrensregister und die Wahrung der Rechte der Betroffenen nach § 8 HDSG betreffen.

2.2.3.4

Besonderheiten bei Chipkarten und ähnlichen Technologien

Schon nach jetzigem allgemeinen Verständnis kann auf einer Chipkarte eine Datenverarbeitung erfolgen; sie ist ein Datenträger.

Zu den Besonderheiten der Chipkarte und ähnlicher Techniken gehört, daß der Betroffene diesen Datenträger ausgehändigt bekommt und daß er nicht ohne weiteres nachvollziehen kann, ob und ggf. welche Daten über ihn auf der Karte oder einem externen Rechner gespeichert werden. Dies bedingt eine andere Handhabung beim Auskunftsrecht. Wichtig erschien außerdem, eine verdeckte Datenverarbeitung auf solchen Systemen zu verhindern, also Transparenz zu schaffen und dem Betroffenen seine Informationsrechte umfassend zu sichern. Außerdem war die Aufklärungspflicht zu erweitern. Die neue Vorschrift in § 8 Abs. 2 HDSG vermeidet dabei bewußt, sich auf eine bestimmte Technik oder Form zu beziehen, um zukunfts offen zu bleiben. Bereits heute gibt es Systeme, z.B. in Ring- oder Armbandform, die man mit dem Begriff **Chipkarte** nicht erfassen kann. Deshalb wurde in den Text der erklärende Zusatz „etwa in Form einer Chipkarte“ als Anwendungsbeispiel aufgenommen, um das derzeit verbreitetste Medium nur beispielhaft zu benennen.

2.2.3.5

Besonderheiten bei der Videoüberwachung

Auch Videoüberwachung ist Datenverarbeitung. Das heißt, daß die Zulässigkeitsanforderungen für die Verarbeitung von Daten auch hier gelten. Nicht jede Videoüberwachung ist erforderlich und angemessen, nicht für jede gibt es eine Rechtsgrundlage. Die Besonderheit bei der Videoüberwachung besteht darin, daß hier Daten nicht gezielt zu einer Person aufgenommen (erhoben) werden, sondern von einem mehr oder weniger bestimmtem Personenkreis. Das erschwert es zu verifizieren, ob der Betroffene Kenntnis von der Datenerhebung hat. Wegen der zunächst unbestimmten Adressaten ist eine vorherige persönliche Information über die Datenerhebung aber auch nicht möglich. Hierfür war eine gesetzliche Regelung erforderlich; die bestehenden Vorschriften des Hessischen Datenschutzgesetzes

reichen nicht aus. § 12 Abs. 2 HDSG sieht deshalb vor, daß es in einem solchen Fall ausnahmsweise anstelle der Erhebung mit Kenntnisnahme des Betroffenen ausreicht, wenn der Betroffene die seinen schutzwürdigen Belangen angemessene Möglichkeit der Kenntnisnahme von der Datenerhebung und -verarbeitung hat.

2.2.4

Landesübergreifende Datenverarbeitung, insbesondere Übermittlung von Daten

Die EG-Datenschutzrichtlinie verfolgt den Grundsatz, daß landesübergreifende Datenverarbeitung, also insbesondere die Datenübermittlung, überall dort zulässig ist, wo ein Datenschutzniveau gewährleistet ist, das dem der Richtlinie entspricht (Art. 25). Innerhalb der Europäischen Union ist deshalb keine andere Behandlung mehr zulässig als bei einer inländischen Datenübermittlung und außerhalb der Europäischen Union richtet sich die Zulässigkeit im wesentlichen danach, ob das Datenschutzniveau ganz oder wenigstens in dem Bereich, in dem die Datenübermittlung erfolgen soll, gleichwertig ist. Die neue Regelung des § 17 HDSG setzt diese Vorschrift einschließlich der in Art. 26 geregelten Ausnahmen in hessisches Recht um. Da die einzelne übermittelnde Stelle nicht den Überblick über das Datenschutzniveau im Drittland haben kann, obliegt die Beurteilung der Angemessenheit meiner Dienststelle, die in diesem Fall einzuschalten ist.

2.2.5

Stellung des Hessischen Datenschutzbeauftragten

Nicht zwingend durch die EG-Datenschutzrichtlinie bedingt aber in gewisser Weise in Ausfüllung des Erfordernisses, eine völlig unabhängige Kontrollstelle zu schaffen (Art. 28 Abs. 1 Satz 2),

sind auch einige Änderungen bei den Vorschriften zu meiner Rechtsstellung erfolgt.

Zu erwähnen ist in diesem Zusammenhang,

- die Klarstellung, daß es sich bei meiner Behörde um eine oberste Landesbehörde handelt (§ 22 HDSG);
- die Einführung des Rechts, an Sitzungen des Landtags (Ausschüsse und Plenum) teilzunehmen und das Wort zu ergreifen, soweit es um Datenschutz geht;
- die Bestellung eines Vertreters für den Fall der vorübergehenden Verhinderung und der Befangenheit (§ 21 Abs. 4 Satz 5 und 6 HDSG).

2.3

Fazit und Ausblick

Hier sind nur die wichtigsten Änderungen dargestellt. Erkenntnisse aus meiner Praxis und aus den Dienststellen sind auch in eine Vielzahl anderer Neuformulierungen eingeflossen. Als ein Beispiel hierfür sei nur genannt, daß die Ergebnisse aus dem von mir gemeinsam mit dem Präsidenten des Hessischen Landtags am 18. Juni 1998 veranstalteten 7. Wiesbadener Forum Datenschutz zum Thema „Datenschutz und Forschung“ in § 33 eingearbeitet wurden (s. hierzu Ziff. 10).

Hessen hat als erstes Bundesland die EG-Datenschutzrichtlinie umgesetzt. Ob dies in allen Punkten vorbildlich gelungen ist und ob die Novellierung der rasanten technischen Entwicklungen gerecht werden kann, wird sich in der praktischen Anwendung der Vorschriften erweisen müssen. Der Gesetzgeber wird auch zukünftig den sich ändernden Normierungsbedarf im Auge behalten müssen. Dies wird schon mit der Novellierung des Bundesdatenschutzgesetzes akut werden. Darüber hinaus legen die Beschlüsse des 62. Deutschen Juristentages, der sich in seiner

Abteilung öffentliches Recht mit Fragen zur Informationsgesellschaft und dem Datenschutzrecht befaßt hat, eine gründliche Revision des Datenschutzrechts durch Einbettung in eine „Informationsverkehrsordnung“ nahe (Beschlüsse des 62. Deutschen Juristentages, s. Anhang 4).

3. Europa

Schengener Durchführungsübereinkommen

Die Gemeinsame Kontrollinstanz für das Schengener Informationssystem hat sich im Berichtszeitraum mit einer Reihe von Einzelproblemen befaßt und entsprechende Stellungnahmen abgegeben (u.a. Auskunftsrecht, Sicherheit der SIRENE-Büros, Zugriff auf das Schengener Informationssystem durch Kfz-Registerbehörden). Sie hat im März 1998 ihren Tätigkeitsbericht vorgelegt.

Auch im Berichtszeitraum war ich als Vertreter der Landesdatenschutzbeauftragten durch eine Mitarbeiterin an sieben Sitzungen der Gemeinsamen Kontrollinstanz für das Schengener Informationssystem vertreten. Im April stellte die Gemeinsame Kontrollinstanz ihren Tätigkeitsbericht für den Zeitraum März 1997 bis März 1998 auf einer Pressekonferenz in Brüssel vor.

Der Vorsitz der Gemeinsamen Kontrollinstanz lud Ende Juni zu einer Sitzung nach Lissabon ein. Zusätzlich organisierte die Portugiesische Datenschutzkontrollinstanz ein Kolloquium über die Rechte der Bürgerinnen und Bürger gegenüber polizeilichen Informationssystemen. Daran nahmen neben den Mitgliedern der Gemeinsamen Kontrollinstanz und anderer Schengen-Gremien Regierungsmitglieder, Polizeibeamte, insbesondere der nationalen Stellen, bei denen sich das Nationale Schengener Informationssystem befindet, Bürgerverbände und Anwältinnen und Anwälte aus den Europäischen Staaten teil.

Die Gemeinsame Kontrollinstanz hat sich u.a. mit folgenden Problemen beschäftigt:

3.1

Auskunftsrecht

Im 25. Tätigkeitsbericht (Ziff. 2.1.1) hatte ich berichtet, daß die Gemeinsame Kontrollinstanz beabsichtigt, die Bürgerinnen und Bürger besser über ihre Rechte gegenüber den für das Schengener Informationssystem zuständigen Stellen zu informieren.

Die Gemeinsame Kontrollinstanz hat zu diesem Zweck eine Broschüre erstellt, die in allen Sprachen der Europäischen Gemeinschaft vorliegt.

@.@.@

Einfügen 1. Seite Broschüre

@.@.@

Darin wird klargestellt, welche Daten überhaupt im Schengener Informationssystem gespeichert werden dürfen. Die Bürgerinnen und Bürger werden darauf aufmerksam gemacht, daß ihnen - unabhängig davon, ob sie Staatsangehörige einer Vertragspartei von Schengen sind - folgende Rechte zustehen:

- Recht auf Auskunft über ihre im Schengener Informationssystem gespeicherten personenbezogenen Daten,
- Recht auf Berichtigung unrichtiger Daten oder Recht auf Löschung unrechtmäßig gespeicherter Daten,
- Recht auf Ersatz des durch unzulässige oder unrichtige Speicherung entstandenen Schadens.

Die Bürgerinnen und Bürger können diese Rechte bei den Datenschutzkontrollinstanzen der Schengen-Staaten - deren Adressen im einzelnen aufgelistet sind - in jedem Schengen-Staat geltend machen. Nach der deutschen Rechtslage können Auskunftersuchen aber auch u.a. an das Bundeskriminalamt oder die Landesbeauftragten für den Datenschutz gerichtet werden. Aus

Gründen der Übersichtlichkeit wurde in der Broschüre nur die Adresse des Bundesbeauftragten für den Datenschutz angegeben.

Die Broschüren werden an den für das Überschreiten der Schengener Außengrenzen zugelassenen Grenzübertrittsstellen ausgelegt. Die Bürgerinnen und Bürger werden durch Plakate darauf aufmerksam gemacht. Die Broschüren und Plakate können auch beim Bundesbeauftragten für Datenschutz oder mir angefordert werden.

3.2

Sicherheit der SIRENE-Büros

Ende November letzten Jahres wurde bekannt, daß ein Mitarbeiter des belgischen SIRENE-Büros, also der Stelle, an der das belgische Nationale Schengener Informationssystem betrieben wird, über Jahre hinweg Listen mit ausgeschriebenen Personen aus dem Gebäude entfernt und an Dritte weitergegeben hat. Nach Presseberichten soll er mit dem Datenmaterial einen lukrativen Handel mit Personen geführt haben, die der organisierten Kriminalität zugeordnet werden. Nähere Einzelheiten sind wegen des noch laufenden strafrechtlichen Ermittlungsverfahrens nicht zu erhalten.

Die Gemeinsame Kontrollinstanz nahm den Vorfall zum Anlaß, um eine Kontrolle aller nationalen SIRENE-Büros vorzunehmen.

Der Bundesbeauftragte für den Datenschutz berichtete vom Bundeskriminalamt, der deutschen SIRENE-Stelle, daß die technisch-organisatorischen Maßnahmen im großen und ganzen zufriedenstellend sind.

Zu der - vor dem Hintergrund des Vorfalls in Belgien - wichtigen Frage der Sicherheitsüberprüfung des mit der Datenverarbeitung im

Rahmen des Schengener Informationssystems betrauten Personals teilte das Bundeskriminalamt mit, daß alle Polizeivollzugsbeamten nach dem Sicherheitsüberprüfungsgesetz überprüft werden. Gegebenenfalls vorhandene Zweifel an einer pflichtgemäßen Ausübung des Dienstgeschäftes führten zu Maßnahmen der Dienstaufsicht. Auch für andere Verwaltungsbeamte erfolgten bei ihrer Einstellung beim Bundeskriminalamt die nach dem Bundesbeamtengesetz erforderlichen Überprüfungsmaßnahmen, d.h. Anfragen bei den einschlägigen Sicherheitsbehörden, was als Sicherheitsüberprüfung i.S.d. Schengener Durchführungsübereinkommens angesehen werden könnte.

Die Gemeinsame Kontrollinstanz ist derzeit dabei, die Prüfberichte der einzelnen Mitgliedsstaaten auszuwerten und einen zusammenfassenden Bericht zu erstellen.

3.3

Zugriff von Verwaltungsbehörden auf das Schengener Informationssystem

In mehreren Schengener Vertragsstaaten haben die für das Kraftfahrzeugregister zuständigen Stellen Interesse geäußert, auf den Datenbestand über gestohlene oder unterschlagene Kraftfahrzeuge Zugriff zu nehmen. Auf diese Weise könnten die Kraftfahrzeugbehörden z.B. bei der Zulassung feststellen, ob das Auto in anderen Schengen-Staaten gestohlen wurde.

So berechtigt die Forderung auch erscheint, sie ist mit den rechtlichen Voraussetzungen des Schengener Durchführungsübereinkommens nicht vereinbar.

Nach Artikel 101 Schengener Durchführungsübereinkommen haben neben bestimmten Ausländerbehörden ausschließlich solche Behörden Zugriff, die für Grenzkontrollen oder für sonstige

polizeiliche und zollrechtliche Überprüfungen im Inland sowie deren Koordinierung zuständig sind.

Nach Auffassung der deutschen Delegation in der Gemeinsamen Kontrollinstanz, die von den meisten Mitgliedern geteilt wird, handelt es sich bei den Kraftfahrzeugbehörden um Verwaltungsbehörden mit einer anderen Aufgabenstellung. In Deutschland und den meisten anderen Schengen-Staaten sind die Kraftfahrzeugbehörden nicht für polizeiliche Überprüfungen zuständig.

Es ist darüber hinaus zu befürchten, daß bei einer Aufweichung der im Schengener Durchführungsübereinkommen vorgesehenen Anforderungen an die zugriffsberechtigten Stellen in Kürze weitere Stellen Interesse an Zugriffsmöglichkeiten geltend machen werden.

Die Gemeinsame Kontrollinstanz wird in einer der nächsten Sitzungen zu diesem Problem einen Beschluß fassen.

3.4

Mißbräuchliche Verwendung von Alias-Personalien

Im 25. Tätigkeitsbericht (Ziff. 2.1.2) hatte ich über Probleme mit der mißbräuchlichen Verwendung von Alias-Personalien berichtet: Es kommt vor, daß eine Person mit gefälschten oder gestohlenen Ausweispapieren, also mit gefälschten Identitätsangaben, im Schengener Informationssystem (SIS) ausgeschrieben wird. Für den rechtmäßigen Inhaber führt dies, beispielsweise bei einer Polizeikontrolle, zu Schwierigkeiten. Das Problem besteht darin, daß die Daten einerseits gelöscht werden müssen, weil sie falsch sind, andererseits die Sicherheitsbehörden ein Interesse daran haben, die Fahndung auch nach solchen Personen fortzusetzen, die unter ihrem falschen Namen auffindbar sein können. Die Gemeinsame Kontrollinstanz hat in einer Stellungnahme

festgehalten, daß diese Interessen gegeneinander abgewogen werden müssen und im Einzelfall eine Beibehaltung der Fahndung in Frage kommen kann. Sie hat weiter darauf verwiesen, daß bis zur Inbetriebnahme einer neuen Generation des Schengener Informationssystems (SIS II) eine angemessene und möglichst gemeinsame Lösung für die Fälle zu finden ist, in denen die Fahndungsnotierung unter falschen Personalien beibehalten wird. Damit ist u.a. die im 25. Tätigkeitsbericht (Ziff. 2.1.2) beschriebene Praxis gemeint, nach der derzeit beim Bundeskriminalamt verfahren wird: Dem rechtmäßigen Inhaber der Personalien wird eine Bescheinigung ausgestellt, welche er bei einer Polizeikontrolle vorzeigen kann.

3.5

Weitere Stellungnahmen der Gemeinsamen Kontrollinstanz

Die Gemeinsame Kontrollinstanz hat sich abschließend zu den im 26. Tätigkeitsbericht angesprochenen Problemen der Aufbewahrung von Fahndungsunterlagen nach Erledigung der Ausschreibung (Ziff. 2.2) und der Praxis der Protokollierung (Ziff. 2.3) geäußert.

Es wurde festgestellt, daß in verschiedenen Schengen-Staaten bei den nationalen Stellen, die für den Betrieb des nationalen Teils des Schengener Informationssystems (NSIS) zuständig sind, Unterlagen, die im Laufe einer Fahndung zu einer Person angefallen sind, über den Zeitpunkt der Erledigung der Fahndung hinaus aufbewahrt werden. Auf deutscher Seite wurde vom Bundeskriminalamt vorgetragen, daß die Unterlagen - auch nach Löschung der Fahndung im Schengener Informationssystem - für Zwecke der Gefahrenabwehr oder der vorbeugenden Verbrechensbekämpfung zur Verfügung stehen sollen. Die Mitglieder der Gemeinsamen Kontrollkommission haben unmißverständlich klargestellt, daß bei Löschung einer

Ausschreibung zur Personenfahndung jede Vertragspartei verpflichtet ist, die personenbezogenen Daten zu löschen und alle zugehörigen Begleitpapiere umgehend zu vernichten.

Aus einer Umfrage bei den entsprechenden Behörden der Schengen-Mitgliedstaaten ergab sich, daß das Verfahren, nachdem die Abrufe aus dem nationalen Teil des Schengener Informationssystems vorgenommen werden, in den einzelnen Staaten unterschiedlich gehandhabt wird und nicht in jedem Fall mit Art. 103 Schengener Durchführungsübereinkommen vereinbar ist. Die Gemeinsame Kontrollinstanz hat eine Reihe von Mindestanforderungen an die Protokollierung aufgestellt: Danach gehören beispielsweise der Grund der Abfrage zur Protokollierung aber auch solche Angaben, die erforderlich sind, um den jeweiligen Benutzer eindeutig feststellen zu können.

3.6

Kontrolle des Zentralen Schengener Informationssystems (CSIS)

Die Gemeinsame Kontrollinstanz hat im März 1994 und Oktober 1996 Kontrollen des CSIS in Straßburg vorgenommen (s. 24. Tätigkeitsbericht, Ziff. 2.2 und 26. Tätigkeitsbericht, Ziff. 2.1). In ihrem Bericht vom März 1998 hat die Zentrale Gruppe von Schengen zur Beantwortung des Tätigkeitsberichts der Gemeinsamen Kontrollinstanz darauf schriftlich reagiert. Aus Sicht der Gemeinsamen Kontrollinstanz ist die Stellungnahme nicht zufriedenstellend. Dies gilt insbesondere für das Problem, daß nach Feststellung der Gemeinsamen Kontrollinstanz die Datenbestände von Frankreich und Luxemburg und teilweise auch von anderen Staaten nicht zu jedem Zeitpunkt - wie gesetzlich vorgesehen - identisch sind. Auch auf die Kritik der Gemeinsamen Kontrollinstanz an Defiziten bei der Datensicherheit wurde zu

wenig eingegangen. Die Gemeinsame Kontrollinstanz steht hierzu in Gesprächen mit Mitgliedern der Zentralen Gruppe.

Derzeit wird eine Prüfung des Zentralen Schengener Informationssystems in Straßburg für Anfang nächsten Jahres vorbereitet.

4. Banken

Geldkarte

Mit der von der deutschen Kreditwirtschaft angebotenen Geldkarte kann anonym bezahlt werden. Bei kontogebundenen Geldkarten könnten allerdings die Zahlungsvorgänge einer bestimmten Person zugeordnet werden, wenn mehrere an dem Zahlungsverkehr beteiligte Stellen zu diesem Zweck in einer vom System nicht vorgesehenen Weise zusammenwirken.

4.1

Kontroverse

Im Frühjahr 1998 hat sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer EntschlieÙung kritisch zu der von der deutschen Kreditwirtschaft angebotenen GeldKarte geäuÙert (s. Ziff. 26.2). Bezweifelt hat die Konferenz vor allem, daß die GeldKarte die Möglichkeit bietet, wie bei Bargeldzahlungen anonym zu bleiben. Die Kreditwirtschaft hat die Kritik als unbegründet zurückgewiesen. Dies war AnlaÙ für mich, in Kooperation mit der Nassauischen Sparkasse, der Buchungszentrale der westfälisch-lippischen Sparkassen und dem Deutschen Sparkassen- und Giroverband die Informationsflüsse dieses neuen Zahlungssystems zu überprüfen.

4.2

Elektronische Geldbörse

GeldKarte ist der Markenname für die von der deutschen Kreditwirtschaft angebotene "elektronische Geldbörse". Das bargeldlose Zahlungsverfahren ist gedacht für Geschäfte bis etwa 25,00 DM, bei denen der Einsatz einer Kreditkarte oder der ec-

Karte unwirtschaftlich wäre. Die Kundin oder der Kunde erhält vom Kreditinstitut eine Karte, auf der sich ein elektronischer Speicher (Chip) befindet. Die elektronische Geldbörse kann auf einer ec-Karte oder einer Bankkundenkarte untergebracht sein; sie kann aber auch als sog. "Weiße Karte", die kontounabhängig ist, ausgegeben werden. Auf der Chipkarte läßt sich ein Geldbetrag speichern, dessen Höhe zur Zeit auf 400,00 DM begrenzt ist.

4.3

Vertragliche Grundlagen

Das System beruht auf folgenden vertraglichen Grundlagen: Vier der fünf im Zentralen Kreditausschuß (ZKA) zusammenarbeitenden Spitzenverbände der deutschen Kreditwirtschaft (Bundesverband der Deutschen Volksbanken und Raiffeisenbanken, Bundesverband deutscher Banken, Deutscher Sparkassen- und Giroverband sowie der Verband öffentlicher Banken - nicht beteiligt ist der Verband deutscher Hypothekenbanken) haben eine "Vereinbarung über das institutsübergreifende System 'GeldKarte'" geschlossen, die am 1. Oktober 1996 in Kraft getreten ist. Jedes Kreditinstitut, das seinen Kundinnen und Kunden die Teilnahme an dem System GeldKarte ermöglichen will, muß diese Vereinbarung anerkennen. Die Rechtsbeziehungen zwischen den kartenausgebenden Kreditinstituten und ihren Kundinnen und Kunden wird durch geänderte "Bedingungen für die Verwendung der ec-Karte" bzw. entsprechende Bedingungen für Kundenkarten geprägt; das Verhältnis der beteiligten Kreditinstitute zu den angeschlossenen Händlern wird durch die "Bedingungen für die Teilnahme am System 'GeldKarte'" gestaltet. Beim Einsatz der Geldkarte entstehen mithin drei Rechtsbeziehungen: Das Deckungsverhältnis zwischen kartenausgebendem Kreditinstitut und Karteninhaber, das Valutaverhältnis zwischen Karteninhaber und Akzeptanzstelle (Unternehmen) und das Vollzugsverhältnis zwischen Unternehmen

und kartenausgebendem Kreditinstitut. Insofern unterscheidet sich die GeldKarte nicht von anderen Kartensystemen.

4.4

GeldKarte-System

4.4.1

Infrastruktur

An den Daten- und Geldflüssen einer Zahlung mit der GeldKarte sind folgende Einrichtungen beteiligt:

- Händlerbank, die dem Händler seine Chipkarte, die Händlerkarte, ausstellt
- Kundenbank, die den Kundinnen und Kunden entweder eine kontogebundene GeldKarte, also eine ec-Karte oder Bankkundenkarte mit GeldKartenfunktion, oder eine kontoungebundene GeldKarte, eine sog. "Weiße Karte", aushändigt
- Ladezentrale
- Händlerevidenzzentrale (HEZ)
- Börsen- oder Kartenevidenzzentrale (KEZ)
- Verrechnungsbanken

Es gibt derzeit in der Bundesrepublik für die Sparkassen, die Volks- und Raiffeisenbanken, die öffentlichen Banken und die Privatbanken je eine Händler- und eine Börsenevidenzzentrale. Da aus praktischen Gründen eine Institution die prinzipiell trennbaren Funktionen Händler- und Börsenevidenzzentrale ausführt, spricht man auch von vier Evidenzzentralen. Für die Sparkassenorganisation ist dies die BWS (Buchungszentrale der westfälisch-lippischen Sparkassen) in Münster.

4.4.2

Abläufe

Die folgende Beschreibung beschränkt sich auf die direkt mit einer Zahlung verbundenen Abläufe. Unberücksichtigt bleiben die Datenflüsse für Gebühren- und Entgeltabrechnungen, die zwischen den Kreditinstituten und zu anderen Stellen stattfinden.

4.4.2.1

Vorbereitung

Die Kreditwirtschaft hat die Organisation zur GeldKarte mit den oben genannten Institutionen aufgebaut. Die einzelnen Kreditinstitute bereiten sich auf Zahlungsflüsse vor, indem sie je Verfallsjahr der Karten ein Börsenverrechnungskonto (BVK) einrichten. Aus diesem Sammelkonto werden später die Zahlungen an die Händler über Verrechnungskonten vorgenommen.

4.4.2.2

Händlerinnen und Händler

Entschließt sich ein Händler, an dem Verfahren "GeldKarte" teilzunehmen, muß er mit einem Kreditinstitut seiner Wahl einen entsprechenden Vertrag schließen. Daraufhin erhält er eine oder mehrere Händlerkarten von seinem Kreditinstitut. Diese Händlerkarten werden, zumindest in der Sparkassenorganisation, von seinem Kreditinstitut mit einer Anwendung bei dem eigenen Rechenzentrum erstellt. Der Händlerevidenzzentrale ist zu diesem Zeitpunkt nicht bekannt, daß die Händlerkarten existieren.

In dem Vertrag verpflichtet sich der Händler, nur Händlerterminals und Kartenlesegeräte einzusetzen, die den Vorgaben der Kreditwirtschaft entsprechen.

4.4.2.3

Kundin und Kunde

Ein Kunde, der die GeldKarte nutzen möchte, hat die Wahl zwischen einer Kombination der Geldkartenfunktion mit Bankkundenkarte bzw. ec-Karte oder, soweit sein Kreditinstitut dies anbietet, einer kontounabhängigen GeldKarte, der sogenannten "Weißen Karte".

Die "Weiße Karte" erhält er von einem Kreditinstitut gegen ein Pfand oder einen Geldbetrag. Das Kreditinstitut muß nicht wissen, wer die Kundin oder der Kunde ist.

4.4.2.4

Laden der GeldKarte

Der Kunde kann von jedem Ladeterminal aus einen Geldbetrag von seinem Konto auf die kontogebundene Karte laden; je nach Kreditinstitut können aber Entgelte anfallen. Da sein Konto belastet wird, muß er seine PIN eingeben. Erst nachdem die PIN geprüft wurde, erfolgt eine Belastung seines Kontos und die Karte wird geladen.

Bei einer "Weißen Karte" geht der Kunde an den Bargeldschalter des Kreditinstituts und zahlt dort den gewünschten Betrag ein. Das Laden des Betrages nimmt dann das Schalterpersonal vor. In diesem Fall wird statt des Kundenkontos ein speziell zu diesem Zweck beim Kreditinstitut eingerichtetes Konto belastet.

Mit der Gutschrift auf die Karte ist eine Buchung vom Kundenkonto, bzw. dem Konto für Einzahlungen, auf das Börsenverrechnungskonto (BVK) des Kreditinstituts verbunden.

Diese Buchung wird durch die Ladezentrale initiiert. In den Datensätzen wird nicht die Kartenummer übertragen. Das BVK ist ein Sammelkonto, auf dem die Summe aller Beträge gespeichert ist, die sich noch auf GeldKarten des Kreditinstituts befinden. (Es wird den Sparkassen empfohlen, je Kartenart und je Kartenverfallsjahr ein Konto einzurichten.)

Gleichzeitig mit der Gutschrift auf dem BVK erhält die Börsenevidenzzentrale eine Lademeldung zur GeldKarte. Der Datensatz enthält keinen Hinweis auf das Konto, von dem geladen wurde. Um den Ladebetrag werden sog. "Schattensalden" erhöht, die die entsprechenden Bestände auf dem BVK und der GeldKarte repräsentieren. Wenn zu der GeldKarte noch kein "Schattensaldo" existiert, wird er neu angelegt. Die Salden sind dazu vorgesehen, Mißbräuche des GeldKarten-Systems zu erkennen. Indizien dafür sind, wenn nach Zahlungen (vgl. 4.4.2.5) die Salden unerklärlicherweise negativ werden.

Von der BWS wurden in einem Testsystem Lade- und Bezahlvorgänge simuliert. (s.a. 4.4.2.5) Hier ist der Datensatz des "Schattensaldos" für eine GeldKarte wiedergegeben, die gerade mit 99,00 DM erstmals geladen wurde.

Tabelle 1:

Aufbau "Schattensaldo"

BLZ	Kartenummer	Datum	Lkey	Datum	Buchung	Betrag	Saldo
67259008	1990000124	98-10-22	0001	98-10-22	14:35:09	09900	9900

Lkey ist der Zähler für Zahlungsvorgänge. Die Karte wurde also erstmals geladen.

@.@ Grafik "Ladevorgang" @.@

4.4.2.5

Zahlung bei der Händlerin und dem Händler

Der Kunde bezahlt mit der GeldKarte. Abhängig von der technischen Ausstattung des Händlers wird der zu zahlende Betrag von der Kasse direkt zum Händlerterminal übertragen oder muß dort noch einmal eingegeben werden. Dieser Betrag muß bestätigt werden; in jedem Fall sollte dies der Kunde selbst machen. Es wird dann die GeldKarte in den Kartenleser geschoben. Durch kryptografische Protokolle gesichert, werden dann die erforderlichen Informationen zwischen Händlerkarte und der GeldKarte ausgetauscht. Der bestätigte Betrag wird von der GeldKarte abgebucht. Anschließend drucken die meisten Händlerterminals noch einen Beleg aus, den der Kunde sinnvollerweise mitnehmen sollte.

Durch diese Zahlung, im folgenden Transaktion genannt, wird ein Datensatz erzeugt, der in dem Händlerterminal bis zur Übertragung an die Händlerevidenzzentrale zwischengespeichert wird. Bei einer Übertragung werden alle seit der letzten Übertragung gespeicherten Transaktionsdatensätze nach Händlerkarten getrennt gesammelt und mit einem durch die Händlerkarte generierten Vor- und einem Summensatz zur Händlerevidenzzentrale übertragen.

Im Folgenden werden ein Zahlungs- und ein Summensatz beschrieben, die das BWS in einem Testsystem erzeugt hat. Der Aufbau stimmt mit Datensätzen tatsächlicher Zahlungen überein. Die Darstellung erfolgt in hexadezimaler Schreibweise. Bei dieser Schreibweise wird jedes Byte, also eine Speicherstelle mit 8 Bit, in zwei Halbbyte zu je 4 Bit geteilt. Jedes Halbbyte kann als Darstellung einer Zahl von 0 bis 9 und der Buchstaben A bis E interpretiert werden. Dies erleichtert das Lesen von gespeicherten Daten.

Tabelle 2:

**Daten der im Testsystem eingesetzten Karten, deren Datensätze
ausgedruckt wurden**

	GeldKarte		Händlerkarte
Bankleitzahl (BLZ)	940 593 08	Bankleitzahl (BLZ)	963 522 22
Kurz-BLZ	672 590 08	Kurz-BLZ	672 560 31
Kartennummer	1990000124	Kartennummer	0000000130
BLZ des Börsenverrechnungs- kontos (BVK)	940 593 08		
Konto-Nr. des BVK	900480492	Konto-Nr. Karte	440

Mit der GeldKarte wurde ein Einkauf von 0,10 DM simuliert. Der folgende Zahlungssatz resultierte aus der Zahlung. (Hexadezimale Schreibweise; ein D am Ende eines Feldes bedeutet, daß die Speicherung hexadezimal erfolgt. Die Ziffer davor ist eine Prüfziffer.)

E96725603100000001300D000000420000008E672590081990000
1249D000100010000109405930809004804929D00000841199810
2214583400CF5D0F9EA330A050000000000000000000000000000
0

Tabelle 3:

Erläuterung eines Zahlungssatzes

Position	Byte	Länge	Wert	Erläuterung
1	1	1	E9	Buchstabe Z (EBCDIC-kodiert) für Zahlungssatz
2	2-11	10	6725603100000001300D	BLZ und Händlerkartennummer
3	12-15	4	00000042	Sequenznummer des Summensatzes der Transaktion; durch das Händlerterminal bei der Bildung des Summensatzes generiert
4	16-19	4	0000008E	Sequenznummer der Transaktion; durch das Händlerterminal bei der Zahlung generiert
5	20-29	10	6725900819900001249D	BLZ und Nummer der GeldKarte

				BLZ und Kontonummer
4	34-37	4	00000042	Sequenznummer des Summensatzes
5	38-41	4	00000001	Anzahl der folgenden Datensätze
6	42-46	5	0000000010	Summe der Transaktionsbeträge
7	47-50	4	19981022	Datum: 22. Okt. 1998
8	51-53	3	145902	Zeit: 14 Uhr 59 Min. 2 Sek.
9	54	1	00	Daten zur Verschlüsselung
10	55-62	8	EFD150CDF6FB4AA2	MAC (Message Authentication Code); eine Prüfsumme, die es erlaubt, Manipulationen am Datensatz zu erkennen.
11	63-80	18	00..00	Reserve

Händlervidenzzentrale

In der Händlervidenzzentrale werden die eingehenden Daten auf Doppeleinreichungen oder andere Unstimmigkeiten geprüft. Wenn die Daten als korrekt angesehen werden, wird für das Händlerkonto eine Gutschrift über den Gesamtbetrag erzeugt. Über die Verrechnungsbank wird die Überweisung veranlaßt.

Die Datensätze der Transaktionen werden nach den jeweils zuständigen Börsenvidenzzentralen sortiert und unverändert dorthin übertragen.

Börsenvidenzzentrale

In den Börsenvidenzzentralen werden entsprechend den Daten einer Transaktion zwei Aktionen durchgeführt.

Von dem bei der Börsenvidenzzentrale geführten "Schattensaldo" zu der GeldKarte wird der Zahlungsbetrag abgezogen.

Tabelle 5:

"Schattensaldo" nach einer Zahlung

	BLZ	Karten-Nr.	Datum	Lkey	Datum	Buchung	Betrag	Saldo
Vorher	67259008	1990000124	98-10-22	0001	98-10-22	14:35:09	09900	9900
Nachher	67259008	1990000124	98-10-22	0001	98-10-22	15:37:36	00010	9890

Gleichzeitig wird für das Börsenverrechnungskonto des Kreditinstituts die Summe der daraus zu leistenden Zahlungen errechnet. Einmal am Tag wird eine Lastschrift zum BVK über die Summe der Zahlungsbeträge erzeugt und der Verrechnungsbank zugeleitet. Zu Abstimmzwecken wird auch die Summe der Ladebeträge des BVK übertragen. Die Verrechnungsbank führt auch den Ausgleich mit den Konten der Händlerinstitute durch.

@.@ Grafik "Zahlung ..." @.@

4.4.2.6

Datenflüsse

Beim Aufladen einer GeldKarte sind in der Ladezentrale sowohl die Kartendaten als auch die Kontodaten des Ladevorgangs bekannt. Diese Daten werden archiviert. Sie erlauben eine Zuordnung zwischen dem Konto, von dem geladen wurde, und der GeldKartenummer.

Die Börsenevidenzzentrale erhält bei einem Ladevorgang keine Informationen über das Kundenkonto, von dem geladen wurde. Das Kreditinstitut erhält keine Datensätze von der Ladezentrale, in denen die Kartenummer auftaucht.

Die Daten über Zahlungstransaktionen beinhalten u.a. Händlerkartenummer, Datum, Uhrzeit und Betrag. Es ist nicht möglich zu erkennen, wieviele Waren gekauft wurden. In der Regel läßt sich auch nicht auf die gekaufte Ware schließen. Bei den Testkäufen ließe sich der Weg der Karte rekonstruieren, wenn eine Zuordnung von Händlerkartenummer zum Händler möglich ist.

Diese Informationen sind beim Kreditinstitut des Händlers bzw. der Händlerevidenzzentrale vorhanden. Derartige Verknüpfungen sind aber nach dem GeldKarten-System nicht vorgesehen.

Die Daten der einzelnen Transaktionen werden sowohl in der Händlerevidenzzentrale als auch in den Börsenevidenzzentralen gespeichert. Die Archivierungsdauer beträgt elf Jahre.

4.5

Abgleichsmöglichkeiten

Die folgenden Überlegungen stellen prinzipiell mögliche Datenabgleiche auf Grund der gespeicherten Daten dar. Es soll damit nicht behauptet werden, daß Kreditinstitute oder ihre Rechenzentren derartige Auswertungen vornehmen oder beabsichtigen, diese vorzunehmen.

Die gespeicherten und archivierten Daten erlauben es, den Weg einer GeldKarte in begrenztem Rahmen auch noch nach längerer Zeit zu verfolgen. Rückschlüsse auf gekaufte Waren dürften in der Regel nicht möglich sein, können aber in Extremfällen nicht ausgeschlossen werden. Um diese Informationen zu erhalten, müssen die Händlerevidenzzentrale oder die Börsenevidenzzentrale und das Händlerinstitut ihre Daten zusammenführen.

Bei einer ec-Karte kann davon ausgegangen werden, daß sie auch von dem Kontoinhaber benutzt wurde, da er ansonsten ein hohes Risiko eingeht. Die Zuordnung von Kartenummer zur Kontonummer, und damit dem Kontoinhaber, können die Ladezentrale und das Kundenkreditinstitut vornehmen. Bei einer "Weißen Karte" kann das Kundenkreditinstitut die Zuordnung nicht herstellen, wenn bei der Aushändigung keine Notizen gemacht wurden.

Eine umfassende Auswertung der Daten und Zuordnung zu einer Person wäre nur möglich, wenn mehrere Institutionen ihre Daten in nicht vorgesehener Weise miteinander abgleichen würden.

Beispiele sind:

- Händlerinstitut, Händlerevidenzzentrale, Kundeninstitut oder
- Händlerinstitut, Börsenevidenzzentrale, Kundeninstitut

Für die Sparkassenorganisation nimmt die BWS folgende Funktionen wahr:

- bundesweite Händlerevidenzzentrale
- bundesweite Börsenevidenzzentrale
- regionale Ladezentrale und
- Rechenzentrum für einige Regionen

Ob ein Kunde bei der Bezahlung mit der GeldKarte anonym bleiben kann, hängt daher entscheidend von den Sicherheitsvorkehrungen der beteiligten Stellen ab. Es muß ausgeschlossen werden, daß institutsübergreifende Auswertungen erstellt werden. Mit dem Hinweis auf das Bankgeheimnis bekräftigt das Kreditgewerbe immer wieder, daß keine derartigen Auswertungen vorgenommen werden und es sich den Wünschen anderer Stellen, soweit rechtlich zulässig, widersetzen werde.

Der Datenabgleich für eigene Geschäftszwecke wäre außerdem gemäß § 28 Abs. 1 Nr. 1 und 2 Bundesdatenschutzgesetz (BDSG) unzulässig, da er weder im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit den Kunden erfolgen würde noch zur Wahrung berechtigter Interessen der speichernden Stellen erforderlich wäre.

§ 28 Abs. 1 BDSG

Das Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig

1. im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen
2. soweit es zur Wahrung berechtigter Interessen der speichernden Stellen erforderlich ist ...

Um das Risiko eines Datenabgleichs möglichst weitgehend zu minimieren, sollte die Aufbewahrungsdauer der bei den Evidenzzentralen kartenbezogen gespeicherten Transaktionsdaten möglichst kurz sein. Gegenwärtig ist eine Speicherdauer von maximal elf Jahren vorgesehen. Die Kreditwirtschaft sieht sich dazu durch § 257 Handelsgesetzbuch verpflichtet. Auf Grund dieser Vorschrift sind Buchungsbelege zehn Jahre aufzubewahren. Die Aufbewahrungsfrist beginnt mit dem Ende des Kalenderjahres, in dem der Buchungsbeleg entstanden ist. Voraussetzung für die Anwendbarkeit der Vorschrift ist, daß sich der Beleg auf ein Handelsgeschäft bezieht. Das ist hier jedoch zweifelhaft. Die kartenbezogenen Transaktionsdaten sind lediglich ein Zwischenschritt für die eigentliche Buchung: den Geldtransfer über die Verrechnungsbanken. Dieser Zwischenschritt ist eine technische Kontrollmaßnahme im Zahlungssystem GeldKarte, auf die man (rechtlich) auch verzichten könnte, was bei Buchungsbelegen über Handelsgeschäfte nicht zulässig wäre. Bei dieser Interpretation der Vorschrift könnte die Aufbewahrungsfrist auf eine für die Sicherheitskontrollen notwendige Dauer beschränkt werden und wäre damit erheblich kürzer.

4.6

Auftragsdatenverarbeitung oder Funktionsübertragung

Die rechtliche Qualifizierung der Beziehung zwischen den kartenemittierenden Kreditinstituten und den Evidenzzentralen ist entscheidend für die Beantwortung der Frage, ob die Nutzung der Geldkarte zur Verarbeitung personenbezogener Daten führt. Wenn die Datenverarbeitung der Evidenzzentralen als Datenverarbeitung im Auftrag i.S.d. Datenschutzgesetzes (vgl. z.B. § 4 HDSG) zu qualifizieren ist, verfügen die Kreditinstitute als Auftraggeber über personenbezogene (Bezahl-)Daten - wenn nicht, sind die Transaktionsdaten weder für die Evidenzzentrale noch die Kreditinstitute personenbezogen.

Ziff. 13 der Vereinbarung verpflichtet die dem System angeschlossenen Kreditinstitute, zur Gewährleistung der Sicherheit des Systems geeignete Maßnahmen durchzuführen und festzustellen, ob gefälschte oder verfälschte Umsätze eingereicht werden, ob Umsätze mehrfach eingereicht werden, Systemangriffe, wie z.B. Laden von GeldKarten ohne vorhergehende Autorisierung, erfolgen oder unberechtigte Reklamationen vorkommen. Mit diesen Prüfungen müssen die Kreditinstitute eine Börsenevidenzzentrale beauftragen. Als beauftragte Stelle können nur solche Einrichtungen tätig werden, die zu einer Kreditinstitutsgruppe gehören oder von der Kreditwirtschaft getragen werden. Die Börsenevidenzzentrale darf ihre Tätigkeit aufnehmen, wenn sie die im "Technischen Anhang" der Vereinbarung dazu enthaltenen Voraussetzungen erfüllt und dies von den Vertragspartnern der Vereinbarung bestätigt worden ist. Ziff. 15 verweist für die Einzelheiten der von der Börsenevidenzzentrale zu erfüllenden Aufgaben auf den "Technischen Anhang". Die Vereinbarung bestimmt in Ziff. 15 außerdem, daß sich die Börsenevidenzzentrale und die sie beauftragenden Kreditinstitute auf Verrechnungsbanken zu verständigen haben. Der Einzug von GeldKarten-Umsätzen durch die Kreditinstitute der Vertragsunternehmen beim kartenausgebenden Kreditinstitut darf nur über die jeweils

zuständigen Verrechnungsbanken erfolgen. Die eingeschalteten Börsenevidenzzentralen haben sicherzustellen, daß den jeweils zuständigen Börsenevidenzzentralen der kartenausgebenden Institute ein Abgleich zwischen dem Betrag der eingezogenen Lastschrift und der zugrunde liegenden Einzelumsätze möglich ist, indem sie die dafür erforderlichen Daten zur Verfügung stellen.

Die Vereinbarung spricht zwar davon, daß die kartenausgebenden Kreditinstitute die Börsenevidenzzentrale "beauftragen". Damit ist jedoch weder eine zivilrechtliche noch datenschutzrechtliche Festlegung beabsichtigt. Zivilrechtlich dürfte es sich um eine entgeltliche Geschäftsbesorgung handeln. Datenschutzrechtlich stellt sich die Frage, ob die Evidenzzentrale als Auftragnehmer für die kartenausgebenden Kreditinstitute tätig wird oder ob sie eigenständig auf Grund einer Funktionsübertragung tätig wird. Ersteres wäre der Fall, wenn die Evidenzzentrale lediglich als Erfüllungsgehilfe für die kartenausgebenden Institute fungierte, wenn die Leistung nur darin bestünde, für die Erfüllung der Aufgaben und Geschäftszwecke der Kreditinstitute die technische Durchführung der Datenverarbeitung zu übernehmen. Die Evidenzzentrale ist jedoch nicht nur eine Relaisstation im vertraglichen Vollzugsverhältnis zwischen Vertragsunternehmen (Akzeptanzstelle) und kartenausgebendem Kreditinstitut, sondern sie nimmt eine eigenständige Funktion im Zahlungssystem GeldKarte wahr. Sie führt die Sicherheitsüberprüfung der von den Unternehmen zur Verrechnung eingereichten Transaktionen durch und liefert die für die Abwicklung des Zahlungsverkehrs durch die Verrechnungsbanken der jeweiligen Evidenzzentrale erforderlichen Daten. Die Evidenzzentrale wird außerdem bei Reklamationen tätig. Stellt sie fehlerhafte Händlereinreichungen fest, informiert sie über seine Händlerbank den betreffenden Händler und bittet um Klarstellung bzw. Korrektur. Bei defekten Börsenkarten kann über die für das kartenausgebende Kreditinstitut zuständige Evidenzzentrale der Restsaldo der GeldKarte festgestellt werden; nur so ist eine Rückerstattung möglich. Die Aufgabenbeschreibung

macht deutlich, daß die Evidenzzentrale mit der Datenverarbeitung auch eigene Geschäftszwecke verfolgt.

Auftragsdatenverarbeitung setzt außerdem voraus, daß der Auftragnehmer nicht selbständig über die Daten verfügen kann, sondern die Verantwortung für die Rechtmäßigkeit der Datenverarbeitung allein beim Auftraggeber verbleibt. Dies trifft jedoch nach Aussagen des BWS für die Transaktionsdaten nicht zu. Die Kreditinstitute erhalten danach grundsätzlich von der Evidenzzentrale keine Auskunft über diese Daten. Nur in Ausnahmefällen teilt ihnen die Evidenzzentrale den Saldo einer Karte mit.

4.7

Personenbezogene oder anonyme Daten

Das Bundesdatenschutzgesetz definiert in § 3 Abs. 1 personenbezogene Daten als Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren Person. Bestimmt ist die Person, wenn die Einzelangaben mit identifizierenden Daten, z.B. Namen oder Kennziffern, verbunden sind, so daß sich unmittelbar der Bezug zu einer Person herstellen läßt. Für die Bestimmbarkeit kommt es auf das verfügbare Zusatzwissen der speichernden Stelle an. Sie muß die Daten mit den ihr normalerweise zur Verfügung stehenden Mitteln und ohne unverhältnismäßig hohen Aufwand an Zeit, Kosten und Arbeitskraft einer Einzelperson zuordnen können (§ 3 Abs. 7 BDSG). Der Begriff personenbezogenes Datum ist also relativ. Es genügt nicht, daß die Daten mit irgendwo vorhandenen anderen Daten zusammengeführt und damit einer Person zugeordnet werden können, sondern das Zusatzwissen muß der speichernden Stelle zugänglich sein.

Die Evidenzzentrale kann die kartenbezogenen Transaktionsdaten keiner Person zuordnen. Sie benötigt dazu das nur bei dem kartenemittierenden Kreditinstitut vorhandene Zusatzwissen, nämlich Nummer des Girokontos und Kontoinhaber. Zu diesen Informationen hat die Evidenzzentrale jedoch keinen Zugang. Für sie sind die Daten daher nicht personenbezogen, sondern anonym. Umgekehrt kann das Kreditinstitut nur mit dem Zusatzwissen der Evidenzzentrale die mit den ausgegebenen GeldKarten vorgenommenen Transaktionen einzelnen Kunden zuordnen. Außer den Ladevorgängen verfügt das Kreditinstitut ebenfalls über keine personenbezogenen Daten. Selbst im Reklamationsfall erhält das Kreditinstitut keine Daten über Einzeltransaktionen, sondern nur den Saldo. Weder die Evidenzzentralen noch die kartenausgebenden Kreditinstitute können daher das Kaufverhalten der Karteninhaber verfolgen.

4.8

Erfahrungen

Einer meiner Mitarbeiter hat an einem Tag dreimal mit der probeweise eingerichteten GeldKarte bezahlt. In den ersten beiden Geschäften mußte betont werden, mit der GeldKarte bezahlen zu wollen. Dieser Wunsch war offensichtlich so selten, daß das Personal gewohnheitsmäßig mit dem POS-Verfahren abrechnen wollte.

POS

POS steht für Point of Sale, ein bargeldloses Zahlungsverfahren an automatisierten Kassen unter Verwendung der ec-Karte, Bankkundenkarte oder Kreditkarte.

In allen drei Fällen wurden die Beträge und die Bestätigung durch das Kassenpersonal eingegeben. Lediglich im ersten Geschäft

wurde meinem Mitarbeiter das Ergebnis gezeigt. Im zweiten Geschäft mußte der gelbe Zahlungsnachweis ausdrücklich verlangt werden, während er in den beiden anderen Geschäften zusätzlich zum Kassenbon sofort ausgehändigt wurde. Die Zahlungen selbst liefen problemlos ab.

4.9

Fazit und Empfehlungen

Die GeldKarte ist wie Bargeld zur anonymen Bezahlung geeignet - allerdings nur, wenn eine sog. „Weiße Karte“ verwendet wird. Bei einer kontogebundenen GeldKarte (ec-Karte oder Bankkundenkarte) entstehen bei den beteiligten Stellen zwar keine personenbezogenen Daten über das Kaufverhalten des Karteninhabers. Führt man die Daten jedoch zusammen, lassen sich personenbezogene Informationen über die Kartennutzung gewinnen. Die an dem System GeldKarte beteiligten Stellen sind sowohl durch das Bankgeheimnis als auch das Datenschutzrecht daran gehindert, einen solchen Datenabgleich vorzunehmen. Dagegen könnten z.B. Strafverfolgungsbehörden, gestützt auf die Strafprozeßordnung, von einer Evidenzzentrale die Herausgabe der Transaktionsdaten zu einem bestimmten Konto verlangen. Würde bei einem Tatverdächtigen eine Weiße Karte sichergestellt, könnte die Strafverfolgungsbehörde auch in diesem Fall, wie bei einer kontogebundenen Karte, eine Zuordnung der Transaktionen herbeiführen.

Empfehlungen:

- Wer eine "Weiße Karte" wählt, sollte darauf achten, daß das Kreditinstitut keine Notizen über die Zuordnung von Namen und Kartenummer anfertigt. Nur dann ist eine bargeldgleiche anonyme Bezahlung gesichert.

- Beim Bezahlen sollte die Kundin und der Kunde sich den eingetippten Zahlungsbetrag zeigen lassen.
- Die Kundin und der Kunde sollte selbst den Betrag bestätigen und dann die Chipkarte einschieben.
- Die Kundin und der Kunde sollte sich den gelben Zahlungsnachweis geben lassen, soweit dieser gedruckt wird. (Es kann Händlergeräte geben, die keinen Nachweis drucken.)
- Wer sicherstellen will, daß seine Zahlungen in keinem Fall hinsichtlich Datum, Uhrzeit oder Ort nachvollzogen werden können, sollte mit Bargeld zahlen oder eine "Weiße Karte" nutzen.

Meine Kontrollkompetenz beschränkt sich auf die Datenverarbeitung öffentlich-rechtlicher hessischer Stellen. Eine endgültige datenschutzrechtliche Bewertung für das private Kreditgewerbe durch die für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörden steht noch aus.

5. Polizei- und Strafverfolgungsbehörden

5.1

DNA-Dateien

Beim Bundeskriminalamt wurde eine Datei zur Speicherung von DNA-Analysen eingerichtet. Zu Einzelaspekten der gesetzlichen Regelung und der Umsetzung der Regelung habe ich kritisch Stellung genommen.

Die Anforderungen aus Sicht des Datenschutzes an die Speicherung der Ergebnisse von DNA-Analysen hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder schon 1997 in einer Entschließung formuliert (vgl. 26. Tätigkeitsbericht, Ziff. 25.2).

Die wesentlichen Punkte sind:

- Festlegung, für welche Delikte eine solche Speicherung von DNA-Analysen überhaupt in Frage kommt
- Aufnahme der Ergebnisse nur nach einer Prognoseentscheidung über mögliche zukünftige Straftaten der Untersuchten
- Keine Speicherung wenn der Tatverdacht ausgeräumt ist oder keine Speicherung der Ergebnisse von "freiwilligen" Reihenuntersuchungen
- Laufende Überprüfung der Verwendbarkeit der Daten unter dem Gesichtspunkt der Verhältnismäßigkeit.

Im April des Jahres wurde eine solche Datei bereits durch einen Erlaß des Bundesministers des Inneren beim Bundeskriminalamt eingerichtet. Als Rechtsgrundlage wurden die allgemeinen

Regelungen des Bundeskriminalamtgesetzes genannt. Begleitet war dieses Vorgehen von einer sehr streitigen Diskussion. Von verschiedenen Seiten, auch von mir und anderen Datenschutzbeauftragten, wurde geltend gemacht, daß ohne eine ausdrückliche gesetzliche Grundlage eine solche Datei nicht zulässig sei. Daraufhin wurde das DNA-Identitätsfeststellungsgesetz (BGBl. I S. 2646) verabschiedet, das am 11. September 1998 in Kraft getreten ist.

Dieses Gesetz enthält in § 1 eine Ergänzung der Strafprozeßordnung (StPO), unter welchen Voraussetzungen zum Zwecke der Identitätsfeststellung Proben von Blut, Körpergewebe etc. entnommen und analysiert werden dürfen. Für die Verwendung dieser Daten wird auf das Bundeskriminalamtgesetz verwiesen.

§ 81g StPO

(1) Zum Zwecke der Identitätsfeststellung in künftigen Strafverfahren dürfen dem Beschuldigten, der einer Straftat von erheblicher Bedeutung, insbesondere eines Verbrechens, eines Vergehens gegen die sexuelle Selbstbestimmung, einer gefährlichen Körperverletzung, eines Diebstahls in besonders schwerem Fall oder einer Erpressung verdächtig ist, Körperzellen entnommen und zur Feststellung des DNA-Identifizierungsmusters molekulargenetisch untersucht werden, wenn wegen der Art oder Ausführung der Tat, der Persönlichkeit des Beschuldigten oder sonstiger Erkenntnisse Grund zu der Annahme besteht, daß gegen ihn künftig erneut Strafverfahren wegen einer der vorgenannten Straftaten zu führen sind.

...

(3) § 81a Abs. 2 und § 81f gelten entsprechend.

Dieses Gesetz hat erhebliche Mängel. Die Regelungen, die ein ordnungsgemäßes, dem Gefährdungspotential angemessenes Verfahren sicherstellen sollen, sind nicht vollständig. So soll ein

Richter die Entnahme der Probe und die Analyse anordnen, ohne daß auch geregelt wäre, welches Gericht zuständig sein soll. Ferner sind im Gesetz keine Regelungen zu der Frage enthalten, wie mit den Analyseergebnissen umgegangen werden soll, wenn durch die Weiterentwicklung der Analysetechnik mittels der Analysen zusätzliche Informationen über die Betroffenen gewonnen werden können, die für die Identitätsfeststellung nicht erforderlich sind (sog. "Überschußinformationen"). Auch die Frage der Dauer der Speicherung der Analyseergebnisse wird nicht konkret geregelt. Insoweit sollen doch wieder die allgemeinen Regelungen des Bundeskriminalamtgesetzes gelten.

Erhebliche Bedenken habe ich auch gegen § 2 des DNA-Identitätsfeststellungsgesetzes, der die Erfassung sog. "Altfälle" regelt.

§ 2 DNA-Identitätsfeststellungsgesetz

Maßnahmen, die nach § 81g der Strafprozeßordnung zulässig sind, dürfen auch durchgeführt werden, wenn der Betroffene wegen einer der in § 81g Abs. 1 der Strafprozeßordnung genannten Straftaten rechtskräftig verurteilt ... worden ist und die entsprechende Eintragung im Bundeszentralregister oder Erziehungsregister noch nicht getilgt ist.

Damit wird die nachträgliche Erfassung von Personen zu einem Zeitpunkt möglich, zu dem diese ihre Strafe verbüßen oder bereits verbüßt haben. Dies ist mit dem Resozialisierungsgedanken nur schwer vereinbar.

Bei der praktischen Umsetzung der neuen Regelung gibt es erhebliche Schwierigkeiten. Eine Arbeitsgruppe der Justiz- und Innenministerien hat vorläufige Hinweise zur Ausführung dieses Gesetzes erarbeitet, um eine möglichst einheitliche Praxis in den Ländern sicherzustellen.

Da die in § 81g Abs. 1 StPO aufgeführten rechtlichen Voraussetzungen einer Datenerfassung relativ weit formuliert sind, muß bei einem großen Personenkreis nachträglich geprüft werden, ob eine Datenerfassung erfolgen soll. In jedem Einzelfall muß ein Richter überprüfen, ob die gesetzlichen Voraussetzungen tatsächlich vorliegen. Um diese Verfahren zu verkürzen und auch um weniger richterliche Kapazitäten in Anspruch zu nehmen, wurde in der Arbeitsgruppe überlegt, von einer richterlichen Überprüfung abzusehen und statt dessen die Einwilligung der Betroffenen in die Datenerfassung einzuholen.

Ich halte dies für unzulässig. Wenn ein Gesetz Bedingungen für eine Speicherung festlegt und ein gerichtliches Verfahren vorschreibt, um die Einhaltung der rechtlichen Vorgaben sicherzustellen, kann dies nicht durch eine Einwilligung umgangen werden. Durch die Analyse der Proben und die Datenspeicherung wird in das Recht auf informationelle Selbstbestimmung eingegriffen. Dieser Eingriff ist nur deshalb zulässig, weil rechtliche Vorgaben festgelegt wurden, die einen hinreichenden Persönlichkeitsschutz der Betroffenen gewährleisten. Diese Schutzrechte, die durch die Entscheidung des Richters gewährt werden, sind nicht disponibel. Die Betroffenen können durch eine Einwilligung nicht selbst die Prognose treffen, daß sie auch künftig von entsprechenden Ermittlungsverfahren betroffen sein werden.

Fraglich ist auch, ob bei dem betroffenen Personenkreis - insbesondere auch Strafgefangene, die kurz vor der (evtl. auch vorzeitigen) Haftentlassung stehen - tatsächlich von einer Freiwilligkeit der Entscheidung über die Einwilligung ausgegangen werden kann.

Nachdem ich meine Vorbehalte gegen diese Praxis angemeldet hatte, hat sich das Justizministerium entschlossen, davon Abstand zu nehmen. Auch in der Arbeitsgruppe konnte keine Mehrheit der

Bundesländer für einen Verzicht auf die richterliche Überprüfung erzielt werden.

5.2

HSOG-Novelle

Auch in Hessen werden einzelne Regelungen des Polizeirechts verschärft. Meine Kritikpunkte wurden nur zum Teil berücksichtigt.

Im Zuge der Einführung des Großen Lauschangriffs wurden in Art. 13 Grundgesetz (GG) Regelungen geschaffen, die es notwendig machten, die im Hessischen Gesetz über die Öffentliche Sicherheit und Ordnung (HSOG) enthaltenen Vorschriften zur Überwachung von Wohnungen im Rahmen der Gefahrenabwehr den verfassungsrechtlichen Vorgaben anzupassen. Dies wurde zum Anlaß genommen, auch andere Ergänzungen des HSOG vorzusehen, die mit Erfordernissen der polizeilichen Praxis begründet wurden.

5.2.1

Wohnraumüberwachung

Die Regelungen des § 15 HSOG zum Einsatz technischer Mittel in Wohnungen wurden an die Anforderungen des Art. 13 GG angepaßt. Dazu gehören die richterliche Anordnung der Maßnahmen und die richterliche Entscheidung über die Rechtmäßigkeit von Maßnahmen zur Eigensicherung, wenn die daraus erlangten Informationen anderweitig zur Gefahrenabwehr oder zu Strafverfolgungszwecken verwertet werden sollen. Schließlich wird es zukünftig jährlich eine Unterrichtung des Landtages über den Einsatz technischer Mittel in Wohnungen geben.

5.2.2

Verdachtsunabhängige Kontrollen

Gleichzeitig wurde bei der Vorbereitung der Novelle zunächst diskutiert, auch in Hessen die sog. Schleierfahndung, d.h. verdachtsunabhängige Kontrollen, einzuführen. Begründet wurde dies mit Hinweisen auf die Zunahme grenzüberschreitender Kriminalität und den Wegfall der Binnengrenzen. Diese Überlegungen haben zu einer sehr streitigen öffentlichen Debatte geführt. Auch ich habe gegen die Einführung der sog. Schleierfahndung rechtsstaatliche Bedenken geltend gemacht. Schleierfahndung bedeutet, daß alle Bürgerinnen und Bürger jederzeit damit rechnen müssen, in eine Ausweiskontrolle zu geraten, ohne daß die Polizei auf Grund bestimmter Verdachtsmomente tätig wird.

Verdachtsunabhängige Fahndung ist stets mit einem Eingriff in die Freiheitsrechte der Bürgerinnen und Bürger verbunden, der nicht nur - wie im Falle von Autobahnsperren - zu erheblichen Beschränkungen der Bewegungsfreiheit führen kann, sondern auch das Recht auf informationelle Selbstbestimmung verletzt.

Es ist ein Wesensmerkmal des Rechtsstaates, daß die Bürgerinnen und Bürger, solange sie sich nicht in eine konkrete Verdachts- oder Gefahrenlage begeben, von Sicherheitsbehörden unbehelligt bleiben. Vom Polizeistaat unterscheidet sich der Rechtsstaat gerade dadurch, daß nicht bereits die allgemeine Gefahr, daß "immer und überall" mit Kriminalität zu rechnen ist, eine Überwachung und Kontrolle rechtfertigt. An diesem Prinzip kann auch festgehalten werden, wenn eine (auch lückenlose) Personenkontrolle an bestimmten Örtlichkeiten oder bei bestimmten Ereignissen, bei denen nach kriminalistischer Erfahrung mit schweren Straftaten zu rechnen ist, zugelassen werden muß.

Soweit die Schleierfahndung auf die Besonderheiten der grenzüberschreitenden Kriminalität abzielen sollte, war auf den Unterschied zwischen den Bundesländern mit Außengrenzen und den Ländern wie Hessen hinzuweisen, in denen dieses Kriterium keinen Sinn ergibt.

Die Novelle des Hessischen Gesetzes über die Sicherheit und Ordnung enthält dementsprechend auch keine allgemeine Ermächtigung mehr, auf allen Verkehrswegen Personenkontrollstellen zu errichten.

5.2.3

Kontrollstellen

Statt der Einführung der Schleierfahndung wurde die Möglichkeit, Kontrollstellen gem. § 18 Abs. 2 Nr. 5 HSOG einzurichten, erweitert:

§ 18 Abs. 2 HSOG

Die Polizeibehörden können die Identität einer Person feststellen, wenn

...

5. die Person an einer Kontrollstelle angetroffen wird, die von der Polizeibehörde auf öffentlichen Straßen oder Plätzen oder an anderen öffentlich zugänglichen Orten eingerichtet worden ist, um eine der in § 100a der Strafprozeßordnung bezeichneten Straftaten oder eine Straftat nach § 27 des Versammlungsgesetzes zu verhüten.

Allgemeine Personenkontrollstellen sind nur dann zu rechtfertigen, wenn besondere Gefahrenlagen bestehen. Ich habe mich nicht dagegen gewandt, für diese Fälle die gesetzlichen Voraussetzungen

für Kontrollstellen der Polizei den Erfordernissen einer zeitgemäßen Gefahrenabwehr anzupassen.

Hierbei ist für die einzelne Maßnahme der Polizei zumindest noch ein Anknüpfungspunkt zu einem konkreten Ereignis vorhanden, auch wenn bei ihr ebenfalls eine Fülle von sich rechtmäßig verhaltenden Bürgerinnen und Bürgern betroffen sein können.

Allerdings halte ich die gewählte Methode der Verweisung auf die Strafprozeßordnung (StPO) nicht für besonders geglückt. Diese hat zur Folge, daß bei einer Änderung der Strafprozeßordnung durch den Bundesgesetzgeber auch die Länderregelung gleichsam automatisch mit geändert wird, ohne daß eine Überprüfung durch den Landesgesetzgeber erfolgen kann.

5.2.4

Vorsorge zur Verfolgung künftiger Straftaten

Bedenken habe ich auch gegen die Erweiterung des § 1 HSOG, der Aufgabenbeschreibung der Gefahrenabwehr- und Polizeibehörden, geäußert. Damit wird jetzt auch in Hessen neben der Verhütung von zu erwartenden Straftaten die Vorsorge zur Verfolgung künftiger Straftaten als vorbeugende Bekämpfung von Straftaten definiert. Begründet wird dies mit dem Vorentwurf zur Änderung des Musterentwurfes eines einheitlichen Polizeigesetzes aus dem Jahre 1986. Den dort enthaltenen Vorschlägen war man in Hessen bei der letzten umfassenden Novellierung des HSOG bewußt nicht gefolgt (vgl. 22. Tätigkeitsbericht, Ziff. 4.2). Wie sich auch bei der Änderung des § 20 Abs. 4 HSOG zeigt (vgl. Ziff. 5.2.5), scheinen sich auch in Hessen die Prämissen des Polizeirechts zu wandeln. Die zunehmende Vermischung zwischen der Gefahrenabwehr als Aufgabe des landesrechtlich zu regelnden Polizeirechts einerseits und den zur bundesrechtlichen Regelungskompetenz gehörenden Aufgaben der Strafverfolgung andererseits führt zu unlösbaren Schwierigkeiten bei den Eingriffskompetenzen auch in das Recht

auf informationelle Selbstbestimmung. Bei der Übernahme von mißverständlichen Formulierungen aus dem Musterentwurf hätte ich zumindest eine Klarstellung in der Gesetzesbegründung erwartet, daß die grundsätzliche Funktionstrennung zwischen Prävention und Repression auch und gerade im Hinblick auf die Verarbeitung personenbezogener Daten nicht aufgehoben werden darf.

5.2.5

Datenspeicherung durch die Polizei

Eine wesentliche Änderung erfährt schließlich § 20 Abs. 4 HSOG. Bisher war die weitere Speicherung von Daten nach Abschluß des Ermittlungsverfahrens von einer Prognoseentscheidung abhängig.

§ 20 Abs. 4 HSOG (alte Fassung)

Die Polizeibehörden können, soweit Bestimmungen der Strafprozeßordnung oder andere gesetzliche Regelungen nicht entgegenstehen, personenbezogene Daten, die sie im Rahmen von strafrechtlichen Ermittlungsverfahren gewonnen haben,

...

2. in automatisierten Dateien nur speichern, verändern oder sonst verwenden, soweit es sich um Daten von Personen handelt, die verdächtig sind, eine Straftat begangen zu haben, wenn die Besorgnis der Begehung weiterer Straftaten besteht.

Auf Grund dieser Regelung gab es einige Verwaltungsgerichtsentscheidungen, die im Einzelfall eine Speicherung für unzulässig erklärt haben, da eine Prognose, die betreffende Person könne wieder straffällig werden, nicht gestellt werden konnte.

Diese Regelung wurde jetzt völlig umgestaltet.

§ 20 Abs. 4 HSOG

Die Polizeibehörden können, soweit Bestimmungen der Strafprozeßordnung oder andere gesetzliche Regelungen nicht entgegenstehen, personenbezogene Daten, die sie im Rahmen der Verfolgung von Straftaten gewonnen haben, zur Abwehr einer Gefahr oder zur vorbeugenden Bekämpfung von Straftaten speichern, verändern oder sonst verwenden. Die Speicherung, Veränderung oder sonstige Verwendung in automatisierten Dateien ist nur zulässig, soweit es sich um Daten von Personen handelt, die verdächtig sind eine Straftat begangen zu haben; entfällt der Verdacht sind die Daten zu löschen.

Zur Begründung wurde angeführt: „Die polizeiliche Aufgabenerfüllung erfordert jedoch die Speicherung personenbezogener Daten auch solcher Personen, bei denen das Ermittlungsverfahren zwar eingestellt worden ist, der Tatverdacht jedoch nicht ausgeräumt werden konnte; die Speicherung dient der Vorsorge für die künftige Verfolgung einer solchen Straftat. Auf die Besorgnis der Begehung weiterer Straftaten kommt es nicht an. § 20 Abs. 4 muß daher so gefaßt werden, daß die Verwendung personenbezogener Daten in automatisierten Dateien zulässig ist, solange der Verdacht besteht, die Person könnte eine Straftat begangen haben.“ (LTDrucks. 14/4017 S. 8)

Mir erscheint es nicht mit dem Recht auf informationelle Selbstbestimmung vereinbar, daß in allen Fällen, in denen der ursprüngliche Tatverdacht nicht durch einen ausdrücklichen Freispruch entfällt, gleichsam automatisch eine (weitere) Speicherung erfolgt. Entscheidungen der Verwaltungsgerichte, die Speicherungen bei Verfahrenseinstellungen gem. §§ 170 Abs. 2 oder 153 ff. StPO oder bei fehlender Prognose zukünftiger Straftaten als unzulässig einzustufen, gehen zu Recht davon aus, daß es sich bei solchen Speicherungen um erhebliche Eingriffe in

die Rechte der Betroffenen handelt. Durch die jetzt vorgenommene Änderung entfällt die Prognoseentscheidung völlig. Dies ist ein unverhältnismäßiger Eingriff. Diese Speicherung dient der Verfolgung zukünftiger Straftaten. Selbst wenn im aktuellen Fall ein Tatverdacht nicht völlig ausgeräumt ist, ist ohne konkrete Anhaltspunkte nicht davon auszugehen, daß diese Person auch zukünftig in Erscheinung treten wird. Es kann im übrigen nicht im Ermessen der Polizei stehen, ob noch ein Tatverdacht besteht, unabhängig von den Wertungen durch die Justiz.

Die neue hessische Vorschrift geht auch über alle vergleichbaren Regelungen hinaus. Das Bundeskriminalamtsgesetz verlangt z.B., daß Grund zu der Annahme besteht, daß Strafverfahren gegen den Beschuldigten oder Tatverdächtigen zu führen sind.

Meine Stellungnahme dazu, auch im Rahmen der Beratungen im zuständigen Landtagsausschuß, konnten leider keine Änderungen bewirken. Für die Zukunft wird sorgfältig zu beobachten sein, nach welchen Kriterien in Einzelfall entschieden wird, ob der Verdacht, eine Straftat begangen zu haben, entfallen ist und die Daten zu löschen sind.

5.3

INPOL-neu

Eine Arbeitsgruppe der Datenschutzbeauftragten begleitet die Arbeit der mit der Überarbeitung des INPOL-Systems befaßten Projektgruppe der Polizei.

Das Bundeskriminalamt führt als Zentralstelle das bundesweite Informationssystem der Polizei (INPOL). Seit mehreren Jahren erarbeitet eine von der Polizei eingesetzte Projektgruppe ein neues Konzept für dieses System, INPOL-neu. Grund sind sowohl die veränderten technischen Rahmenbedingungen als auch die sich

verändernden polizeifachlichen Anforderungen an ein solches Informationssystem. Schon in meinem 22. Tätigkeitsbericht (Ziff. 4.4) hatte ich die aus Sicht des Datenschutzes notwendigen Rahmenbedingungen für dieses Projekt dargestellt.

Mit der Novellierung des Bundeskriminalamtgesetzes (BKAG) im Jahre 1997 sind konkretere Regelungen für die Verarbeitung personenbezogener Daten in das Gesetz aufgenommen worden. Die datenschutzrechtlichen Vorgaben für INPOL-neu sind jedoch im wesentlichen unverändert geblieben.

Die Verfolgung und die vorbeugende Bekämpfung von Straftaten sind grundsätzlich Aufgabe der Bundesländer. Also muß auch die Verantwortung für die Zulässigkeit, Richtigkeit und Dauer der Speicherung der Daten im INPOL-System bei den Ländern als denjenigen, die die Daten ins System einstellen, verbleiben. Die bereichsspezifischen Regelungen zur Datenverarbeitung der Polizei in der Strafprozeßordnung und in den Ländergesetzen dürfen nicht unterlaufen werden. Insbesondere dürfen die unterschiedlichen Regelungen zu Erhebungsmethoden (z.B. Einsatz technischer Mittel, Einsatz verdeckter Ermittler) und Verwendungsbeschränkungen (z.B. Katalogtaten) nicht ausgehöhlt werden.

Die Beurteilung dessen, was die Projektgruppe erarbeitet, ist nicht immer einfach. Dies liegt nicht zuletzt daran, daß INPOL-neu in der derzeit vorgesehenen Form als Rahmen entwickelt wird, der durch fachliche Entscheidungen über die konkrete Nutzung und Ausgestaltung ergänzt werden muß.

Die konkrete Nutzung des Systems soll in weiten Teilen auch weiterhin in der Verantwortung der angeschlossenen Nutzer bleiben. Die derzeitige Entwicklung von INPOL-neu bezieht sich nur auf die beim Bundeskriminalamt stattfindende Datenverarbeitung. Entscheidend bleibt aber auch weiterhin, was

auf der anderen Seite der Schnittstelle zu den Landessystemen passiert. Da es offensichtlich Schwierigkeiten gibt, das Zusammenwirken der einzelnen Landessysteme mit INPOL-neu (rechtzeitig) zu realisieren, gibt es nunmehr auch Überlegungen, zusammen mit INPOL-neu eine Musterschnittstelle zu entwickeln, die dann den Ländern für die eigene Arbeit zur Verfügung gestellt werden kann.

Dieser nicht immer einfache Weg der Entwicklung bedingt es aber auch, daß derzeit keine umfassende Stellungnahme zu diesem System aus Sicht des Datenschutzes abgegeben werden kann. Daher hat der Arbeitskreis Sicherheit der Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Arbeitsgruppe eingesetzt, die die Arbeit der Projektgruppe der Polizei begleitet. Diese Vorgehensweise ermöglicht es einerseits, auch kurzfristig zu einzelnen Aspekten Stellung zu nehmen. Sie erleichtert andererseits die Entwicklung des Verfahrens, da schon während des laufenden Entstehungsprozesses auf die Entwicklung Einfluß genommen werden kann. Dadurch wird auch verhindert, daß eine nachträgliche Beurteilung durch die Datenschutzbeauftragten aufwendige Änderungen des Systems verursachen. Bis jetzt wurde vor allem zu den im folgenden beschriebenen Teilaspekten Stellung genommen.

5.3.1

Kriterien für die Speicherung in INPOL

In INPOL dürfen nach den Vorgaben des § 2 BKAG nur solche Daten erfaßt werden, die im Rahmen der Prävention und der Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung erforderlich sind.

§ 2 BKAG

- (1) Das Bundeskriminalamt unterstützt als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei die Polizeien des Bundes und der Länder bei der Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung.
- (2) Das Bundeskriminalamt hat zur Wahrung dieser Aufgabe
 1. alle hierfür erforderlichen Informationen zu sammeln und auszuwerten, ...

In der Projektgruppe INPOL-neu gab es Überlegungen, die bisherige Funktion des Kriminalaktennachweises (KAN) zu erweitern.

KAN

Der Kriminalaktennachweis dient dem Nachweis von Kriminalakten, die bei den Polizeibehörden des Bundes und der Länder zu Beschuldigten oder sonst Tatverdächtigen angelegt sind. Damit ermöglicht er eine dezentrale Auskunft, bei welchen Polizeidienststellen Kriminalakten über eine Person geführt werden. Er enthält neben den Personalien Eintragungen über Fundstellen zu Kriminalakten.

Zukünftig sollten die vorhandenen Informationen zum einen erweitert werden um Fallgrunddaten, d.h. alle fachlich erforderlichen Informationen zu einem polizeilichen Sachverhalt. Zum anderen sollten - mindestens dann, wenn es zu einer Person Eintragungen in INPOL gibt – alle anderen Ermittlungsverfahren, unabhängig von der dem Verfahren zugrundeliegenden Tat, ebenfalls in INPOL gespeichert werden. Damit stellt der KAN nicht mehr nur wie bisher einen Verweis auf die Akten zu INPOL-relevanten Straftaten sicher, sondern er enthält Basisinformationen zu allen Ermittlungsverfahren gegen einen Straftäter, der (auch) INPOL-relevante Straftaten begangen hat.

Diesem Konzept hat die Arbeitsgruppe der Datenschutzbeauftragten widersprochen. Die Konzeption einer Fallkurzauskunft, die die gesamten zu einer Person gespeicherten Fälle enthält, unabhängig von ihrer bundesweiten Bedeutung, ist mit den gesetzlichen Regelungen nicht vereinbar. Die Speicherung einer Straftat in INPOL-neu setzt gem. § 2 Abs. 1 BKAG voraus, daß die Straftat von überörtlicher oder erheblicher Bedeutung ist.

5.3.2

Protokollierung

Zwischen dem Bundesinnenministerium einerseits und den Datenschutzbeauftragten und dem Bundeskriminalamt andererseits ist umstritten, in welchem Umfang Zugriffe der Polizeibehörden auf das Informationssystem zu protokollieren sind.

Dabei geht es darum, ob § 11 Abs. 6 BKAG nur einen Mindestumfang der Protokollierung festschreibt.

§ 11 Abs. 6 Satz 1 BKAG

Werden beim Bundeskriminalamt Daten abgerufen, hat es bei durchschnittlich jedem zehnten Abruf für Zwecke der Datenschutzkontrolle den Zeitpunkt, die Angaben, die die Feststellung der aufgerufenen Datensätze ermöglichen, sowie die für den Abruf verantwortliche Dienststelle zu protokollieren.

Nach meiner - vom Bundeskriminalamt geteilten - Auffassung schließt diese Regelung eine häufigere Protokollierung nicht aus. Es ist wünschenswert, daß sämtliche Abrufe personenbezogener Daten vollständig protokolliert werden. Nur eine vollständige Protokollierung macht im Konfliktfall eine Datenschutzkontrolle aussagekräftig. Sonst ist nicht ausgeschlossen, daß unberechtigte

Zugriffe unentdeckt bleiben. Bei einer Teilprotokollierung kann nie geklärt werden, ob es einen unberechtigten Zugriff nicht gegeben hat oder ob er nur nicht protokolliert worden ist.

In diesem Zusammenhang ist im übrigen darauf hinzuweisen, daß eine sinnvolle Protokollierung über die Feststellung, von welchem Terminal auf den Datensatz zugegriffen wurde, hinausgehen muß. Einen echten Aussagewert haben Protokolldaten nur, wenn auch klar ist, welcher Mitarbeiter auf diesen Datensatz zugegriffen hat.

Die Nutzung der INPOL-Protokolldaten hat sich grundsätzlich auf die in § 11 Abs. 6 Satz 2 BKAG genannten Zwecke – die datenschutzrechtliche Kontrolle und die Sicherstellung eines ordnungsgemäßen Betriebes der Datenverarbeitungsanlage - zu beschränken. Die im Gesetz darüber hinaus unter bestimmten Voraussetzungen zugelassene Nutzung der Protokolldaten für kriminalpolizeiliche Belange birgt Gefahren in sich, denen durch flankierende Maßnahmen entgegenzutreten ist. Solche Maßnahmen sind besondere Aufzeichnungspflichten und Genehmigungsvorbehalte sowie eine zeitnahe Unterrichtung des Bundesbeauftragten für den Datenschutz.

Darüber hinaus ist vom System automatisiert, also unabhängig von einer Einzelfallentscheidung, jede Verwendung der Protokolldaten aufzuzeichnen.

5.3.3

Anzuwendendes Recht für Speicherungen von Länderpolizeien in INPOL-Verbunddateien

Das Bundeskriminalamt hat die Funktion einer Zentralstelle, die die für ihre Aufgaben erforderlichen Daten sammelt und auswertet. Das Polizeirecht, das festlegt, welche Daten die einzelnen Polizeibehörden erheben und dann auch weiter übermitteln dürfen,

bleibt Landesrecht. Das hat zur Folge, daß die Rechtsgrundlagen für die Verarbeitung personenbezogener Daten durch die Polizei und damit auch der Umfang der Erhebungsbefugnisse unterschiedlich sind.

Im Rahmen der Errichtung verschiedener Dateien beim Bundeskriminalamt hat das Bundesinnenministerium die Rechtsauffassung vertreten, daß auf Grund der Zentralstellenfunktion des Bundeskriminalamts für die rechtliche Beurteilung der Speicherungen allein das Bundeskriminalamtsgesetz maßgeblich ist, und zwar nicht nur für die Beurteilung der rechtlichen Zulässigkeit der Speicherung der Daten in INPOL, sondern auch für die Beurteilung der rechtlichen Zulässigkeit der Erhebung der Daten in den Ländern.

Diese Auffassung des Bundesministeriums des Innern ist unzutreffend. Die Beschreibung der Zentralstellenfunktion des Bundeskriminalamts stellt keine Erhebungsnorm für die Polizei dar. Dies wird auch an anderer Stelle des Bundeskriminalamtsgesetzes bestätigt. So legt zum Beispiel § 12 Abs. 2 BKAG konsequenterweise fest, daß die Verantwortung für die bei der Zentralstelle gespeicherten Daten, namentlich für die Rechtmäßigkeit der Erhebung, bei den Stellen liegt, die die Daten unmittelbar eingeben.

§ 12 Abs. 2 BKAG

Im Rahmen des polizeilichen Informationssystems obliegt die datenschutzrechtliche Verantwortung für die bei der Zentralstelle gespeicherten Daten, namentlich für die Rechtmäßigkeit der Erhebung, die Zulässigkeit der Eingabe sowie die Richtigkeit oder Aktualität der Daten, den Stellen, die die Daten unmittelbar eingeben. Die verantwortliche Stelle muß feststellbar sein. Die Verantwortung für die Zulässigkeit des Abrufs im automatisierten Verfahren trägt der Empfänger.

Eine andere Regelung wäre nach der Kompetenzverteilung des Grundgesetzes auch gar nicht zulässig.

5.4

Schutz privater Rechte

Zum Schutz privater Rechte ist es in bestimmten Situationen zulässig, daß die Polizei personenbezogene Daten an private Dritte weitergibt. Der Routinefall ist die polizeiliche Unterstützung des Personaliaustauschs beim Verkehrsunfall. Die datenschutzrechtlichen Belange der Betroffenen werden durch detaillierte Regelungen gesichert. Verschiedene Einzelfälle waren für mich Anlaß, auf die Notwendigkeit der Beachtung dieser Regelungen hinzuweisen.

5.4.1

Der Parkverstoß

Nachdem die Garagenausfahrt eines Metzgermeisters zugeparkt war und er sich ein Taxi nehmen mußte, beschimpfte dessen Frau die Ehegattin des Falschparkers. Dieser wiederum beschwerte sich bei mir wegen der Übermittlung seiner Adresse an den Geschäftsinhaber durch die Polizei.

Die Polizei führte in der von mir erbetenen Stellungnahme aus, sie sei von dem Metzger um Hilfe gebeten worden, weil er mit seinem Fahrzeug seine Garage nicht verlassen konnte. Sie habe sich von diesem Zustand überzeugt und eine Ordnungswidrigkeitenanzeige gefertigt. Zu diesem Zweck habe sie bei der Kraftfahrzeug-Zulassungsstelle des Landkreises die Daten des Halters des falsch parkenden Fahrzeuges abgefragt. Diese Datenübermittlung ist nach § 35 Abs. 1 Nr. 3 des Straßenverkehrsgesetzes (StVG) zulässig. Der Polizei steht dafür ein automatisiertes Direktabrufverfahren zur

Verfügung. Der Direktabruf war durch die Regelung des § 36 Abs. 2 StVG zugelassen.

§ 36 Abs. 2 StVG

Die Übermittlung nach § 35 Abs. 1 Nr. 1 bis 4 aus dem Zentralen Fahrzeugregister darf durch Abruf im automatisierten Verfahren erfolgen

1. an die Polizeien des Bundes und der Länder sowie an den Zoll, soweit er grenzpolizeiliche Aufgaben wahrnimmt,
 - a) zur Kontrolle, ob die Fahrzeuge einschließlich ihrer Ladung und die Fahrzeugpapiere vorschriftsmäßig sind,
 - b) zur Verfolgung von Ordnungswidrigkeiten nach § 24 oder 24a,
 - c) zur Verfolgung von Straftaten oder zur Vollstreckung oder zum Vollzug von Strafen oder
 - d) zur Abwehr von Gefahren für die öffentliche Sicherheit ...
und
2. an die Zollfahndungsstellen zur Verfolgung von Steuer- und Wirtschaftsstraftaten.

Satz 1 gilt entsprechend für den Abruf der örtlich zuständigen Polizeidienststellen der Länder aus den örtlichen Fahrzeugregistern.

Durch das verbotswidrige Parken vor der Garagenausfahrt wurde aber auch die Privatsphäre des Garagenbesitzers beeinträchtigt. Denn ihm entstanden wegen der Benutzung eines Taxis Kosten, die er zivilrechtlich gegenüber dem Verursacher geltend machen konnte. Er bat daher - mit Erfolg - die Polizei um die Personalien des Falschparkers. Zur Rechtmäßigkeit der Datenübermittlung an den Geschädigten berief sich die Polizei auf die Regelung des § 23 Abs. 1 Nr. 3 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG).

§ 23 HSOG

(1) Die Gefahrenabwehr- und Polizeibehörden können personenbezogene Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs übermitteln, soweit dies zur

1. Erfüllung gefahrenabwehrbehördlicher oder polizeilicher Aufgaben,
2. Verhütung oder Beseitigung erheblicher Nachteile für das Gemeinwohl oder
3. Verhütung oder Beseitigung einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist.

(2) § 22 Abs. 2 Satz 2 und Abs. 4 gilt entsprechend.

(3) Der Empfänger ist darauf hinzuweisen, daß die übermittelten Daten nur zu dem Zweck verwendet werden dürfen, zu dessen Erfüllung sie ihm übermittelt wurden. Die Prüfung der Zulässigkeit der Übermittlung obliegt der übermittelnden Behörde.

(4) Über die Übermittlungen ist ein besonderes Verzeichnis zu führen, aus dem der Zweck der Übermittlung, der Empfänger und die Aktenfundstelle hervorgehen. Es ist am Ende des Kalenderjahres, das dem Jahr seiner Erstellung folgt, zu vernichten.

Der Verweis in Absatz 2 bedeutet, daß die Betroffenen über die Datenübermittlung zu informieren sind, sobald der Zweck der Übermittlung dem nicht mehr entgegensteht.

Die Bewertung, daß in diesem Fall die Datenübermittlung an den Geschädigten zur Verhütung oder Beseitigung einer schwerwiegenden Beeinträchtigung seiner Rechte erforderlich war, kann in Frage gestellt werden. Der Geschädigte hätte gem. § 39 Abs. 1 StVG unmittelbar von der Kraftfahrzeug-Zulassungsstelle Auskunft erhalten können. Allerdings war die Polizei im Zuge ihrer Bearbeitung der Ordnungswidrigkeit rechtmäßig in den Besitz der

Information über den Fahrzeughalter gekommen. Es gab einen unmittelbaren Sachzusammenhang zwischen der Ordnungswidrigkeit und dem privaten Recht. Die Polizei konnte in dieser Situation sehr gut beurteilen, inwieweit das Informationsinteresse auch tatsächlich begründet war. Nur sehr schwer wäre die recht bürokratisch erscheinende Verweigerung der Auskunft und der Verweis an die Kraftfahrzeug-Zulassungsstelle verständlich zu machen gewesen. Ich habe dem Petenten mitgeteilt, daß ich die Übermittlung seiner Daten als noch mit § 23 Abs. 1 HSOG vereinbar ansehe.

5.4.2

Das Hausverbot

Ein Bürger aus Kassel bat mich zu folgendem Geschehen um Hilfe: Als er in einem Lebensmittelmarkt zwei gerade gekaufte Dosen Bier eingepackt habe, habe ihm ein Mitarbeiter eines privaten Sicherheitsdienstes unterstellt, alkoholisiert zu sein, ihm ein Hausverbot ausgesprochen und ihn aufgefordert, sich auszuweisen. Als er sich geweigert habe und das Gebäude verlassen wollte, sei er von zwei Bediensteten des Sicherheitsdienstes gewaltsam daran gehindert worden. Als dann zwei per Handy herbeigerufene Polizeibeamte das Verlangen des privaten Sicherheitsdienstes unterstützten, habe er den Polizeibeamten seinen Ausweis gegeben. Seine Daten seien von dem Sicherheitsdienst aufgenommen worden. Dann durfte er die Einkaufspassage verlassen.

Der Betroffene fragte mich, ob die Weitergabe seiner von der Polizei erhobenen Daten an den privaten Sicherheitsdienst zulässig war. Ich bat das Polizeipräsidium Kassel um eine Stellungnahme. Der Kasseler Polizeipräsident zitierte in seiner Stellungnahme die sog. "Taschenkontroll-Entscheidung" des Bundesgerichtshofes (BGHZ 124, 39). Nach dieser Entscheidung gestattet der Inhaber bei Öffnung eines Ladengeschäftes für den allgemeinen

Publikumsverkehr generell und unter Verzicht auf eine Prüfung im Einzelfall allen Kunden den Zutritt zu seinem Geschäft, die sich im Rahmen des "üblichen Käuferverhaltens" bewegen. Hieran ist er gebunden und kann das Hausrecht nur noch gegenüber solchen Kunden ausüben, die die Grenzen dieser allgemeinen Zulassung überschreiten und den Betriebsablauf stören.

Es sei daher davon auszugehen, daß - solange keine individuelle Zugangskontrolle (wie z. B. bei Diskotheken) erfolgt - ein willkürliches und diskriminierendes Hausverbot unwirksam ist. Daraus folge, daß die Polizei in diesen Fällen eine Identitätsfeststellung weder aus dem Aspekt der Verfolgung einer vermeintlichen Straftat noch zum Schutz privater Rechte (§ 1 Abs. 3 HSOG) vornehmen dürfe.

Soweit herbeigerufenen Beamten jedoch glaubhaft gemacht werde, daß ein wirksames, d.h. nicht willkürliches, sondern sachlich begründetes Hausverbot ausgesprochen wurde, die betreffende Person sich jedoch nicht daran gehalten habe, so erscheine eine Identitätsfeststellung und Personalienweitergabe auf Grund des § 1 Abs. 3 HSOG zur Durchsetzung des Hausrechts erforderlich. Leider sei das Geschehen in seiner Behörde nicht mehr nachvollziehbar. Sollte die Darstellung des Petenten uneingeschränkt zutreffen, so entbehrte die von seinen Beamten vorgenommene Personalienfeststellung und -weitergabe einer rechtlichen Grundlage. Unter dieser Prämisse wurde das Vorgehen der Beamten ausdrücklich bedauert - so der Polizeipräsident Kassel.

§ 1 Abs. 3 HSOG legt fest, wann die Polizei die Aufgabe hat, private Rechte zu schützen.

§ 1 Abs. 3 HSOG

Der Schutz privater Rechte obliegt den Gefahrenabwehr- und den Polizeibehörden nach diesem Gesetz nur dann, wenn gerichtlicher Schutz nicht rechtzeitig zu erlangen ist und wenn ohne gefahrenabwehrbehördliche oder polizeiliche Hilfe die Verwirklichung des Rechts vereitelt oder wesentlich erschwert werden würde.

Bei einem unrechtmäßig ausgesprochenen Hausverbot braucht (muß) die Polizei erst gar nicht tätig werden. Will (oder muß) sie aber tätig werden und will sie dann auch personenbezogene Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs übermitteln, reicht die Aufgabenzuweisung des § 1 Abs. 3 HSOG als Rechtsgrundlage jedoch nicht aus. Rechtsgrundlage für die Verarbeitung personenbezogener Daten kann nur die Befugnisnorm des § 23 HSOG (s.o.) sein.

Dies festzustellen war mir deshalb wichtig, weil § 23 HSOG eine Reihe datenschutzrechtlicher Kautelen enthält. U. a. ist der Empfänger darauf hinzuweisen, daß er die Daten nur zweckgebunden verwenden darf (Abs. 3). Der Betroffene ist von der Datenübermittlung zu informieren (Abs. 2). Außerdem muß ein Verzeichnis (Abs. 4) über solche Datenübermittlungen geführt werden. Wäre § 23 HSOG von den Polizeibeamten umgesetzt worden, so wäre die Schilderung des Betroffenen nachvollziehbar gewesen. Da dies nicht der Fall war, mußte ich annehmen, daß § 23 HSOG bislang nicht oder zumindest nicht ausreichend Beachtung fand. Ich bat den Kasseler Polizeipräsidenten entsprechende Vorkehrungen organisatorischer Art zu treffen.

Er teilte mir mit, daß auf Grund meines Schreibens alle Beamten im Wege des Dienstunterrichts über die rechtliche Beurteilung und die Voraussetzungen von Personalienfeststellungen zur Durchsetzung von Hausverboten geschult wurden. Alle Beamten wurden angehalten, der Hinweispflicht auf die Zweckbindung nachzukommen und auch besonders auf die Information der

Betroffenen zu achten. Auch der Dokumentationspflicht wurde durch Anordnung nachgekommen, die übermittelten Personalien, den Empfänger sowie den Zweck der Datenweitergabe künftig im polizeilichen Tätigkeitsbuch einzutragen. Ergänzend dazu erschien in einem internen Mitteilungsblatt der Behörde ein Aufsatz zu diesem Thema. Damit ist weitgehend sichergestellt, daß in künftigen Fällen die datenschutzrechtlichen Belange der Betroffenen ausreichend berücksichtigt werden. Den betroffenen Bürger habe ich entsprechend informiert.

5.4.3

Der nachträglich aufgenommene Verkehrsunfall

Eine Frau aus Bruchköbel schilderte mir einen Bagatellunfall, bei dem sie sich am Unfallort mit der anderen Beteiligten verständigt habe, daß kein Schaden entstanden sei. Die Polizei sei nicht gerufen worden. Zwei Tage später habe sich die andere Frau nun doch mit Schadensersatzansprüchen an sie gewandt. Das 2. Polizeirevier Hanau habe ihr auf telefonische Anfrage mitgeteilt, daß keine Anzeige gegen sie vorliege und Auskünfte über Kraftfahrzeug-Halter an private Dritte nicht erteilt würden. Die Betroffene bat mich, zu überprüfen, wie die andere am Unfall beteiligte Frau ihre Daten erhalten hatte.

Ich habe zunächst bei der Kraftfahrzeug-Zulassungsstelle des Main-Kinzig-Kreises festgestellt, daß eine Auskunft an eine Privatperson über das Kraftfahrzeug-Kennzeichen nicht registriert war. Dann bat ich das Kraftfahrt-Bundesamt Flensburg um Auswertung der Protokolldaten über die Abfragen im Zentralen Verkehrsregister (ZEVIS), dem bundesweiten Kraftfahrzeug-Zulassungsregister. Es stellte fest, daß unter dem entsprechenden Kraftfahrzeug-Kennzeichen eine Abfrage stattfand. Die Datenabfrage konnte einem Terminal der Polizeidirektion Hanau - 2. Polizeirevier - zugeordnet werden.

Da nach der Angabe der Betroffenen die Polizei den Unfall gar nicht aufgenommen hatte, bat ich die Polizeidirektion Hanau um Stellungnahme, ob es einen dienstlichen Anlaß zu der Abfrage gab und auf Grund welcher Rechtsgrundlage eventuelle Datenübermittlungen stattfanden. Die Polizei verfügte zwar noch über die Adresse der Auskunftsempfängerin, doch sah sie sich offenbar nicht in der Lage, meine Fragen zu beantworten. Doch statt mir dieses mitzuteilen, forderte sie nun - ca. ein halbes Jahr nach dem Geschehen - die andere Unfallbeteiligte auf, den Unfallhergang darzustellen. Die von dieser jetzt angefertigte Beschreibung des Unfallhergangs legte für den zuständigen Polizeibeamten den Verdacht des unerlaubten Entfernen vom Unfallort durch die andere Beteiligte nahe. Er legte der Staatsanwaltschaft eine Strafanzeige vor. Zu meinen Fragen teilte mir die Polizeidirektion mit, die Datenübermittlung an die Unfallbeteiligte sei zulässig gewesen, weil sie ein berechtigtes Interesse an den Informationen glaubhaft gemacht habe, außerdem sei eine vereinfachte Unfallaufnahme erfolgt und die "Unfallaufnahmeleitlinien" (StAnz. 1996 S. 211) sähen die Datenweitergabe vor.

Letzteres trifft zwar zu, doch stimmte diese Darstellung nicht mit dem mir zu diesem Zeitpunkt bekannten Geschehensablauf überein. Ich bat daher die Polizei um Vorlage des Tagebuchauszuges über die erste Vorsprache der Unfallbeteiligten und um eine Kopie der Unfallaufnahme. Von dem Tagebuchauszug hatte ich mir durch entsprechende chronologische Eintragungen zu anderen Sachverhalten kurz vor und nach der in Rede stehenden Datenübermittlung versprochen, ich könne die Annahme der Betroffenen, die Grundlagen der polizeilichen Maßnahmen seien erst im nachhinein geschaffen worden (wie die Aussage), widerlegen. Die Unfallaufnahme hätte wenigstens dargelegt, daß die Datenabfrage nicht ausschließlich zum Zwecke der Weitergabe an die Anfragerin erfolgte. Beide Schriftstücke wurden mir nicht

vorgelegt bzw. nachgereicht. Statt dessen erhielt ich ein Exemplar der Unfallaufnahme, die erst ca. ein halbes Jahr später angefertigt wurde, sowie einer "Protokollierung einer Datenübermittlung nach § 23 Abs. 4 HSOG ..." und eines Unterrichtungsschreibens an die Betroffene nach § 23 Abs. 2 HSOG. Diese Unterlagen enthielten aber zahlreiche Mängel. So war das Protokoll nicht unterzeichnet, es enthielt keine Tagebuchnummer und entgegen § 23 Abs. 4 HSOG keinen Hinweis auf die Aktenfundstelle; außerdem war der Empfänger falsch bzw. unleserlich bezeichnet. Das Unterrichtungsschreiben war nicht korrekt adressiert, enthielt eine unvollständige Anrede, von den im Vordruck alternierend zu streichenden Rechtsgrundlagen war keine gestrichen bzw. als zutreffend gekennzeichnet, der Empfänger war falsch angegeben und das an anderer Stelle anzugebende Zitat einer Rechtsgrundlage (§ 1 Abs. 3 HSOG) begründete nicht die Rechtmäßigkeit der Datenübermittlung, sondern machte gerade Zweifel daran deutlich. Insgesamt fiel es auf Grund der Form und der sehr schlechten Lesbarkeit des handschriftlich ausgefertigten Schriftstückes schwer, anzunehmen, es handle sich um die Durchschrift eines Briefes einer Behörde an einen Bürger. Jedenfalls war die Angabe der Betroffenen, das Unterrichtungsschreiben nicht erhalten zu haben, angesichts der Auffälligkeiten nicht von vornherein unglaubwürdig. Entsprechendes gilt für die Angabe, damals telefonisch vom 2. Polizeirevier die Auskunft erhalten zu haben, von dort würden keine Daten an Dritte übermittelt.

Die Rechtmäßigkeit der Datenabfrage und -weitergabe konnte ich letztlich nicht klären, da ich nicht feststellen konnte, ob eine - auch nur vereinfachte - Unfallaufnahme überhaupt stattgefunden hatte. Erfolgte die Datenabfrage ausschließlich zum Zwecke der Weitergabe der Daten, war sie zweckwidrig und damit unzulässig. Wünscht ein Bürger eine Auskunft über Kraftfahrzeug-Inhaber und wendet er sich dazu an die Polizei, so ist er grundsätzlich an die zuständige Behörde, d.h. die örtlich zuständige Straßenverkehrszulassungsstelle, zu verweisen. Sie erteilt

Auskünfte über ihre Daten. Sie - nicht die Polizei - beurteilt, ob die Voraussetzungen des § 39 StVG vorliegen, demzufolge Privaten im Einzelfall Auskunft über Kraftfahrzeug-Halter erteilt werden darf.

Die Betroffene - wie auch das Hessische Innenministerium und die Polizeidirektion Hanau - habe ich informiert. Denn sie sah sich plötzlich der strafrechtlichen Verfolgung ausgesetzt. Das Hessische Innenministerium hat mir mitgeteilt, daß es meine Rechtsauffassung hinsichtlich der Abfrage von Daten über Kraftfahrzeug-Inhaber beim Zentralen Verkehrsinformationssystem (ZEVIS) durch Polizeibehörden und die Weitergabe der Daten zur Sicherung privater Rechte teilt. Die Polizeidirektion Hanau hat den Vorfall zum Anlaß genommen, die Zulässigkeit von ZEVIS-Abfragen im Rahmen der dienstlichen Fortbildung zu thematisieren. Damit ist zumindest künftig weitgehend sichergestellt, daß Datenabfragen nur für die im Gesetz genannten Zwecke stattfinden.

6. Justiz und Strafvollstreckung

6.1

Datenverarbeitung bei der Justiz

Die zunehmende Automatisierung auch im Bereich der Justiz macht ausreichende gesetzliche Grundlagen für den Umgang mit personenbezogenen Daten dringend erforderlich.

In allen Bereichen der Justiz - bei Staatsanwaltschaften, Gerichten und Gerichtsvollziehern - werden im Zuge von Modernisierungsvorhaben umfassende Systeme automatisierter Datenverarbeitung eingeführt mit der Folge, daß sensible personenbezogene Daten auch hier in viel stärkerem Maße verfügbar werden als bisher. Sogar die Beauftragung Privater mit der Verarbeitung sensibler Justizdaten wird teilweise erwogen. Gerade vor dem Hintergrund dieser vollkommen neuen Qualität der Datenverarbeitung in der Justiz wird deutlich, daß die Rechtsprechung des Bundesverfassungsgerichtes zum sog. "Übergangsbonus" - derzufolge für eine nicht näher definierte Frist Eingriffe in das Recht auf informationelle Selbstbestimmung auch ohne ausdrückliche gesetzliche Grundlage erfolgen dürfen, soweit dies zur staatlichen Aufgabenerfüllung zwingend notwendig ist - keine tragfähige Grundlage mehr darstellen kann. Vielmehr müssen die Entscheidungen des Gesetzgebers den Maßstab für die weitere technische Ausgestaltung der Datenverarbeitung innerhalb der Justiz bilden und nicht umgekehrt. Dabei ist nicht nur für formell ausreichende Rechtsgrundlagen Sorge zu tragen. Auch Fragen der Datensicherheit und der Ordnungsmäßigkeit der Datenverarbeitung bedürfen der Regelung.

Diese Problematik war Anlaß für die 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, sich mit diesen Themen zu beschäftigen und mehrere Entschlüsse zu verabschieden.

6.1.1

Bereichsspezifische Rechtsgrundlagen für alle Bereiche der Justiz

Die 56. Konferenz fand kurz nach Beginn der neuen Legislaturperiode statt. Anknüpfend an Entschlieungen der letzten Jahre hat die Konferenz den Gesetzgeber auf die Defizite im Bereich der Rechtsgrundlagen fur die Datenverarbeitung der Justiz hingewiesen. Gefordert werden u.a. in Anknpfung an die Entschlieung zum StVAG 96 (26. Tatigkeitsbericht Ziff. 25.1) Regelungen fur das Strafverfahren, zur Untersuchungshaft, Forschung usw. (vgl. Ziff. 26.3).

6.1.2

Prufungskompetenz der Datenschutzbeauftragten bei den Gerichten

Diese Entschlieung greift ein Thema nochmals auf, das ich schon im letzten Jahr dargestellt habe (vgl. 26. Tatigkeitsbericht Ziff. 6.4). In den Datenschutzgesetzen der einzelnen Bundeslander sind die Abgrenzungen zum Kontrollbereich soweit die richterliche Unabhangigkeit betroffen ist, unterschiedlich formuliert. Einige Kollegen haben wiederholt berichtet, da sie zum Teil erhebliche Schwierigkeiten haben, ihren Kontrollaufgaben im Bereich der Justiz nachzukommen, da von Seiten der Justiz der Bereich der richterlichen Unabhangigkeit hufig sehr weit ausgelegt wird. Um diese Schwierigkeiten einzuschranken, regt die Entschlieung eine einheitliche Formulierung fur die Abgrenzung an (vgl. Ziff. 26.8). Eine entsprechende nderung des HDSG hatte auch ich in das Gesetzgebungsverfahren eingebracht, diese wurde auch vom Landtag ubernommen.

§ 24 Abs. 1 S. 3 HDSG

Die Gerichte unterliegen der Kontrolle des Hessischen Datenschutzbeauftragten, soweit sie nicht in richterlicher Unabhängigkeit tätig werden.

Diese Neuformulierung ist hilfreich, da mit ihr m.E. deutlicher wird, daß nur ein kleiner Teil der Justiz von meiner Kontrolle ausgenommen ist. In den letzten Jahren hatte ich gelegentlich den Eindruck, daß meine grundsätzliche Zuständigkeit für die Gerichte nicht bekannt ist und ich deshalb bei Automatisierungsvorhaben einzelner Gerichte nicht beteiligt werde. Dies dürfte auf das Mißverständnis zurückzuführen sein, daß der gesamte Justizbereich sich mit Rücksicht auf die richterliche Unabhängigkeit einer Kontrolle von außen entzieht. Daß dies nicht richtig ist, weil die Staatsanwaltschaft und die gesamte Justizverwaltung davon nicht betroffen sind, konnte zwar in allen Fällen, in denen ich von mir aus Prüfungen vornahm, geklärt werden. Die jetzt erfolgte gesetzliche Klarstellung dürfte aber dazu beitragen, daß das Justizpersonal auch und auf eigene Initiative häufiger als bisher eine Abstimmung mit mir sucht.

6.1.3

Entwicklungen im Sicherheitsbereich

In den letzten Jahren sind zum Teil erhebliche neue Eingriffsbefugnisse für die Sicherheitsbehörden, d.h. Polizei und Staatsanwaltschaften, aber auch die Nachrichtendienste geschaffen worden, von der Ausdehnung des Kataloges, der eine Telefonüberwachung begründen kann, über die Möglichkeiten des Bundesnachrichtendienstes, den Telekommunikationsverkehr mit dem Ausland abzuhören, sowie die Rechte der Strafverfolgungsbehörden auf Auskünfte gegenüber Betreibern von Telekommunikationsanlagen bis zuletzt zum sog. "großen

Lauschangriff". Dabei war oft zu beobachten, daß Erfahrungen mit neuen Eingriffsmöglichkeiten selten abgewartet, in der Regel auch gar nicht ausgewertet wurden, bevor neue Instrumente mit erheblicher Eingriffsintensität entwickelt wurden. Ich habe auch in der Vergangenheit schon auf diese Problematik hingewiesen, etwa im Zusammenhang mit vermehrten Eingriffen in das Fernmeldegeheimnis (vgl. 25. Tätigkeitsbericht Ziff. 14.2).

Die 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat den Gesetzgeber dazu aufgefordert, diese Eingriffsbefugnisse einer Evaluierung zu unterziehen und ggf. die gesetzlichen Grundlagen zu überarbeiten. Die Evaluierung kann sich dabei sowohl auf die Notwendigkeit der Eingriffsbefugnisse, z.B. bei der Schleppnetzfahndung, als auch auf den Umfang der auf der Grundlage der Eingriffsbefugnisse vorgenommenen Erhebung personenbezogener Daten, wie z.B. bei der Telefonüberwachung, beziehen (vgl. Ziff. 26.5).

6.2

Strafvollzug - Weihnachtspaketmarken

Wer seinem in einer Justizvollzugsanstalt einsitzenden Angehörigen zu Weihnachten ein Paket schicken will, muß den Postbediensteten nicht offenbaren, daß der Adressat im Gefängnis sitzt.

Ein Insasse einer Justizvollzugsanstalt hat mich gebeten, auf die Leitung der Strafanstalt dahingehend einzuwirken, daß die dort verwendeten Paketmarken nicht mehr ausgehändigt werden. Die Paketmarken enthielten neben dem Landeswappen und einer Nummer den Aufdruck

JUSTIZVOLLZUGSANSTALT

Butzbach

Weihnachtspaketmarke

1997

Durch die Verpflichtung, die Paketmarke aufzubringen, seien seine in einer ländlichen Gegend wohnenden Familienangehörigen gehalten, den Postbediensteten, denen sie teilweise persönlich bekannt sind, zu offenbaren, daß der Adressat in einer Justizvollzugsanstalt einsitzt. Dies sei für seine Angehörigen unzumutbar.

Rechtsgrundlage der Verwendung von Paketmarken ist § 33 Abs. 1 des Strafvollzugsgesetzes (StVollzG). Näheres dazu regelt noch eine Verwaltungsvorschrift zu § 33 StVollzG.

§ 33 Abs. 1 StVollzG

Der Gefangene darf dreimal jährlich in angemessenen Abständen ein Paket mit Nahrungs- und Genußmittel empfangen. Die Vollzugsbehörde kann Zeitpunkt und Höchstmengen für die Sendung und für einzelne Gegenstände festsetzen...

Verwaltungsvorschrift zu § 33 StVollzG (JMBl. 1986 S. 987)

1. Der Empfang eines Paketes ist zugelassen zu Weihnachten, zu Ostern und zu einem von dem Gefangenen zu wählenden weiteren Zeitpunkt (z.B. Geburtstag)...
4. ... Die Verwendung einer von der Anstalt ausgegebenen Paketmarke kann vorgeschrieben werden.

Die zitierten Bestimmungen stellen allerdings im Sinne des Datenschutzrechtes keine ausreichende Rechtsgrundlage dar, um die Angehörigen zu dem ausdrücklichen Hinweis auf das Einsitzen des Paketempfängers in der Justizvollzugsanstalt zu verpflichten.

Ich habe das Justizministerium um Stellungnahme gebeten und gleichzeitig angeregt, nicht nur die Weihnachts-, sondern alle Paketmarken und nicht nur die Justizvollzugsanstalt Butzbach, sondern alle Justizvollzugsanstalten in eine vorzunehmende Korrektur einzubeziehen.

Das Justizministerium hat daraufhin veranlaßt, daß die Paketmarken mit dem erwähnten Aufdruck eingezogen und durch neutrale Paketmarken ersetzt wurden. Damit ist für einen Außenstehenden nicht mehr ersichtlich, daß der Adressat in einer Justizvollzugsanstalt einsitzt. Die Angehörigen können das Paket ohne den ausdrücklichen Hinweis auf die Justizvollzugsanstalt, z.B. unter Angabe der Postfachadresse des Gefängnisses, adressieren.

Eine Umfrage des Justizministeriums in allen anderen Justizvollzugsanstalten des Landes hat ergeben, daß in keiner Anstalt Paketmarken verwendet werden, aus denen ersichtlich ist, daß der Adressat in einer Justizvollzugsanstalt einsitzt.

Damit wurde dem Anliegen des Gefangenen aus datenschutzrechtlicher Sicht Rechnung getragen.

6.3

Staatsanwaltschaften - Das Verfahren MESTA

Das länderübergreifende automatisierte Verfahren MESTA enthält vielfältige Elemente eines datenschutzfreundlichen Verfahrens, die aber noch genutzt bzw. eingesetzt werden müssen. MESTA würde auch den automatisierten Austausch personenbezogener Daten zwischen den verschiedenen hessischen Staatsanwaltschaften ermöglichen. Hierfür fehlt derzeit die Rechtsgrundlage.

Das Projekt MESTA (Mehrländer-Staatsanwaltschafts-Automation) hatten die Länder Brandenburg, Hamburg und

Schleswig-Holstein beschlossen und die Datenzentrale Schleswig-Holstein mit der Programmentwicklung beauftragt. Das Land Hessen ist dem Vertrag beigetreten. MESTA soll zu einer Vereinfachung und Verkürzung der Verfahrensabläufe in den Staatsanwaltschaften beitragen. Es handelt sich also um ein Vorgangsbearbeitungs- und Vorgangsverwaltungssystem, das speziell auf die Anforderungen von Staatsanwaltschaften zugeschnitten ist. Kernpunkt ist eine komfortable Schriftguterstellung, in der einmal erfaßte Daten zu verschiedenen Zwecken, von der Registratur eines Neueingangs bis zum Abschluß des Vollstreckungsverfahrens, unterschiedlich aufbereitet werden können. So liegen z.B. ca. 80 Vordrucke bereit, die automatisch mit Falldaten gefüllt werden können. Alle innerbehördlichen Funktionseinheiten sollen - soweit erforderlich - auf die Daten zugreifen dürfen. Bislang notwendige Aktentransporte fallen weg. Schnittstellen erlauben die Kommunikationsbeziehungen zu externen Partnern wie z. B. dem Bundeszentralregister in Berlin oder dem Verkehrszentralregister in Flensburg.

Aus der Sicht des Datenschutzes ist gegen die Einführung eines Datenverarbeitungsverfahrens, das den Justizbehörden zu einer zeitgemäßen Büroausstattung verhilft, nichts einzuwenden. Die neuen Systeme können vielfach auch die Umsetzung der datenschutzrechtlichen Vorgaben erleichtern. So ist es z.B. technisch kein Problem mehr, differenzierte Zugriffsrechte vorzusehen und umfassende und einfach auszuwertende Protokolle anzufertigen. Bei der Inanspruchnahme offener Netze können Verschlüsselungsmaßnahmen den Datenschutz sicherstellen.

Seit Januar 1998 wird das Verfahren MESTA bei der Staatsanwaltschaft bei dem Landgericht Fulda getestet. Weitere Pilotanwender sind die Staatsanwaltschaften in Limburg und Gießen. Ich habe mir bei der Staatsanwaltschaft bei dem Landgericht Fulda den Testeinsatz angesehen. Dabei habe ich mich davon überzeugt, daß das Verfahren ein sehr fein untergliedertes

Zugriffsschutzsystem technisch ermöglicht. Allerdings fehlte zum damaligen Zeitpunkt noch das Konzept, nach welchen Kriterien den einzelnen Nutzern Befugnisse eingeräumt werden. Zum Umfang der Protokollierung war noch keine abschließende Entscheidung getroffen. Vor einem flächendeckenden Einsatz des Verfahrens müssen dazu noch Festlegungen erfolgen.

MESTA ermöglicht auch den automatisierten Informationsaustausch der hessischen Staatsanwaltschaften untereinander. Hierfür bedarf es einer konkreten bereichsspezifischen Regelung (s. Ziff. 26.3). Zwar sah der Entwurf des Strafverfahrensänderungsgesetzes 1996 eine Regelung vor, derzeit ist aber der Zeitpunkt der dringend notwendigen Novellierung der Strafprozeßordnung nicht abzusehen (vgl. dazu auch Ziff. 6.1). Wenn diese Funktion von MESTA zeitnah genutzt werden soll, muß die Landesregierung entscheiden, ob dazu eine eigene landesgesetzliche Regelung ergehen soll - etwa wie sie in Schleswig-Holstein durch das Gesetz über die staatsanwaltschaftlichen Verfahrensregister vom 9. Januar 1996 geschaffen wurde.

7. Gesundheit

7.1

Krebsregister für Hessen

Der Hessische Landtag hat 1998 ein Gesetz zur Ausführung des Krebsregistergesetzes verabschiedet. Die von mir geforderten datenschutzrechtlichen Verbesserungen sind in das Gesetz aufgenommen worden.

7.1.1

Das Krebsregistergesetz des Bundes von 1994

1995 ist das Bundeskrebsregistergesetz (KRG, BGBl. S. 3351) in Kraft getreten, in dem die Länder verpflichtet werden, bis zum 1. Januar 1999 flächendeckende Krebsregister einzurichten mit dem Ziel fortlaufender einheitlicher Erhebung von Daten über das Auftreten von Krebserkrankungen. Dem Gesetz sind jahrelange kontroverse Diskussionen vorausgegangen, die insbesondere innerhalb der Ärzteschaft umstrittene fachliche Aspekte, kompetenzrechtliche sowie datenschutzrechtliche Aspekte zum Gegenstand hatten. Was die datenschutzrechtlichen Aspekte angeht, so ist die Frage von zentraler Bedeutung, unter welchen gesetzlichen Voraussetzungen der Arzt (bzw. Zahnarzt) zur Meldung von Patientendaten über Krebserkrankungen an das Krebsregister berechtigt ist und in welchem Umfang personenbezogene Daten im Register verarbeitet werden. Die Patientendaten unterliegen der ärztlichen Schweigepflicht i.S.v. § 203 Strafgesetzbuch (StGB). Der Arzt darf sie Dritten nur befugt offenbaren. Die Meldung der Patientendaten an das Krebsregister ist auch ein Eingriff in das verfassungsrechtlich gewährleistete Recht der Patienten auf informationelle Selbstbestimmung. Der Rechtsprechung des Bundesverfassungsgerichts zufolge sind Einschränkungen dieses Rechts u.a. nur dann zulässig, wenn der Gesetzgeber den Grundsatz der Verhältnismäßigkeit beachtet.

Konkret bedeutet dies im vorliegenden Zusammenhang vor allem, daß die Verarbeitung der personenbezogenen Patientendaten für den angestrebten Zweck geeignet und notwendig sein muß und es keine Alternative geben darf, die für die Patienten weniger belastend ist.

Dem 1994 verabschiedeten Krebsregistergesetz des Bundes liegt ein insbesondere von Prof. Michaelis vom Universitätsklinikum Mainz konzipiertes und u.a. mit den Datenschutzbeauftragten weiterentwickeltes sog. Treuhandmodell zugrunde, das eine neue Form des Ausgleichs zwischen den Forschungsinteressen und dem Recht auf informationelle Selbstbestimmung der betroffenen Patientinnen und Patienten vorsieht. Kernpunkte des Modells sind die folgenden:

- Personenbezogene Daten dürfen vom Arzt an das Register (Vertrauensstelle) ohne Einwilligung des Patienten gemeldet werden. Der Patient ist aber von der beabsichtigten Meldung zu unterrichten und kann der Meldung widersprechen. Unter bestimmten Voraussetzungen kann eine Unterrichtung des Patienten zunächst unterbleiben.
- Die Verarbeitung personenbezogener Daten im Krebsregister und die Gefahr eines Mißbrauchs der Daten wird durch die Aufteilung auf zwei räumlich, organisatorisch und personell selbständige Stellen des Krebsregisters (Vertrauensstelle und Registerstelle) und eine Verschlüsselung der Identitätsdaten des Patienten auf ein Minimum reduziert. Der Arzt meldet die personenbezogenen Daten an die Vertrauensstelle. Die Daten werden aufgeteilt in die den Patienten identifizierenden Daten (Name, Anschrift, Geburtsdatum etc.) und die epidemiologischen Daten (Beruf, Tumordiagnose, Art der Therapie etc.). Die Vertrauensstelle verschlüsselt die Identitätsdaten. Die verschlüsselten Identitätsdaten und die epidemiologischen Daten werden zusammen mit einer

gemeinsamen Kontrollnummer sowie den Angaben zu den meldenden Ärzten an die Registerstelle übermittelt. Auf diese Weise können nachfolgende Meldungen zu demselben Patienten den vorhergehenden Meldungen zugeordnet werden. Die Registerstelle speichert die verschlüsselten Identitätsdaten und die epidemiologischen Daten dauerhaft. Die Registerstelle selbst kann keinen Personenbezug der Daten wiederherstellen. Bei der Vertrauensstelle werden unverzüglich nach der abschließenden Bearbeitung der Daten durch die Registerstelle, spätestens jedoch drei Monate nach Übermittlung, alle zu dem betreffenden Patienten gehörenden Daten gelöscht und die der Meldung zugrunde liegenden Unterlagen vernichtet. Eine Entschlüsselung der Identitätsdaten ist im Einzelfall durch die Vertrauensstelle für Maßnahmen des Gesundheitsschutzes und für wichtige, im öffentlichen Interesse stehende Forschungsaufgaben zulässig. Eine Weitergabe personenbezogener Patientendaten vom Register an externe Stellen (z.B. Forschungsinstitute) ist nur mit Einwilligung der Patienten möglich.

- Personenbezogene Daten dürfen vom Arzt an das Register (Vertrauensstelle) ohne Einwilligung des Patienten gemeldet werden. Der Patient ist aber von der beabsichtigten Meldung zu unterrichten und kann der Meldung widersprechen. Unter bestimmten Voraussetzungen kann eine Unterrichtung des Patienten zunächst unterbleiben.

Das Krebsregistergesetz sieht ein Melderecht für den Arzt vor, nicht jedoch eine Meldepflicht. In die Rechte von Ärzten wird daher durch das Krebsregistergesetz nicht eingegriffen. Die Meldungen erfolgen auf freiwilliger Basis.

Das Krebsregistergesetz des Bundes eröffnet den Ländern die Möglichkeit, zu bestimmten konkret aufgeführten Fragen abweichende Regelungen zu treffen, soweit die Vergleichbarkeit

der registrierten Daten gewahrt bleibt. Diese Möglichkeiten sind auch von den Ländern in unterschiedlichem Ausmaß genutzt worden.

7.1.2

Das hessische Ausführungsgesetz

Das hessische Ausführungsgesetz sieht vor, daß die Vertrauensstelle in Hessen bei der Landesärztekammer eingerichtet wird, die Registerstelle beim Regierungspräsidium Darmstadt. Die Aufgaben der Entschlüsselungsstelle soll der Hessische Datenschutzbeauftragte wahrnehmen, ebenso soll der Hessische Datenschutzbeauftragte in bestimmten Fällen (z.B. bei einer Praxisaufgabe) die Referenzlisten der Ärzte aufbewahren.

Gegenstand datenschutzrechtlicher Diskussionen waren in Hessen 1998 insbesondere die folgenden Punkte:

7.1.2.1

Meldepflicht statt Melderecht der Ärztinnen und Ärzte

Im hessischen Gesetz ist – ebenso wie in einigen anderen Landesgesetzen – abweichend vom Bundeskrebsregistergesetz nicht nur ein Melderecht, sondern eine Meldepflicht für die Ärzte vorgesehen. Hierzu habe ich eine eingehende Begründung gefordert. Zwar ist mir bekannt, daß Krebsregister eine hohe Meldevollständigkeit aufweisen müssen, damit valide Forschungsergebnisse erzielt werden können, es ist jedoch keineswegs selbstverständlich, daß durch die Einführung einer Meldepflicht eine höhere Meldevollständigkeit erreicht werden kann. Die derzeit bestehenden Meldepflichten werden in weiten Teilen in der Praxis nur sehr fragmentarisch umgesetzt. Andererseits gibt es eine Reihe von Empfehlungen für Meldungen,

die auf freiwilliger Basis wirksam umgesetzt werden. Die Landesregierung hat daraufhin ihre Gründe ausführlicher dargelegt:

"Die Meldepflicht ist erforderlich, um eine ausreichend hohe Erfassungsquote der tatsächlichen Erkrankungen zu erreichen. Für die wissenschaftliche Anerkennung als epidemiologisches Krebsregister ist nach internationalen Standards eine Meldevollständigkeit von mindestens 90 v.H. aller Erkrankungsfälle erforderlich. Eine Begrenzung auf ein Melderecht würde diesem Erfordernis kaum entsprechen, denn bei einer Informationsverpflichtung gegenüber den Patientinnen und Patienten bei namentlicher Meldung verbessert die Meldepflicht die Rechtfertigungsposition der Meldenden ebenso wie bei anonymer Meldung und erhöht somit ihre Bereitschaft zur Meldung. Gleichzeitig stärkt die Meldepflicht, auch ohne ausdrückliche Sanktionierung, die Position des Registerpersonals bei Rückfragen an die Meldenden, wodurch die Vollständigkeit der Datensätze ebenfalls erhöht wird. Wichtig ist es, daß den Meldepflichtigen die Meldepflicht als in ihrem Interesse liegend vermittelt wird. In den Ländern Mecklenburg-Vorpommern, Sachsen und Schleswig-Holstein gilt für Ärzte ebenfalls eine Meldepflicht, in den übrigen Ländern ein Melderecht."

Diese Begründung habe ich aus datenschutzrechtlicher Sicht als ausreichend angesehen.

7.1.2.2

Ausgestaltung der codierten Meldungen

Das hessische Gesetz unterscheidet zwischen namentlicher Meldung (einschließlich Familienname, Vorname, Postleitzahl, Straße und Hausnummer) und codierter Meldung an das Register. Eine namentliche Meldung an das Register darf nur erfolgen, wenn die Patientin bzw. der Patient von der vorgesehenen Meldung

unterrichtet wurde und nicht widersprochen hat. Hat der Patient einer namentlichen Meldung widersprochen oder ist er über die beabsichtigte Meldung nicht unterrichtet worden (z.B. weil er aus gesundheitlichen Gründen über seine Krebserkrankung noch nicht aufgeklärt wurde), so ist der Arzt ausschließlich zu einer codierten Meldung berechtigt und verpflichtet. Diese Ausgestaltung des Patientenrechts ist aus datenschutzrechtlicher Sicht grundsätzlich angemessen. Eine namentliche Meldung aller Patientendaten soll nicht gegen den Willen des Betroffenen und auch nicht „an dem Betroffenen vorbei“ erfolgen, d.h., ohne daß er die Möglichkeit hat, seinen gegenteiligen Willen zum Ausdruck zu bringen.

Andererseits kann durch die Verpflichtung der Ärzte zu codierten Meldungen eine gewisse Vollständigkeit des Datenbestandes im Register erreicht werden.

Allerdings enthielt der Entwurf zunächst eine Verwendung des Begriffs Anonymisierung, die nicht im Einklang mit der allgemeinen datenschutzrechtlichen Diskussion steht. § 3 Abs. 7 BDSG enthält eine gesetzliche Definition des Anonymisierens.

Anonymisieren ist das Verändern personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmaren natürlichen Person zugeordnet werden können.

Die im Entwurf zunächst vorgesehene, als „anonym“ bezeichnete Meldung sollte die folgenden Daten enthalten:

- sechstelliger Namenscode
- Geschlecht
- fünfstellige Postleitzahl der Anschrift zum Zeitpunkt des Auftretens der bösartigen Neubildung und Referenznummer
- vollständiges Geburtsdatum
- Datum der ersten Tumordiagnose

- Sterbedatum

Dieser Datensatz ist auf Grund meiner Stellungnahme reduziert worden. Auch die neue Fassung des Datensatzes war jedoch noch so umfassend, daß eine Reidentifizierung der Betroffenen nicht ausgeschlossen werden konnte. Ich habe daher vorgeschlagen, daß der Datensatz noch weiter reduziert wird oder - wenn dies aus fachlicher Sicht zu problematisch ist - auf die Verwendung des Begriffs „Anonymisierung“ in dem Gesetz verzichtet und statt dessen z.B. der Begriff „codierte Meldung“ verwendet wird. Dies ist insbesondere auch deshalb wichtig, weil die Anforderungen an eine hinreichende Anonymisierung häufig Gegenstand datenschutzrechtlicher Diskussionen sind, z.B. bei einzelnen Forschungsprojekten, und eine problematische Verwendung dieses Begriffs im Gesetz als Präjudiz für eine entsprechende problematische Verwendung dieses Begriffs auch in anderen Bereichen verstanden werden könnte. Auf Grund meines Vorschlags wird jetzt im Gesetz die Bezeichnung „codierte Meldung“ verwendet.

7.1.2.3

Speicherung von Gauß-Krüger-Koordinaten in der Registerstelle

Im hessischen Entwurf war zunächst eine Erweiterung der im Krebsregistergesetz aufgeführten, vom Arzt zu meldenden epidemiologischen Daten enthalten, die u.a. die folgenden Angaben umfaßte:

epidemiologisch notwendige Angaben zum Wohnort nach Gauß-Krüger-Koordinaten, auf Grund derer jedoch nicht die Anschrift feststellbar sein darf.

Diese Erweiterung des Datenkatalogs wurde als erforderlich angesehen, um diejenigen Faktoren zu identifizieren, die an der

Entstehung bösartiger Neubildungen beteiligt sind. Argumentiert wurde, daß in der Registerstelle oder in anderen Forschungseinrichtungen auch kleinräumige Auswertungen vorgenommen werden können, um die hypothetische Wirkung bestimmter Noxen zu überprüfen. Das Bedürfnis nach kleinräumigen Auswertungen im Einzelfall war für mich grundsätzlich nachvollziehbar. Die vorgesehene Regelung stand jedoch nicht im Einklang mit der datenschutzrechtlichen Konzeption des Krebsregisters, insbesondere damit, daß die Registerstelle keine unverschlüsselten Identitätsdaten erhalten und weiterverarbeiten darf. Mit den Angaben zum Wohnort mit Gauß-Krüger-Koordinaten, die eine Genauigkeit von 30 bis 60 m haben sollten und den weiteren zur Meldung vorgesehenen epidemiologischen Daten wäre in vielen Fällen die Anschrift feststellbar bzw. der Betroffene identifizierbar gewesen. Wenn in die bei der Registerstelle gespeicherten epidemiologische Daten Angaben aufgenommen worden wären, die eine Reidentifizierung der Betroffenen ohne großen Aufwand ermöglicht hätten, so hätte dies insgesamt die Konzeption einer getrennten Vertrauens- und Registerstelle mit jeweils anderen Datenbeständen und Aufgaben in Frage gestellt. Zwar sah der Entwurf vor, daß durch die Angaben die Anschrift nicht feststellbar sein darf. Mir war jedoch nicht nachvollziehbar, in welchem Verfahren dies verhindert werden könnte. Dieser Punkt erwies sich auch in verschiedenen Gesprächen als nicht klärbar. Im Gesetz ist nunmehr festgelegt, daß die Vertrauensstelle eine einheitliche Übertragung der Anschriften der namentlichen Meldungen in punktgenaue Gauß-Krüger-Koordinaten vornehmen soll, die dann ebenso wie die übrigen Identitätsdaten zu verschlüsseln sind und erst in verschlüsselter Form an die Registerstelle übermittelt werden. Damit ist meinen Bedenken Rechnung getragen und die grundsätzliche Konzeption des Registers aufrechterhalten worden.

7.1.3

Zur Umsetzung des hessischen Ausführungsgesetzes

Das hessische Gesetz sieht vor, daß die Registerstelle beim Regierungspräsidium Darmstadt eingerichtet wird. Das Regierungspräsidium Darmstadt verarbeitet allerdings derzeit eine Vielzahl personenbezogener Daten für die ihm zugewiesenen vielfältigen Aufgaben. Es muß daher sichergestellt werden, daß die Daten der Registerstelle ausschließlich zweckgebunden für die Aufgaben der Registerstelle verwendet werden und der Datenbestand hinreichend von den sonstigen Aufgabenbereichen des Regierungspräsidiums abgeschottet wird. Andernfalls wäre mit den umfangreichen personenbezogenen Daten des Regierungspräsidiums möglicherweise doch eine Reidentifizierung der Betroffenen möglich. Auch bei der Einrichtung der Vertrauensstelle bei der Landesärztekammer sind datenschutzrechtliche Aspekte zu beachten. Die für die Zwecke des Krebsregisters verarbeiteten personenbezogenen Daten dürfen nicht für andere Aufgaben der Landesärztekammer verwendet werden. Ich werde die Umsetzung des Gesetzes aus datenschutzrechtlicher Perspektive weiterverfolgen.

7.2

Umsetzung des Psychotherapeutengesetzes

Das neue Psychotherapeutengesetz schreibt vor, daß die Approbation und Kassenzulassung beantragende Psychologinnen und Psychologen Nachweise über ihre bisherige berufliche Tätigkeit vorlegen müssen. Meiner Forderung, ein Verfahren zu entwickeln, das die Rechte der betroffenen Patientinnen und Patienten wahrt, wurde im hessischen Ausführungserlaß Rechnung getragen.

Zum 1. Januar 1999 tritt das Gesetz über die Berufe des Psychologischen Psychotherapeuten und des Kinder- und Jugendlichen-Therapeuten (PsychThG) in Kraft. Verschiedene Institutionen sowie Bürgerinnen und Bürger haben mich gebeten, zu der Umsetzung der neuen Vorschriften aus datenschutzrechtlicher Sicht Stellung zu nehmen.

Nach dem in § 12 Abs. 3 und 4 Psychotherapeutengesetz und in § 95 Abs. 10 und 11 Sozialgesetzbuch V (SGB) vorgesehenen Übergangsbestimmungen müssen die Approbation und ggf. Kassenzulassung beantragenden Psychologinnen und Psychologen Nachweise über ihre bisherige Berufstätigkeit und Ausbildung gegenüber den Approbationsbehörden der Länder und den sozialrechtlichen Zulassungsausschüssen für die gesetzliche Krankenversicherung führen, u.a. eine mindestens 4.000 Stunden umfassende psychotherapeutische Berufstätigkeit oder die Durchführung von 60 dokumentierten und abgeschlossenen Behandlungsfällen. Anlaß dieser Regelung ist die Tatsache, daß in der Vergangenheit etwa 6.000 Psychologinnen und Psychologen Patienten behandelt haben, die die Behandlungskosten im Rahmen eines sog. Kostenerstattungsverfahrens der gesetzlichen Krankenversicherung (§ 13 SGB V) erhielten bzw. die sog. Selbstzahler waren. Auch diesen Behandlern wollte der Gesetzgeber auf Grund von Überlegungen zum "Besitzstandsrecht" die Approbation bzw. Kassenzulassung unter bestimmten Voraussetzungen nach speziellen Übergangsbestimmungen ermöglichen.

Soweit die Berufstätigkeit von Psychologinnen und Psychologen durch den Nachweis von Behandlungsstunden oder Behandlungsfällen belegt werden soll, die von der gesetzlichen Krankenversicherung im Rahmen des Kostenerstattungsverfahrens bezahlt wurden, kommt in erster Linie eine Bestätigung des jeweiligen Kostenträgers als Nachweismöglichkeit in Betracht. Bei einer direkten Abrechnung des Psychologen mit dem Patienten

kommt die Vorlage von Rechnungen und Behandlungsunterlagen in Betracht. Aus datenschutzrechtlicher Sicht ist die zentrale Frage, ob diese Nachweise mit personenbezogenen Daten der Patientinnen und Patienten geführt werden müssen. Es handelt sich hier um sehr sensitive Daten, an deren Geheimhaltung die Betroffenen ein erhebliches Interesse haben.

Die personenbezogenen Daten der Patientinnen und Patienten unterliegen grundsätzlich der Schweigepflicht i.S.v. § 203 StGB. Sie dürfen daher nur "befugt" offenbart werden. Eine Befugnis zur Offenbarung kann sich insbesondere aus einer gesetzlichen Regelung ergeben. In den neuen Vorschriften des Psychotherapeutengesetzes ist nicht festgelegt, daß und ggf. welche personenbezogenen Daten der Patientinnen und Patienten zum Nachweis der bisherigen Tätigkeit gegenüber der zuständigen Behörde anzugeben sind. Eine Weitergabe der personenbezogenen Daten der Patientinnen und Patienten wäre ein Eingriff in ihr Recht auf informationelle Selbstbestimmung. Nach der ständigen Rechtsprechung des Bundesverfassungsgerichts ist ein derartiger Eingriff nur im überwiegenden Interesse der Allgemeinheit zulässig und bedarf einer gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Einschränkungen des Rechts auf informationelle Selbstbestimmung klar und für die Bürgerin und den Bürger erkennbar ergeben und die dem Grundsatz der Verhältnismäßigkeit entspricht (vergl. z.B. BVerfGE 65, 1 ff., 44). Diesen verfassungsgerichtlichen Anforderungen genügt das Psychotherapeutengesetz nicht. Es kommt daher als gesetzliche Offenbarungsbefugnis nicht in Betracht. Es ist auch fraglich, ob eine gesetzliche Festlegung der Weitergabe personenbezogener Daten aller Patientinnen und Patienten als verhältnismäßig angesehen werden könnte, denn die Weitergabe und zentrale Speicherung der Daten aller Patientinnen und Patienten ist für die Verhinderung eventueller Täuschungsversuche in diesem Umfang nicht erforderlich.

Die Nachweise können daher entweder auf der Grundlage einer Einwilligung der jeweiligen Patientinnen und Patienten personenbezogen erbracht werden oder sie können mit anonymisierten Angaben eingereicht werden.

Dem Hessischen Ministerium für Umwelt, Energie, Jugend, Familie und Gesundheit habe ich mitgeteilt, daß eine Übermittlung personenbezogener Daten der Patientinnen und Patienten im Rahmen der Umsetzung des Psychotherapeutengesetzes grundsätzlich unzulässig ist und es den zuständigen Ministerien obliegt, ein datenschutzgerechtes Verfahren zu entwickeln, das die Vorlage von Nachweisen unter Wahrung der Schweigepflicht ermöglicht. Sofern sich im Einzelfall bei der Prüfung der vorgelegten Nachweise Anhaltspunkte für falsche Darstellungen ergeben, sehe ich es als zulässig an, daß die Angaben durch die Aufsichtsbehörden überprüft werden. In diesem Fall kann eine Befugnis der Nachweispflichtigen zur Offenbarung unter dem allgemein anerkannten Gesichtspunkt der Wahrnehmung berechtigter Interessen i.S.v. § 193 StGB in Betracht kommen.

Die datenschutzrechtlichen Aspekte sind auch im Arbeitskreis Gesundheit und Soziales der Konferenz der Datenschutzbeauftragten des Bundes und der Länder entsprechend diskutiert worden. Die Bundesländer haben sich bei ihren Beratungen am 14. September 1998 darüber verständigt, daß den datenschutzrechtlichen Forderungen an die Ausgestaltung des Nachweisverfahrens nachgekommen wird.

Der Ausführungserlaß des Hessischen Ministeriums für Umwelt, Energie, Jugend, Familie und Gesundheit zur Umsetzung des Gesetzes über die Berufe des Psychologischen Psychotherapeuten und des Kinder- und Jugendlichen-Psychotherapeuten, zur Änderung des Fünften Buches Sozialgesetzbuch und anderer Gesetze (Psychotherapeutengesetz) im Hinblick auf die Nachqualifizierungsvorschriften des Gesetzes vom 28. September

1998 trägt den datenschutzrechtlichen Aspekten hinreichend Rechnung. Die entsprechenden Bestimmungen lauten wie folgt:

7.

Soweit die einzelnen Voraussetzungen durch die Antragstellerin und Antragsteller "nachzuweisen" sind, überträgt ihnen das Gesetz die Obliegenheit, die jeweiligen Nachweise zu führen. Dabei haben sie die Schweigepflicht (§ 203 StGB) und den Datenschutz (Einwilligung der Patienten) zu beachten. Die vorgeschriebenen Nachweise sind soweit wie möglich durch Fremdbelege, ggf. in Kombination mit Eigenbelegen, vorzunehmen (z.B. Bewilligungsbescheide, Kostenzusagen, Abrechnungsunterlagen wie Rechnungen mit Zahlungseingangsbegleiten, Bescheinigungen durch Ärztinnen und Ärzte und Supervisorinnen oder Supervisoren, Angaben über den Behandlungsfall wie z.B. chiffrierte Patientenbezeichnung, Alter, Geschlecht, Setting (Einzel, Paar, Gruppe), Diagnose, Indikationsstellung, psychotherapeutisches Behandlungsverfahren, Zeitraum der Behandlung (Anfang/Ende), Behandlungsverlauf, Anzahl der Sitzungen, Behandlungsstunden, Kostenträger). In besonderen Ausnahmefällen können auch ausschließlich Eigenbelege ausreichen.

8.

Der Nachweis von Behandlungstätigkeiten kann insbesondere durch Bestätigung der Kostenträger erfolgen (z.B. anhand von Aufstellungen). Wo dies nicht möglich ist, kann der Nachweis von Behandlungstätigkeiten insbesondere anhand von Aufstellungen vorgenommen werden, in denen die Art der vorhandenen Unterlagen aufgeführt wird; ein Muster hierfür ist beigelegt. Die Nachweise müssen für die Vorlage bei den Approbationsbehörden in geeigneter Weise

anonymisiert sein (z.B. durch Chiffrierung). Sofern sich im Einzelfall bei der Prüfung der vorgelegten Unterlagen Anhaltspunkte für falsche Darstellungen ergeben, dürfen die Angaben der Nachweispflichtigen überprüft werden. Die Nachweispflichtigen dürfen dann personenbezogene Daten unter dem Gesichtspunkt der Wahrnehmung berechtigter Interessen offenbaren. Im Rahmen der Nachweispflicht besteht kein Hindernis, eine vorgelegte Versicherung an Eides Statt (§ 27 Abs. 1 VwVfG) angemessen zu berücksichtigen.

Entsprechend den für das Approbationsverfahren dargelegten nach § 12 PsychThG bestehenden Grundsätzen muß auch im Verfahren für die Kassenzulassung sichergestellt werden, daß die Nachweise keine personenbezogenen Daten enthalten.

1999 werde ich mich über die Handhabung der Verfahren bei den zuständigen Stellen informieren.

7.3

Prüfung des Rechenzentrums der AOK ARGE-Mitte

Im gemeinsamen Rechenzentrum der AOK Hessen, AOK Rheinland-Pfalz und AOK Saarland sind die Datenbestände ausreichend gegeneinander abgeschottet.

In meinem letztjährigen Tätigkeitsbericht (26. Tätigkeitsbericht, Ziff. 7.4) hatte ich berichtet, daß die AOK Hessen, AOK Rheinland Pfalz und AOK Saarland ein gemeinsames Rechenzentrum betreiben wollen. Dazu wurde die Arbeitsgemeinschaft „AOK-Rechenzentrum Mitte“ (ARGE-Mitte) gegründet. 1998 ist auch die AOK Thüringen der Arbeitsgemeinschaft beigetreten. Zusammen mit dem Landesbeauftragten für den Datenschutz Rheinland-Pfalz

habe ich in diesem Jahr die Datensicherheitsmaßnahmen der ARGE-Mitte dahingehend überprüft, ob die Datenbestände der drei Landeskrankenkassen hinreichend gegeneinander abgeschottet waren. Auf die personenbezogenen Daten der Versicherten einer Landeskrankenkasse dürfen nur die jeweils dieser Landeskrankenkasse zugehörigen Beschäftigten Zugriff haben sowie Beschäftigte der ARGE, soweit diese Datenverarbeitung zu ihrem konkreten Aufgabenbereich gehört.

Bei der Prüfung konnte ich Schwachstellen feststellen, die aber entweder sofort beseitigt wurden oder deren Beseitigung bereits begonnen wurde. Im folgenden beschränke ich mich auf solche Schwachstellen, die auch für andere datenverarbeitende Stellen von Bedeutung sein können.

7.3.1

Technisches Umfeld

7.3.1.1

Das Betriebssystem Multiple Virtual Storage (MVS)

Bei der ARGE wird für den Großrechner das Betriebssystem MVS genutzt, das es vielen Benutzern gestattet, mit vielen verschiedenen Programmen gleichzeitig auf dem DV-System zu arbeiten. MVS übernimmt die Verwaltung der Betriebsmittel und Ressourcen wie Hauptspeicher, Plattenspeicher, Datenträger, Ausgabegeräte und Systemprogramme gegenüber den Anwendungsprogrammen, die von Benutzern eingesetzt werden.

Das von IBM entwickelte Betriebssystem MVS ist seit 1974 auf dem Markt. Im Laufe der Zeit wurde es immer weiter entwickelt, aber Grundzüge haben sich in den fast 25 Jahren erhalten. Die Ursprünge reichen also noch in die Zeit zurück, als den Rechnern mit Lochkarten Programme und Daten eingespielt wurden. Damals

hatten nur die Maschinenbediener Kontakt zu dem Rechner und einem normalen Benutzer lagen Ergebnisse eigentlich nur in Form von Listen vor, d.h. es gab keine Dialogverarbeitung von Daten. Eine vorrangige Anforderung an MVS war folglich sicherzustellen, daß sich die verschiedenen Programme nicht gegenseitig stören, während die Kontrolle von Benutzern und deren Zugriffe auf Dateien kaum berücksichtigt wurden. Die Belange des Datenschutzes und Datensicherheit sind im MVS selbst nicht ausreichend berücksichtigt.

7.3.1.2

Schutzfunktionen von MVS

Es sind unter MVS sogenannte Adreßräume eingerichtet, in denen jeweils die durch MVS zu trennenden Programme ablaufen. Die Ressourcenverwaltung des MVS stellt sicher, daß die Programme isoliert sind, d.h. die verschiedenen Adreßräume sind bezüglich der Ausführung von Programmen und Dateizugriffen getrennt.

In einem Adreßraum können die unterschiedlichsten Programme ablaufen:

- Anwendungsprogramme, die in einem festen Ablauf als sogenannter Job Daten verarbeiten (Jobs sind Verarbeitungsaufträge an das Betriebssystem)
- Datenbanksysteme, die Programmen in anderen Adreßräumen Daten zur Verfügung stellen.
- TP (Teleprocessing)-Monitore, die Programme steuern, die von Benutzern im Dialog aufgerufen und genutzt werden. Ein sehr verbreiteter TP-Monitor ist CICS (Customer Information Control System der Fa. IBM).

- TSO (Time Sharing Option), ein Programm, mit dem ein Benutzer den Rechner in einem eigenen Adreßraum systemnah nutzen kann.

Wenn ein Benutzer Anwendungen in mehreren Adreßräumen nutzen muß, ist es aufwendig, bei einem Wechsel zwischen den Anwendungen sich jedesmal erneut anzumelden. Deshalb werden Session-Manager eingesetzt, die es erlauben, sich in mehreren Adreßräumen parallel anzumelden und zwischen den Anwendungen zu springen.

MVS ordnet einem Adreßraum zum Ausführungszeitpunkt Dateien zu, die verarbeitet werden sollen. Neben anderen Steuerungsinformationen wird je Adreßraum eine Kennung gespeichert, die u.a. den Prüfungen durch die Schutzsoftware zugrunde gelegt wird. Sie läßt sich auf unterschiedliche Arten generieren; so ist es beispielsweise bei der Nutzung von TSO die Kennung, die der Benutzer bei der Anmeldung eingegeben hat.

7.3.1.3

Grenzen der Schutzfunktionen von MVS

Solange es keine Zugriffskollisionen gibt, erlaubt es MVS jedem Programm, auf (fast) jede Datei zuzugreifen. Wenn ein Benutzer selbst bestimmen kann, welche Dateien verarbeitet werden sollen, hat er umfassende Zugriffsmöglichkeiten. Dies können beispielsweise Benutzer, die eine TSO-Berechtigung haben. Um doch noch Einschränkungen vornehmen zu können, ist es erforderlich, eine Schutzsoftware einzusetzen. Die bekanntesten Produkte sind ACF2, Top Secret und RACF (Resource Access Control Facility). Die ARGE setzt RACF ein.

Ohne weitere Schnittstellen kann eine Kontrolle nur auf Ebene der MVS bekannten Strukturen vorgenommen werden. Hierzu gehört

auch der Adreßraum. Wenn sich an einem TP-Monitor also mehrere Benutzer anmelden und ihre Programme ausführen, so kennt MVS, und damit auch die Schutzsoftware, nur den Adreßraum mit seiner Kennung und kann diese Benutzer nicht unterscheiden. Es ist weder möglich, unterschiedliche Zugriffe auf eine Datei noch innerhalb einer Datei umzusetzen.

Um bei der Umsetzung systemseitiger Schutzmaßnahmen das Problem zu lösen, muß über eine Schnittstelle der Schutzsoftware mitgeteilt werden, welcher Benutzer einen Zugriff verlangt. Dazu muß beispielsweise die Schnittstelle zwischen RACF und CICS aktiv sein. Dadurch wird bekannt, welcher Benutzer sich am CICS angemeldet hat. Die Benutzerkennung steht nun für die Zugriffskontrolle im Anwendungsprogramm zur Verfügung; dies geschieht bei IDVS II mit dem Modul ZUBER. Im Zusammenspiel von RACF, CICS und ZUBER wird also bei der ARGE die Zugriffskontrolle für Sachbearbeiter vorgenommen.

7.3.2

Konzeptioneller Rahmen

In dem Rechenzentrum der ARGE-Mitte in Ziegenhain wurde nur der Produktionsbetrieb durchgeführt. Es fand keine Programmentwicklung statt und sonstige Dienstleistungen wurden ebenfalls nicht angeboten.

7.3.2.1

DV-Konzept

Es war ein DV-Konzept umgesetzt, welches auf einem physischen Rechner mehrere logische Rechner vorsah, von denen jeder ein eigenes MVS besaß. Entsprechend diesem Konzept war der AOK-Hessen exklusiv ein eigener logischer Rechner zugeordnet. Die

AOK-Saarland und AOK-Rheinland-Pfalz nutzten gemeinsam einen anderen logischen Rechner.

Jedem logischen Rechnern waren lediglich die Festplatten zugeordnet, auf denen sich die jeweils benötigten Dateien befanden. Da sich die Daten der AOK-Hessen in anderen Dateien befanden als die Daten der anderen Krankenkassen, war es möglich, je AOK unterschiedliche Festplatten zur Speicherung zu wählen und eine restriktive Zuordnung vorzunehmen. Dies hatte zur Folge, daß es beispielsweise vom logischen Rechner der AOK-Hessen aus nicht möglich war, auf Daten der AOK-Rheinland-Pfalz zuzugreifen und umgekehrt.

Die Planungen der ARGE sahen aber vor, von diesem Konzept abzuweichen und eine Streuung von Dateien auf allen Festplatten zuzulassen. Spätestens zu diesem Zeitpunkt wäre die gezielte Sperre von Festplatten für einzelne logische Rechner nicht mehr möglich. Die dann erforderlichen Zugriffseinschränkungen auf Systemebene können nur durch RACF erreicht werden, wie es bereits heute für den Rechenzentrumsbetrieb der Fall ist. Die Zuordnung aller Platten an jedes MVS ist aus datenschutzrechtlicher Sicht erst dann zulässig, wenn vorher das erarbeitete RACF-Konzept strikt umgesetzt wurde.

Für die Mitarbeiterinnen und Mitarbeiter der AOK Hessen waren mehr als 4.000 Benutzerkennungen definiert. Üblicherweise arbeiteten sie mit IDVS II, einem Anwendungsprogramm, das alle für die Sachbearbeitung erforderlichen Datenzugriffe bereitstellt. Außer für einige weitergehende Funktionen - z.B. Revision oder Benutzeradministration -, die Zugriff auf die Systemebene haben müssen und deshalb eine TSO-Berechtigung benötigen, war nur IDVS II als Anwendung vorgesehen. IDVS II läuft unter dem TP-Monitor CICS. Die normalen Benutzerkennungen erlaubten es deshalb nur, sich am CICS anzumelden und mit IDVS II zu arbeiten. Ein Zugriff auf die Ebene des Betriebssystems war nicht

möglich. Den Mitarbeiterinnen und Mitarbeitern, die umfassendere Funktionen wahrnehmen, wurde es mit einem Sessionmanager ermöglicht, sich gleichzeitig in mehreren Anwendungen anzumelden.

IDVS II

Informations- und Datenverarbeitungsystem

Es handelt sich um ein Auskunftssystem, bei dem die Datenbestände für lesende Zugriffe zur Verfügung stehen. Änderungen werden in gesonderten Dateien zwischengespeichert und in nächtlichen Änderungsläufen eingespielt. Abfragen zu Änderungen des Tages müssen gezielt aus diesen Zwischendateien vorgenommen werden.

Die Datenübertragung soll in Zukunft vermehrt verschlüsselt erfolgen. In einem ersten Ansatz fand zu anderen AOKen und zu derzeit etwa fünfzig Arbeitgebern und einem Krankenhaus die Datenübertragung bereits verschlüsselt statt. Dabei wurde ein System genutzt, das die Schlüsselverwaltung durch ein Trustcenter realisiert (vgl. 23. Tätigkeitsbericht, Ziff. 26).

Damit nur zugelassene Programmänderungen aktiv werden konnten, lag ein detailliert beschriebenes Test- und Freigabeverfahren vor. Dabei wurden die erstellten Programme ausgiebig getestet, bevor sie von der Qualitätssicherung für den Produktionsbetrieb freigegeben und durch das Rechenzentrum in Produktion genommen wurden.

Zur Schulung und Unterstützung der Mitarbeiterinnen und Mitarbeiter gab es ein spezielles Testsystem. Es handelte sich um ein eigenes CICS mit den aktuell in Produktion befindlichen Programmen, das auf Testdatenbestände zugreift. Alle Beschäftigten besaßen umfassende Zugriffsrechte, damit sie sich mit den Programmen vertraut machen und sie unklare

Konstellationen testen konnten. Dieser Ansatz trägt dazu bei, korrekte Daten zu speichern, und ist daher begrüßenswert.

7.3.2.2

RACF-Konzept

Grundlage des RACF-Konzepts waren die Namenskonventionen für Systemressourcen und hier insbesondere für Produktionsdateien, die es erlaubten, einfache Regeln vorzugeben und diese mit vertretbarem Aufwand nachzuvollziehen.

Ziel des RACF-Einsatzes war es, den Zugang zu den EDV-Systemen nur von berechtigten Benutzerinnen und Benutzern innerhalb ihres Aufgabengebietes im zulässigen Rahmen zuzulassen und unerlaubte Aktivitäten aufzudecken. Dazu dienen die in RACF vorhandenen Funktionen der Identifikation und Authentisierung, Prüfung und Autorisierung sowie der Protokollierung.

Eingeschränkt auf den eigenen Zuständigkeitsbereich administrierte jede AOK die Zugriffsrechte mit ZUBER bzw. RACF. Auf Systemebene nahm die ARGE diese Funktion wahr. Die Revision erfolgte durch Mitarbeiterinnen und Mitarbeiter der Krankenkassen.

7.3.3

Feststellungen

7.3.3.1

Räumliche Sicherungsmaßnahmen

Bei der Zugangskontrolle, also den räumlichen Sicherungsmaßnahmen, gab es zwei Schwachstellen, die Anlaß zur

Kritik boten. An einem auch für Besucherinnen und Besucher zugänglichen Ort befand sich ein Übersichtsplan der Alarmanlage, dem beispielsweise zu entnehmen war, wo sich Bewegungsmelder befanden. Ferner war der Zugang zum Gebäude, zu den Teilbereichen und zu einzelnen Räumen zwar mit einer Schließanlage gesichert, aber alle Mitarbeiterinnen und Mitarbeiter hatten einen Generalschlüssel. Es gab folglich keine funktionsbezogenen Einschränkungen des Zutritts durch das Personal (mit Ausnahme des Bandarchives). Diese Schwachstelle war bekannt und es waren zum Zeitpunkt der Prüfung bereits Maßnahmen eingeleitet, um durch die Schließanlage wieder die erforderlichen Zutrittseinschränkungen zu erreichen.

7.3.3.2

Benutzerkennungen mit besonderen Zugriffsrechten

Wie in jedem Rechenzentrum gab es Mitarbeiterinnen und Mitarbeiter, die zur Erfüllung ihrer Aufgaben besondere Zugriffsrechte benötigten. In einigen Fällen waren diese Zugriffsrechte aber nicht oder nicht mehr erforderlich.

Mit speziellen Kommunikationsrechnern wurde die verschlüsselte Datenübertragung durchgeführt. Drei Mitarbeiter administrierten die Kommunikationssoftware unter einer Kennung mit sog. "root-Rechten" (d.h. mit den umfassenden Zugriffsrechten eines Systemadministrators), obwohl die Systemadministration durch einen anderen Mitarbeiter vorgenommen wurde. Deshalb war es nicht möglich, die Tätigkeiten eines einzelnen Mitarbeiters nachzuvollziehen. Außerdem konnten diese Mitarbeiter absichtlich oder zufällig Änderungen am System vornehmen, obwohl dies nicht zu ihrem Aufgabenbereich gehörte. Hier war es erforderlich, jedem Mitarbeiter eine eigene Kennung mit reduzierten Zugriffsrechten zuzuordnen.

Bei der Durchsicht des "Selected User Attribute Report" im RACF wurden einige Kennungen gefunden, die historisch bedingt mit besonderen Rechten ausgestattet waren und für die nicht erklärt werden konnte, warum sie noch damit versehen oder wieso sie nicht gelöscht waren. Beispielsweise gab es allein auf Gruppenebene sechs Kennungen mit SPECIAL-Rechten zusätzlich zu einer Notfallkennung. Auch waren eine große Anzahl Benutzerkennungen auf REVOKE (d.h. gesperrt) gesetzt, von denen einige gelöscht werden konnten.

Im RACF gibt es Attribute für Benutzerkennungen, die mit besonderen Rechten verbunden sind:

SPECIAL

Unter einer Benutzerkennung mit diesem Attribut können alle RACF-Kommandos abgesetzt werden. Es ist damit die volle Kontrolle über alle RACF-Profile verbunden. Ein sog. GROUP-SPECIAL kann nur die zu seinem Zuständigkeitsbereich, also auf Ebene seiner Gruppe, gehörenden Profile ändern.

AUDITOR

Mit diesem Attribut können alle RACF-Profile und alle Protokolldateien gelesen und ausgewertet werden.

OPERATIONS

Mit diesem Attribut ist der umfassende Zugriff auf alle Dateien möglich, es sei denn, der Benutzerkennung ist explizit in dem jeweiligen RACF-Profil ein anderes Zugriffsrecht gegeben.

Bemerkenswert waren ferner die zwei Personen zugeordneten Kennungen, denen sowohl die Attribute SPECIAL, OPERATIONS als auch AUDITOR zugeordnet waren. In einer Person sollten diese Zugriffsrechte nicht gebündelt sein. Zumindest das AUDITOR Attribut sollte auf die Revisoren beschränkt sein.

Insgesamt habe ich gefordert, daß die ARGE und die AOK prüfen, welche Benutzerkennungen gelöscht werden und bei welchen die Attribute geändert und herabgesetzt werden können.

7.3.3.3

RACF

7.3.3.3.1

Anmeldung am Rechner

Im Konzept war vorgesehen, daß RACF jede Anmeldung am Rechner kontrollieren soll. Dazu müssen Schnittstellen zu den anderen Verfahren vorhanden sein.

CICS / IDVS II

Die Schnittstelle zwischen CICS, IDVS II und RACF war aktiviert, wodurch die Anmeldeprozedur unter der Kontrolle von RACF ablief.

Sessionmanager

Die Schnittstelle zwischen dem Sessionmanager und RACF war nicht aktiviert. Das Manager- und das RACF-Paßwort sowie die Benutzerkennungen waren nicht synchronisiert, d.h. sie konnten auseinanderfallen. Während die Übereinstimmung der Kennungen durch die Einträge der ARGE erzwungen werden konnte, waren

beim Paßwort die Benutzerin und der Benutzer gefordert. Folglich mußten sich die Beschäftigten eventuell zwei Paßwörter merken. Protokolle über Systemanomalien fielen sowohl beim Sessionmanager als auch in RACF an, weshalb in zwei Systemen die Protokolle kontrolliert werden mußten.

Ich habe daher gefordert, die Schnittstelle zwischen dem Sessionmanager und RACF zu aktivieren.

7.3.3.3.2

Zugriffskontrolle

Zugriffsrechte für CICS

Die Vorgabe der Startparameter inclusive der von dem jeweiligen CICS zur Verarbeitung herangezogenen Dateien erfolgt über eine Verkettung von Einträgen in verschiedenen Systemdateien. Zum Zeitpunkt des Starts eines CICS steht dadurch fest, welche Dateien mit welchen Zugriffsrechten dem CICS und damit den Nutzern des CICS zur Verfügung stehen. Wenn, wie bei der ARGE der Fall, sich die Daten der AOK Hessen, der AOK Rheinland-Pfalz und der AOK Saarland in unterschiedlichen Dateien befanden, wurde durch diese Definitionen festgelegt, daß nur Daten einer AOK im Zugriff eines CICS waren.

Jedem CICS wurde zusätzlich beim Start eine Kennung zugeordnet, deren Zugriffsrechte stellvertretend für das CICS durch RACF geprüft wurden. RACF erlaubte dann entsprechend den in den Dateiprofilen hinterlegten Zugriffsrechten der CICS-Kennung Zugriffe auf die beim Start vorgegebenen Dateien.

Die Schnittstelle zwischen RACF und CICS war aktiv. RACF prüfte nach Eingabe der Benutzerkennung im CICS Startbildschirm, ob die Kennung zu einer Gruppe gehörte, die mit

diesem CICS arbeiten durfte. Anschließend erfolgte in ZUBER, dem anwendungsinternen Schutzmodul von IDVS II, die Kontrolle, ob und mit welchen Rechten die Kennung für IDVS II zugelassen war.

Mitarbeiterinnen und Mitarbeiter der ARGE pflegen die Einträge im RACF (soweit nicht auf Gruppenebene die AOK zuständig ist), im CICS und auf Netzebene, während die jeweilige AOK Einträge in ZUBER und auf Gruppenebene im RACF vornimmt.

Die Trennung der Datenbestände war hinsichtlich der CICS-Anwendungen (also bei IDVS II) mit hinreichender Sicherheit gewährleistet.

TSO

Die Zugriffe auf Dateien mit TSO waren durch die Zuordnung von Festplatten zum jeweiligen logischen Rechner und durch die in RACF vorgegebenen Zugriffsregeln eingeschränkt.

Batch-Job-Verarbeitung (durch Beschäftigte der ARGE)

Jeder Mitarbeiter der Produktionssteuerung und weitere Mitarbeiter aus anderen RZ-Bereichen hatten unter ihrer TSO-Kennung Zugriffrechte auf die Daten aller Kunden. Insofern war es ihnen zum Beispiel möglich, absichtlich oder versehentlich in einem Job Daten der AOK-Hessen auszuwerten und das Ergebnis in eine Druckdatei der AOK-Rheinland-Pfalz zu stellen.

Um die Mitarbeiterinnen und Mitarbeiter der Arbeitsvorbereitung und der Produktionssteuerung zu entlasten und Fehler zu reduzieren, wurde ein Programm eingesetzt, mit welchem Jobs erstellt, verknüpft und gestartet werden können. Von der

Systematik her war eine Benutzerkennung für die Batchverarbeitung der AOK-Hessen vorgesehen; also für die Jobs, die auf Produktionsdateien zugreifen, deren Namen mit dem Kürzel der AOK-Hessen beginnen. Für Rheinland-Pfalz und für das Saarland galten gleiche Regelungen. Da es Fälle gibt, in denen Jobs auf Dateien aller Krankenkassen zugreifen müssen, z.B. bei Datenübermittlungen großer Arbeitgeber, wurde eine Benutzerkennung definiert, die auf alle Produktionsdateien zugreifen kann. Die vorgesehenen Zugriffsbeschränkungen müssen durch entsprechende RACF-Profile umgesetzt werden.

Mitarbeiterinnen und Mitarbeiter der Produktionssteuerung konnten auf die Daten aller Kunden zugreifen. Mit dem Hilfsprogramm wurde ihre Arbeit unterstützt und es war damit möglich, für Jobs Zugriffsbeschränkungen umzusetzen, soweit Beschäftigte das Programm nutzen.

Ich habe daher gefordert, in einer Arbeitsanweisung alle Mitarbeiterinnen und Mitarbeiter zu verpflichten, bei der Durchführung von Aufträgen das Hilfsprogramm zu nutzen. Ferner sollte jedem Beschäftigten der Produktion eine Kennung je Kunde eingerichtet werden. Hierdurch wird es nachvollziehbar, wer einen bestimmten Job gestartet hat.

RACF Dateiprofile

Die Dateien mit den RACF-Informationen besaßen einen UACC (READ), d.h. sie konnten von jedem Benutzer mit Zugang zur Systemebene gelesen werden. Dies stellte eine erhebliche Sicherheitslücke dar, da die Datei und damit die Paßwörter lesbar waren. Die RACF-Dateien müssen mit einem UACC(NONE) geschützt werden.

UACC

Universal Access Code

Allgemeines Zugriffsrecht, also das Zugriffsrecht für Kennungen, zu denen keine besonderen Vorgaben existieren.

READ

Lesender Zugriff wird erlaubt.

NONE

Es wird kein Zugriff gewährt.

Ich habe stichprobenhaft Dateiprofile für Produktionsdateien der AOK-Hessen geprüft.

In zwei Fällen war als UACC(READ) gesetzt und alle Mitarbeiter der Produktionssteuerung sowie die Kennungen für die Jobsteuerung hatten unbeschränkte Zugriffsrechte. Folglich hatten alle Benutzer mit TSO-Berechtigung (zukünftig auch solche der AOK-Rheinland-Pfalz) lesenden Zugriff. Außerdem setzte das Jobsteuerungsprogramm nicht alle Möglichkeiten zur Zugriffskontrolle um.

In einem weiteren Fall war zwar der UACC(NONE) vorgesehen, aber für eine größere Zahl anderer Kennungen waren lesende Zugriffsrechte vergeben, ohne daß dies in jedem Fall erklärt werden konnte.

Es mußten daher die Einträge überarbeitet und den Anforderungen angepaßt werden.

7.3.3.3.3

RACF-Parameter und DES-EXIT

Wenn RACF auf einen Rechner installiert wird, läßt es alle Zugriffe auf Dateien zu, es sei denn, diese werden durch Zugriffsprofile explizit verboten. Insbesondere sind Zugriffe auf Dateien möglich, zu denen kein Zugriffsprofil definiert ist. Ist der Parameter PROTECTALL gesetzt, so wird der Zugriff auf Dateien ohne Zugriffsprofil abgewiesen. Um einen fließenden Übergang zu ermöglichen, kann der Parameter durch die Option WARNING ergänzt werden. In diesem Fall wird ein Zugriff erlaubt, auch wenn er wegen PROTECTALL unzulässig wäre. Der Administrator erhält aber eine Meldung über diesen Zugriff. Er kann dann entscheiden, ob Profile fehlen oder unzulässige Versuche vorgenommen wurden.

Das RACF-Konzept sah vor, den Zugriff auf alle Dateien mit RACF zu schützen. Es war aber der Parameter PROTECTALL mit der Option WARNING gesetzt. Ich habe gefordert, daß die Option so schnell wie möglich gelöscht wird, damit die Vorgabe des Konzepts umgesetzt ist.

Die anderen Parameter entsprachen den Vorgaben aus dem Konzept und lehnten sich an Vorstellungen der Datenschutzbeauftragten an.

RACF-EXIT

Der RACF-EXIT, mit dem eine (nach DES) verschlüsselte Speicherung der Paßwörter erreicht wird, war nicht vorhanden. Die Paßwörter wurden deshalb nur in komprimierter Form gespeichert und waren mit im Internet verfügbaren Tools zu knacken. Zusammen mit dem READ-Zugriff auf die RACF-Dateien ergab sich daher für alle Personen, die auf diese Datei zugreifen können (RZ-Mitarbeiter, AOK-Mitarbeiter mit TSO und Job

Berechtigung), die Möglichkeit, von beliebigen Usern deren Paßwort zu erfahren.

Dies war eine Lücke im Sicherheitssystem, die geschlossen werden mußte. Dazu sollte der RACF-Exit installiert und der Zugriff auf die RACF-Dateien mit einem UACC(NONE) versehen werden.

7.3.3.3.4

Kontrolle

Es fand keine regelmäßige Kontrolle der RACF-Einträge und RACF-Protokolle statt.

Im Rahmen eines Revisionskonzepts muß festgelegt werden, wann welche sicherheitsrelevanten Protokolle und Einträge kontrolliert und wie bei festgestellten Vorkommnissen zu verfahren ist.

7.3.3.4

Einzelprobleme

Zugriff auf Banddateien

In meinem 24. Tätigkeitsbericht (Ziff. 14.1) hatte ich Probleme aufgezeigt, die auftreten, wenn die Schnittstelle zwischen Bandverwaltungssystem und RACF nicht funktioniert. Bei der ARGE habe ich jetzt versucht, ein Band an der Kontrolle durch das Bandverwaltungssystem vorbei zu verarbeiten. Wenn das Band im Bandverwaltungssystem geführt war, wurde der Versuch abgewiesen, weil das Band bereits bekannt war. Wurde versucht, eine Datei mit geändertem Namen auf einem Band zu lesen, das dem Bandverwaltungssystem bekannt war, so erfolgte die

Fehlermeldung „falscher Dateiname“. Die Banddateien waren somit ausreichend geschützt.

Zugriff mit ADRSSU

Ein lesender Zugriff auf Festplatten mit dem Programm ADRSSU, das auf Festplatten unter Angabe eines physischen Speicherplatzes zugreifen kann, war nur möglich, wenn die Benutzerkennung zumindest lesenden Zugriff auf alle Dateien hatte, die auf der Platte gespeichert waren.

In RACF vorgegebene Zugriffsbeschränkungen wurden eingehalten.

Sonstige systemnahe Software

Prinzipiell kann jedoch Software, die direkt auf Festplatten zugreift und ohne RACF-Schnittstelle ist, Zugriffsbeschränkungen von RACF umgehen. Es ist also bei jeder systemnahen Software zu prüfen, ob mit ihr Plattenzugriffe ohne RACF-Kontrolle möglich sind. Insbesondere Systemprogramme und systemnahe Programme sind so zu speichern, daß nur berechtigte Personen die Programme ändern, lesen oder ausführen können.

7.3.4

Fazit

Bei der Prüfung habe ich festgestellt, daß die Daten der AOK-Hessen im wesentlichen ausreichend von den anderen Produktionsdaten abgeschottet waren. Mit einer Beseitigung der Schwachstellen wurde sofort begonnen. Die Zugriffsrechte

innerhalb der Anwendung IDVS II waren nicht Prüfungsgegenstand und sie wurden nicht untersucht.

7.4

Mitarbeiterdatenschutz bei der AOK Hessen

Die Sozialdaten der Beschäftigten einer gesetzlichen Krankenkasse unterliegen dem Sozialgeheimnis gemäß § 35 Sozialgesetzbuch I.

Die Krankenkasse als Leistungsträger hat die Pflicht, Vorkehrungen zu treffen, um den Mitarbeiter-Sozialdatenschutz sicherzustellen.

Ein schwerbehinderter Mitarbeiter der AOK Hessen hat mir in einer Eingabe mitgeteilt, daß bei der Krankenkasse im Umgang mit den Sozialdaten der Beschäftigten, die zugleich bei der AOK Hessen krankenversichert sind, datenschutzrechtliche Defizite bestehen, die dem Anspruch auf Wahrung des Sozialgeheimnisses nach § 35 Sozialgesetzbuch (SGB) I zuwider laufen. Insbesondere seien die technischen und organisatorischen Maßnahmen zur Sicherstellung des Mitarbeiter-Sozialdatenschutzes nach § 35 Abs. 1 Satz 3 SGB I nicht ausreichend. Die Sozialdaten könnten innerhalb der Allgemeinen Ortskrankenkasse allgemein abgerufen und zur Kenntnis genommen werden.

§ 35 Abs. 1 Satz 3 SGB I

Sozialdaten der Beschäftigten und ihrer Angehörigen dürfen Personen, die Personalentscheidungen treffen oder daran mitwirken können, weder zugänglich sein noch von Zugriffsberechtigten weitergegeben werden.

Die Vorschrift beinhaltet für die Krankenkasse als Leistungsträger auch die Verpflichtung, aktiv Vorkehrungen zu treffen, um den

Sozialdatenschutz aller Mitarbeiterinnen und Mitarbeiter zu gewährleisten.

Auf Grund meiner Anfrage hat mir der Datenschutzbeauftragte der AOK Hessen dargelegt, wie die rechtlichen Vorgaben des § 35 Abs. 1 Satz 3 SGB I in der AOK Hessen umgesetzt wurden, und Material hierzu vorgelegt. Anschließend habe ich in zwei Geschäftsstellen der AOK Hessen die Praxis der getroffenen Maßnahmen überprüft.

Nach meinen Feststellungen stellt der Datenschutzbeauftragte der AOK Hessen bei Bedarf datenschutzrechtlich relevante Mitarbeiterinformationen in das automatisierte System der Krankenkasse ein, die dort jedem Mitarbeiter zur Verfügung stehen. Hierzu gehören auch Informationen zum Mitarbeiterdatenschutz, die seit Anfang 1996 fortgeschrieben und zuletzt im März 1998 ergänzt wurden.

Die aktuelle Mitarbeiterinformation ist auszugsweise nachfolgend wiedergegeben:

Mitarbeiterdatenschutz

Sozialdaten von Beschäftigten und deren Angehörigen unterliegen einem besonderen Schutz (Sozialgeheimnis). Die Wahrung des Sozialgeheimnisses umfaßt die Verpflichtung auch innerhalb des Leistungsträgers sicherzustellen, daß diese Sozialdaten nur Befugten zugänglich sind oder nur an diese weitergegeben werden.

Für Mitarbeiter/innen oder deren Angehörige, die noch nicht geschützt sind, wird nach schriftlicher Mitteilung an den Datenschutzbeauftragten der AOK - Die Gesundheitskasse in Hessen - dieser besondere Schutz aufgebaut.

Die schriftliche Mitteilung sollte neben Namen, Vornamen und Geburtsdatum der/des zu Schützenden auch den Absender mit Telefonnummer für evtl. Rückfragen enthalten.

Nach einer hessenweiten Umfrage des Gesamtpersonalrats zum Mitarbeiterdatenschutz hat sich die Mehrzahl der Mitarbeiterinnen und Mitarbeiter für eine dezentrale Bearbeitung von Mitarbeiterangelegenheiten ausgesprochen.

Bestandteil der Information ist eine Liste derjenigen Mitarbeiterinnen und Mitarbeiter, denen innerhalb der AOK Hessen die Aufgabe zugewiesen wurde, die Angelegenheiten der bei der AOK Hessen Versicherten zu bearbeiten, die zugleich Beschäftigte der AOK Hessen sind. Nur diese Mitarbeiterinnen und Mitarbeiter haben Zugriff auf die geschützten Daten und nur der Datenschutzbeauftragte der Krankenkasse vergibt die Zugriffsberechtigungen auf geschützte Mitarbeiterdaten.

Bei meinem Besuch in einer Geschäftsstelle der AOK Hessen konnte ich mich davon überzeugen, daß anderen Personen innerhalb der AOK keine Zugriffsmöglichkeiten auf die geschützten Daten eingeräumt wurden. Auch der zuständige Geschäftsstellenleiter hatte keine Zugriffsmöglichkeit.

Bei einem weiteren Besuch in einer anderen Geschäftsstelle der AOK Hessen habe ich mir den Arbeitsplatz eines für die Mitarbeiterdatenverarbeitung Zuständigen angesehen. Obwohl es sich um ein Großraumbüro mit mehreren Arbeitskabinen handelte, war die Geräuschkulisse so gedämpft, daß z.B. Telefongespräche außerhalb der Kabine nicht verstanden werden können. Ebenso war ein Einblick in Unterlagen, die auf dem Schreibtisch des betroffenen Beschäftigten liegen, von einer Stelle außerhalb der Kabine nicht möglich. Die Unterlagen werden sicher in einem abgeschlossenen Metallschrank aufbewahrt, zu dem nur der zuständige Bedienstete und seine Stellvertreterin Schlüssel

besaßen. Zu archivierende Sozialdaten der Mitarbeiter der AOK Hessen wurden im Archiv der Geschäftsstelle ebenfalls gesondert und abgeschlossen aufbewahrt.

Den Mitarbeitern der Krankenkasse, die auch bei der AOK Hessen krankenversichert sind, stehen besonders gekennzeichnete Briefumschläge zur Verfügung, die den Leistungserbringern, also z.B. Ärzten oder Krankenhäusern, zur Benutzung weitergegeben werden. Diese Briefumschläge werden, wenn sie in der Geschäftsstelle eingehen, ungeöffnet an den für die Verarbeitung von Mitarbeiterdaten zuständigen Beschäftigten weitergeleitet. Ausgehende Post wird von für die Verarbeitung von Mitarbeiterdaten zuständigen Beschäftigten kuvertiert und an die Poststelle gegeben.

Alle von mir angesprochenen Beschäftigten der Krankenkasse haben versichert, daß dieses Verfahren zu ihrer Zufriedenheit abgewickelt wird. Das Verfahren erfordert eine gewisse Mitwirkung der Betroffenen. Daß im Einzelfall einmal ein Fehler vorkommt, ist - wie auch in anderen Bereichen - nicht völlig auszuschließen.

Als Ergebnis meiner Überprüfung ist festzuhalten, daß die Verfahrensweise der AOK Hessen nicht unzulässig oder in besonderem Maße fehlerträchtig ist.

7.5

Feststellung der sachlichen Zuständigkeit des überörtlichen Sozialhilfeträgers nach dem Bundessozialhilfegesetz bei stationärer Krankenhausbehandlung

Sozialhilfe wird in Hessen von örtlichen Trägern und vom überörtlichen Träger gewährt. Die von mir angeregte Einführung

eines einheitlichen Vordrucks mit präziser Fragestellung macht die Anforderung von Arztberichten und Krankenakten entbehrlich.

Sozialleistungsträger, insbesondere die gesetzlichen Krankenkassen und die Sozialämter, benötigen Patientendaten zur Feststellung ihrer Leistungspflicht. Für den Bereich der gesetzlichen Krankenkassen ist die Datenübermittlung vom Krankenhaus an den Kostenträger in § 301 Sozialgesetzbuch (SGB) V geregelt. Eine entsprechende Vorschrift der vom Krankenhaus an Sozialhilfeträger zur Feststellung der Leistungspflicht zu übermittelnden Daten gibt es nicht.

Von einigen Krankenhäusern wurde ich im Lauf des Jahres darauf hingewiesen, daß Sozialämter Epikrisen, Arztbriefe, Entlassungsberichte und sogar komplette Krankenakten anfordern. In einem mir dokumentierten Fall hat das Sozialamt der Stadt Offenbach die Bezahlung der Krankenhausrechnung von der Vorlage eines ärztlichen Behandlungsberichtes abhängig gemacht. Das Sozialamt hat mir auf telefonische Anfrage zudem mitgeteilt, daß die von Krankenhäusern angeforderten Epikrisen und Berichte grundsätzlich dem Gesundheitsamt zur Stellungnahme vorgelegt werden.

Aus von mir im Landessozialamt Hessen in Wiesbaden durchgesehenen Sozialhilfeakten war ersichtlich, daß auch andere hessische Sozialämter so verfahren. Ausgangspunkt und Grundlage für die Entscheidung der Sozialhilfeträger sind die Kostenübernahmeersuchen der Krankenhäuser. Ein Krankenhaus ist im Rahmen des § 12 Abs. 2 Nr. 7 des Hessischen Krankenhausgesetzes (HKHG) befugt, Patientendaten ohne Einwilligung des Betroffenen an die Sozialleistungsträger zur Feststellung der Leistungspflicht zu übermitteln, soweit dies erforderlich ist. Im Rahmen der Prüfung durch einen Sozialhilfeträger werden zunächst Feststellungen getroffen, ob Krankenhilfeberechtigung gegeben ist bzw. ob

Sozialhilfebedürftigkeit vorliegt. Krankenhilfe wird vom örtlichen Sozialhilfeträger im Rahmen des § 37 Bundessozialhilfegesetz (BSHG) gewährt.

§ 37 BSHG

(1) Kranken ist Krankenhilfe zu gewähren.

(2) Die Krankenhilfe umfaßt ärztliche und zahnärztliche Behandlung, Versorgung mit Arzneimitteln, Verbandmitteln und Zahnersatz, Krankenhausbehandlung sowie sonstige zur Genesung, zur Besserung oder zur Linderung der Krankheitsfolgen erforderliche Leistungen. Die Leistungen sollen in der Regel den Leistungen entsprechen, die nach den Vorschriften über die gesetzliche Krankenversicherung gewährt werden.

Wird die Frage der Krankenhilfeberechtigung bejaht, erfolgt die Prüfung, ob die Zuständigkeit des überörtlichen Trägers der Sozialhilfe gem. § 100 BSHG gegeben ist.

§ 100 Abs. 1 Nr. 1 BSHG

Der überörtliche Träger der Sozialhilfe ist sachlich zuständig, soweit nicht nach Landesrecht der örtliche Träger sachlich zuständig ist,

1. für die Hilfe in besonderen Lebenslagen, für die in § 39 Abs. 1 Satz 1 und Abs. 2 genannten Personen, für Geisteskranke, Personen mit einer sonstigen geistigen oder seelischen Behinderung oder Störung, Anfallskranke und Suchtkranke wenn es wegen der Behinderung oder des Leidens dieser Personen in Verbindung mit den Besonderheiten des Einzelfalles erforderlich ist, die Hilfe in einer Anstalt, einem Heim oder einer gleichartigen Einrichtung oder in einer Einrichtung zur teilstationären Betreuung zu gewähren; dies gilt nicht, wenn die Hilfestellung in der Einrichtung überwiegend

aus anderem Grunde erforderlich ist.

...

Die vom Krankenhaus zu übermittelnden Patientendaten müssen dem Sozialhilfeträger auch die Feststellung ermöglichen, ob Schadenersatzansprüche gem. § 116 SGB X an Dritte bestehen. Diese Ansprüche können z.B. bestehen, wenn die Erkrankung Folge einer Wehrdienstbeschädigung, einer Gewalttat, eines Unfalles oder eines Impfschadens ist.

Ich habe festgestellt, daß der Datenkatalog des § 301 SGB V der an die gesetzliche Krankenkasse übermittelt wird, grundsätzlich nicht ausreicht, in Zweifelsfällen die sachliche Zuständigkeit des örtlichen bzw. des überörtlichen Sozialhilfeträgers zu begründen. Die Kenntnis von Epikrisen, Behandlungs- sowie Entlassungsberichten oder gar einer kompletten Krankenakte ist für die Feststellung der Zuständigkeit zur Durchführung der Aufgaben des Sozialhilfeträgers jedoch nicht erforderlich. Die genannten Berichte enthalten eine Fülle von Daten, die ein Sozialhilfeträger für die Klärung der Zuständigkeit nicht benötigt. Die Übersendung von kompletten Arztberichten durch das Krankenhaus an einen Sozialhilfeträger ist somit nicht zulässig.

Dies bedeutet jedoch keinesfalls, daß ein Sozialhilfeträger die für seine Zuständigkeitsprüfung erforderlichen Daten nicht erhalten kann. Der Anspruch eines Sozialhilfeträgers an ein Krankenhaus bzw. den Arzt richtet sich auf die Erteilung einer Auskunft zur Feststellung der Leistungspflicht. Dies setzt seitens des Sozialhilfeträgers eine konkrete Fragestellung an das Krankenhaus bzw. den Arzt voraus. Die Fragestellung hat sich im Rahmen des für die Zuständigkeitsprüfung Erforderlichen zu halten. Für die Anforderung dieser Daten zur Klärung der Zuständigkeit ist die Zustimmung eines Patienten nicht erforderlich. § 12 Abs. 2 Nr. 7 HKHG bietet eine ausreichende Rechtsgrundlage für die Übermittlung erforderlicher Daten an den Kostenträger.

Das Sozialamt der Stadt Wiesbaden hat bereits vor einigen Jahren zusammen mit Wiesbadener Kliniken einen Kostenübernahmeantrag für stationäre Krankenhausbehandlung mit zusätzlichen Angaben des Krankenhausarztes für die Zuständigkeitsprüfung entwickelt, der sich weitgehend - so wurde mitgeteilt - bewährt hat. Auch das Landessozialamt Hessen benutzt bereits seit geraumer Zeit für Rückfragen wegen unzureichender Angaben beim Krankenhaus einen Ergänzungsbogen.

Um eine einheitliche, den gesetzlichen Vorgaben entsprechende Verfahrensweise zu erreichen, habe ich den Landeswohlfahrtsverband Hessen in Kassel gebeten, auf der Grundlage des Fragenkatalogs, wie er bereits vom Sozialamt Wiesbaden benutzt wird, einen unter sozialhilferechtlichen Gesichtspunkten zweckmäßigen Vordruck zu entwickeln, der das Verfahren zur Feststellung der sachlichen Zuständigkeit des überörtlichen Sozialhilfeträgers bei nicht krankenversicherten Patienten vereinfachen und gleichzeitig datenschutzrechtlichen Aspekten Rechnung tragen soll. Seit Mitte des Jahres liegt mir der Entwurf des vom Landeswohlfahrtsverbandes Hessen erstellten Vordrucksatzes vor, der nach Auswertung von Änderungs- oder Ergänzungswünschen der örtlichen Sozialämter hessenweit benutzt werden soll. Der Vordrucksatz wurde vom Landeswohlfahrtsverband Hessen in Zusammenarbeit mit dem Magistrat der Stadt Kassel entwickelt. Der Fragenkatalog entspricht den datenschutzrechtlichen Vorgaben und macht - so die Aussage des Landeswohlfahrtsverbandes Hessen - die Anforderung anderer, oder weitergehender ärztlicher Stellungnahmen entbehrlich.

7.6

EDV- und Software-Ausstattung hessischer Gesundheitsämter

Eine mir von der Kommunalen Informationsverarbeitung in Hessen für Testzwecke überlassene Software zum Einsatz in hessischen Gesundheitsämtern kann unter datenschutzrechtlichen Gesichtspunkten empfohlen werden.

Ausgehend von einer Anfrage des Kreisgesundheitsamtes Offenbach zur datenschutzrechtlichen Beurteilung des Softwareprogramms OCTOWARE der Firma easy-soft GmbH in Dresden, das von der Kommunalen Informationsverarbeitung (KIV) in Hessen, Standort Gießen, zum Einsatz in hessischen Gesundheitsämtern angeboten wird, habe ich das Programmpaket geprüft.

Für diese Zwecke hat mir die KIV eine vollständige Programmbeschreibung sowie eine Version der Software für Demonstrationszwecke auf CD-ROM zur Verfügung gestellt.

Die Testversion beinhaltet die Fachmodule meldepflichtige Krankheiten (Tuberkulose-Fürsorge), Kommunalhygiene, Trink- und Badewasser, amtsärztlicher Dienst, Jugend- und jugendzahnärztlicher Dienst, Amtsapotheker sowie den Projekt-Administrator. Jedes Fachmodul stellt eine in sich abgeschlossene Anwendung dar und kann im Gesundheitsamt abteilungsbezogen eingesetzt werden.

Die unter Microsoft Windows NT 4.0 lauffähige Version habe ich auf einem Arbeitsplatzrechner in meiner Dienststelle getestet. Unterstützt hat mich hierbei der Datenschutzbeauftragte des Gesundheitsamtes Wiesbaden, der die Fachmodule und die Systemadministration unter fachlichen Gesichtspunkten als geeignet für den Einsatz im Gesundheitsamt bewertete.

Ich habe im Testlauf der Software und anhand der vorliegenden Programmbeschreibung festgestellt, daß sich die Administration der Nutzer mit dem Modul "Projekt-Administrator"

datenschutzgerecht verwalten läßt. Die einzelnen Fachmodule wie z.B. amtsärztlicher Dienst, sozialpsychiatrischer Dienst oder Bundesseuchengesetz können strikt getrennt den einzelnen Abteilungen eines Gesundheitsamtes zugeordnet werden und hier wiederum können nach dem vorliegenden Rechtenkonzept den jeweiligen Benutzern abgestufte Zugriffs- und Bearbeitungsmöglichkeiten zugewiesen werden.

Im Februar 1998 habe ich Fragen des praktischen Einsatzes des Projekts beim Main-Kinzig-Kreis in Gelnhausen mit dem Datenschutzbeauftragten des Main-Kinzig-Kreises, dem Verwaltungsleiter des Kreisgesundheitsamtes und der Systembetreuerin der KIV Gießen besprochen. Der Datenschutzbeauftragte des Main-Kinzig-Kreises hat mir ein Datenschutzkonzept für den PC-Einsatz im Gesundheitsamt vorgelegt. Das Konzept ist sehr allgemein gehalten und orientiert sich nicht an den spezifischen Eigenschaften der Software oder den besonderen Anforderungen der Tätigkeit eines Gesundheitsamtes im Hinblick auf die Vorschriften des Hessischen Datenschutzgesetzes und der ärztlichen Schweigepflicht i.S.d. § 203 Strafgesetzbuch.

In der Ergänzung des vorliegenden Datenschutzkonzepts ist insbesondere die Umsetzung der technisch möglichen differenzierten Ausgestaltung der Zugriffsrechte darzustellen. Auch wäre, wenn das Projekt administriert wird, in dem Datenschutzkonzept festzulegen, welche Rechte und Zugriffsbefugnisse der Administrator auf personenbezogene Daten hat. Zum Zeitpunkt der Erstellung dieses Berichts verfügte noch kein Gesundheitsamt über eine Komplettversion der Software. Lediglich in einzelnen Abteilungen von Gesundheitsämtern werden bisher Fachmodule eingesetzt.

Die Erstellung eines auf das Projekt abgestimmten Datenschutzkonzepts wurde daher noch nicht realisiert.

8. Internet

8.1

Datenschutzrechtliche Verantwortlichkeit für Internet-Links

Stellen, die auf ihrer Internet-Homepage einen Link auf fremde Dokumente einrichten, sind dafür datenschutzrechtlich nicht verantwortlich.

Im vergangenen Jahr baten mich mehrere Behörden, die eine eigene Homepage betreiben, um ein Gutachten zur datenschutzrechtlichen Verantwortlichkeit für Links im Internet.

8.1.1

Teledienstegesetz oder Mediendienste-Staatsvertrag

Für eine Homepage im Internet kann entweder das Teledienstegesetz (TDG) vom 22. Juni 1997 (BGBl. I S. 1870) oder der Mediendienste-Staatsvertrag (MDStV; GVBl. 1997 S. 135) maßgeblich sein.

§ 2 Abs. 2 Nr. 2 TDG zählt zu den Telediensten Angebote zur Information und Kommunikation, soweit nicht die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht. Als Beispiel für einen Teledienst erwähnt das Gesetz u.a. die Verbreitung von Informationen über Waren- und Dienstleistungsangebote. Die Begründung zum Gesetzentwurf zählt dazu ausdrücklich Homepages (BTDrucks. 13/7385 zu Nr. 2 S. 19). Richtet sich der Informationsdienst (die Homepage) an die Allgemeinheit, d.h. eine beliebige Öffentlichkeit, und stehen nicht der individuelle Leistungsaustausch oder die reine Datenübermittlung im Vordergrund, handelt es sich gem. § 2 Abs. 2 Nr. 4 Mediendienste-Staatsvertrag um einen als Mediendienst zu wertenden Abrufdienst. Das trifft beispielsweise

zu, wenn eine Behörde auf einer Homepage Tätigkeitsberichte zum Abruf bereithält.

8.1.2

Vermittlung fremder Inhalte

Sowohl § 5 Abs. 3 TDG als auch der weitgehend gleichlautende § 5 Abs. 3 MDStV zeichnen Anbieter von der Verantwortung für fremde Inhalte, zu denen sie lediglich den Zugang zur Nutzung vermitteln, frei.

§ 5 Abs. 3 TDG

Diensteanbieter sind für fremde Inhalte, zu denen sie lediglich den Zugang zur Nutzung vermitteln, nicht verantwortlich. Eine automatische und kurzzeitige Vorhaltung fremder Inhalte aufgrund Nutzerabfrage gilt als Zugangsvermittlung.

§ 5 Abs. 3 MDStV

Anbieter sind für fremde Inhalte, zu denen sie lediglich den Zugang zur Nutzung vermitteln, nicht verantwortlich. Eine automatische und kurzzeitige Vorhaltung fremder Inhalte aufgrund Nutzerabfrage gilt als Zugangsvermittlung. § 18 Abs. 3 bleibt unberührt.

Mit Vermitteln ist hier nicht nur der rein telekommunikationstechnische Vorgang gemeint, wie beispielsweise bei Internet-Zugangsdiensten. Im streng technischen Sinne ist der Link auf einer Homepage keine Vermittlung, da nicht der Link, sondern das Brauser-Programm des Nutzers und dessen Internet-Provider die Verbindung zu dem fremden Dokument herstellen. Der Link liefert aber dem Nutzer die Internet-Adresse

des neuen Dokuments und läßt sich insofern als Vermittlung des Zugangs zur Nutzung ansehen. Nach dem Willen des Gesetzgebers soll ein Diensteanbieter, der fremde Inhalte lediglich zum Nutzer durchleitet, ohne auf sie Einfluß nehmen zu können, nicht für diese Inhalte eintreten müssen. Der Tele- oder Mediendienste-Anbieter wird in diesem Fall gleichgestellt mit dem Anbieter von Telekommunikationsdienstleistungen. Der Inhaber einer Homepage wird durch den bloßen Hinweis auf Inhalte, die von anderen Anbietern bereitgehalten werden, nicht für diese fremden Inhalte verantwortlich.

Dagegen ist der Link selbst kein fremder Inhalt. Er ist Inhalt der Homepage, für den der Inhaber der Homepage gem. § 5 Abs. 1 TDG oder § 5 Abs. 1 MDStV verantwortlich ist. Der Link ist jedoch lediglich ein markiertes Wort, das mit einem anderen Dokument in Beziehung steht. Auf der Homepage verbirgt sich hinter dem markierten Wort nur die Adresse eines anderen Dokuments, das erscheint, wenn das Wort angeklickt wird. Datenschutzrechtlich ist die Quellenangabe selbst daher in der Regel bedeutungslos.

8.1.3

Link als Teil des eigenen Informationsangebots

Nur wenn der Inhaber der Homepage den Eindruck erweckt, daß er den Inhalt, auf den der Link verweist, als Teil des eigenen Informationsangebotes verstanden wissen will, kommt eine Verantwortung in Frage. Die Rechtsfolgen bestimmen sich in diesem Fall gem. § 5 Abs. 1 TDG und § 5 Abs. 1 MDStV nach den allgemeinen Gesetzen.

§ 5 Abs. 1 TDG

Diensteanbieter sind für eigene Inhalte, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich.

§ 5 Abs. 1 MDStV

Anbieter sind für eigene Inhalte, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich.

Zu diesen zählen auch die allgemeinen Datenschutzgesetze. Das Hessische Datenschutzgesetz (HDSG) gilt jedoch nicht für personenbezogene Daten, solange sie in allgemein zugänglichen Quellen gespeichert sind (§ 3 Abs. 5). Die auf einem Web-Server zur Nutzung bereitgehaltene Homepage ist eine solche Datenquelle. Damit ist z.B. für die Schadensersatzhaftung des Inhabers der Homepage, auf welcher der Link gesetzt wurde, nicht die Haftungsregelung des § 20 HDSG, die eine Gefährdungshaftung vorschreibt, maßgeblich, sondern das allgemeine Haftungsrecht.

Das allgemeine Datenschutzrecht paßt nicht auf einen Sachverhalt wie das Einrichten eines Links. Die Rechte und Pflichten des Bundesdatenschutzgesetzes (BDSG) knüpfen an die "speichernde Stelle" und die des Hessischen Datenschutzgesetzes an die "datenverarbeitende Stelle" bzw. an den Träger der datenverarbeitenden Stelle an. Unter datenverarbeitender Stelle versteht § 2 Abs. 3 HDSG eine Stelle, welche personenbezogene Daten für sich selbst verarbeitet oder durch andere für sich verarbeiten läßt. Entscheidend ist, ob eine Verfügungsgewalt über die Daten besteht. Wer auf fremde Datenbestände verweist, sei es indirekt oder direkt, gewinnt dadurch keine Verfügungsgewalt über diese Daten. Das wird daran deutlich, daß er den fremden Inhalt nicht beeinflussen kann. Er kann die Daten weder berichtigen, noch sperren oder löschen. Diese datenschutzrechtlichen Pflichten kann nur erfüllen, wer die Verfügungsgewalt hat.

8.1.4

Unterlassungspflicht

Das bedeutet freilich nicht, daß ohne nähere Prüfung des Inhalts, auf den verwiesen werden soll, Links gesetzt werden dürfen. § 5 Abs. 4 stellt klar, daß die aus dem öffentlichen Recht wie dem Zivilrecht resultierenden Verpflichtungen der Diensteanbieter, Rechtsgutverletzungen zu unterlassen, in jedem Falle gelten.

§ 5 Abs. 4 TDG

Verpflichtungen zur Sperrung der Nutzungen rechtswidriger Inhalte nach den allgemeinen Gesetzen bleiben unberührt, wenn der Diensteanbieter unter Wahrung des Fernmeldegeheimnisses gem. § 85 des Telekommunikationsgesetzes von diesen Inhalten Kenntnis erlangt und eine Sperrung technisch möglich und zumutbar ist.

In einer Homepage darf daher nicht bewußt auf einen rechtswidrigen fremden Inhalt verwiesen werden. Das Teledienstegesetz verlangt jedoch von demjenigen, der einen Link eingerichtet hat, nicht, daß er den fremden Inhalt auf spätere Änderungen, die zur Rechtswidrigkeit geführt haben könnten, überprüft.

Fazit: Es besteht zwar keine datenschutzrechtliche Verantwortlichkeit für Links, eine eventuelle strafrechtliche, zivilrechtliche oder auch urheberrechtliche Verantwortlichkeit bleiben davon jedoch unberührt.

8.2

Orientierungshilfe Internet

Die Orientierungshilfe Internet der Datenschutzbeauftragten des Bundes und der Länder ist aktualisiert worden.

Bereits im 24. Tätigkeitsbericht (Ziff. 17.2) und im 25. Tätigkeitsbericht (Ziff. 21.8 und Ziff. 22) habe ich mich mit der Thematik "Internet" auseinandergesetzt; die dort getroffenen Aussagen sind weiterhin gültig. Das Internet ist auf einem Siegeszug durch die öffentliche Verwaltung. Die Chancen des Internets werden genutzt. Durch neue Technologien sind allerdings neue Risiken hinzugekommen. Der Gesetzgeber hat darauf mit dem Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (IuKDG) reagiert. Eine Reihe juristischer Fragen, die sich im Zusammenhang mit der Anwendung des Gesetzes stellen, sind freilich noch unbeantwortet.

Wegen der neuen Technologien mußte die „Orientierungshilfe für den Anschluß der öffentlichen Verwaltung an das Internet“ (Stand 12.95) aktualisiert werden. Eine Arbeitsgruppe des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ der Datenschutzbeauftragten des Bundes und der Länder“, in der ich durch eine Mitarbeiterin vertreten war, hat sich dieser Aufgabe angenommen. Die aktuelle Fassung ist im Anhang 2 abgedruckt. Die Orientierungshilfe erhielt eine neue Struktur. Sie ist nun wie folgt aufgebaut:

1. Einleitung
2. Vorbereitung und Planung
3. Firewall-Systeme
4. Auswahl und Umsetzung der Sicherungsmaßnahmen;
Betriebsphase
5. Ausblick
6. Anhang

Besonderes Augenmerk wurde auf das Kapitel 2.3 „Sicherheitsrisiken und Schutzmaßnahmen“ gelegt. Für alle dort

beschriebenen Sicherheitsrisiken werden entsprechende Schutzmaßnahmen angeboten. Das Kapitel „Aktive Elemente/Aktive Inhalte“ ist neu und verdient besondere Aufmerksamkeit. Es beschäftigt sich mit Java, JavaScript, ActiveX, Plug Ins und Cookies. In Kapitel 3 werden Firewall-Systeme beschrieben. Die Auswahl und die Umsetzung der Sicherungsmaßnahmen sowie die Bedingungen und die Voraussetzungen für die Betriebsphase werden in Kapitel 4 definiert.

9. Entwicklungen im Bereich der Technik

PERKEO - Programm zur Identifizierung strafrechtlich relevanter Darstellungen

Je nach Anwendungsbereich sind beim Einsatz des Suchprogramms PERKEO in der Landesverwaltung unterschiedliche Anforderungen zu beachten.

Das Hessische Landeskriminalamt bietet das Programm den Stellen der Landesverwaltung kostenlos für den Einsatz im Systemverwalterbereich an. Gegenüber dem Landesautomationsausschuß habe ich mich deshalb zu den datenschutzrechtlichen Nutzungsvoraussetzungen geäußert.

9.1

Funktionsweise des Programms

Mit dem von einem Mitarbeiter des Landeskriminalamtes entwickelten Programm können strafrechtlich relevante Darstellungen in DV-Anlagen durch einen automatischen Suchlauf aufgespürt werden. Es arbeitet im Prinzip wie ein Virens scanner. Das Programm durchsucht, ausgehend von einem vorgegebenen Startverzeichnis, alle Dateien, die in diesem Verzeichnis und seinen Unterverzeichnissen gespeichert sind. Dabei wird für jede Datei ein Hash-Wert gebildet und mit Referenzwerten abgeglichen, die in einer vom Landeskriminalamt zur Verfügung gestellten Prüfdatei vorgegeben sind. Bei einem Treffer wird die Datei in einer Trefferliste angezeigt.

Die Verfahrensbeschreibung nennt als Anwendungsbereiche Universitäten, Fachhochschulen, Schulen mit Internet-Zugang, Internet-Provider, Mailboxen, Firmennetze, CD-ROMs und lokale PC. Je nach Anwendungsbereich außerhalb der Strafverfolgung

gelten für den Einsatz eines solchen Suchprogramms unterschiedliche Zulässigkeitsvoraussetzungen.

9.2

Keine Kontrollpflicht der Betreiber von Rechnernetzen

Das Landeskriminalamt geht davon aus, daß Betreiber von Rechnernetzen (Systemverwalter, Internet-Provider, Mailboxbetreiber) verpflichtet sind, ihre Datenbestände regelmäßig hinsichtlich strafbarer Dateien zu kontrollieren. Diese Auffassung teile ich nicht. Für Teledienste hat der Gesetzgeber mit § 5 Teledienstegesetz (TDG) eine sehr differenzierte (strafrechtliche) Verantwortlichkeit geschaffen (s. hierzu auch Ziff. 8.1).

Nach den allgemeinen Gesetzen uneingeschränkt verantwortlich ist lediglich der Diensteanbieter, der eigene Inhalte zur Nutzung bereitstellt (Absatz 1). Hier gilt das Prinzip: Was offline strafbar ist, ist auch online strafbar. Die Verantwortlichkeit für fremde Inhalte, welche Diensteanbieter auf eigenen Rechnern zur Nutzung bereithalten, wird dagegen eingeschränkt. Der Diensteanbieter ist nur dann verantwortlich, wenn er von diesen Inhalten Kenntnis hat und es ihm technisch möglich und zumutbar ist, deren Nutzung zu verhindern (Absatz 2). Völlig freigestellt von strafrechtlicher Verantwortlichkeit wird schließlich der Access-Provider (Absatz 3). Anbieter von Zugangsdiensten zu Datennetzen machen sich nicht strafbar. Das gilt selbst dann, wenn sie sog. Proxyserver einsetzen oder die übermittelten Daten kennen.

Proxyserver sind zur Leitungsentlastung eingesetzte Zwischenspeicher, die häufig aufgerufene Internetseiten kurzfristig speichern, damit sie nicht bei der Originaladresse angefordert werden müssen.

Die Anbieter unterliegen lediglich verschuldensunabhängigen zivilrechtlichen Ansprüchen und verwaltungsrechtlichen Pflichten. Aber auch hier gilt die Einschränkung, daß der Diensteanbieter unter Wahrung des Fernmeldegeheimnisses von den Inhalten Kenntnis erlangt haben muß und eine Sperrung technisch möglich und zumutbar ist (Absatz 4). Access-Provider werden durch diese Regelung den Anbietern von Telekommunikationsdienstleistungen gleichgestellt, denn die Deutsche Telekom AG oder andere Netzbetreiber sind schließlich auch nicht für strafbare Inhalte, die über ihr Netz vermittelt werden, verantwortlich.

§ 5 TDG

(1) Diensteanbieter sind für eigene Inhalte, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich.

(2) Diensteanbieter sind für fremde Inhalte, die sie zur Nutzung bereithalten, nur dann verantwortlich, wenn sie von diesen Inhalten Kenntnis haben und es ihnen technisch möglich und zumutbar ist, deren Nutzung zu verhindern.

(3) Diensteanbieter sind für fremde Inhalte, zu denen sie lediglich den Zugang zur Nutzung vermitteln, nicht verantwortlich. Eine automatische und kurzzeitige Vorhaltung fremder Inhalte auf Grund Nutzerabfrage gilt als Zugangsvermittlung.

(4) Verpflichtungen zur Sperrung der Nutzung rechtswidriger Inhalte nach den allgemeinen Gesetzen bleiben unberührt, wenn der Diensteanbieter unter Wahrung des Fernmeldegeheimnisses gemäß § 85 des Telekommunikationsgesetzes von diesen Inhalten Kenntnis erlangt und eine Sperrung technisch möglich und zumutbar ist.

Dementsprechend haben weder Service-Provider, die fremde Inhalte zur Nutzung bereithalten, noch Access-Provider eine

Kontrollpflicht. Es stellt sich daher die Frage, inwieweit sie trotz fehlender Verpflichtung Inhaltskontrollen vornehmen dürfen.

9.3

Das Fernmeldegeheimnis als Grenze der Kontrollmöglichkeiten

Restriktiv wirkt das Fernmeldegeheimnis, an das auch Anbieter von Telediensten gebunden sind, wenngleich dies im Teledienstegesetz und Teledienstedatenschutzgesetz nicht ausdrücklich geregelt ist. Sowohl § 5 Abs. 4 TDG als auch § 6 Abs. 4 TDDSG setzen voraus, daß Anbieter von Telediensten das Fernmeldegeheimnis zu beachten haben. Dessen Inhalt konkretisiert § 85 Telekommunikationsgesetz (TKG). Danach darf der Diensteanbieter sich über das für die geschäftsmäßige Erbringung des Dienstes erforderliche Maß hinaus keine Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation verschaffen (§ 85 Abs. 3 TKG).

§ 6 Abs. 4 TDDSG

Hat der Diensteanbieter mit einem Dritten einen Vertrag über die Abrechnung des Entgelts geschlossen, so darf er diesem Dritten Abrechnungsdaten übermitteln, soweit es für diesen Zweck erforderlich ist. Der Dritte ist zur Wahrung des Fernmeldegeheimnisses zu verpflichten.

§ 85 Abs. 3 TKG

Den nach Abs. 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Sie dürfen Kenntnisse über Tatsachen, die dem

Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang.

Anbieter von Telediensten dürfen demnach das Suchprogramm PERKEO dort nicht einsetzen, wo sie an das Fernmeldegeheimnis gebunden sind. Das betrifft z.B. den E-Mail-Dienst. Auf einer fremden Homepage, die der Diensteanbieter auf seinem Rechner zur Nutzung bereithält, darf er nur die Bereiche durchsuchen, die allgemein zugänglich sind.

Soweit firmen- und behördeneigene Telekommunikationsnetze den Beschäftigten zur privaten Nutzung zur Verfügung gestellt werden, gilt ebenfalls das Fernmeldegeheimnis (§ 85 Abs. 2 TKG), mit der Folge, daß die privaten Kommunikationsvorgänge (E-Mails) nicht mit dem Suchprogramm kontrolliert werden dürfen.

§ 85 Abs. 2 TKG

Zur Wahrung des Fernmeldegeheimnisses ist verpflichtet, wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

9.4

Kontrollmöglichkeiten bei dienstlich genutzten Rechnern

Für die Verwendung des Suchprogramms auf Netzwerkservern oder auf lokalen PC, die den Beschäftigten für dienstliche Zwecke

zur Verfügung gestellt werden, ist § 34 Abs. 1 Hessisches Datenschutzgesetz (HDSG) maßgeblich.

§ 34 Abs. 1 HDSG

Öffentliche Stellen dürfen Daten ihrer Beschäftigten nur verarbeiten, wenn dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung innerdienstlicher organisatorischer, sozialer und personeller Maßnahmen erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung es vorsieht.

Die Dienststelle hat ein berechtigtes Interesse, daß DV-Anlagen nicht zweckwidrig genutzt werden. Die Speicherung kinder- oder tierpornographischer Darstellungen ist nicht nur ein arbeitsvertraglicher Verstoß und eine Dienstpflichtverletzung, sondern auch eine Straftat. Das Suchprogramm scheint ein geeignetes Mittel zu sein, derartige Verstöße aufzudecken. Wenn die Beschäftigten wissen, daß ein solches Programm verwendet wird, dürfte es zudem eine präventive Wirkung haben. Es ist allerdings nicht angemessen, das Programm ständig einzusetzen, zumal damit dem Systemverwalter ein permanenter Zugriff zu allen Speicherbereichen ermöglicht werden müßte. Dies würde auch für lokale Festplatten gelten, auf die der Systemverwalter nicht zugreifen können muß. Bei einzelnen Arbeitsplatzrechnern dürfen nur Stichprobenkontrollen durchgeführt werden.

Dabei wären folgende Bedingungen zu berücksichtigen:

- Die Anwender müssen über die Möglichkeit des Einsatzes des Suchprogramms informiert werden.
- Es darf nur die vom Landeskriminalamt zur Verfügung gestellte Prüfdatei bei den Kontrollen benutzt werden.

- Die Kontrolle eines Arbeitsplatzrechners sollte grundsätzlich im Beisein des Nutzers durchgeführt werden. Für die Kontrolle eines Servers muß das Vier-Augen-Prinzip gelten.
- Es muß schriftlich festgelegt werden, wie bei angezeigten Treffern zu verfahren ist.

Das Landeskriminalamt wird auf meine Bitte in einem Merkblatt auf die rechtlichen Nutzungsvoraussetzungen des Suchprogramms hinweisen.

10. Forschung

Datenschutz und Forschung – kontroverse Diskussionen

Datenschutzrechtliche Regelungen im Bereich der Forschung sind in den letzten Jahren immer wieder kritisiert worden. Eine Analyse der Kritik ergibt ein sehr differenziertes Bild der Ursachen. Als Vorsitzender des Arbeitskreises Wissenschaft der Konferenz der Datenschutzbeauftragten habe ich mich auch in diesem Jahr für einen verstärkten Dialog zwischen den Forscherinnen und Forschern und den Datenschutzbeauftragten eingesetzt.

10.1

Kritik am Datenschutz und ihr Hintergrund

Forschung und Datenschutz stehen seit jeher in einem Spannungsverhältnis zueinander. Beide Rechtspositionen sind im Grundgesetz verfassungsrechtlich gewährleistet (Art. 5 Abs. 3 und Art. 2 Abs. 1 i.V.m. Art. 1 Grundgesetz). Sie können bei Forschungsvorhaben, für die personenbezogene Daten benötigt werden, miteinander in Konflikt geraten. Es steht außer Frage, daß für wissenschaftliche Forschungsvorhaben personenbezogene Daten - zumindest vorübergehend - vielfach unentbehrlich sind. Die verfassungsrechtliche Gewährleistung der Forschung erschöpft sich daher auch nicht in ihrer Funktion als Abwehrrecht gegen staatliche Eingriffe. Als objektive Wertentscheidung verpflichtet sie den Staat darüber hinaus, einer Aushöhlung der Forschungsfreiheit vorzubeugen und die tatsächlichen Voraussetzungen der Forschungsfreiheit sicherzustellen. Zu den tatsächlichen Voraussetzungen der Forschung zählt auch das Recht auf Zugang zu den personenbezogenen Daten, die tatsächlich für die Durchführung der Forschung benötigt werden und auf andere Weise nicht erlangt werden können. Die Durchführung von Forschungsvorhaben kommt letztlich auch wieder der Bürgerin und dem Bürger zugute.

Wissenschaftliche Zielsetzungen können allerdings keine pauschale Ausnahme vom Persönlichkeitsschutz rechtfertigen. Es ist in erster Linie Aufgabe des Gesetzgebers, den potentiellen Grundrechtskonflikt so zu regeln, daß beide Grundrechte möglichst weitgehend realisiert werden. Konkret bedeutet dies, daß der Gesetzgeber die rechtlichen Rahmenbedingungen für die Forschung mit personenbezogenen Daten durch die Normierung der inhaltlichen Voraussetzungen sowie durch Verfahrensregelungen, Zweckbindungs- und Löschungsgebote etc. konkret festlegen muß. Auch die EG-Datenschutzrichtlinie verlangt ein Tätigwerden des Gesetzgebers. Nach Art. 6 Abs. 1, Art. 8 Abs. 4 der Richtlinie ist z.B. eine Zweckentfremdung bei öffentlichen Stellen vorhandener personenbezogener Daten zu wissenschaftlichen Zwecken möglich, sofern die Mitgliedsstaaten "geeignete Garantien" bzw. "besondere Garantien" für den Persönlichkeitsschutz vorsehen.

Wie das Verhältnis von Datenschutz und Forschung im Einzelnen festzulegen ist, darüber hat es allerdings immer wieder kontroverse Diskussionen gegeben. So kritisierte z.B. die Deutsche Forschungsgemeinschaft in ihrer Denkschrift von 1996 zum Thema "Forschungsfreiheit - Ein Plädoyer für bessere Rahmenbedingungen in Deutschland" - in einem Kapitel zum Datenschutz insbesondere zu restriktive Rechtsinterpretationen, zu enge Zweckbindungsregelungen und zu aufwendige und inhaltlich und problematische Zustimmungs- und Genehmigungserfordernisse. In einzelnen Publikationen wurden immer wieder pauschale Vorwürfe laut wie z.B. "im Datenschutz bestehen unverantwortbare Blockaden medizinischer Forschung", "Datenschutz treibt Forscher ins Ausland", "Epidemiologie wird durch Datenschutzhysterie behindert", "Datenschutz macht Forschung mit Personaldaten unmöglich" etc.

Eine von mir vorgenommene Analyse der Kritiken ergibt ein sehr unterschiedliches Bild ihres jeweiligen Hintergrundes:

- Bisweilen waren den Kritikern des Datenschutzes die Regelungen weitgehend unbekannt und die rechtlichen Aussagen schlicht falsch. Auch in der Denkschrift der Deutschen Forschungsgemeinschaft waren zum Teil die zu diesem Zeitpunkt geltenden datenschutzrechtlichen Bestimmungen, die weitgehende Möglichkeiten des Zugangs der Wissenschaft zu personenbezogenen Daten zum Inhalt hatten, in die Stellungnahme nicht einbezogen worden. Nachfragen zu einzelnen kritischen Zeitungsartikeln ergaben, daß die Kritik der Verfasser sich zum Teil ausschließlich auf - nicht zutreffende - Vermutungen bezüglich der rechtlichen Schwierigkeiten des Datenzugangs stützte. Eine konkrete Untersuchung des Umfangs der tatsächlichen Probleme hatte nicht stattgefunden.
- Zum Teil wurden sehr unterschiedliche Fragen in unangemessener Weise zu einer Pauschalkritik "am Datenschutz" vermengt, so daß die unterschiedlichen Ursachen der kritisierten Probleme nicht hinreichend deutlich und damit auch evtl. Problemlösungen erschwert wurden. Bei den Diskussionen wurden insbesondere Fragen des angemessenen Inhalts von Zugangsregelungen für die Forschung, der Auslegung der Regelungen durch Verwaltungsbehörden - die gelegentlich Datenschutz auch als Vorwand vorschoben -, und des fehlenden Tätigwerdens des Gesetzgebers vermengt. Wenn etwa Forscherinnen und Forscher mit personenbezogenen Daten forschen wollen, so bedarf es insbesondere auch aus verfassungsrechtlichen Gründen einer konkreten gesetzlichen Regelung des Zugangs zu den Daten für Forschungszwecke. Wenn entsprechende Regelungen vom Gesetzgeber nicht geschaffen werden, so ist der Zugang zu den Daten rechtlich nicht möglich. Auch die Datenschutzbeauftragten können ihn

in diesem Fall - auch wenn sie ihn grundsätzlich als angemessen ansehen - nicht ermöglichen. Pauschale Kritik am Datenschutz bzw. an den Datenschutzbeauftragten ist in diesem Fall irreführend und wenig hilfreich. Ein Beispiel hierfür ist der in den letzten Jahren vielfach erhobene Vorwurf, daß Datenschutz die Ahnenforschung unmöglich macht. Es erreichten mich auch eine Reihe von Beschwerden von Bürgerinnen und Bürgern, die von Standesämtern zur Erforschung ihrer Familiengeschichte mit einem pauschalen Hinweis auf Datenschutz keine Informationen aus den Personenstandsregistern erhielten. Die Ablehnung der Auskünfte durch die Standesämter beruhte jedoch auf einer Bestimmung des Personenstandsgesetzes, das 1957, also vor Beginn der datenschutzrechtlichen Diskussionen, verabschiedet wurde. Das verfassungsrechtlich gewährleistete Recht auf informationelle Selbstbestimmung läßt durchaus auch andere gesetzliche Regelung des Zugangs zu den Personenstandsbüchern zu. Im Rahmen der Diskussion über eine Novellierung des Personenstandsgesetzes habe ich mich für eine Öffnung der Bücher auch für die Ahnenforschung eingesetzt (s. hierzu auch 25. Tätigkeitsbericht, Ziff. 11.1). Der Bundesgesetzgeber hat eine entsprechende Gesetzesänderung immer noch nicht vorgenommen.

- Die - teilweise divergierenden - datenschutzrechtlichen Regelungen auf Landes-, Bundes- und europäischer Ebene sind für die Wissenschaftlerinnen und Wissenschaftler nicht immer einfach nachzuvollziehen. Hier bedarf es verbesserter Fortbildungs- und Informationsangebote für die Forscher - auch bereits im Rahmen der Ausbildung. Forscher müssen auch - ebenso wie andere Personen, die personenbezogene Daten verarbeiten - bereit sein, sich mit den datenschutzrechtlichen Rahmenbedingungen der Verarbeitung personenbezogener Daten auseinanderzusetzen.

- Angesichts der vielfältigen Kritik bedarf auch die Frage, inwieweit durch die derzeitigen gesetzlichen Regelungen das Ziel einer angemessenen Zuordnung von Forschungsfreiheit einerseits und Datenschutz andererseits erreicht wurde und in welchen Punkten die Regelungen der Weiterentwicklung bedürfen, der Diskussion. Ein zentrales Thema ist etwa die Frage, inwieweit die gegenwärtigen Regelungen zur Zweckbindung der dem Forscher zur Verfügung gestellten Daten bzw. ihre Interpretation der wissenschaftlichen Tätigkeit gerecht werden, denn wissenschaftliche Fragestellungen können sich im Rahmen eines Forschungsprojekts erweitern und verändern. Je umfassender allerdings der Forscher personenbezogene Daten ohne konkrete Eingrenzung des Zwecks verwenden oder aufbewahren will, desto dringlicher stellt sich u.a. die Frage, wie die beim Forscher vorhandenen personenbezogenen Daten vor dem Zugriff durch Dritte geschützt werden können. Während z.B. Patientendaten, die sich beim behandelnden Arzt befinden, der ärztlichen Schweigepflicht i.S.v. § 203 Strafgesetzbuch unterliegen und in der Strafprozeßordnung durch ein Zeugnisverweigerungsrecht des Arztes und Beschlagnahmeverbot geschützt sind, existiert ein vergleichbarer Schutz der Daten im wissenschaftlichen Bereich nicht. Es gibt kein "Forschungsgeheimnis", das Dritten den Zugriff auf die Daten verwehrt. An der gesetzlichen Regelung eines sog. Forschungsgeheimnisses haben daher Wissenschaftler und Datenschützer gleichermaßen Interesse.

10.2

Gemeinsame Diskussionen von Forscherinnen und Forschern und Datenschutzbeauftragten

Vor dem Hintergrund der kontroversen Diskussionen habe ich als für den Arbeitskreis Wissenschaft der Konferenz der

Datenschutzbeauftragten des Bundes und der Länder zuständiger Datenschutzbeauftragter zunächst 1997 ein Gespräch zwischen der Deutschen Forschungsgemeinschaft und den Datenschutzbeauftragten über die aktuellen datenschutzrechtlichen Rahmenbedingungen in der Forschung initiiert. Das Gespräch war wohl nach Auffassung aller Teilnehmer eine gute Grundlage zum besseren Verständnis der gegenseitigen Gesichtspunkte. Deutlich wurde in dem Gespräch auch, daß datenschutzrechtliche Kontroversen durch das Problem der Wissenschaftsorganisation verursacht sein können. Die Wissenschaft muß ihre Interessen im Rahmen von Gesetzgebungsverfahren klar artikulieren, begründen und zur Diskussion stellen. Dies ist in der Vergangenheit nicht immer erfolgt. Wenn Gesetze verabschiedet werden, die die Interessen der Forschung nicht hinreichend berücksichtigen, sind Probleme schwierig zu lösen.

In diesem Jahr wurden zwischen der Deutschen Arbeitsgemeinschaft für Epidemiologie und dem Arbeitskreis Wissenschaft der Datenschutzbeauftragten aktuelle datenschutzrechtliche Fragen aus dem Bereich der Epidemiologie diskutiert. Die Ergebnisse der Diskussionen sind in einem gemeinsamen Arbeitspapier "Epidemiologie und Datenschutz" (s. Ziff. 29) zusammengestellt, das als Hilfestellung für die datenschutzgerechte Durchführung von Forschungsprojekten allen Interessierten zur Verfügung gestellt wird.

Angesichts der vielfältigen Fragestellungen habe ich auch "Forschung und Datenschutz" zum Thema des gemeinsamen, vom Präsidenten des Hessischen Landtags und mir am 18. Juni 1998 im Plenarsaal des Hessischen Landtags veranstalteten 7. Wiesbadener Forums Datenschutz gemacht. Im Rahmen des Forums wurden aktuelle, nationale und internationale datenschutzrechtliche Aspekte aus verschiedenen Forschungsbereichen aus unterschiedlichen Perspektiven dargelegt und diskutiert (s. auch

Hamm/Möller (Hrsg.), Datenschutz und Forschung, Baden-Baden 1999).

Im Rahmen des diesjährigen Wiesbadener Forums Datenschutz kam u.a. auch das von den Professoren Hauser, Wagner und Zimmermann 1998 verfaßte Memorandum "Erfolgsbedingungen empirischer Wirtschaftsforschung und empirisch gestützter wirtschafts- und sozialpolitischer Beratung" zur Sprache, das neben grundsätzlichen Fragen der künftigen Aufgabenwahrnehmung der amtlichen Statistik auch datenschutzrechtliche Fragen des Zugangs von Wissenschaftlern zu statistischen Daten beinhaltet. Das Memorandum hat in der Öffentlichkeit erhebliche Aufmerksamkeit gefunden. Auf Anregung von Professor Wagner habe ich im November 1998 eine gemeinsame Diskussion des Arbeitskreises Wissenschaft der Konferenz der Datenschutzbeauftragten mit Professor Wagner sowie u.a. dem Präsidenten des Statistischen Landesamts initiiert. Gegenstand der gemeinsamen Diskussion waren einerseits die rechtlichen Rahmenbedingungen und die Rechtsprechung des Bundesverfassungsgerichts zur Geheimhaltung statistischer Daten, andererseits wurden die grundsätzlichen Möglichkeiten erörtert, die im Memorandum angesprochenen Probleme des Zugangs der Wissenschaft zu den statistischen Daten zu lösen, z.B. die Integration der Wissenschaftler in Statistischen Ämtern, die Erstellung von Mikrodatenfiles mit faktisch anonymisierten Daten für die Wissenschaft durch die Statistischen Ämter, die Durchführung von Sonderauswertungen durch die Statistischen Ämter im Auftrag der Wissenschaft und verstärkte eigene Auswertungen der Daten bzw. die Übernahme von Forschungsaufträgen durch die Statistischen Ämter (s. auch Metschke/Wellbrock, Allgemeines Statistisches Archiv, Heft 1, 1999).

10.3

Neufassung des § 33 HDSG

Auf Grund der vorangegangenen Diskussionen zum Thema "Datenschutz und Forschung" habe ich eine Änderung der Forschungsregelung in dem Hessischen Datenschutzgesetz vorgeschlagen, die vom Gesetzgeber entsprechend verabschiedet wurde (§ 33, s. Ziff. 27). Mein Änderungsvorschlag umfaßte neben einigen Präzisierungen im Detail vor allen Dingen eine wichtige inhaltliche Änderung der Bestimmung. Nach dem alten Hessischen Datenschutzgesetz war eine Verarbeitung zu Forschungszwecken ohne Einwilligung des Betroffenen nur dann zulässig, wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Betroffenen *erheblich* überwiegt und der *Zweck der Forschung nicht auf andere Weise erreicht werden kann*. In der Neufassung ist zum einen das Erfordernis "erheblich" gestrichen worden. Das Grundgesetz gewährleistet das Gesetz auf informationelle Selbstbestimmung als Bestandteil des allgemeinen Persönlichkeitsrechts i.S.v. Art. 2 i.V.m. Art. 1 Grundgesetz (GG). Ebenso gewährleistet das Grundgesetz die Freiheit von Wissenschaft und Forschung in Art. 5 GG. Diese beiden Grundrechte sind grundsätzlich gleichwertig und evtl. Konflikte zwischen den beiden Grundrechten sind so zu regeln, daß beide Grundrechte möglichst weitgehend realisiert werden können. Vor diesem verfassungsrechtlichen Hintergrund ist die Neuformulierung adäquater. In der Praxis in Hessen sind diese verfassungsrechtlichen Aspekte bereits bei der Interpretation der bisherigen Formulierung berücksichtigt worden. Zum anderen ist eine Verarbeitung zu Forschungszwecken ohne Einwilligung des Betroffenen jetzt auch dann zulässig, wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Betroffenen überwiegt und die Forschung ohne personenbezogene Daten einen unverhältnismäßigen Aufwand verursachen würde. Die Praxis hat gezeigt, daß eine ergänzende Festlegung dieser Ausnahme im Interesse der Forschung notwendig und auch angemessen ist.

11. Ausländer

11.1

Gesetz zur Änderung des Ausländerzentralregisters und zur Errichtung einer Warndatei

Ein Entwurf des Bundesministeriums des Innern zur Änderung des Ausländerzentralregistergesetzes sah eine Ausweitung des Umfangs der gespeicherten Daten, eine Erweiterung der zugriffsberechtigten Stellen und den Aufbau einer Warndatei vor. Zu den vorgesehenen Änderungen habe ich eine kritische Stellungnahme abgegeben.

Mitte Dezember 1997 wurden Pläne des Bundesministeriums des Innern zur Novellierung des Ausländerzentralregistergesetzes bekannt. In meiner Stellungnahme gegenüber dem Hessischen Ministerium des Innern und für Landwirtschaft, Forsten und Naturschutz habe ich an Teilen des Gesetzentwurfs Kritik geübt. Die wichtigsten Änderungen waren folgende:

- Hinzukommen sollte, daß auch Angaben zu solchen Ausländerinnen oder Ausländern im AZR gespeichert werden, die kurzfristig zu einem Besuch einreisen wollen und zu diesem Zweck eine sog. Verpflichtungserklärung eines Dritten benötigen. Gemeint ist damit, daß sich eine dritte Person zur Übernahme der Lebenshaltungskosten während des Aufenthalts in Deutschland verpflichtet.
- Auch bei der Anzahl der Behörden, die auf das Register zugreifen können, war eine einschneidende Änderung vorgesehen. Neben dem bisher schon vorgesehenen Zugriff u.a. der Polizeibehörden, Staatsanwaltschaften, Gerichte, Nachrichtendienste sollte nun auch ein Anschluß für die Träger der Sozialhilfe bzw. die nach dem Asylbewerberleistungsgesetz zuständigen Behörden eingerichtet werden.

Ich habe gegenüber dem Hessischen Ministerium des Innern und für Landwirtschaft, Forsten und Naturschutz darauf hingewiesen, daß das Ausländerzentralregistergesetz damit wiederum eine neue Funktion erhalte. Bisher hatte das Register die Aufgabe, die Ausländerbehörden bei ihrer Arbeit zu unterstützen sowie den Sicherheitsbehörden, insbesondere bei der Kriminalitätsbekämpfung, zur Verfügung zu stehen.

Nach den neuen Bestimmungen sollte das Register auch ökonomischen Interessen dienen, nämlich die Sozialbehörden bei der Geltendmachung von Erstattungsansprüchen und bei der Verhinderung rechtswidriger Inanspruchnahme von Leistungen unterstützen. Ich habe bereits bei den geltenden Bestimmungen des Ausländerzentralregistergesetzes Bedenken gegen die Nutzung des Datenbestands für unterschiedliche Zwecke geäußert: Informationen aus den verschiedensten Lebensbereichen eines Menschen werden zusammengeführt und für unterschiedliche Interessenten - neben den Ausländerbehörden auch die Sicherheitsbehörden - bereitgehalten. Der Betroffene kann gar nicht mehr überblicken, in welchem Zusammenhang die zu einem bestimmten Zweck über ihn erhobenen Daten demnächst verwandt werden. Träte jetzt - wie im Gesetzentwurf vorgesehen - eine weitere Funktion des Registers hinzu, nämlich die Geltendmachung ökonomischer Interessen, würden meine Bedenken gegen die sog. Multifunktionalität des Registers noch verstärkt.

- Vorgesehen war im Gesetzentwurf weiterhin, daß in einer neu aufzubauenden "Warndatei" Personen und Organisationen, die für eine Ausländerin oder einen Ausländer eine sog. Verpflichtungserklärung abgegeben haben, unter bestimmten Voraussetzungen gespeichert werden sollen. Geplant war eine Speicherung u.a. auch dann, wenn der Betroffene - auch aus nicht von ihm zu vertretenden Gründen - seiner Verpflichtung bei Inanspruchnahme nicht nachkommen konnte oder wenn

der eingeladene Ausländer nach der Einreise einen Asylantrag stellte.

Gegen eine derartige Regelung, die die Aufnahme von Daten zu einer Person in eine Datei von dem Verhalten eines Dritten abhängig macht oder von Umständen, auf die der Betroffene keine Einwirkungsmöglichkeiten hat, habe ich massive Bedenken geäußert. Der Eingriff in das Recht auf informationelle Selbstbestimmung, der mit der Einstellung von Daten in eine Datei verbunden ist, kann nicht dadurch gerechtfertigt werden, daß ein Dritter beispielsweise einen Asylantrag stellt - eine nach unserer Rechtsordnung vorgesehene legale Handlung.

- In die Warndatei sollten ebenfalls Daten von Personen eingestellt werden, die wegen bestimmter Straftaten nach dem Ausländergesetz verurteilt wurden oder bei denen Anhaltspunkte für den Verdacht bestehen, daß sie eine solche Straftat planen, begehen oder begangen haben.

Unklar erschien mir, welche Kriterien zugrunde gelegt werden sollten, damit man von dem Verdacht auf Planung bzw. die bevorstehende Begehung der Straftaten ausgehen kann. Ich habe gegenüber dem Hessischen Ministerium des Innern und für Landwirtschaft, Forsten und Naturschutz darauf hingewiesen, daß die mangelnde Konkretheit der Formulierung dazu führt, daß eine große Anzahl von Bürgerinnen und Bürgern, die sich nichts haben zuschulden kommen lassen, in die Datei aufgenommen würde. Ein derartiger Eingriff in das Recht auf informationelle Selbstbestimmung, der auf bloßen Einschätzungen, Prognosen und nicht verifizierbaren Anhaltspunkten beruht, sei nach meiner Auffassung nicht vertretbar.

Viele meiner Kollegen haben sich gegenüber den zuständigen Behörden in ähnlicher Weise geäußert.

Nach meinen Informationen wird der Gesetzentwurf vom Bundesministerium des Innern nicht weiter verfolgt.

11.2

Verpflichtungserklärung von Gastgebern ausländischer Bürgerinnen und Bürger

Ausländer, die sich in Deutschland aufhalten wollen, müssen unter bestimmten Voraussetzungen die Erklärung eines Dritten vorlegen, in der dieser sich verpflichtet, für den Lebensunterhalt des Ausländers aufzukommen. Bei dieser Erklärung wurden deutliche datenschutzrechtliche Verbesserungen erreicht.

Wenn die Sicherung des Lebensunterhalts aus eigenen Mitteln Voraussetzung für die Gewährung des Aufenthaltsrechts ist und der Ausländer diese Voraussetzung nicht selbst erfüllen kann, ist für die Gewährung eines derartigen Rechts eine sog.

Verpflichtungserklärung eines Dritten nach § 84 Ausländergesetz (AuslG) erforderlich. Darin verpflichtet sich der Dritte, für die Kosten des Lebensunterhalts des Ausländers aufzukommen, und er muß, wenn er hierzu nicht in der Lage ist, die Zwangsvollstreckung in sein Vermögen dulden.

Vorgaben für die Ausgestaltung und das Verfahren der Verpflichtungserklärung schrieb ein Erlaß des Bundesministeriums des Innern aus dem Jahr 1996 vor. Darin wurden u.a. detaillierte Angaben des Gastgebers zu seinen Einkommens- und Vermögensverhältnissen sowie den Arbeits- und Wohnverhältnissen verlangt. Vom Verfahren her war vorgesehen, daß der ausländische Bürger ein Exemplar des Formulars erhielt und verpflichtet war, diese Unterlage z.B. bei der Visumsbeantragung oder beim Grenzübertritt vorzuzeigen. Auf diese Weise erhielten sowohl der einzuladende Ausländer als auch andere Stellen Kenntnis von detaillierten Daten des Gastgebers.

In der Folge beschwerte sich eine ganze Reihe von Bürgern bei mir. Sie kritisierten die undifferenzierte Datenerhebung zur Überprüfung ihrer finanziellen Leistungsfähigkeit im Rahmen ihrer Verpflichtungserklärung und insbesondere die Tatsache, daß selbst die einzuladende Person von diesen Angaben Kenntnis erhielt.

Ich habe darauf das Hessische Ministerium des Innern gebeten, darauf hinzuwirken, daß die Verpflichtungserklärung überarbeitet wird. Insbesondere habe ich darauf hingewiesen, daß die Kenntnis des einzuladenden Ausländers von den finanziellen Verhältnissen des Gastgebers in keiner Weise erforderlich ist. Das Hessische Ministerium des Innern teilte meine Auffassung und erließ zur Umsetzung des Bundeserlasses eigene Hinweise an die Ausländerbehörden, die schon eine datenschutzrechtliche Verbesserung darstellten.

Nunmehr hat auch das Bundesministerium des Innern seinen Erlaß abgeändert. Folgende Einschränkungen der Datenerhebung sind darin enthalten:

- An den Nachweis der finanziellen Leistungsfähigkeit des Gastgebers sind abhängig von der Länge des beabsichtigten Aufenthalts des Ausländers unterschiedliche Anforderungen zu stellen.
- In jedem Fall dürfen auf dem Formular keine Angaben zu Einkommens- und Vermögensverhältnissen erfragt werden. Das Formular enthält ausschließlich die Bemerkung, daß die finanzielle Leistungsfähigkeit des Betroffenen glaubhaft gemacht wurde.
- Auch die Angaben, über wieviel Wohnraum der Gastgeber verfügt und ob er Mieter oder Eigentümer einer Wohnung ist, ist entfallen.

Auf die Angabe des Berufs des sich Verpflichtenden und die Angabe des Arbeitgebers konnte aus Sicht des Bundesministeriums des Innern nicht verzichtet werden, da daraus Rückschlüsse auf die finanziellen Verhältnisse gezogen werden könnten. Diese Auffassung halte ich für vertretbar.

Insgesamt konnten damit meine Bedenken gegen das Verfahren der Verpflichtungserklärung ausgeräumt werden.

11.3

Medizinische Unterlagen in Ausländerakten

In Ausländerakten enthaltene medizinische Daten sind besonders gegen unberechtigte Einsichtnahme zu schützen.

In verschiedenen Zusammenhängen ist es erforderlich, daß Ausländerbehörden bei der Wahrnehmung ihrer Aufgaben medizinische Daten verarbeiten. Um mich über die Art und Weise des Umganges mit solchen Daten bei den Ausländerbehörden zu informieren, habe ich im Berichtszeitraum eine Ausländerbehörde geprüft. Gegenstand der Prüfung war die Frage, ob und in welcher Weise medizinische Unterlagen in den Akten des Ausländeramts aufbewahrt werden. Zu diesem Zweck habe ich bei der Ausländerbehörde des Landkreises Groß-Gerau eine Reihe von Akten eingesehen. Die Akten betrafen vorwiegend Flüchtlinge aus Bosnien-Herzegowina. Diese Personen sind nach dem Erlaß des Hessischen Ministeriums des Innern vom 23. Juni 1997 u.a. dann von der Rückführung in ihr Heimatland ausgeschlossen, wenn bei ihnen eine Traumatisierung vorliegt, die "nachgewiesenermaßen einen Krankheitswert darstellt".

Nach meinen Feststellungen werden zum Nachweis der Traumatisierung ausführliche psychiatrische oder

psychotherapeutische Gutachten erstellt, in denen sensible Daten aus dem höchstpersönlichen Lebensumfeld der Betroffenen enthalten sind. Diese Gutachten werden entweder vom Betroffenen selbst, dessen Arzt oder anderen Stellen an die Ausländerbehörde geschickt und dort in der Regel zu der entsprechenden Akte genommen. In einem Fall wurde das Gutachten vom Arzt im verschlossenen Umschlag über das Ausländeramt an das Gesundheitsamt geschickt. Das Amt prüfte das Gutachten, traf eine Aussage zur Reisefähigkeit und teilte diese Entscheidung dem Ausländeramt mit.

In einer Reihe weiterer Akten befanden sich andere ärztliche Atteste mit einer teilweise ausführlichen Darstellung über bei den Betroffenen oder deren Angehörigen vorhandene Krankheiten. In einer Akte befand sich ein medizinisches Testergebnis über eine Person, die die Betroffene adoptieren will.

Datenschutzrechtlich sind sensitive Daten, wie sie in psychiatrischen oder psychotherapeutischen Gutachten aber auch in anderen ärztlichen Attesten zu finden sind, besonders gegen unberechtigte Einsichtnahme zu schützen. Vorzugswürdig ist deshalb das oben geschilderte Verfahren, bei dem das Ausländeramt vom Gesundheitsamt nur über bestimmte Ergebnisse informiert wird und sich keine detaillierten Angaben in der Ausländerakte befinden. In den Fällen, in denen ein derartiges Verfahren nicht durchgeführt werden kann, habe ich vorgeschlagen, daß die psychiatrischen und psychotherapeutischen, aber auch die sonstigen ärztlichen Atteste in verschlossenen Umschlägen in der Akte aufbewahrt und ggf. Einsichtnahmen dokumentiert werden. Falls es für die Arbeit erforderlich erscheint, können wesentliche Aussagen des Gutachtens in einem Vermerk zusammengefaßt werden, der in der Akte frei zugänglich ist.

Die Ausländerbehörde sagte zu, die beanstandeten Einzelfälle, in denen medizinische Unterlagen ungeschützt aufbewahrt wurden, zu

bereinigen und künftig nur noch in verschlossenen Umschlägen zu den Akten zu nehmen. Um zu erreichen, daß künftig alle hessischen Ausländerbehörden so verfahren, habe ich mit der Aufsichtsbehörde - dem Hessischen Ministerium des Innern und für Landwirtschaft, Forsten und Naturschutz - Kontakt aufgenommen.

Außerdem wurden noch von mir beiläufig festgestellte Datensicherheitsmängel bezüglich der Zugangssicherung zu Registraturräumen abgestellt.

11.4

Anmeldung von Ausländervereinen

Durch das Justizmitteilungsgesetz und einen Erlaß des Hessischen Ministeriums des Innern wurde das Verfahren bei der Anmeldung von Ausländervereinen verändert. Die neue Verfahrensweise berücksichtigt die datenschutzrechtlichen Belange der Betroffenen besser als die frühere.

Die Bildung von Vereinen ist nach Art. 9 des Grundgesetzes frei. Vereine, deren Mitglieder sämtlich oder überwiegend Ausländerinnen und Ausländer sind, müssen sich jedoch bei der zuständigen Verwaltungsbehörde - das sind in Hessen die Landräte und die Oberbürgermeister der kreisfreien Städte - anmelden. Wenn sie sich politisch betätigen und z.B. die innere Sicherheit gefährden, können sie verboten werden. Das Verfahren, insbesondere die Meldepflicht, die Auskunftspflicht und der Auskunftsumfang der Ausländervereine sowie eine Mitteilungspflicht der Verwaltungsbehörde an das Bundesverwaltungsamt regeln die §§ 19 bis 22 der Durchführungsverordnung zum Vereinsgesetz (VereinsG-DVO).

Nach § 61 Abs. 2 des Bürgerlichen Gesetzbuchs (BGB) konnte bislang die zuständige Verwaltungsbehörde gegen die Eintragung

eines Vereines in das Vereinsregister Einspruch einlegen. Dieses Einspruchsrecht ist durch das Inkrafttreten des Justizmitteilungsgesetzes (BGBl. I S. 1430) mit Wirkung vom 01. Juni 1998 entfallen. Statt dessen trat zum selben Termin eine Änderung des Gesetzes über die Angelegenheiten der freiwilligen Gerichtsbarkeit (FGG) in Kraft, die lediglich eine nachträgliche Information der zuständigen Verwaltungsbehörde über die Eintragung des Vereins vorsieht.

§ 159 Abs. 2 FGG

Das Amtsgericht hat die Eintragung eines Vereins oder einer Satzungsänderung der zuständigen Verwaltungsbehörde mitzuteilen, wenn Anhaltspunkte bestehen, daß es sich um einen Ausländerverein oder eine organisatorische Einrichtung eines ausländischen Vereines gemäß den §§ 14 und 15 des Vereinsgesetzes handelt.

Damit wurde für die seit jeher praktizierte Übermittlung personenbezogener Daten durch die Amtsgerichte an die Verwaltungsbehörden über die Angehörigen von Ausländervereinen, die sich in das Vereinsregister eintragen lassen wollen, erstmals eine Rechtsgrundlage geschaffen.

Die Änderungen im Bürgerlichen Gesetzbuch und im Gesetz über die Angelegenheiten der freiwilligen Gerichtsbarkeit nahm das Hessische Innenministerium zum Anlaß, einen Erlaß, der u.a. auch die genaue Ausgestaltung der Datenerhebung bei den Vereinen und die Information der Betroffenen über den Zweck der Datenerhebung nach § 12 Abs. 4 HDSG (alt) regelte, der neuen Rechtslage anzupassen. Meine Verbesserungsvorschläge aus datenschutzrechtlicher Sicht wurden bei der Neufassung des Erlasses berücksichtigt. Der neue Erlaß ist im Staatsanzeiger für das Land Hessen (1998, S. 1963) abgedruckt.

Insgesamt wurde der Umfang der über den Vorstand und die Mitglieder der Vereine zu erhebenden Daten auf das erforderliche Maß reduziert. In einem durch den Erlaß vorgeschriebenen Merkblatt werden die Betroffenen ausführlich und verständlich über den Zweck und die Rechtsgrundlage der Datenerhebung, über die teilweise vorhandene Auskunftspflicht bzw. über die Freiwilligkeit von Angaben sowie über die Mitteilung an das Bundesverwaltungsamt informiert. Eine früher regelmäßig vorgesehene Datenübermittlung an die Aufsichtsbehörde ist entfallen, sie erfolgt nur noch bei Anhaltspunkten für ein Verbot. Zuvor war bereits eine regelmäßige Mitteilung an die Polizei entfallen.

Damit sind die datenschutzrechtlichen Belange der Betroffenen bei der Anmeldung von Ausländervereinen ausreichend berücksichtigt.

11.5

Gemeinsame Arbeitsgruppe der Polizei und Ausländerbehörde in Frankfurt zur Bekämpfung von ausländischen Intensivstraftätern

Ausländer- und Polizeibehörden dürfen bei der Bekämpfung ausländischer "Intensivstraftäter" zusammenarbeiten und dabei auch im erforderlichen Umfang personenbezogene Daten verarbeiten und austauschen.

In Frankfurt wurde eine "Gemeinsame Arbeitsgruppe der Ausländerbehörde und der Polizei zur Bekämpfung von Intensivstraftätern (GAI)" gebildet. Ziel der Arbeitsgruppe ist es, den Aufenthalt von ausländischen Mehrfach- und sog. Intensivstraftätern in der Bundesrepublik beschleunigt zu beenden. Unumgänglich ist dabei, daß die beteiligten Behörden zusammenarbeiten und personenbezogene Daten untereinander austauschen. Die Stadtverwaltung Frankfurt hat mich zu der

vorgesehenen Zusammenarbeit und dem damit verbundenen Datenaustausch um eine Beratung gebeten. Ich habe die "Gemeinsame Arbeitsgruppe" vor Ort besucht, mich über die geplante Datenverarbeitung informiert und die beteiligten Behörden aus datenschutzrechtlicher Sicht beraten.

Rechtsgrundlage für die Zusammenarbeit zwischen Polizei- und Ausländerbehörde ist das Hessische Gesetz über die öffentliche Sicherheit und Ordnung (HSOG). § 1 Abs. 6 HSOG verpflichtet die Gefahrenabwehrbehörden allgemein zur Zusammenarbeit. § 22 Abs. 1 Satz 3 HSOG läßt die Datenübermittlung zwischen der Polizei und den Gefahrenabwehrbehörden (hier der Ausländerbehörde) unter rechtlichen Voraussetzungen zu, die weiter gefaßt sind als diejenigen in den allgemeinen Übermittlungsregelungen des Hessischen Datenschutzgesetzes. Voraussetzung ist lediglich, daß die Kenntnis der Daten zur Erfüllung der Aufgaben des Empfängers erforderlich erscheint.

§ 1 Abs. 6 HSOG

Alle Behörden haben bei der Gefahrenabwehr zusammenzuarbeiten. Insbesondere haben sie sich unverzüglich gegenseitig über Vorgänge, deren Kenntnis für die Aufgabenerfüllung der anderen Behörde bedeutsam erscheint, zu unterrichten. Die Vorschriften über den Schutz personenbezogener Daten (§§ 12 bis 29) bleiben unberührt.

§ 22 Abs. 1 Satz 3 HSOG

Zwischen den Gefahrenabwehrbehörden, anderen für die Gefahrenabwehr zuständigen Behörden oder öffentlichen Stellen und den Polizeibehörden können personenbezogene Daten übermittelt werden, soweit die Kenntnis dieser Daten zur Erfüllung der Aufgaben des Empfängers erforderlich erscheint.

Ich habe die Arbeitsgruppe gebeten festzulegen, welche Informationen sowohl zur Aufgabenerfüllung der Ausländerbehörde als auch zur Aufgabenerfüllung der Polizei erforderlich erscheinen. Aufgeführt wurden von der Arbeitsgruppe über die Personalien des betroffenen Personenkreises hinaus eine Reihe von Daten, die bisher entweder nur der Polizei oder nur der Ausländerbehörde bekannt waren. Der Arbeitsgruppe zufolge muß die Polizei z.B. von der Ausländerbehörde erfahren können, daß ein Ausländer vollziehbar abgeschoben werden kann. Ebenso müsse sie die Information erfahren können, daß eine Abschiebung ausgesetzt wurde (s. Ziff. 11.6). Umgekehrt müsse die Ausländerbehörde von der Polizei über Straftaten des Ausländers informiert werden, denn die Ausländerbehörde hat die aufenthaltsbeendenden Maßnahmen zu verfügen.

Die Zugriffsberechtigung auf die jeweiligen Datenbestände beschränkt sich ausschließlich auf die Mitarbeiterinnen und Mitarbeiter der Arbeitsgruppe. Durch geeignete Datensicherungsmaßnahmen wird gewährleistet, daß Unbefugte keinen Zugriff auf die Datenbestände nehmen können.

Ich habe der Stadtverwaltung mitgeteilt, daß ich gegen die vorgesehene Datenverarbeitung keine Einwände habe.

11.6

Inaktuelle Ausschreibungen in polizeilichen Fahndungsdateien

Inaktuelle Fahndungsausschreibungen der Ausländerbehörden können für die Betroffenen erhebliche Belastungen verursachen. Vom Innenministerium muß ein Verfahren entwickelt werden, das künftig inaktuelle Fahndungsausschreibungen verhindert.

11.6.1

Die Beschwerde

Ein als asylberechtigt anerkannter libanesischer Staatsangehöriger wurde im Jahre 1996 von der Grenzpolizei aus einem Zug zur Polizeidienststelle verbracht, weil er nach einer Datenspeicherung im polizeilichen Informationssystem als abzuschiebender Ausländer festzunehmen war. Im März 1998 wurde er erneut verhaftet, weil die Fahndungsausschreibung auch nach dieser langen Zeit noch nicht gelöscht war. Der Betroffene wandte sich an den Bayerischen Datenschutzbeauftragten, der mich in die Überprüfung des Sachverhaltes einschaltete.

Nach meinen durch eine Akteneinsicht bei der Ausländerbehörde des Landkreises Groß-Gerau getroffenen Feststellungen, war für die Unterlassung der Löschung der Fahndungsausschreibung die Ausländerbehörde des Landrates des Main-Taunus-Kreises verantwortlich. Der Sachverhalt hat sich folgendermaßen zugetragen:

Der Libanese wurde im Jahre 1991 von der Ausländerbehörde des Main-Taunus-Kreises zum Verlassen der Bundesrepublik aufgefordert. Die zwangsweise Abschiebung wurde angedroht. Damit verbunden wurde u.a. ein unbefristetes Wiedereinreiseverbot und Datenspeicherungen im polizeilichen Fahndungsbestand, im Ausländerzentralregister und im Bundeszentralregister.

Als der Betroffene im Februar 1994 nach dem Verbüßen einer Haftstrafe in der Heimat erneut nach Deutschland einreiste, erteilte die für seinen Wohnort in Bayern zuständige Ausländerbehörde ihm eine sog. Aufenthaltsgestattung und forderte beim Landratsamt des Main-Taunus-Kreises die zu seiner Person bis zum Jahre 1991 geführte Ausländerakte an. Zu diesem Zeitpunkt hätte das Landratsamt des Main-Taunus-Kreises die von ihm veranlaßten Datenspeicherungen u.a. im polizeilichen Datenbestand und im

Ausländerzentralregister korrigieren lassen und die Akten abgeben müssen. Statt dessen teilte das Landratsamt des Main-Taunus-Kreises mehrmals telefonisch und schriftlich mit, es könne die Ausländerakte nicht finden.

Nach der Anerkennung des Betroffenen als Asylbewerber (im April 1996) forderte das bayerische Landratsamt das Landratsamt des Main-Taunus-Kreises auf, das im Ausländerzentralregister noch immer registrierte unbefristete Wiedereinreiseverbot zu korrigieren. Denn die hessische Ausländerbehörde hatte 1991 - zu diesem Zeitpunkt korrekt - diese Datenspeicherung veranlaßt. Auf Grund der Regelungen über die Verantwortlichkeit für Datenspeicherungen im Ausländerzentralregister war nur sie befugt, die Datenspeicherung auch wieder zu löschen. Zu demselben Zweck übersandte das bayerische Landratsamt auch noch den Anerkennungsbescheid sowie die Mitteilung über die Rechtskraft des Bescheides des Bundesamtes für die Anerkennung ausländischer Flüchtlinge.

Trotzdem erfolgte im August 1996 die Verhaftung, weil der Ausländer nach wie vor im polizeilichen Fahndungssystem ausgeschrieben war. Die Grenzpolizeibehörde erkannte anhand des Reiseausweises des Libanesen den Behördenfehler, entließ den Betroffenen wieder aus der Haft und forderte die Ausländerbehörde zur Prüfung und Richtigstellung der Datenspeicherung auf.

In der Ausländerakte befindet sich ein Telefonvermerk, demzufolge eine Bearbeiterin des Landratsamtes des Main-Taunus-Kreises dem bayerischen Landratsamt die Auskunft gab, daß eine Löschung von Daten im Ausländerzentralregister einen schriftlichen Antrag des Betroffenen voraussetze. Das bayerische Landratsamt übersandte daher der Ausländerbehörde des Main-Taunus-Kreises einen Antrag des Betroffenen. Daraufhin korrigierte das Landratsamt des Main-Taunus-Kreises die Datenspeicherung im

Ausländerzentralregister, nicht aber die Datenspeicherung über die polizeiliche Fahndung.

Nach dem Umzug des Ausländers in den Landkreis Groß-Gerau im Oktober 1996 forderte die jetzt zuständige Ausländerbehörde des Landratsamtes Groß-Gerau die Akten der bayerischen Ausländerbehörde an. Das bayerische Landratsamt prüfte noch die Korrektur im Ausländerzentralregister und gab dann die Akte nach Groß-Gerau ab. Die Ausländerbehörden haben keinen Direktzugriff auf den polizeilichen Fahndungsdatenbestand. Weder das Landratsamt in Bayern noch das jetzt zuständige Landratsamt wurden daher darauf aufmerksam, daß die Ausländerbehörde des Main-Taunus-Kreises die Fahndung immer noch nicht gelöscht hatte. Im März 1998 ging bei der Ausländerbehörde die Mitteilung eines baden-württembergischen Polizeireviers über eine weitere Festnahme des Betroffenen ein. Die Festnahme erfolgte auf Grund der Fahndungsausschreibung. Die Freilassung erfolgte erst, nachdem der Betroffene einen Tag in Haft verbracht hatte und über die Polizeistation des Wohnortes der Reiseausweis des Ausländers vorgelegt werden konnte. Die baden-württembergische Polizeibehörde ersuchte die Ausländerbehörde dringend, die Angelegenheit zu prüfen und die Rücknahme der Ausschreibung zu veranlassen.

Die neu zuständige Ausländerbehörde des Landkreises Groß-Gerau schrieb nun an die Ausländerbehörde des Main-Taunus-Kreises, bat um Löschung der Daten im Fahndungssystem und um Prüfung, ob sich nicht doch noch eine Akte fände. In der Zwischenzeit hatte auch ich, veranlaßt durch meinen bayerischen Kollegen, an den sich der Betroffene zunächst wandte, das Landratsamt des Main-Taunus-Kreises aufgefordert, die Löschung der Fahndungsdaten zu veranlassen. Nach einer Woche verfügte das Landratsamt des Main-Taunus-Kreises die Löschung der Personenfahndung, schickte die nun aufgefundene Akte an die Ausländerbehörde Groß-Gerau und bestätigte u.a. die Fahndungslöschung.

Den Betroffenen habe ich über meine Feststellungen informiert und ihm bestätigt, daß er in seinen datenschutzrechtlichen Belangen verletzt wurde. In der von mir erbetenen Stellungnahme räumt der Landrat u.a. ein, im Falle des Betroffenen sei es leider zu einer Folge von Fehlleistungen und Mißverständnissen gekommen, die er im nachhinein nur bedauern kann.

Mich interessierte, ob es sich bei dem Vorgang um einen Einzelfall handelte oder ob solche Fälle häufiger vorkommen. Immerhin war mir schon einmal die Verhaftung eines Ausländers auf Grund einer unterlassenen Löschung im polizeilichen Fahndungsbestand aufgefallen (24. Tätigkeitsbericht, Ziff. 11.1). Ich ging dieser Frage zunächst bei der Ausländerbehörde des Landkreises Groß-Gerau, bei der ich u.a. die Akteneinsicht vorgenommen hatte, nach. Danach habe ich bei der Ausländerbehörde des Main-Taunus-Kreises eine größere Anzahl von Fällen geprüft.

11.6.2

Prüfungen

11.6.2.1

Ausländerbehörde des Landkreises Groß-Gerau

Ich bat die Ausländerbehörde um die Vorlage von zufällig ausgewählten ca. 130 Ausländerakten, die ich nach Fahndungsausschreibungen durchsah. In weniger als zehn Fällen wurde nach den Personen, zu denen die Akte geführt wurden, gefahndet. Die rechtlichen Voraussetzungen einer Fahndung waren auch weitgehend gegeben. Allerdings war in einem Falle der Verfahrensablauf ähnlich wie in dem oben beschriebenen Einzelfall: Der Betroffene war zunächst als Asylbewerber abgelehnt worden, mußte ausreisen und wurde, nachdem er bis zu einem bestimmten Zeitpunkt die Ausreise nicht nachgewiesen

hatte, zur Fahndung ausgeschrieben. Als er dann nach seiner Wiedereinreise zunächst geduldet und dann als Asylbewerber anerkannt wurde, war die Fahndung zu löschen. Die Durchschrift der Lösungsverfügung befand sich auch in der Akte. Das Original war an das Landeskriminalamt abgeschickt. Sicherheitshalber sah ich auch noch bei der Polizei in der Fahndungsdatei nach. Dies stellte sich als notwendig heraus: Nicht nur nach dem Betroffenen, auch noch nach seiner Ehefrau und seinen drei Kindern wurde nach wie vor gefahndet.

Ich habe sofort die erforderlichen Löschungen beim Landeskriminalamt veranlaßt und die Polizei um eine Stellungnahme gebeten. Das Landeskriminalamt hat den Fall überprüft, konnte aber lediglich feststellen, daß die Lösungsverfügungen des Ausländeramtes vermutlich nicht beim Landeskriminalamt ankamen. Dieses Ergebnis ist nicht zufriedenstellend. Die Lösungsverfügungen stammen aus dem Jahre 1994. Offenbar hatte seit Jahren keiner der Familienangehörigen Kontakt mit der Polizei. Sonst wäre mit Verhaftungen zu rechnen gewesen.

Eine weitere Fahndungsausschreibung - sie war förmlich nicht zu beanstanden - betraf eine 83jährige Frau. Ich bat die Ausländerbehörde um Prüfung, ob die vor kurzem um weitere zehn Jahre verlängerte Fahndungsausschreibung auf Grund des hohen Alters der Betroffenen mit dem Verhältnismäßigkeitsgrundsatz vereinbar ist.

Die Ausländerbehörde verzichtete daraufhin auf die Fahndung nach der 83jährigen Frau.

Vergleichbare Fälle einer pflichtwidrigen Unterlassung einer Löschung der Fahndungsdaten habe ich anhand der Akteneinsicht nicht festgestellt.

11.6.2.2

Ausländerbehörde des Main-Taunus-Kreises

Da es um die Aktualität von Fahndungsnotierungen ging, bat ich vor der Überprüfung das Hessische Landeskriminalamt, mir alle im Hessischen Polizeiinformationssystem (HEPOLIS) gespeicherten Personenfahndungsdatensätze aufzulisten, für deren Speicherung die Ausländerbehörde des Main-Taunus-Kreises verantwortlich ist. Diese Liste umfaßte ca. 1.100 Personenfahndungen - zu viele für eine umfassende Kontrolle durch meine Dienststelle.

Ich wählte daher aus dieser Liste stichprobenhaft 200 Fälle aus und bat die Ausländerbehörde um Vorlage der Ausländerakten. In ca. 30 Fällen konnte eine Prüfung nicht stattfinden, weil die Akten auf Grund eines Zuständigkeitswechsels an andere Ausländerbehörden abgegeben waren. Es wurden also ca. 170 Akten eingesehen, das entspricht etwa 15 Prozent aller Betroffenen, nach denen gefahndet wird. Bei Durchsicht der Akten stellte ich folgendes fest:

In den meisten Fällen waren die Fahndungsnotierungen korrekt. Bei 13 Personen mußten die Fahndungsdaten berichtigt werden. Von den 13 Betroffenen waren zwei Personen verstorben. In drei Fällen war die Löschung der Fahndung von der Ausländerbehörde verfügt, aber die Verfügungen waren bei der Polizei nicht angekommen bzw. wurden dort nicht verarbeitet (wie bei der Familie in Groß-Gerau). Teilweise hätte die Löschung der Fahndungsdaten schon vor mehreren Jahren von der Ausländerbehörde verfügt werden müssen. Teilweise war die Fahndung aber auch nur - bis zu einer erneuten Änderung im Sachverhalt - zwischenzeitlich zu löschen gewesen.

In den Fällen, in denen die Lösungsverfügungen der Ausländerbehörde von der Polizei nicht verarbeitet worden waren, habe ich dies beim Landeskriminalamt veranlaßt. Soweit der

Verantwortungsbereich des Main-Taunus-Kreises betroffen war, wurden die notwendigen Fahndungslöschungen dort verfügt.

Auch zu den nachfolgend aufgeführten während der Prüfung zufällig festgestellten Problemen wurden seitens der Ausländerbehörde die erforderlichen Korrekturen veranlaßt: Im Falle eines libanesischen Staatsangehörigen war die Mitteilung seines Bevollmächtigten, der eine neue Anschrift des Ausländers bekanntgab, ignoriert worden. Bescheide usw. wurden weiterhin öffentlich zugestellt. Im Falle eines türkischen Staatsangehörigen (nebst Familie) wurde einer Information einer außerhessischen Ausländerbehörde, derzufolge die Familie unter einem anderen Namen in einer bestimmten Stadt lebt, nicht nachgegangen. In einer Ausländerakte befand sich eine Aktenanforderung, die eine ganz andere Person betraf. Die Ausländerakte eines irakischen Staatsangehörigen war an die Ausländerbehörde Chemnitz abzugeben.

Es fiel weiterhin auf, daß in einer sehr hohen Anzahl von Fällen die Datenspeicherungen im Ausländerzentralregister nicht vollständig oder nicht präzise waren.

Die 13 von mir festgestellten Fälle nicht korrekter Fahndungsnottierungen entsprechen, wenn man die Repräsentativität der Stichprobe unterstellt, einer Fehlerquote von mehr als sieben Prozent. Das bedeutet, daß der "Fall" des libanesischen Staatsangehörigen kein Einzelfall war. Mit Ausnahme der Fälle der Datenspeicherungen von inzwischen Verstorbenen hätte es in allen Fällen - ähnlich wie in dem ausführlich beschriebenen Einzelfall - zu ungerechtfertigten Verhaftungen mit weitreichenden belastenden Folgen für die Betroffenen kommen können.

11.6.3

Konsequenzen

Das Prüfungsergebnis habe ich dem Landrat des Main-Taunus-Kreises zur Kenntnis gegeben und ihm mitgeteilt, daß auch der restliche Bestand von Fahndungsdaten dringend einer Überprüfung bedarf.

Da es sich um ein landesweites Problem handelt, habe ich das Innenministerium von dem Einzelfall und meinen Prüfergebnissen informiert und um ein Gespräch gebeten. Sicherzustellen ist, daß nicht nur im Main-Taunus-Kreis, sondern in allen Ausländerbehörden der Bestand an Fahndungsausschreibungen von Ausländerbehörden auf aktuelle Notierungen hin überprüft wird. Es bedarf eines Verfahrens, das künftig inaktuelle Fahndungsausschreibungen ausschließt, wobei insbesondere auch die Verantwortlichkeits- und Zuständigkeitsregelungen überprüft werden müssen. Es ist auch nicht angemessen, daß es zur Korrektur einer offensichtlich fehlerhaften Datenspeicherung eines Antrages des Betroffenen bedarf. Gewährleistet sein muß auch, daß Lösungsverfügungen der Ausländerbehörden tatsächlich zur Löschung der Fahndung bei der Polizei führen.

Über die getroffenen Maßnahmen werde ich in meinem nächsten Tätigkeitsbericht berichten.

12. Kommunen

12.1

Pressemitteilung über die Höhe eines beantragten Verdienstauffalls für die Teilnahme an Sitzungen kommunaler Gremien

Die öffentliche Bekanntgabe eines beantragten Verdienstauffalls für die Teilnahme an Sitzungen kommunaler Gremien kann dann zulässig sein, wenn der Betroffene bereits selbst Anhaltspunkte über die Höhe der geltend gemachten Forderungen in öffentlicher Diskussion bekanntgegeben hat.

Ein ehrenamtlich tätiger Stadtrat einer hessischen Kommune hatte eine Datenschutzverletzung gerügt, weil der Bürgermeister seiner Stadt gegenüber der Presse den genauen Betrag genannt hatte, den der Stadtrat als stündlichen Verdienstauffall für seine Teilnahme an den Sitzungen des Magistrats geltend gemacht hatte.

Den ehrenamtlich tätigen Magistratsmitgliedern steht nach § 27 Abs. 1 der Hessischen Gemeindeordnung (HGO) eine Verdienstauffallentschädigung zu, die sich an einem in Kommunalen Satzung festgesetzten Durchschnittssatz orientiert. Der Betroffene kann stattdessen auch den tatsächlichen Verdienstauffall als Ersatz verlangen.

§ 27 Abs. 1 Satz 1 und Satz 4 HGO

Ehrenamtlich Tätige haben Anspruch auf Ersatz von Verdienstauffall. Durch Satzung ist ein Durchschnittssatz festzusetzen, der nur denjenigen zu gewähren ist, denen nachweisbar ein Verdienstauffall entstehen kann.

...

Anstelle des Durchschnittssatzes kann der tatsächlich entstandene und nachgewiesene Verdienstauffall verlangt werden; ...

Der Stadtrat hatte im vorliegenden Fall als selbständiger Unternehmer von der zweiten Variante Gebrauch gemacht. Die Höhe des beantragten Verdienstaufalles geriet in die politische Diskussion. Im Rahmen dieser Diskussion offenbarte der Bürgermeister gegenüber der Presse die tatsächlich beantragte Höhe des Verdienstaufalles. Zunächst ging ich davon aus, daß es sich dabei um eine unzulässige Datenübermittlung gehandelt hatte. Gem. § 16 Hessisches Datenschutzgesetz (HDSG) ist eine Übermittlung von Daten an Stellen oder Personen nur zulässig, wenn keine Anhaltspunkte dafür bestehen, daß schutzwürdige Belange des Betroffenen beeinträchtigt werden können. Die öffentliche Bekanntgabe der beantragten Höhe des Verdienstaufalles war durchaus geeignet, schutzwürdige Belange des Stadtrates zu verletzen. Zu berücksichtigen ist hierbei auch, daß ein Stadtrat nach der gegenwärtigen Rechtslage nicht verpflichtet ist, seine persönliche Einkommens- und Geschäftssituation gegenüber der Öffentlichkeit zu offenbaren.

Im Zuge der Aufklärung des Sachverhalts im Rahmen von Darstellung und Gegendarstellung der verschiedenen Beteiligten stellte sich dann allerdings heraus, daß der Stadtrat selbst öffentlich Hinweise zu der beantragten Höhe gegeben hatte. In einem Interview einer ortsansässigen Zeitung hatte er offen selbst die Höhe des ihm für seine Schöffenstätigkeit bezahlten Verdienstaufalles mitgeteilt. Dieses Interview hatte vor der Verlautbarung durch den Bürgermeister stattgefunden. Die in dem Interview genannte Zahl deckte sich mit der durch den Bürgermeister offenbarten.

Damit hatte der Stadtrat die umstrittene Zahl selbst ins Gespräch gebracht. Der Bürgermeister konnte daher nach diesem Interview davon ausgehen, daß die geltend gemachte Höhe der Verdienstaufallentschädigung bereits in der öffentlichen

Diskussion stand und keiner besonderen Geheimhaltungspflicht unterlag.

§ 3 Abs. 4 HDSG

Dieses Gesetz gilt nicht für personenbezogene Daten, solange sie in allgemein zugänglichen Quellen gespeichert sind sowie für Daten des Betroffenen, die von ihm zur Veröffentlichung bestimmt sind.

Eine unzulässige Datenübermittlung lag nicht vor.

12.2

Öffentliche Bekanntgabe des Wasserverbrauchs eines Gemeindevertreters

Offensichtlich fehlerhafte Angaben dürfen auch dann öffentlich richtiggestellt werden, wenn sie personenbezogene Daten enthalten.

Datenschutz-Argumente sind immer wieder Teil politischer Auseinandersetzungen. Das gilt vor allem für die Kommunalpolitik. In diesem Jahr fragte eine Fraktion an, ob der Bürgermeister gegen datenschutzrechtliche Bestimmungen verstößt, wenn er im Rahmen einer Diskussion zur Gebührenerhöhung der Wasserpreise den häuslichen Wasserverbrauch eines Gemeindevertreters in einer öffentlichen Sitzung bekanntgibt.

Die von mir angeforderte Stellungnahme des Bürgermeisters ergab, daß der betroffene Gemeindevertreter bereits vorher in einer öffentlichen Ausschußsitzung mit seinen eigenen Verbrauchsdaten eine Ablehnung der Gebührenerhöhung begründet hatte. Da dieser genannte Wasserverbrauch dem Bürgermeister ungewöhnlich hoch vorkam, hatte er den tatsächlichen Verbrauch dieses Haushalts

festgestellt und in der nachfolgenden Gemeindevertretersitzung die tatsächlichen Verbrauchsdaten bekanntgegeben.

Sicher steht dem Bürgermeister grundsätzlich nicht das Recht zu, Verbrauchsdaten von Gemeindevertretern zu erheben und in der öffentlichen Diskussion preiszugeben. Für eine sachliche Diskussion hätte die Angabe von statistischen Durchschnittswerten des Wasserverbrauchs verschiedener Haushaltstypen ohne Zweifel ausgereicht. Da aber bereits der Gemeindevertreter selbst mit eigenen Verbrauchsdaten statt mit allgemeinen Erfahrungswerten argumentiert hatte, muß dem Bürgermeister das Recht zustehen, offensichtlich fehlerhafte Angaben auch öffentlich richtigzustellen. Eine Verletzung schutzwürdiger Belange des Gemeindevertreters konnte ich aus diesem Grunde nicht feststellen.

12.3

Prüfung und Beratung hessischer Kommunen

Auch 1998 besuchte ich neun hessische Gemeinden. Bis auf eine Ausnahme habe ich nur wenige datenschutzrechtliche Mängel festgestellt.

Die Überwachung der Einhaltung von Datenschutzbestimmungen in hessischen Dienststellen gehört nach § 24 Abs. 1 Hessisches Datenschutzgesetz (HDSG) zu meinen Aufgaben. Ohne besonderen Anlaß habe ich vom Lahn-Dill-Kreis bis in den Odenwald neun Gemeinden ausgewählt und im Laufe des Jahres 1998 besucht. Besonderes Augenmerk galt dabei vor allem der Gebäudesicherheit, Archiven, Meldeämtern und der DV-Ausstattung.

Bei acht Kommunen habe ich nur kleinere datenschutzrechtliche Mängel festgestellt wie z.B. unbesetzte, aber offene Diensträume oder Archive und die Nutzung von PC ohne Schutzsoftware. Eine

kurzfristige Beseitigung dieser Mängel wurde mit den jeweiligen Beauftragten für den Datenschutz vereinbart.

Eine mittelhessische Kommune jedoch wies in allen überprüften Bereichen teilweise gravierende Datenschutzmängel auf. Das auf den ersten Blick moderne und räumlich relativ großzügig ausgestattete Rathaus war über Nebeneingänge im Keller und im Dachgeschoß über das Feuerwehrhaus bzw. Vereinsräume Tag und Nacht frei zugänglich. Das Rathaus verfügte zwar über eine Schließanlage, die Schlüsselvergabe erfolgte jedoch ohne ein schlüssiges Konzept. Da einige Mitarbeiterinnen und Mitarbeiter keinen Schlüssel zum Rathaus hatten und andere kein Schloß in der Bürotür, standen außer dem Haupteingang alle Türen unabhängig von den Rathausprechzeiten durchgehend offen.

Während meines Besuches sah ich verschiedene Diensträume mit offenen Schränken und einen eingeschalteten PC ohne Bedienstete. Erschwerend kam hinzu, daß in einigen Büros eingebaute Schränke nicht verschlossen werden konnten. Nur der Kassenraum und die Standesamtsbücher waren vor unberechtigten Zugriffen ausreichend geschützt.

In unverschlossenen Flurschränken fand ich Akten der Finanzverwaltung, Sammelakten zu Familienbüchern und Gehaltsabrechnungen der Bediensteten. Das allgemeine Archiv im Keller war zwar verschlossen, innerhalb des Archivs waren jedoch auch Personalakten und Gehaltsabrechnungen für alle Mitarbeiterinnen und Mitarbeiter zugänglich aufbewahrt. Eine kurze Überprüfung des DV-Netzes ergab, daß unberechtigte Zugriffe auf Dateien fremder Sachgebiete möglich waren.

Der Datenschutzbeauftragte dieser Kommune ist gleichzeitig Leiter des Haupt- und Organisationsamtes. Nach § 5 Abs. 2 HDSG (auch schon vor der Novellierung) darf jedoch nur derjenige zum Beauftragten für den Datenschutz bestellt werden, der dadurch

keinem Interessenkonflikt mit dienstlichen Aufgaben ausgesetzt wird. Erfahrungsgemäß kann für den Leiter des Haupt- und Organisationsamtes ein solcher Konflikt nicht ausgeschlossen werden, da er z.B. auch über den Einsatz von Automatisierungsverfahren entscheidet. Ich habe daher empfohlen, einen anderen geeigneteren Mitarbeiter zum Beauftragten für den Datenschutz zu bestellen.

Die Beseitigung der festgestellten Mängel habe ich im Oktober schriftlich gefordert. Eine Mitteilung der Gemeinde über getroffene Maßnahmen lag mir bis zum Redaktionsschluß dieses Tätigkeitsberichts noch nicht vor.

12.4

Parallele Führung eines landwirtschaftlichen Unternehmerverzeichnisses bei Kommunen und der Land- und forstwirtschaftlichen Berufsgenossenschaft

Datenschutz kann zum Infragestellen langjähriger Verwaltungspraxis und damit zur Verwaltungsvereinfachung führen

Die Anfrage einer Gemeinde, warum aus datenschutzrechtlichen Gründen die Übermittlung des gesamten Katasterbestandes ihres Zuständigkeitsbereichs durch die Land- und forstwirtschaftliche Berufsgenossenschaft nicht mehr möglich ist, machte mich auf die parallele Führung eines landwirtschaftlichen Unternehmerverzeichnisses sowohl bei den Kommunen als auch bei der Land- und forstwirtschaftlichen Berufsgenossenschaft aufmerksam.

Bei der praktischen Arbeit hatte sich herausgestellt, daß landwirtschaftliche Unternehmerverzeichnisse über tatsächlich bewirtschaftete Flächen der Landwirte bei den Kommunen häufig

nicht dem aktuellen Stand bei der Land- und forstwirtschaftlichen Berufsgenossenschaft entsprachen. Daher war es in jedem Einzelfall erforderlich, mit telefonischer Rückfrage bei der Land- und forstwirtschaftlichen Berufsgenossenschaft Daten der jeweiligen Gemeinde zu aktualisieren. Um dies zu vereinfachen, beantragten die Kommunen immer wieder die Übermittlung ihres gesamten Katasterbestandes bei der Land- und forstwirtschaftlichen Berufsgenossenschaft. Bis 1986 gab es regelmäßig solche Übermittlungen. Erst eine Prüfung der Land- und forstwirtschaftlichen Berufsgenossenschaft durch den Bundesbeauftragten für den Datenschutz erklärte diese Verwaltungspraxis für nicht rechtmäßig. Eine Offenbarung der Verzeichnisse durch die Land- und forstwirtschaftliche Berufsgenossenschaft wäre nach § 810 Reichsversicherungsordnung (RVO) nur zulässig, wenn die Beiträge von den Gemeinden eingezogen würden, dies ist in Hessen jedoch nicht der Fall. Die Erleichterung der Arbeit in den Gemeindeverwaltungen rechtfertigt eine solche Übermittlung nicht.

Die Kommunen sahen in dieser Anweisung des Bundesdatenschutzbeauftragten für den Datenschutz eine Verschlechterung ihrer Arbeitsbedingungen. Da an der rechtlichen Unzulässigkeit einer solchen Übermittlung nicht zu zweifeln ist, ich das Problem der Kommunen aber durchaus verstehen konnte, versuchte ich festzustellen, aus welchen Gründen eine solche parallele Führung des landwirtschaftlichen Unternehmerverzeichnisses erforderlich ist.

Die Land- und forstwirtschaftliche Berufsgenossenschaft führt das Verzeichnis zum Berechnen und Abrechnen ihrer Beiträge. Diese Abrechnung erfolgt direkt mit den Landwirten. Hier besteht also ein direktes materielles Interesse auf beiden Seiten, das Verzeichnis komplett und aktuell zu führen. Gründe der Kommunen, das Unternehmerverzeichnis zu führen liegen in § 795 RVO und daran anknüpfend in § 23 der Satzung der Land- und

forstwirtschaftlichen Berufsgenossenschaft. Danach muß die Eröffnung eines landwirtschaftlichen Unternehmens bei der Land- und forstwirtschaftlichen Berufsgenossenschaft und der zuständigen Gemeindebehörde angezeigt werden. Änderungen sind nach § 25 der Satzung jedoch nur der Berufsgenossenschaft anzuzeigen. Dies führt langfristig zu größeren Differenzen zwischen den jeweiligen Beständen des Unternehmerverzeichnisses. Nach § 808 RVO besteht für die Gemeinden eine Unterstützungspflicht gegenüber der Land- und forstwirtschaftlichen Berufsgenossenschaft; diese wurde festgelegt, um der Land- und forstwirtschaftlichen Berufsgenossenschaft eine Partizipationsmöglichkeit an besonderen Ortskenntnissen der Gemeindebehörden zu geben. Für den Einzelfall ist eine solche Unterstützungspflicht durchaus sinnvoll. Allerdings halte ich hierfür die ständige Bereithaltung aller Daten dieses Verzeichnisses durch die Kommunen nicht für erforderlich. Im Einzelfall können jederzeit die erforderlichen Daten durch die Land- und forstwirtschaftliche Berufsgenossenschaft der Kommune zur Verfügung gestellt werden.

Zum Zeitpunkt der Anfrage im Jahr 1996 galten die Bestimmungen der Reichsversicherungsordnung (RVO). Diese wurden durch das Gesetz zur Einordnung des Rechts der gesetzlichen Unfallversicherung in das Sozialgesetzbuch (UVEG) vom 7. August 1996 in das Sozialgesetzbuch aufgenommen. Die §§ 795 und 810 RVO wurden hierbei ersatzlos aufgehoben. Die Unterstützungspflicht der Gemeinden gegenüber der Berufsgenossenschaft (§ 808 RVO) regelt jetzt § 197 SGB VII.

Ein Bedarf zur Führung des landwirtschaftlichen Unternehmensverzeichnisses bei den Kommunen ergab sich nur unter dem Gesichtspunkt der Agrarwahlen. Hierfür werden im Abstand von ca. fünf Jahren lediglich Informationen darüber benötigt, welche Landwirte mit einer Wirtschaftsfläche von über einem Hektar in der Gemeinde ansässig und damit wahlberechtigt

sind. Hier könnte eine Legitimierung der Übermittlung eines entsprechenden Auszugs aus dem Unternehmensverzeichnis der Land- und forstwirtschaftlichen Berufsgenossenschaft an die Kommunen zur Durchführung der Agrarwahlen die Notwendigkeit zur Führung eines eigenen Verzeichnisses bei den Kommunen ersetzen.

Ich habe daher das Hessische Ministerium des Innern und für Landwirtschaft, Forsten und Naturschutz gebeten, dieses Verfahren zu überprüfen und im Rahmen der Verwaltungsvereinfachung entsprechend zu ändern. Inzwischen hat mir das Ministerium mitgeteilt, daß die Wahlordnung für die Agrarwahlen bereits vor dem Erhalt meines Schreibens geändert wurde und die Führung eines eigenständigen Unternehmerverzeichnisses bei den Kommunen aus Sicht des Ministeriums des Innern und für Landwirtschaft, Forsten und Naturschutz entfallen kann. Die kommunalen Spitzenverbände wurden entsprechend informiert.

13. Landwirtschaft und Umwelt

13.1

Gesamtnovelle Hessisches Wassergesetz

Im Zuge der Gesamtnovelle zum Hessischen Wassergesetz muß auch eine Anpassung der Datenverarbeitungsnorm an die Vorgaben des Volkszählungsurteils des Bundesverfassungsgerichts erfolgen.

Am 27. November 1997 hat die Landesregierung den Entwurf zur Gesamtnovellierung des Hessischen Wassergesetzes vorgelegt. Ich habe die Vorlage zum Anlaß genommen, hinsichtlich der Datenverarbeitungsregelung eine präzisere Formulierung dafür anzuregen, für welche Zwecke personenbezogene Daten verwandt werden dürfen; denn nach meiner Auffassung entsprach sowohl die alte Regelung des § 105 Hessisches Wassergesetz (HWG) als auch die im wesentlichen gleichgebliebene Norm des § 84 HWG-E nicht dem rechtsstaatlichen Gebot der Normenklarheit.

§ 84 Abs. 1 HWG-E

Die Wasserbehörden, das Hessische Landesamt für Bodenforschung, die Hessische Landesanstalt für Umwelt und die kommunalen Abwasserbeseitigungspflichtigen sind berechtigt, soweit es für die Erreichung der in Satz drei aufgeführten Zwecke erforderlich ist, die notwendigen personenbezogenen Daten zu erheben und in sonstiger Weise zu verarbeiten. Eine Erhebung auch ohne Kenntnis des Betroffenen ist zulässig, wenn andernfalls die Erfüllung der Aufgaben für die in Satz drei genannten Zwecke gefährdet würde. Zwecke nach Satz eins sind:

1. Durchführung der Wasseraufsicht,
2. Durchführung von Genehmigungs-, Anzeige- oder Zulassungsverfahren,

3. Durchführung der Abwasser- und Gewässerüberwachung und von wasserwirtschaftlichen Planungen und wissenschaftlichen Untersuchungen zur Erfüllung der Aufgaben des Gewässerschutzes.

Die in § 84 Abs. 1 Satz 3 HWG-E genannten Zwecke waren mit Ausnahme der Durchführung von Genehmigungs-, Anzeige- oder Zulassungsverfahren nicht bestimmt genug.

Zwar enthält das Hessische Wassergesetz in § 3 eine Regelung für die Wasseraufsicht, sie ist aber nicht mehr als konkrete Gefahrenabwehr geregelt, sondern sie umfaßt alle erforderlichen Maßnahmen, "um die Zielsetzung des Hessischen Wassergesetzes zu verwirklichen". Damit können nicht nur die im Hessischen Wassergesetz beschriebenen Maßnahmen, sondern alle den Zielen des Hessischen Wassergesetzes dienenden Maßnahmen durchgeführt werden. Nach meiner Auffassung entspricht eine solche Formulierung nicht dem Bestimmtheitsgebot.

Auch der unter Nummer drei genannte Zweck ist nicht hinreichend bestimmt genug. Zum einen ist die Aufgabe des Gewässerschutzes, die sowohl alleine als auch innerhalb der wasserwirtschaftlichen Planungen angeführt wird, nicht hinreichend definiert. Sollte hier das Ziel nach § 1 Satz 1 HWG-E gemeint sein, so habe ich es für empfehlenswert gehalten, dies deutlich zu machen.

§ 1 Satz 1 HWG-E

Die oberirdischen Gewässer mit ihren Ufern und Auen und das Grundwasser sind als Bestandteil des Naturhaushaltes nachhaltig zu schützen und so zu bewirtschaften, daß sie dem Wohl der Allgemeinheit und im Einklang mit ihm auch dem Nutzen einzelner Personen dienen.

Auch für die Aufgabe der Abwasser- und Gewässerüberwachung konnte ich keine hinreichende gesetzliche Definition finden.

Da in der Begründung zur Umformulierung der Ziele nichts näheres ausgesagt ist, ist auch nicht ersichtlich, was mit der Änderung des Wortlauts bezweckt werden sollte.

Die Hessische Landesregierung hat in einer überarbeiteten Fassung des Gesetzentwurfs mit Stand vom 3. April 1998 meine Anregungen im wesentlichen aufgegriffen, so daß die Nummer 1 und Nummer 3 wie folgt formuliert worden sind:

1. Durchführung der Wasseraufsicht, soweit es um die Abwehr von Gefahren von der Allgemeinheit, dem oder der einzelnen oder den Gewässern geht,
...
3. Durchführung der Abwasser- und Gewässerüberwachung und von wasserwirtschaftlichen Planungen und wissenschaftlichen Untersuchungen zur Erfüllung der Aufgaben nach § 60 Abs. 1 Satz 1.

Der Anwendungsbereich des § 84 Abs. 1 Satz 3 Nr. 3 HWG-E wird damit beschränkt auf die Aufgaben, die die Landesanstalt für Umwelt und das Landesamt für Bodenforschung gem. § 60 HWG-E zu erfüllen haben.

In der zweiten Jahreshälfte stellte sich dann allerdings heraus, daß der Gesetzentwurf in der laufenden Legislaturperiode nicht mehr verabschiedet werden wird. Ich werde mich weiterhin für eine Präzisierung der Datenverarbeitungsnorm einsetzen.

13.2

Errichtung eines Herkunftssicherungs- und Informationssystems für Tiere

Gegen die Einrichtung und den Betrieb einer nationalen Datenbank der Bundesländer, in der neben der Kennzeichnung und Registrierung von Rindern auch die personenbezogenen Daten der Tierhalter eingespeichert werden und an der sich auch Hessen beteiligt, habe ich keine grundsätzlichen datenschutzrechtlichen Bedenken. Allerdings fehlt es bislang an einem Konzept technischer und organisatorischer Maßnahmen, die einen ausreichenden Datenschutzstandard sicherstellen.

Die Europäische Gemeinschaft hat mit der Verordnung Nr. 820/97 vom 21. April 1997 (Amtsblatt der Europäischen Gemeinschaften Nr. L 117/1) die Mitgliedstaaten zur Einführung eines Systems zur Kennzeichnung und Registrierung von Rindern verpflichtet. Ein Element dieses Systems ist die Einrichtung einer zentralen Datenbank, in der die in der Verordnung festgelegten Daten gespeichert werden sollen. Aus Gründen der Effektivität und Wirtschaftlichkeit haben sich die für die Durchführung der Verordnung zuständigen Länder entschlossen, Daten in einer von allen Bundesländern gemeinsam betriebenen Datenbank zu speichern.

13.2.1

Zweck der Datenbank

Durch die zentrale Speicherung der Daten soll eine rasche, aktuelle und umfassende Information über die in der Bundesrepublik Deutschland vorhandenen Rinder sichergestellt werden. Dem Datensatz über die Tiere vorangestellt ist ein sogenannter Betriebsstammsatz. In diesen Datenfeldern sind die personenbezogenen Daten des Betriebsinhabers (z.B. Name, Anschrift, Geburtsdatum etc.) enthalten. Der personenbezogene Teil des Datensatzes ist mit den Datenfeldern über die Rinder

verknüpft. Eine externe Abfrage führt also grundsätzlich auch zur Übermittlung der Angaben über den Tierhalter.

Anlaß für die Errichtung der Datenbank sind die in den vergangenen Jahren gemachten Erfahrungen mit nicht bzw. unzureichend gekennzeichnetem Rindfleisch und die damit verbundene Verunsicherung der Endverbraucher.

Gemäß einem Beschluß der zuständigen Länderressorts vom Dezember 1997 wurde das Bayerische Staatsministerium für Ernährung, Landwirtschaft und Forsten mit der Errichtung und dem Betrieb der Datenbank im Rahmen des Herkunftssicherungs- und Informationssystems beauftragt.

13.2.2

Datenschutzrechtliche Defizite der Vereinbarung

Die Erhebung und Weiterverarbeitung personenbezogener Daten von Rinderhaltern im Rahmen des Systems zur Kennzeichnung und Registrierung von Rindern ist durch Titel I Art. 5 der Verordnung (EG) Nr. 820/97 des Rates vom 21. April 1997 i.V.m. Art. 14 und 18 der Richtlinie 87/12EG des Rates vom 17. März 1997 (Amtsblatt der Europäischen Gemeinschaften Nr. L 109/9) gedeckt.

Danach kann die zuständige Behörde eines Mitgliedstaats ein System von Überwachungsnetzen einführen. In Art. 14 Nr. 3 Buchst. C Nr. 2 ist festgelegt, daß für jeden Betrieb u.a. der Name und die Anschrift des Tierhalters zu erheben sind. Die Hauptziele des Überwachungsnetzes sind die amtliche Qualifikation der Betriebe, die Durchführung regelmäßiger Inspektionen, die Sammlung epidemiologischer Daten und die Überwachung der Krankheiten der Tiere.

Wesentliche Grundlage für eine abschließende datenschutzrechtliche Beurteilung des angestrebten Verfahrens ist nicht nur das Verfahren der Einspeisung und Löschung von personenbezogenen Daten in das Informationssystem. Bislang fehlen mir auch detaillierte Regelungen der Zugriffsberechtigung auf die Daten sowie Aussagen zu den technischen und organisatorischen Maßnahmen nach § 10 Hessisches Datenschutzgesetz (HDSG). Die am 30. September in Kraft getretenen Regelungen der Ländervereinbarung, denen zufolge ein Koordinierungsausschuß Grundsatzfragen des Datenschutzes und der Zugangsberechtigung erörtern und über technische und organisatorische Verfahrensgrundsätze beschließen soll (Art. 7 und 8 der Ländervereinbarung über die Errichtung und Nutzung einer gemeinsamen Datenbank), sind zu unbestimmt. Außerdem bleibt offen, wann das Gremium seine Arbeit aufnehmen soll.

Bereits im April 1998 hatte ich das Ministerium des Innern und für Landwirtschaft, Forsten und Naturschutz angeschrieben und darum gebeten, mir die für die datenschutzrechtliche Beurteilung notwendigen Unterlagen zur Verfügung zu stellen. Inhalt, Aufbau und Umfang der von Bayern aus betriebenen Datenbank sowie die Gewährleistung der nach § 10 HDSG erforderlichen technischen und organisatorischen Maßnahmen sind unklar. Im August habe ich gegenüber dem Hessischen Ministerium des Innern und für Landwirtschaft, Forsten und Naturschutz eine vorläufige Stellungnahme abgegeben, in der ich zwar keine grundsätzlichen datenschutzrechtlichen Bedenken gegen die Einrichtung und den Betrieb der Datenbank geäußert habe, aber erneut auf noch fehlende Unterlagen und eine unzureichende Klärung der Fragen der Zugriffsberechtigung und des technischen und organisatorischen Datenschutzes hingewiesen habe. In einem Schreiben vom 25. August an das Hessische Ministerium für Frauen, Arbeit und Sozialordnung bezog sich das Hessische Ministerium des Innern und für Landwirtschaft, Forsten und Naturschutz auf meine vorläufige Stellungnahme und schlug vor,

die erforderlichen datenschutzrechtlichen Aspekte bei der Beleihung des Hessischen Verbandes für Leistungs- und Qualitätsprüfungen in der Tierzucht e.V. zu berücksichtigen. Der Verband fungiert dabei gemäß Art. 2 Abs. 1 Nr. 2 der Ländervereinbarung als sog. "Regionalstelle" (Art. 6 Abs. 4). Die Regionalstelle ist u.a. für die Pflege und Verwaltung der Betriebs- und Tierdaten sowie der Vergabe der Zugangsberechtigungen zuständig.

Festzuhalten bleibt, daß die Einrichtung der zentralen Datenbank sowie deren Betrieb durch die EG-Verordnung Nr. 820/97 rechtlich zulässig ist. Das erforderliche Datenschutzkonzept ist noch nicht zu meiner Zufriedenheit fixiert. Im Zusammenhang mit der Errichtung der Regionalstelle werde ich die Konkretisierung der Datenschutzmaßnahmen einfordern. Allerdings steht der Beleihungsakt nach den mir vorliegenden Informationen noch aus.

14. Soziales

14.1

Automatisierte Datenabgleiche im Zusammenhang mit Sozialhilfe

Auf der Grundlage des § 117 Bundessozialhilfegesetz ist ein automatisierter Datenabgleich zwischen den Trägern der Sozialhilfe untereinander und mit den Trägern der gesetzlichen Unfall- und Rentenversicherung sowie der Bundesanstalt für Arbeit zulässig.

Nachdem am 1. Januar 1998 die auf § 117 Bundessozialhilfegesetz (BSHG) gestützte Sozialhilfedatenabgleichsverordnung in Kraft getreten ist - den Normen ging eine Diskussion über deren Verhältnismäßigkeit voraus - habe ich mich bei der Stadt Frankfurt über erste Ergebnisse der Umsetzung dieser Normen informiert, um weitere Anhaltspunkte für die Frage der Verhältnismäßigkeit dieser Regelungen zu gewinnen.

§ 117 BSHG

(1) Die Träger der Sozialhilfe sind befugt, Personen, die Leistungen nach diesem Gesetz beziehen, auch regelmäßig im Wege des automatisierten Datenabgleichs daraufhin zu überprüfen, ob und in welcher Höhe und für welche Zeiträume von ihnen Leistungen der Bundesanstalt für Arbeit (Auskunftsstelle) oder der Träger der gesetzlichen Unfall- oder Rentenversicherung (Auskunftsstellen) bezogen werden oder wurden und in welchem Umfang Zeiten des Leistungsbezuges nach diesem Gesetz mit Zeiten einer Versicherungspflicht oder Zeiten einer geringfügigen Beschäftigung zusammentreffen. Sie dürfen für die Überprüfung nach Satz 1 Name, Vorname (Rufname), Geburtsdatum, Geburtsort, Nationalität, Geschlecht, Anschrift und Versicherungsnummer der Personen, die Leistungen nach diesem

Gesetz beziehen, den Auskunftsstellen übermitteln. Die Auskunftsstellen führen den Abgleich mit den nach Satz 2 übermittelten Daten durch und übermitteln die Daten über Feststellungen im Sinne des Satzes 1 an die Träger der Sozialhilfe. Die ihnen überlassenen Daten und Datenträger sind nach Durchführung des Abgleichs unverzüglich zurückzugeben, zu löschen oder zu vernichten. Die Sozialhilfeträger dürfen die ihnen übermittelten Daten nur zur Überprüfung nach Satz 1 nutzen. Die übermittelten Daten der Personen, bei denen die Überprüfung zu keinen abweichenden Feststellungen führt, sind unverzüglich zu löschen. Das Bundesministerium für Gesundheit wird ermächtigt, das Nähere über das Verfahren des automatisierten Datenabgleichs und die Kosten des Verfahrens durch Rechtsverordnung im Einvernehmen mit dem Bundesministerium für Arbeit und Sozialordnung und mit Zustimmung des Bundesrates zu regeln; dabei ist vorzusehen, daß die Zuleitung an die Auskunftsstellen durch eine zentrale Vermittlungsstelle (Kopfstelle) zu erfolgen hat, deren Zuständigkeitsbereich zumindest das Gebiet eines Bundeslandes umfaßt.

(2) Die Träger der Sozialhilfe sind befugt, Personen, die Leistungen nach diesem Gesetz beziehen, auch regelmäßig im Wege des automatisierten Datenabgleichs daraufhin zu überprüfen, ob und in welcher Höhe und für welche Zeiträume von ihnen Leistungen nach diesem Gesetz durch andere Träger der Sozialhilfe bezogen werden oder wurden. Hierzu dürfen die erforderlichen Daten gemäß Absatz 1 Satz 2 anderen Sozialhilfeträgern oder einer zentralen Vermittlungsstelle im Sinne des Absatzes 1 Satz 7 übermittelt werden. Diese führen den Abgleich der ihnen übermittelten Daten durch und leiten Feststellungen im Sinne des Satzes 1 an die übermittelnden Träger der Sozialhilfe zurück. Sind die ihnen übermittelten Daten oder Datenträger für die Überprüfung nach Satz 1 nicht mehr erforderlich, sind diese unverzüglich zurückzugeben, zu löschen oder zu vernichten. Überprüfungsverfahren nach diesem Absatz können

zusammengefaßt und mit Überprüfungsverfahren nach Absatz 1 verbunden werden. Das Bundesministerium für Gesundheit wird ermächtigt, das Nähere über das Verfahren durch Rechtsverordnung mit Zustimmung des Bundesrates zu regeln.

Die Stadt Frankfurt hat mir einen präzisen Vermerk zugeleitet, in dem u.a. folgende Details der Datenabgleiche dokumentiert sind:

Im Vorfeld des ersten automatisierten Datenabgleichs wurden die Hilfeempfängerinnen und Hilfeempfänger mittels Serienbrief und Merkblatt über die bevorstehende Aktion informiert. Für den Fall einer freiwilligen Ergänzung von Einkommensangaben bis zum 15. Mai 1998 wurde der Verzicht auf Strafanzeigen zugesichert.

Parallel hierzu wurde in allen Organisationseinheiten des Sozialamtes mit Informationsplakaten und Merkblättern auf den Datenabgleich und die Möglichkeit der Ergänzungen der Angaben hingewiesen.

Insgesamt wurden in 74 Leistungsfällen "freiwillige" Ergänzungen der Einkommensangaben vorgenommen. Der Rückforderungsbetrag aus dieser Aktion liegt bei rund 181.500 DM.

Für den Anfragezeitraum 1. Januar 1998 bis 31. März 1998 wurden aus dem DV-Verfahren PROSOZ 29.359 Anfragesätze erstellt. Diese bezogen sich auf Hilfeempfängerinnen und Hilfeempfänger zwischen 18 und 65 Jahren und die Hilfearten HLU (Hilfe zum Lebensunterhalt), HbL (Hilfe in besonderen Lebenslagen) oder AsylbLG (Asylbewerberleistungsgesetz).

Der Personenkreis der bis siebzehnjährigen Hilfeempfängerinnen und Hilfeempfänger wurde ebenso wie die über 65-jährigen Hilfeempfängerinnen und Hilfeempfänger (letztere wegen der generellen Nutzung des Rentenauskunftsverfahrens) zunächst nicht

in die Überprüfung einbezogen. Beide Personenkreise sind für künftige Datenabgleiche vorgesehen, wenn die Programme ihre Zuverlässigkeit bewiesen haben.

Als Ergebnis des Datenabgleichs wurden 8.495 positive Antwortsätze rückgemeldet. Durch die Mitarbeiterinnen und Mitarbeiter der Wirtschaftlichen Sozialhilfe waren im besonderen die positiven Antwortdatensätze mit den Angaben der Wirtschaftsakten abzugleichen.

In 626 Fällen wurde ein unrechtmäßiger Leistungsbezug festgestellt, die Gesamthöhe der festgestellten unrechtmäßigen Leistungen beträgt hierbei 1.275.154,10 DM.

In diesen Fällen aufgedeckter zusätzlicher Einkommen sind sowohl einmalige Einkünfte als auch dauernde Einkommen oder Renten enthalten. Dementsprechend kann die "Schadenssumme" nicht für die Zukunft hochgerechnet werden. Ob der Gesamtbetrag durch Rückforderungen oder Verrechnungen im Rahmen der weiteren Hilfestellung zurückerstattet wird, bleibt abzuwarten.

Die durchschnittlichen HLU-Fallzahlen aus PROSOZ liegen bei 23.650 Fällen, die festgestellten 626 Fälle entsprechen somit 2,64 Prozent dieses Bestandes.

Die Gesamtausgaben für HLU und HbL liegen ohne die Ausgaben der Altenhilfe bei ca. 600 Millionen DM jährlich.

Die Gesamthöhe der unrechtmäßig bezogenen Leistungen von 1.275.154,10 DM entsprechen somit 0,2 Prozent der Jahresausgaben für HLU und HbL bzw. 0,4 Prozent der reinen HLU-Jahresausgaben aus PROSOZ.

Das bisherige Ergebnis ist insofern erfreulich, als verdachtsunabhängige Kontrollen den Vorteil haben können, den

gelegentlich anzutreffenden generellen Verdacht massiven Sozialhilfemißbrauchs zu falsifizieren. Freilich ist angesichts der aufgedeckten geringen Mißbrauchsquote die datenschutzrechtliche Verhältnismäßigkeit besagter Abgleiche fraglich. Mit Blick auf die Gesamthöhe der festgestellten unrechtmäßig bezogenen Leistungen - über 1 Million DM - ist die Verhältnismäßigkeit meines Erachtens aber noch zu bejahen. Ich werde mich auch zukünftig bei der Stadt Frankfurt über die weitere Entwicklung bei der Umsetzung des § 117 BSHG informieren.

14.2

Zusammenarbeit des Jugendamtes mit anderen Behörden und freien Trägern der Kinder- und Jugendhilfe

Das Datenschutzrecht steht weder der Förderung des Wohls von Kindern und Jugendlichen noch der Abwehr von Gefahren entgegen.

Jugendämter und freie Träger der Kinder- und Jugendhilfe bitten mich häufig darum, sie in datenschutzrechtlicher Hinsicht zu beraten. Dabei werde ich oft mit der Befürchtung konfrontiert, der Datenschutz könne möglicherweise einer sinnvollen Kinder- und Jugendhilfearbeit entgegenstehen, insbesondere was die aus fachlicher Sicht für geboten gehaltene Zusammenarbeit mit anderen Stellen betrifft.

Diese Befürchtung ist unbegründet. Im Sozialgesetzbuch VIII, das die Kinder- und Jugendhilfe regelt, sind bereichsspezifische Datenschutzregelungen enthalten, die sich am Wohl der Kinder und Jugendlichen orientieren. Die Datenverarbeitung ist zulässig, soweit sie für die Aufgabenerfüllung der Jugendämter und freien Träger (§ 61 Abs. 4 SGB VIII) erforderlich ist. Es ist insbesondere auch Aufgabe dieser Stellen, die Kinder und Jugendlichen zu fördern und zu schützen.

§ 1 SGB VIII

(1) Jeder junge Mensch hat ein Recht auf Förderung seiner Entwicklung und auf Erziehung zu einer eigenverantwortlichen und gemeinschaftsfähigen Persönlichkeit.

...

(3) Jugendhilfe soll zur Verwirklichung des Rechts nach Abs. 1 insbesondere

1. junge Menschen in ihrer individuellen und sozialen Entwicklung fördern und dazu beitragen, Benachteiligungen zu vermeiden oder abzubauen,
2. Eltern und andere Erziehungsberechtigte bei der Erziehung beraten und unterstützen,
3. Kinder und Jugendliche vor Gefahren für ihr Wohl schützen,
4. dazu beitragen, positive Lebensbedingungen für junge Menschen und ihre Familien sowie eine kinder- und familienfreundliche Umwelt zu erhalten oder zu schaffen.

Diese Verantwortung der Jugendhilfeträger wird auch in der einschlägigen Literatur und Rechtsprechung immer wieder betont, wobei die strafrechtliche und zivilrechtliche Perspektive nicht ausgeblendet bleibt. So ist das Thema "Kommunale Jugendhilfe und strafrechtliche Garantenhaftung" der Titel eines jüngeren Beitrags (Bringewat, NJW 1998, S. 944 ff.), und das Landgericht Hamburg hat entschieden, daß einem Vater kein Schmerzensgeld gegen eine Psychologin zusteht, weil diese ihn durch eine gutachterliche Stellungnahme in den - später ausgeräumten - Verdacht gebracht hat, seine Tochter sexuell mißbraucht zu haben (NJW 1998, S. 85). Freilich ist das Urteil mitnichten ein Freibrief, Väter zu denunzieren, sondern das Gericht sah im konkreten Fall kein rechtswidrig-schuldhaftes Handeln der Psychologin.

Die durch das Kinder- und Jugendhilferecht den Jugendämtern auferlegte Pflicht, das Kindes- und Jugendwohl zu fördern, kann gerade auch die eingangs angesprochene Kooperation mit anderen Stellen zur Folge haben. So ist etwa die mir von einem Jugendamt vorgetragene Überlegung, man habe es mit einem sich illegal seit kurzem in der Bundesrepublik aufhaltenden ausländischen Jugendlichen zu tun und man wolle die Ausländerbehörde kontaktieren, weil es für den Jugendlichen besser sei, schnell als nach längerer Verfestigung abgeschoben zu werden, aus datenschutzrechtlicher Sicht ebensowenig zu kritisieren wie die Ansicht eines anderen Jugendamtes, für die Entwicklung eines zu abweichendem Verhalten neigenden Jugendlichen sei es förderlich, mit der Polizei Kontakt aufzunehmen, um den Jugendlichen mit dieser Behörde zu konfrontieren.

In Fällen des Verdachts auf sexuellen Mißbrauch eines Kindes oder Jugendlichen sind die Jugendämter auch zur Strafanzeige berechtigt; darauf hat schon der baden-württembergische Landesbeauftragte für Datenschutz in seinem 18. Tätigkeitsbericht hingewiesen (S. 69 f.).

14.3

Bekämpfung von Sozialhilfemißbrauch mit falschen Mitteln

Für die Datenerhebung eines Sozialamtes gilt der Grundsatz, daß die Daten beim Betroffenen selbst zu erheben sind. Dieser Grundsatz gilt auch im Rahmen der Mißbrauchsbekämpfung.

Die Gewährung einer einmaligen Beihilfe zum Kauf von Hausrat gehört zu den Leistungen nach dem Bundessozialhilfegesetz (BSHG), deren bestimmungsgemäße Verwendung ein Hilfeempfänger in geeigneter Weise gegenüber dem Sozialamt nachzuweisen hat.

Ein Hilfeempfänger hat sich an mich gewandt, weil die Vorlage einer Quittung mit detaillierter Aufstellung für die Anschaffung von gebrauchtem Hausrat aus einer Haushaltsauflösung dem Sozialamt einer Taunusgemeinde als Nachweis nicht ausreichte und das Sozialamt die Richtigkeit der Quittungsangaben überprüfte.

Nach Darstellung des Hilfeempfängers erfragte ein Mitarbeiter des Sozialamtes telefonisch die Richtigkeit der Quittung bei der Ausstellerin, d.h. bei einer nicht-öffentlichen Stelle. Diese Darstellung hat mir das betroffene Sozialamt bestätigt.

Nach § 67a Sozialgesetzbuch (SGB) X sind Sozialdaten grundsätzlich beim Betroffenen selbst zu erheben. Eine Befragung Dritter bringt immer einen stärkeren Eingriff in die Persönlichkeit des Betroffenen mit sich, insbesondere auch deshalb, weil damit immer zugleich auch eine Offenbarung personenbezogener Daten über den Betroffenen an den Dritten verbunden ist. Nach dem Grundsatz der Verhältnismäßigkeit ist daher zunächst der Betroffene selbst zu fragen. Einige Ausnahmen sind gesetzlich festgelegt.

§ 67a SGB X

(1) Das Erheben von Sozialdaten durch in § 35 des ersten Buches genannte Stellen ist zulässig, wenn ihre Kenntnis zur Erfüllung einer Aufgabe der erhebenden Stelle nach diesem Gesetzbuch erforderlich ist.

(2) Sozialdaten sind beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden,

1. bei den in § 35 des Ersten Buches oder in § 69 Abs. 2 genannten Stellen, wenn
 - a) diese zur Übermittlung der Daten an die erhebende Stelle

befugt sind,

b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und

c) keine Anhaltspunkte dafür bestehen, daß überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden,

2. bei anderen Personen oder Stellen, wenn

a) eine Rechtsvorschrift die Erhebung bei ihnen zuläßt oder die Übermittlung an die erhebende Stelle ausdrücklich vorschreibt oder

b) aa) die Aufgaben nach diesem Gesetzbuch ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich machen oder

bb) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte dafür bestehen, daß überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

(3) Werden Sozialdaten beim Betroffenen mit seiner Kenntnis erhoben, so ist der Erhebungszweck ihm gegenüber anzugeben. Werden sie beim Betroffenen aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf sowie auf die Rechtsvorschrift, die zur Auskunft verpflichtet und die Folgen der Verweigerung von Angaben, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen.

(4) Werden Sozialdaten statt beim Betroffenen bei einer nicht-öffentlichen Stelle erhoben, so ist die Stelle auf die Rechtsvorschrift, die zur Auskunft verpflichtet, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen.

Im konkreten Fall lagen die Voraussetzungen der Ausnahmeregelungen nicht vor. Das Sozialamt hatte nicht die

Möglichkeiten ausgeschöpft, den Sachverhalt mit dem Betroffenen selbst durch ein Gespräch, evtl. Hausbesuch etc. zu klären.

Bei der telefonischen Anfrage bei der Ausstellerin der Quittung hat das Sozialamt auch nicht beachtet, daß es gemäß § 67a Abs. 4 SGB X auf die Rechtsvorschrift, die zur Auskunft verpflichtet, sonst auf die Freiwilligkeit der Angaben, hinweisen muß.

Das Sozialamt hat unter den von mir dargelegten Gesichtspunkten meine Rechtsauffassung bestätigt und die Mitarbeiterinnen angewiesen, derartige Anfragen nicht mehr durchzuführen.

14.4

Verdeckte Ermittlungen durch eine vom Sozialamt beauftragte Detektei

Das geltende Sozialdatenschutzrecht enthält keine Rechtsgrundlage für verdeckte Ermittlungen

Ein Frankfurter Bürger hat sich mit der Frage an mich gewandt, ob es zulässig sei, daß er und seine Frau wegen des Verdachts des Sozialamtes, sie bezögen unberechtigt Sozialhilfe, mehrere Tage akribisch von einer Detektei überwacht wurden.

Anders als im Hessischen Datenschutzgesetz (§ 12 Abs. 3, 5) ist im einschlägigen Sozialgesetzbuch X und im Bundessozialhilfegesetz die Datenerhebung beim Betroffenen ohne seine Kenntnis nicht vorgesehen.

Ich habe dies zum Anlaß genommen, in die betreffenden Sozialhilfeakten Einsicht zu nehmen und der Stadtverwaltung Gelegenheit zu geben, ihre Entscheidung zur Beauftragung der privaten Detektei zu begründen. Zur Wahrung des Datenschutzes bin ich nicht befugt, die den Einzelfall betreffenden

Verfahrensabläufe, die der Auftragserteilung an die private Detektei vorausgingen, der Öffentlichkeit mitzuteilen. Ich beschränke mich deshalb auf die Auskunft, daß das Sozialamt Umstände dargelegt hat, die es verständlich erscheinen lassen, daß die Stadt den Fall als außergewöhnlich angesehen und nach Mitteln zur Überprüfung der Voraussetzungen der Sozialhilfe gesucht hat, die über das übliche Verwaltungsinstrumentarium hinausgehen.

Der Auftrag an eine private Detektei, eine Observation durchzuführen, wäre nur zulässig, wenn es dafür eine gesetzliche Grundlage gäbe. Eine solche ist nicht vorhanden. Dies habe ich dem Betroffenen und der Stadt Frankfurt mitgeteilt; auch habe ich kritisiert, daß vor der Überwachung der behördliche Datenschutzbeauftragte und meine Behörde nicht konsultiert worden sind.

15. Personalwesen

15.1

Kontrollrecht des behördlichen Datenschutzbeauftragten

Der behördliche Datenschutzbeauftragte hat nicht das Recht, den Personalrat gegen dessen Willen zu kontrollieren.

Der behördliche Datenschutzbeauftragte einer Kommune hat angefragt, ob er berechtigt sei, die Personaldatenverarbeitung des Personalrats auch dann zu überprüfen, wenn dieser nicht damit einverstanden ist.

Anlaß der Anfrage des behördlichen Datenschutzbeauftragten war ein Urteil des Bundesarbeitsgerichts (Beschluß vom 11. November 1997 - 1 ABR 21/97, NJW 1998, 2466), in dem ein Kontrollrecht des betrieblichen Datenschutzbeauftragten gegenüber dem Gesamtbetriebsrat verneint wird. Die Frage eines Kontrollrechts des betrieblichen Datenschutzbeauftragten wird allerdings bereits seit einiger Zeit kontrovers diskutiert. Sie ist auch von erheblicher praktischer Bedeutung, denn der Betriebsrat verarbeitet in zunehmendem Umfang sensitive personenbezogene Daten von Arbeitnehmerinnen und Arbeitnehmern.

Für ein Kontrollrecht des betrieblichen Datenschutzbeauftragten gegenüber dem Betriebsrat sind in den bisherigen Diskussionen insbesondere die folgenden Argumente vorgetragen worden:

- Der Betriebsrat eines Unternehmers ist kein Dritter, sondern Teil der speichernden Stelle.
- Das Bundesdatenschutzgesetz sieht keine Einschränkungen des Kontrollrechts des betrieblichen Datenschutzbeauftragten innerhalb des Unternehmens vor.

- Der zunehmende Umfang der vom Betriebsrat - auch automatisiert - verarbeiteten Daten der Arbeitnehmerinnen und Arbeitnehmer erfordert eine effektive Datenschutzkontrolle vor Ort.
- Eine Selbstkontrolle des Betriebsrates ist schwierig, da der Vorsitzende des Betriebsrates nur geschäftsführende Funktion und nicht die Befugnis eines Vorgesetzten gegenüber den übrigen Betriebsratsmitgliedern hat.

In der Diskussion sind allerdings auch eine Reihe von Argumenten gegen ein Kontrollrecht des internen Datenschutzbeauftragten vorgebracht worden. Diese Aspekte waren letztlich auch für die Entscheidung des Bundesarbeitsgerichts maßgeblich:

- Das Betriebsverfassungsgesetz steht einer Kontrolle des Betriebsrates durch den betrieblichen Datenschutzbeauftragten entgegen. Der Datenschutzbeauftragte wird vom Arbeitgeber ausgewählt und ist daher der Arbeitgeberseite zuzurechnen. Er kann nicht aus eigenem Recht für die Einhaltung des Datenschutzes sorgen und evtl. Verstöße abstellen, er hat weder eigene Anordnungs- noch Klagebefugnisse. Andernfalls ist die Unabhängigkeit der Betriebsräte vom Arbeitgeber gefährdet. Arbeitgeber und Betriebsräte müssen sich unabhängig voneinander ihre Meinung bilden können, insbesondere Verhandlungsziele etc. entwickeln können.
- Das Bundesdatenschutzgesetz ist lückenhaft, weil es das Verhältnis der beiden Organe zueinander nicht regelt. Der Gesetzgeber wollte aber mit der Verabschiedung des Bundesdatenschutzgesetzes nicht in die Strukturprinzipien des Betriebsverfassungsgesetzes eingreifen.
- Der Arbeitgeber hat nach dem Betriebsverfassungsgesetz keine Verantwortung für die Rechtmäßigkeit der Amtsausübung des

Betriebsrates.

- Der Arbeitgeber haftet Dritten gegenüber nicht für unerlaubte Handlungen des Betriebsrates.
- Die im Bundesdatenschutzgesetz festgelegte Verschwiegenheitspflicht des internen Datenschutzbeauftragten bezieht sich nicht auf Daten, die den Meinungsbildungsprozeß des Betriebsrates betreffen.

Nach meiner Auffassung sind die zentralen Argumente gegen ein Kontrollrecht des betrieblichen Datenschutzbeauftragten im wesentlichen auf den öffentlichen Bereich übertragbar. Das Bundesverwaltungsgericht hat die Frage hinsichtlich der Personalvertretungen im öffentlichen Dienst allerdings bislang offen gelassen (BVerwG Beschluß vom 4. September 1990 - 6 P 28.87 - AP Nr. 1 zu § 68 BPersVG). Die Überlegungen zur Unabhängigkeit des Betriebsrates treffen meiner Ansicht nach auch auf die Unabhängigkeit des Personalrates zu. Auch die Tatsache, daß der behördliche Datenschutzbeauftragte nur im Zusammenwirken mit der Personalvertretung bestellt werden kann, gibt zu einer grundsätzlich anderen rechtlichen Bewertung keinen hinreichenden Anlaß. Dies schließt selbstverständlich nicht aus, daß der interne Datenschutzbeauftragte den Personalrat in datenschutzrechtlichen Fragen berät.

Ich habe das dem anfragenden behördlichen Datenschutzbeauftragten der Kommune mitgeteilt. Gleichzeitig habe ich darauf hingewiesen, daß die Datenverarbeitung der Personalräte hessischer Stellen meiner Kontrolle unterliegt, und eine solche Kontrolle auch vom behördlichen Datenschutzbeauftragten angeregt werden kann.

Umgekehrt können Personalräte, gerade auch im Bereich der automatisierten Personaldatenverarbeitung der Dienststelle, meine Kontrolltätigkeit veranlassen.

§ 34 Abs. 5 HDSG

Vor Einführung, Anwendung, Änderung oder Erweiterung eines automatisierten Verfahrens zur Verarbeitung von Daten der Beschäftigten hat die Dienststelle das Verfahrensverzeichnis (§ 6) der Personalvertretung im Rahmen des personalvertretungsrechtlichen Beteiligungsverfahrens mit dem Hinweis vorzulegen, daß sie eine Stellungnahme des Hessischen Datenschutzbeauftragten fordern kann. Macht die Personalvertretung von dieser Möglichkeit Gebrauch, beginnt die von ihr einzuhaltende Frist erst mit der Vorlage der von der Dienststellenleitung einzuholenden Stellungnahme.

15.2

Personaldatenverarbeitung

Das im Hessischen Beamtengesetz geregelte Personalaktenrecht geht den das Personalwesen betreffenden Vorschriften im Hessischen Datenschutzgesetz vor.

Mich erreichen regelmäßig Anfragen von personalverwaltenden Stellen, die grundsätzliche Fragen der Personaldatenverarbeitung betreffen. Offenbar ist noch nicht überall bekannt, daß das in den §§ 107 ff. Hessisches Beamtengesetz (HGB) geregelte Personalaktenrecht gegenüber § 34 Hessisches Datenschutzgesetz (HDSG) vorrangig ist.

§ 34 HDSG (neue Fassung)

(1) Der Dienstherr oder Arbeitgeber darf Daten seiner

Beschäftigten nur verarbeiten, wenn dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung innerdienstlicher planerischer, organisatorischer, sozialer und personeller Maßnahmen erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung es vorsieht. Die für das Personalaktenrecht geltenden Vorschriften des Hessischen Beamtengesetzes sind, soweit tarifvertraglich nichts anderes geregelt ist, auf Angestellte und Arbeiter im öffentlichen Dienst entsprechend anzuwenden.

(2) Abweichend von § 16 Abs. 1 ist eine Übermittlung der Daten von Beschäftigten an Personen und Stellen außerhalb des öffentlichen Bereichs nur zulässig, wenn der Empfänger ein rechtliches Interesse darlegt, der Dienstverkehr es erfordert oder der Betroffene eingewilligt hat. Die Übermittlung an einen künftigen Dienstherrn oder Arbeitgeber ist nur mit Einwilligung des Betroffenen zulässig.

(3) Das Auskunftsrecht nach § 18 Abs. 3 umfaßt auch die Art der automatisierten Auswertung der Daten des Beschäftigten. § 18 Abs. 6 findet keine Anwendung.

(4) Im Falle des § 19 Abs. 3 Satz 1 sind die Daten der Beschäftigten zu löschen. Daten, die vor der Eingehung eines Dienst- oder Arbeitsverhältnisses erhoben wurden, sind unverzüglich zu löschen, sobald feststeht, daß ein Dienst- oder Arbeitsverhältnis nicht zustande kommt. Dies gilt nicht, wenn Grund zu der Annahme besteht, daß durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden.

(5) Vor Einführung, Anwendung, Änderung oder Erweiterung eines automatisierten Verfahrens zur Verarbeitung von Daten der Beschäftigten hat die Dienststelle das Verfahrensverzeichnis (§ 6) der Personalvertretung im Rahmen des

personalvertretungsrechtlichen Beteiligungsverfahren mit dem Hinweis vorzulegen, daß sie eine Stellungnahme des Hessischen Datenschutzbeauftragten fordern kann. Macht die Personalvertretung von dieser Möglichkeit Gebrauch, beginnt die von ihr einzuhaltende Frist erst mit der Vorlage der von der Dienststellenleitung einzuholenden Stellungnahme.

(6) Daten der Beschäftigten, die im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen nach § 10 Abs. 2 gespeichert werden, dürfen nicht zu Zwecken der Verhaltens- oder Leistungskontrolle ausgewertet werden.

Zwar ist § 34 HDSG eine bereichsspezifische Vorschrift zum Datenschutz bei Dienst- und Arbeitsverhältnissen, sie ist aber im Verhältnis zum im Hessischen Beamtengesetz geregelten Personalaktenrecht nachrangig, weil im Beamtenrechtsrahmengesetz des Bundes für die Länder verbindliche Vorgaben für das Personalaktenrecht normiert worden sind, die durch das Hessische Datenschutzgesetz nicht verdrängt werden können. Was die Zulässigkeit der Personaldatenverarbeitung betrifft, hat das z.T. gravierende Auswirkungen.

So sah der bisherige § 34 Abs. 8 HDSG die Verarbeitung von Personaldaten zu Planungszwecken nur unter einschränkenden Voraussetzungen vor, während § 107 Abs. 4 HBG dies generell zuläßt.

§ 107 Abs. 4 HBG

Der Dienstherr darf personenbezogene Daten über Bewerber, Beamte und ehemalige Beamte nur erheben, soweit dies zur Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu

Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift dies erlaubt. Fragebogen, mit denen solche Daten erhoben werden, bedürfen der Genehmigung durch die oberste Dienstbehörde.

Da § 107 Abs. 4 HBG den bisherigen § 34 Abs. 8 HDSG obsolet werden ließ, ist letzterer konsequenterweise im neuen Hessischen Datenschutzgesetz nicht mehr enthalten.

Das gleiche rechtliche Schicksal hat auch die Bestimmung ereilt, die die automatisierte Verarbeitung von Beurteilungen der Beschäftigten rigoros verbot, § 34 Abs. 6 HDSG (alte Fassung). Das Personalaktenrecht im Hessischen Beamtengesetz enthält zwar nach wie vor eine restriktive Regelung hinsichtlich der automatisierten Datenverarbeitung sensibler Personaldaten, es läßt jedoch die automatisierte Verarbeitung jetzt in bestimmten Grenzen zu.

§ 107g HBG

...

(3) Von den Unterlagen über medizinische oder psychologische Untersuchungen und Tests dürfen im Rahmen der Personalverwaltung nur die Ergebnisse automatisiert verarbeitet oder genutzt werden, soweit sie die Eignung betreffen und ihre Verarbeitung oder Nutzung dem Schutz des Beamten dient.

(4) Beamtenrechtliche Entscheidungen dürfen nicht ausschließlich auf Informationen und Erkenntnisse gestützt werden, die unmittelbar durch automatisierte Verarbeitung personenbezogener Daten gewonnen werden.

...

Das im Hessischen Beamtengesetz plazierte Personalaktenrecht gilt nicht nur für die Beamten. § 34 Abs. 1 Satz 2 HDSG legt fest, daß es entsprechend auf Angestellte und Arbeiter im öffentlichen

Dienst anzuwenden ist, soweit tarifvertraglich nichts anderes geregelt ist. Soweit ersichtlich ist dies bislang nicht der Fall.

Personalverwaltende Stellen müssen sich also generell und vorrangig am Personalaktenrecht des Hessischen Beamtengesetzes orientieren. Nur soweit dieses keine Regelung trifft, gilt § 34 HDSG; das gilt etwa für das personalvertretungsrechtliche Beteiligungsverfahren nach § 34 Abs. 5 HDSG.

16. Verfassungsschutz

16.1

Untergesetzliche Vorschriften des Landesamtes für Verfassungsschutz

Das Landesamt für Verfassungsschutz hat im Berichtszeitraum einen Arbeitsplan für die Abteilung Auswertung erstellt. Meine Änderungsvorschläge wurden aufgenommen.

Im letzten Tätigkeitsbericht (Ziff. 14.2) hatte ich berichtet, daß das Landesamt für Verfassungsschutz (LfV) eine Reihe von untergesetzlichen Vorschriften erlassen hat, die die entsprechenden Normen des Gesetzes über das Landesamt für Verfassungsschutz vom 19. Dezember 1990 (VerfSchG) konkretisieren. Die damals angesprochene Dienstvorschrift Auswertung ist nun wiederum - wie vorgesehen - durch einen Arbeitsplan Auswertung ergänzt worden. Die Entwürfe des Arbeitsplans wurden auf meine Anregung mehrmals geändert.

Der Arbeitsplan Auswertung ist als "VS-Vertraulich" eingestuft, so daß ich dessen Inhalt hier nicht wiedergeben kann.

Gegenstand des Arbeitsplans sind Konkretisierungen der Vorschriften des Verfassungsschutzgesetzes zur Speicherung und Löschung von Daten in Dateien. Im vorliegenden Fall geht es um die Verarbeitung von personenbezogenen Informationen im Nachrichtendienstlichen Informationssystem (NADIS) und in der Arbeitsdatei (LARGO).

§ 3 Abs. 1 Satz 1 VerfSchG

Das Landesamt für Verfassungsschutz darf zur Erfüllung seiner Aufgaben nach § 2 die erforderlichen Informationen erheben und

weiterverarbeiten, soweit nicht der Zweite Teil dieses Gesetzes besondere Bestimmungen für personenbezogene Daten enthält.

§ 6 VerfSchG

(1) Umfang und Dauer der Speicherung personenbezogener Daten sind auf das für die Aufgabenerfüllung des Landesamtes für Verfassungsschutz erforderliche Maß zu beschränken.

...

(6) Das Landesamt für Verfassungsschutz prüft bei der Einzelfallbearbeitung und im übrigen nach von ihm festgesetzten angemessenen Fristen, spätestens jedoch nach fünf Jahren, ob gespeicherte Daten zur Aufgabenerfüllung noch erforderlich sind. Gespeicherte personenbezogene Daten über Bestrebungen nach § 2 Abs. 2 Nr. 1 und 3 sind spätestens zehn Jahre nach dem Zeitpunkt der letzten gespeicherten relevanten Information zu sperren, es sei denn, der Behördenleiter oder sein Vertreter trifft im Einzelfall die Entscheidung, daß sie weiter gespeichert bleiben. Soweit Daten automatisiert verarbeitet oder Akten automatisiert erschlossen werden, ist auf den Ablauf der Fristen nach Satz 1 und 2 hinzuweisen.

Einer der Diskussionspunkte zwischen dem LfV und mir war die vorgesehene Speicherung von Daten zu bisher nicht identifizierbaren Personen und Objekten. Gemeint sind damit Personen und Objekte, deren Identifizierungsdaten (z.B. Namen, Geburtsdatum, Wohnort) dem LfV nicht bekannt sind. Eine Speicherung kommt nur dann in Frage, wenn zumindest eine Personenbeschreibung oder eine Information vorliegt, die eine eindeutige Unterscheidung von anderen Personen oder Objekten zuläßt. Vorgesehen ist weiterhin eine zeitlich begrenzte Speicherung für diese Fälle.

Ersatzlos gestrichen hat das LfV eine Bestimmung über die Speicherung von Daten zu Personen, bei denen nach meiner Auffassung die Voraussetzungen des Gesetzes über das Landesamt für Verfassungsschutz nicht vorliegen.

Präzisierungen im Arbeitsplan erfolgten auf meine Anregung bei der im Gesetz über das Landesamt für Verfassungsschutz vorgesehenen Speicherung von Daten Unbeteiligter.

§ 3 Abs. 1 Satz 2 VerfSchG

Zur Aufgabenerfüllung nach § 2 Abs. 2 dürfen unbeschadet des § 4 Abs. 1 personenbezogene Daten von Personen, bei denen keine tatsächlichen Anhaltspunkte dafür vorliegen, daß sie selbst Bestrebungen oder Tätigkeiten im Sinne des § 2 Abs. 2 nachgehen (Unbeteiligte), nur erhoben, verarbeitet oder genutzt werden, wenn

1. dies für die Erforschung von Bestrebungen oder Tätigkeiten nach § 2 Abs. 2 vorübergehend erforderlich ist,
2. die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre und
3. überwiegende schutzwürdige Belange der betroffenen Personen nicht entgegenstehen.

Eine Klarstellung des Gesetzestextes erfolgte u.a. auch bei dem sog. Prüffall:

§ 6 Abs. 4 VerfSchG

Personenbezogene Daten, die erhoben worden sind, um zu prüfen, ob Bestrebungen oder Tätigkeiten nach § 2 Abs. 2 vorliegen, dürfen in Dateien erst gespeichert werden, wenn sich tatsächliche Anhaltspunkte für derartige Bestrebungen oder Tätigkeiten ergeben haben. Bis zu diesem Zeitpunkt dürfen auch keine Akten angelegt werden, die zur Person geführt werden.

Unter dem Prüffall versteht man Personen oder Organisationen, bei denen noch keine förmliche Entscheidung über die Frage der Beobachtung durch den Verfassungsschutz getroffen wurde, bei denen aber gewisse Anhaltspunkte auf verfassungswidrige Tätigkeiten oder Bestrebungen hinweisen. Informationen zu derartigen Personen oder personenbezogene Daten zu derartigen Organisationen dürfen nicht in Dateien gespeichert werden.

16.2

System LARGO beim Verfassungsschutz

Das Datenverarbeitungssystem des Landesamtes für Verfassungsschutz wird seit Anfang 1998 im Bereich Linksextremismus eingesetzt. Meine Verbesserungsvorschläge wurden aufgenommen.

Im letzten Tätigkeitsbericht (Ziff. 14.3) hatte ich dargestellt, daß das Landesamt für Verfassungsschutz (LfV) ein neues Datenverarbeitungssystem entwickelt. Die Arbeit daran ist im letzten Jahr weiter fortgeschritten. Bei mehreren Besuchen haben sich meine Mitarbeiter die Neuerungen auf dem Bildschirm zeigen lassen und dabei Verbesserungsvorschläge aus datenschutzrechtlicher Sicht gemacht.

Im Unterschied zum Nachrichtendienstlichen Informationssystem (NADIS) der Verfassungsschutzämter, das in erster Linie zum Auffinden der zu einer Person angelegten Akte dient, können in LARGO die zu einer Person oder zu einem Objekt gehörenden Texte und Informationen im Sinne einer "elektronischen Aktenführung" direkt eingespeichert werden.

Vorgesehen ist, daß beim LfV eingehende oder von ihm erhobene Informationen in aufgearbeiteter und konzentrierter Weise in LARGO eingespeichert werden. Darin liegen aus

datenschutzrechtlicher Sicht Vorteile und Nachteile gegenüber der Informationssammlung in der herkömmlichen Akte:

Vorteilhaft ist die Reduzierung auf das Wesentliche, allerdings kommt es auf Grund des subjektiven Filters des einzelnen Mitarbeiters um so mehr auf die richtige Wertung und Einschätzung von Sachverhalten sowie darauf an, daß klar ist, von wem und von wann die verarbeitete Information stammt. Ich werde diesen Punkt auch künftig aufmerksam verfolgen.

Bei einer Textdatei kann es konsequenterweise dazu kommen, daß die parallele Aktenführung überflüssig ist. Das LfV hat diesen Schritt - viel schneller als ich erwartet habe - im Bereich Linksextremismus vollzogen. Dort werden seit Beginn dieses Jahres Informationen zu neuen Personen ausschließlich in LARGO gespeichert und keine neuen Personenakten mehr angelegt. Originalunterlagen werden in Sachakten gesammelt. Nach Auskunft des LfV ist dies auch für andere Aufgabenbereiche vorgesehen.

Weitere Vorteile aus Sicht des LfV bestehen in verschiedenen weiteren Funktionen, die mit LARGO erfüllt werden: Neue Informationen können in Sekundenschnelle an eine Reihe verschiedener Datensätze verteilt werden, und es können in vielfacher Hinsicht Informationen miteinander verknüpft werden.

Hier kommt es aus datenschutzrechtlicher Sicht darauf an, daß festgelegt wird, wer diese Aktion durchführen darf, und daß dies hinterher rekonstruierbar ist. Andernfalls können beispielsweise Datensätze verfälscht werden, ohne daß der Verantwortliche festgestellt werden kann. Im Gespräch mit Mitarbeitern des LfV haben wir Verbesserungen bei der Protokollierung und Authentifizierung angeregt.

Ich werde die weitere Entwicklung von LARGO beratend begleiten.

17. Schulen

17.1

Die Verschwiegenheitspflicht der Schülervertretung

Beauftragte der Schüler können von einer weiteren Teilnahme an der Klassenkonferenz ausgeschlossen werden, wenn sie ihre Verschwiegenheitspflicht verletzen.

Eine Lehrerin wandte sich an meine Behörde mit der Frage, wie das Schulrecht die Einhaltung der Verschwiegenheitspflicht durchsetzt, wenn Schülerinnen und Schüler an Klassenkonferenzen teilnehmen und dort von oft massivem Fehlverhalten anderer Schülerinnen und Schüler erfahren. Die schulordnungsrechtlichen Konsequenzen werden offen diskutiert. Nicht von der Hand zu weisen ist die Möglichkeit, daß der teilnehmende Schüler sein Wissen in anderen Zusammenhängen mißbraucht. Die Frage kann daher im Schulalltag immer wieder Bedeutung erlangen.

Gem. § 3 der Verordnung über das Verfahren bei Ordnungsmaßnahmen (ABl. 1993, S. 688) hat die Klassenkonferenz die Möglichkeit, beim Schulleiter einen Antrag auf Verfügung bestimmter Ordnungsmaßnahmen zu stellen.

§ 3 Abs. 1 Verordnung über das Verfahren bei Ordnungsmaßnahmen

Die Entscheidung über den Ausschluß von besonderen Klassen- oder Schulveranstaltungen sowie vom Unterricht in Wahlfächern und freiwilligen Unterrichtsveranstaltungen (§ 82 Abs. 2 Nr. 2 Hessisches Schulgesetz (HSchulG)) und über die Androhung der Zuweisung und die Zuweisung einer Parallelklasse oder in eine andere Lerngruppe (§ 82 Abs. 2 Nr. 3 und 4 HSchulG) trifft die Schulleiterin oder der Schulleiter auf Antrag der Klassenkonferenz.

Das Teilnahmerecht der Schülervertretung an der Klassenkonferenz wiederum ergibt sich aus § 122 Abs. 5 Satz 4 HSchulG.

§ 122 Abs. 5 Satz 4 HSchulG

An den sonstigen Konferenzen der Lehrkräfte, mit Ausnahme der Zeugnis- und Versetzungskonferenzen und solcher Konferenzen, in denen ausschließlich Personalangelegenheiten der Lehrerinnen und Lehrer behandelt werden, können bis zu drei Beauftragte des Schülerrats teilnehmen.

Dieses Teilnahmerecht hat eine besondere schuldemokratische Bedeutung: Die Mitbestimmung der Schülerinnen und Schüler an bestimmten schulischen Entscheidungen trägt ihrer Pflicht und ihrem Recht Rechnung, bei der Verwirklichung der Bildungs- und Erziehungsziele der Schule eigenverantwortlich mitzuwirken. Das Einbringen der Schülersicht, gerade bei Themen der Klassenkonferenz, ist eine der zentralen Aufgaben der Schülervertretung. Der Gesetzgeber hat jedoch auch das Problem der Verschwiegenheitspflicht bei Schülern ausreichend berücksichtigt. § 122 Abs. 5 Satz 8 HSchulG verpflichtet die Schülervertretung zur Verschwiegenheit i.S.v. § 103 HSchulG.

§ 122 Abs. 5 Satz 6 HSchulG

§ 103 gilt mit der Maßgabe entsprechend, daß die Konferenz die Schülervertreterinnen und Schülervertreter, die ihre Pflicht zur Verschwiegenheit verletzen, auf Dauer oder Zeit von der weiteren Teilnahme ausschließen können.

§ 103 HSchulG

(1) Bei Angelegenheiten, die ihrer Bedeutung nach einer vertraulichen Behandlung bedürfen, haben die Elternvertreterinnen

und -vertreter auch nach Beendigung ihrer Amtszeit
Verschwiegenheit zu wahren.

(2) Verstößt eine Elternvertreterin oder ein Elternvertreter
hiergegen vorsätzlich oder fahrlässig, so kann der Elternbeirat den
Ausschluß dieses Mitglieds aus der Elternvertretung mit einer
Mehrheit von 2/3 der Mitglieder beschließen.

Gem. § 122 Abs. 5 Satz 6 HSchulG kann daher der betroffene
Schülervertreter bei Verletzung der Verschwiegenheitspflicht von
der weiteren Teilnahme an den Konferenzen ausgeschlossen
werden. Wenn tatsächlich eine Verletzung dieser Pflicht vorliegt,
sollte die Klassenkonferenz von dieser Möglichkeit konsequent
Gebrauch machen, insbesondere auch deshalb, damit künftigen
weiteren Verletzungen der Vertraulichkeit vorgebeugt wird.

17.2

Internet-Nutzung im Schulunterricht

*Die multimediale Nutzung des Internet im Schulunterricht erfordert
eine Einweisung der Schülerinnen und Schüler in die Risiken dieses
Mediums. Eine schulische Benutzungsordnung sollte die jeweiligen
Bedingungen des Internet-Zugangs festlegen.*

Die Verbreitung multimedialer Technik macht auch vor den
Schulstoren nicht halt. Vergleiche im internationalen Rahmen mit
Ländern ähnlich hohen Bildungsstandards lassen die nüchterne
Feststellung zu, daß der schulische Erwerb der Medienkompetenz
in Deutschland erschreckend rückständig ist. In Japan sind alle
Schulen schon heute vernetzt, in den USA soll dies im Jahre 2000
vollzogen sein. In Deutschland konnten 1997 nur fünf Prozent der
Schülerinnen und Schüler einen PC im Unterricht nutzen. Deshalb
hatte die Bundesregierung vor einigen Jahren zusammen mit der
Deutschen Telekom die bundesweite Aktion "Schulen ans Netz"

ins Leben gerufen. In Zusammenarbeit mit den Kultusverwaltungen der Länder sollten binnen drei Jahren ca. 10.000 Schulen einen kostengünstigen Internet-Anschluß bekommen. Die gegenwärtige Umsetzung dieser Praxis wird zunehmend ergänzt durch privates Sponsoring von Computerfirmen und Stiftungen, die den Medieneinsatz in Schulen fördern.

Die Bedeutung neuer Medien in der hessischen Schulentwicklung fand zuletzt ihren Niederschlag in der Beschreibung aktueller Maßnahmen für das Management des schulischen Medieneinsatzes durch das Hessische Kultusministerium (Abl. 1998 S. 641).

Die datenschutzrechtliche Begleitung dieser Entwicklung erfordert allerdings auch konkrete Informationen meines Hauses, deren Kenntnis die Schulverwaltung und die Schülerinnen und Schüler in die Lage versetzen soll, den spezifischen Gefahren der Internet-Nutzung zu begegnen. Die schulischen Nutzungen dieses Mediums sind vielfältig, Schülerinnen und Schüler können "surfen", sich informieren, spielen, Nachrichten versenden und lernen. Dabei werden jedoch auch personenbezogene Daten preisgegeben und Spuren hinterlassen. Es erschien daher sinnvoll, in Zusammenarbeit mit dem Hessischen Kultusministerium eine gemeinsame Richtlinie zu entwickeln, die der Schulleitung, der Informatiklehrkraft und den Schülerinnen und Schülern die notwendigen datenschutzrechtlichen Hinweise vermittelt. Bei Redaktionsschluß lag die Endfassung dieses Papiers noch nicht vor, folgende wesentliche Gefahrenpunkte werden jedoch u.a. angesprochen:

1. Die Nutzung des Internet erfolgt grundsätzlich personenbezogen oder mittels eines Pseudonyms. Es werden Datenspuren hinterlassen, deren Analyse zu Nutzungs- und Kommunikationsprofilen führen kann. Die Kommunikationsdaten lassen sich auf dem Weg durch das öffentliche Netz problemlos auslesen.

2. Die unsichere Netzinfrastruktur des Internet, die bekannten Schwächen bei den Protokollen für die Datenübertragungen und die Nutzung der Programme für die Internet-Dienste lassen Sicherheitslücken entstehen, die dem Hacker bekannt sind und es ihm problemlos ermöglichen, den benutzten Rechner auszuforschen und Daten zu manipulieren oder sogar zu löschen.
3. Werden über das Internet Nachrichten versandt (E-Mail), besteht die Gefahr, daß die Daten mitgelesen werden, ohne daß dies der Absender oder der Empfänger bemerkt (Verlust der Vertraulichkeit). Auch können die Informationen auf ihrem Weg inhaltlich verändert werden, ohne daß dies der Empfänger feststellen kann (Verlust der Authentizität).
4. Mit der elektronischen Post können Programme und Textdokumente übermittelt werden, die Viren tragen und am benutzten Rechner erhebliche Schäden verursachen können.

Diesen Gefahren steht eine ganze Palette von Gegen- und Schutzmaßnahmen gegenüber, deren Kenntnis und Nutzung den Lehrkräften und Schülern ermöglicht werden sollte. Neben technikgestützten Maßnahmen (s. "Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet", s. Ziff. 28) sollten inhaltliche Schutzmechanismen treten: So können etwa anonyme oder pseudonyme Nutzungsformen empfohlen werden, gerade dann, wenn der Schüler eine eigene Internet-Zugangsberechtigung mit persönlicher Kennung erhält.

Sinnvoll ist in allen Fällen eine Benutzungsordnung, die sich jede Schule selbst erstellt und als Vereinbarung zwischen Schulverwaltung, Schülern und Eltern darüber zu verstehen ist, unter welchen Bedingungen der Schul-PC mit Internet-Nutzung

genutzt werden kann. Aufzubauen ist dabei auf ein vorhandenes schulabhängiges Sicherheitsprofil und Nutzungskonzept.

18. Hochschulen

Prüfung der Gesamthochschule Universität Kassel

Eine Prüfung der Gesamthochschule Universität Kassel bestätigte die Erfahrung, daß die Verwaltung großer Behörden in datenschutzrechtlicher Hinsicht deutliche Stärken, aber auch immer kleinere Schwachpunkte haben kann.

Nachdem ich im letzten Jahr bereits einer Fachhochschule einen Prüfbesuch abgestattet hatte (s. 26. Tätigkeitsbericht, Ziff. 16.3), stand in diesem Jahr eine Universität auf dem Prüfprogramm. Um einen Einblick in Verwaltungsabläufe einer großen Einrichtung dieser Art zu gewinnen, wählte ich die Gesamthochschule Universität Kassel (GhK), die in etwa 17.500 Studentinnen und Studenten hat. Die Auswahl stand allerdings auch im Zusammenhang mit dort anstehenden wesentlichen Änderungen der Verwaltungsnetz-Nutzung, die zu diesem Zeitpunkt vorgenommen und von mir beratend begleitet wurden.

Wiederum zwangen mich die begrenzten personellen Kapazitäten, den Prüfbesuch auf wenige Verwaltungsbereiche zu begrenzen. Als Gesamteindruck ließ sich zunächst feststellen, daß die Gesamthochschule Kassel - trotz ihrer Größe - über eine übersichtliche und effizient geführte Verwaltung verfügt, die durch ein modernes, großzügig ausgestattetes DV-System unterstützt wird. Die vorhandene datenschutzrechtliche Sensibilität bei den Führungskräften der Verwaltungsbereiche führte zu schnellen, unbürokratischen Ergebnissen offen angesprochener Probleme; zentrale, gravierende Mängel habe ich nicht festgestellt. Zwar hatte das Hessische Ministerium für Wissenschaft und Kunst - präventiv - im Frühjahr 1998 meinen o.g. Prüfbericht zur Fachhochschule Fulda allen hessischen Hochschulen zur Überprüfung eigener Schwachstellen und zur Stellungnahme

übermittelt. Gleichwohl habe ich Defizite festgestellt, die bereinigt werden konnten.

18.1

Aufbewahrungsfrist für Altakten

Als positiv ist hervorzuheben, daß bei der Gesamthochschule Kassel eine detaillierte Regelung zu den Aufbewahrungsfristen der Verwaltungsakten als Anlage zur Aktenordnung seit langem vorhanden ist und auch umgesetzt wird. Ich habe sie über die regelmäßig tagende Arbeitsgemeinschaft der Datenschutzbeauftragten der Hochschulen an andere Hochschulen weitergeleitet in der Hoffnung, daß es die Arbeit an entsprechenden Regelwerken bei den weiteren Hochschulen erleichtert. Konsequenz ist die Gesamthochschule Kassel auch bei ihrem Versuch, der Pflicht zur Aussonderung der Altakten nach Ablauf der Aufbewahrungsfrist nachzukommen und die Akten dem Staatsarchiv zur Archivierung anzubieten.

18.2

Personalakten

Ein Besuch der zentralen Personalabteilung ist bei jeder größeren Behörde wichtig, weil dort eine beachtliche Sammlung sensitiver Daten existiert. Meine bisherigen Prüferfahrungen veranlaßten zunächst einen stichprobenartigen Blick in den Inhalt der Personalakten der Beamten. Ihr Inhalt ging - wie so oft - über den gesetzlichen Rahmen hinaus. § 107 Abs. 1 Satz 2 Hessisches Beamtengesetz (HBG) enthält folgende Vorgabe:

§ 107 Abs. 1 Satz 2 HBG

Zur Personalakte gehören alle Unterlagen einschließlich der in Dateien gespeicherten, die den Beamten betreffen, soweit sie mit seinem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen (Personalaktendaten); andere Unterlagen dürfen in die Personalakte nicht aufgenommen werden.

Konkretisiert wird diese Regelung durch entsprechende Verwaltungsvorschriften (s. StAnz. 1995, S. 3094 ff.). Die in den geprüften Personalakten vorgefundenen Unterlagen wie etwa Stellenbewertung, Beantragung von Gesundheitszeugnis usw. gehören eindeutig nicht in die Personalakte, da sie den strengen Erforderlichkeitsgrundsätzen nicht entsprechen. Sie sind also Sachakten zuzuordnen. Da die inhaltliche Prüfung und Korrektur aller Beamtenakten jedoch einen recht großen Aufwand bedeutet, habe ich dafür eine längere Frist zugestanden.

Zu beanstanden war auch die freie Zugriffsmöglichkeit aller Bediensteten der Personalabteilung auf alle Personalakten. Dies widerspricht § 107 Abs. 3 HBG.

§ 107 Abs. 3 HBG

Zugang zur Personalakte dürfen nur Beschäftigte haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind, und nur soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist; dies gilt auch für den Zugang im automatisierten Abrufverfahren.

Die Zugriffsmöglichkeit der Bediensteten auf die Akten muß dem Umfang ihrer jeweiligen internen Zuständigkeit für einen abgegrenzten Sachbearbeitungsbereich entsprechen. Nicht hinnehmbar waren auch offene Schränke im Flur und unverschlossene Schränke in den Abteilungen Kindergeld und

Einstellungsvorbereitungen. Diese Mängel wurden umgehend abgestellt.

18.3

Studentensekretariat

Im Bereich des zentralen Studentensekretariats hatte ein Vorfall aus dem letzten Jahr bei der neuen Abteilungsleitung für Nachdenklichkeit gesorgt. Auf Bitten einer privaten Marketing-Firma hatte die Abteilungsleitung Name und Adresse derjenigen Studierenden, die im Bereich der Nahverkehrsbetriebe wohnen, dieser Firma übermittelt zur Vorbereitung einer Umfrage, die für die Verkehrsbetriebe durchgeführt werden sollte. Es ergab sich in der gemeinsamen Bewertung dieses Falles schnell Einigkeit, daß diese Datenübermittlung nur mit Einwilligung der betroffenen Studierenden zulässig gewesen wäre und sich in der geschehenen Form nicht wiederholen darf. Anzuwenden ist hier § 16 Abs. 1 Hessisches Datenschutzgesetz.

§ 16 Abs. 1 HDSG

Die Übermittlung personenbezogener Daten an Personen oder Stellen außerhalb des öffentlichen Bereiches ist über §§ 11 und 13 hinaus zulässig, wenn der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und keine Anhaltspunkte dafür bestehen, daß schutzwürdige Belange des Betroffenen beeinträchtigt werden können.

Zweifellos hatten die Nahverkehrsbetriebe bzw. die Marketing-Firma ein "berechtigtes Interesse" an den Adreßdaten, da sich die geplante Umfrage im Rahmen der Rechtsordnung hielt und nachvollziehbaren Interessen diente. Die Weitergabe der Adreßdaten der Studierenden beeinträchtigte jedoch deren schutzwürdige Belange. Nicht auszuschließen war die Gefahr der

Mißachtung der Zweckbindung bei der Verwendung der Adressen, gerade bei Marketing-Unternehmen. Das gleiche Ziel, Studierende gezielt zu befragen oder zu informieren, wäre erreichbar gewesen mit dem sog. Adreßmittlungsverfahren. Bei diesem Verfahren versieht die Behörde die vorbereiteten Schreiben bzw. Briefkuverts selbst mit Namen und Adressen und versendet die Briefe - gegen Kostenerstattung - unmittelbar. Auf diese Weise wird die Adreßübermittlung an Dritte vermieden.

Kritisiert habe ich auch den nachträglich aufgebrauchten Hinweis auf dem Studentenausweis, daß der Ausweisinhaber die Gebühr für die hochschulinterne Internet-Nutzung entrichtet hat. Diese Ergänzung widerspricht § 4 Abs. 1 der Verordnung über die Verarbeitung personenbezogener Daten und über das Verfahren der Immatrikulation an den Hochschulen (GVBl. 1996, S. 274).

§ 4 Abs. 1 Verordnung über die Verarbeitung personenbezogener Daten und über das Verfahren der Immatrikulation an den Hochschulen

Jede Studentin und jeder Student erhält einen Studenausweis. Der Studenausweis enthält folgende Angaben: Familienname, Vorname, Geburtsdatum, Geburtsort, Studiengang, Datum der Immatrikulation, Matrikelnummer und Gültigkeitsdauer.

Weitere Hinweise zur Person des Ausweisinhabers sind danach nicht zulässig. Der künftige Wegfall des Aufdrucks wurde auch zugesagt.

19. Statistik

Prüfung von kommunalen Statistikstellen

Die Aufgaben der Kommunalstatistik müssen einer Stelle innerhalb der Gemeindeverwaltung übertragen werden, die organisatorisch von anderen Verwaltungsstellen getrennt und räumlich sowie personell abgeschottet ist. Sie darf über Aufgaben der amtlichen Statistik sowie der Kommunalstatistik hinaus keine auf den einzelnen Betroffenen gerichtete Verwaltungsaufgabe wahrnehmen.

19.1

Vorgaben aus dem Landesstatistikgesetz

Im Zusammenhang mit der Durchführung der Volkszählung 1987 hatten die Städte und Gemeinden Erhebungsstellen eingerichtet, die von der übrigen Verwaltung räumlich und personell getrennt sein mußten. Die Einhaltung dieser gesetzlichen Vorgabe haben meine Mitarbeiterinnen und Mitarbeiter seinerzeit intensiv vor Ort geprüft. Nicht zuletzt auf Grund der Volkszählung wurde am 19. Mai 1987 das Gesetz über die Statistik im Land Hessen (Hessisches Landesstatistikgesetz - HessLStatG, GVBl. I S. 67, geändert durch Gesetz zur Änderung des HessLStatG vom 24. November 1994, GVBl. I S. 677) erlassen. Das Gesetz bildet die Grundlage u.a. für die Durchführung von statistischen Umfragen (§ 10 HessLStatG) sowie Kommunalstatistiken (§ 12 HessLStatG) durch die Städte.

Nach diesen Regelungen sind die Gemeinden befugt, zur Wahrnehmung ihrer Aufgaben kommunale Statistiken durchzuführen. Sie regeln die Einzelheiten der Durchführung durch eine Satzung, die u.a. die Erhebungsmerkmale, die Hilfsmerkmale, Art und Weise der Durchführung, den Kreis der zu Befragenden und die Berichtszeit regeln muß (§ 7 Abs. 2 HessLStatG). Die Statistiken sind grundsätzlich ohne Auskunftspflicht der zu

Befragenden durchzuführen. Besteht jedoch eine Auskunftspflicht und werden Erhebungsbeauftragte eingesetzt, kann der Auskunftspflichtige die Auskunft auch schriftlich erteilen (§ 13 HessLStatG). Allerdings haben nur wenige, große Städte die Gelegenheit wahrgenommen, eigenständige, von der Verwaltung getrennte kommunale Statistikstellen einzurichten.

Bei der Einrichtung und Organisation dieser Stellen war ich seinerzeit beteiligt und habe meine Erfahrungen aus der Volkszählung 1987 vermitteln können.

Nach mehr als zehn Jahren habe ich eine Prüfserie begonnen, die zum Ziel hat, die augenblickliche Situation in den Statistikstellen - unter Berücksichtigung der gesetzlichen Vorgaben des Landesstatistikgesetzes - zu kontrollieren. Nach den gesetzlichen Festlegungen sind die kommunalen Statistikstellen organisatorisch von anderen Verwaltungsstellen zu trennen und räumlich sowie personell abzuschotten. Über die Aufgaben der Kommunalstatistik hinaus dürfen von dort aus keine auf den einzelnen Betroffenen gerichtete Verwaltungsaufgaben wahrgenommen werden (§ 12 Abs. 3 HessLStatG). Mit dieser Rechtsnorm soll die eindeutige und für jedermann nachvollziehbare Trennung der amtlichen Statistik von der übrigen Verwaltung sichergestellt werden. Dies war auch eine zentrale Forderung aus dem Volkszählungsurteil von 1983. Für die Übermittlung von Einzelangaben aus Bundesstatistiken an die Gemeinden ist die Existenz einer vom Verwaltungsvollzug abgeschotteten Statistikstelle ebenfalls zwingend erforderlich (§ 16 Abs. 5 BStatG). Da ohne diese organisatorische Maßnahme auch keine kommunalen Umfragen zulässig sind (vgl. dazu 16. Tätigkeitsbericht, Ziff. 5.1.3.2 und 17. Tätigkeitsbericht, Ziff. 7.2.2), ist eine funktionierende Kommunalstatistik ohne eine solche Verwaltungseinheit kaum noch möglich.

19.2

Prüfkriterien

Rechtliche Grundlage für die Arbeit der Kommunalen Statistikstelle ist neben dem Hessischen Landesstatistikgesetz die Satzung, die von der jeweiligen Stadtverordnetenversammlung per Beschluß erlassen wird. In der Satzung sind u.a. die Einzelstatistiken genannt, die erhoben und verarbeitet werden, Übermittlungsverfahren beschrieben sowie Erhebungs- und Hilfsmerkmale festgelegt.

Die Arbeit in der Statistikstelle selbst wird durch eine Organisationsverfügung bzw. eine besondere Dienstanweisung geregelt. In der Dienstanweisung sind die räumliche Unterbringung der Stelle, die Verpflichtung der Mitarbeiterinnen und Mitarbeiter u.a. auf die Wahrung der statistischen Geheimhaltung (§ 16 BStatG und § 16 HessLStatG) sowie Einsichtsrechte und Verfahrensabläufe geregelt. Die Organisationsverfügung beschreibt im einzelnen die Aufgaben, die von der Statistikstelle wahrgenommen werden.

Wegen der korrekten Umsetzung der genannten Regelungen war ein Prüfkriterium auch die Frage, wie mit personenbezogenen Unterlagen umgegangen wird, wo und wie lange diese Unterlagen aufbewahrt werden und wie die erforderliche Trennung von Erhebungs- und Hilfsmerkmalen vollzogen wird.

19.3

Prüfergebnisse

Ich habe im letzten Jahr drei Statistikstellen geprüft. Dabei handelte es sich um die Organisationseinheiten in Kassel, Darmstadt und Fulda.

19.3.1

Statistikstelle der Stadt Darmstadt

Die Statistikstelle der Stadt Darmstadt war bis in das Jahr 1994 dem Amt für Stadtentwicklung zugeordnet. Mit Verfügung des Oberbürgermeisters vom 1. Juni 1994 wurde die Stelle in das Amt für Einwohnerwesen und Wahlen eingegliedert und in die Grafenstraße 30 (Stadthaus) verlagert. Die Kommunale Statistikstelle befand sich im ersten Stock. Zutritt in diesen abgeschotteten Bereich erhielt ein Besucher nur, wenn er sich durch Klingelzeichen bemerkbar gemacht hatte und die Tür von innen geöffnet wurde. Er betrat einen Empfangsraum, in dem in der Regel eine Sekretärin saß, und wurde dort bedient. In den sich anschließenden Räumen waren der Abteilungsleiter sowie mehrere Mitarbeiterinnen und Mitarbeiter untergebracht.

Bei meiner Prüfung hatte ich festgestellt, daß Unterlagen aus der Bautätigkeitsstatistik (Baugenehmigungen), die vom Bauamt an die Statistikstelle übermittelt werden, über Gebühr lange lagerten. Dabei handelte es sich um einen Aktenordner, in dem Genehmigungsanträge abgelegt waren, die teilweise älter als fünf Jahre waren. Der zuständige Mitarbeiter teilte mir mit, daß er z.Z. eine Aussonderungsaktion durchführe und im Zuge dessen auch diese Unterlagen vernichtet würden. Im übrigen hielt er bei diesen Unterlagen eine Aufbewahrungsfrist von zwei Jahren für erforderlich. Diese Einschätzung habe ich geteilt. Gegen eine Lagerung dieser Daten für diesen Zeitraum bestehen deshalb keine datenschutzrechtlichen Bedenken. Die Umsetzung dieser Vorgaben muß jedoch durch regelmäßige Aussonderungsprüfungen sichergestellt werden.

Die Daten aus der Beherbergungsstatistik, die vom Hessischen Statistischen Landesamt über die kommunalen Statistikstellen erhoben werden, wurden in Darmstadt vor dem Rücklauf an das

Hessische Statistische Landesamt nach Wiesbaden erfaßt und ausgewertet. Dagegen bestanden insofern rechtliche Bedenken, als der Beherbergungsbetrieb seine Auskunft dem Hessischen Statistischen Landesamt und nicht der Kommune erteilt. Allenfalls mit ausdrücklicher Einwilligung der betroffenen Betriebe war eine eigene Auswertung durch die kommunale Statistikstelle rechtlich möglich. Aus diesem Grund hatte ich die Verantwortlichen aufgefordert, so zu verfahren, wie es die Statistikstelle in Frankfurt schon seit Jahren praktiziert. Dort hatte man die Betriebe angeschrieben und um eine schriftliche Einverständniserklärung gebeten. Fast alle Betriebe hatten in Frankfurt diesem Wunsch entsprochen.

Im Zusammenhang mit der automatisierten Datenverarbeitung habe ich darauf hingewiesen, daß die Paßworte der Mitarbeiterinnen und Mitarbeiter mindestens acht Stellen lang sein sollten. Außerdem ist ein regelmäßiger Paßwortwechsel vorzusehen. Eine Frist für den Paßwortwechsel darf nicht länger als 90 Tage sein, ein kürzerer Zeitpunkt ist besser.

Die Daten der Statistikstelle und des Einwohnermeldeamtes sowie die Daten anderer Behörden (Ordnungsamt) waren auf einem gemeinsamen Server im Erdgeschoß gespeichert. Da nach den mir gegebenen Informationen keine personenbezogenen Daten auf diesem Server abgelegt waren, hatte ich auf die Forderung nach einer physikalischen Trennung der Daten, z.B. durch den Einbau einer zusätzlichen Festplatte, verzichtet. Sollte sich an den Gegebenheiten allerdings in Zukunft etwas ändern, wären zusätzliche Vorkehrungen zur Sicherstellung der Zweckbindung der Daten erforderlich.

Die von der Stadt getroffenen Maßnahmen zur Gewährleistung der Zugangskontrolle waren bei dem Raum, in dem der Server untergebracht war, nicht ausreichend. So bot die Holztür zum Serverraum keinen hinreichenden Schutz. Auch das ebenerdig

gelegene Fenster im Hof war ein Schwachpunkt. Hinzu kam, daß der Rechner frei zugänglich auf einem Tisch stand.

In diesem Punkt waren Nachbesserungen erforderlich. So habe ich gefordert, daß der Server unter Verschuß zu nehmen ist.

Außerdem sollte überlegt werden, wie der Zugang zu dem Raum besser gesichert werden kann.

19.3.2

Statistikstelle der Stadt Kassel

Die Statistikstelle der Stadt Kassel war beim Hauptamt angesiedelt. Sie befand sich im vierten Stock des Nordflügels des Rathauses. Der Zutritt zu den insgesamt drei Räumen erfolgte von einem Flur aus. Die Türen ließen sich von außen nicht öffnen.

Auf Grund einer Verwaltungsverfügung des Oberbürgermeisters war die Statistikstelle nicht mehr dem Verkehrsamt, sondern dem Hauptamt zugeordnet.

Die Aufgaben der amtlichen Statistik sind bei der Stadt Kassel im Verlauf der letzten Jahre erheblich reduziert bzw. auf Fachämter zurückverlagert worden. So wurde beispielsweise die Bautätigkeitsstatistik direkt vom Bauamt der Stadt abgewickelt.

Im Zusammenhang mit der Beherbergungsstatistik waren in Kassel - anders als in Frankfurt und Darmstadt zum Zeitpunkt der Prüfung - noch keine eigenen Auswertungen durchgeführt worden. Es waren ausschließlich Unterlagen, die das Hessische Statistische Landesamt zur Verfügung stellt, veröffentlicht worden. Die Bögen, die von den Betrieben an die Statistikstelle geschickt wurden, sind nur auf ihre Vollzähligkeit hin kontrolliert und einer Plausibilitätsprüfung unterzogen worden.

Auch mit der Bevölkerungsfortschreibung hatte die Statistikstelle nichts mehr zu tun. Die Erhebung und Weitergabe der Daten an das Hessische Statistische Landesamt wurde direkt durch das Einwohnermeldeamt bzw. Standesamt der Stadt abgewickelt.

Bei der Agrarstatistik diente die kommunale Statistikstelle ebenfalls nur als Durchlaufstation. Auch hier wurde - ähnlich wie bei der Beherbergungsstatistik - eine Plausibilitätskontrolle durchgeführt und ggf. Rückfragen vorgenommen.

Die automatisierte Datenverarbeitung fand zum Zeitpunkt der Prüfung mit drei PC im Stand-alone-Betrieb statt. Dabei handelte es sich um alte Geräte (386er mit zwei Megabyte Arbeitsspeicher). Es wurde das Statistikprogramm SPSS benutzt. Darüber hinaus wurden die PC zur Erstellung von Schriftverkehr verwendet. Aus diesem Grund waren auch Adreßdateien gespeichert.

Jede Nutzerin und jeder Nutzer hatte ein eigenes Paßwort. Den mir gegebenen Informationen zufolge erfolgte ein regelmäßiger Paßwortwechsel, die Länge des Paßwortes betrug acht Stellen. Im übrigen verfügte die Statistikstelle über ein eigenes Faxgerät.

Bei einem Rundgang hatte ich festgestellt, daß noch Unterlagen aus der Bautätigkeitsstatistik ab dem Jahre 1988 vorhanden waren. Es handelte sich um insgesamt 14 Ordner. Auch aus der Bodennutzungshaupterhebung gab es personenbezogene Unterlagen, die bis in das Jahr 1969 hinein reichten. Ich habe den Leiter der Statistikstelle aufgefordert, diese Unterlagen so schnell wie möglich zu vernichten.

Aus einer Milieuschutzbefragung des Jahres 1986 gab es noch Adressen von Mietern bzw. Mietunterlagen. Auch existierte noch eine Quittungsliste aus dem Jahre 1977, auf der Erhebungsbeauftragte den Empfang von Vergütungen bestätigt hatten. Auch diese Unterlagen müssen vernichtet werden.

Auf dem Flur gegenüber der Statistikstelle standen insgesamt 14 Stahlschränke, die alle verschlossen waren. Diese Schränke dienten vornehmlich der Archivierung von statistischen Berichten, Jahrbüchern und anderen Unterlagen. In einem Schrank wurden noch die Unterlagen einer weiteren Milieuschutzbefragung aus den 70er Jahren aufbewahrt. Der Leiter der Statistikstelle schilderte mir das Problem des Zeitaufwandes, die personenbezogenen Daten aus diesen Unterlagen herauszusortieren und zu vernichten. Letztendlich führt jedoch kein Weg daran vorbei, dies innerhalb eines angemessenen Zeitraumes zu tun.

19.3.3

Statistikstelle der Stadt Fulda

Im Zusammenhang mit der Volkszählung 1987 hatte die Stadt Fulda eine Volkszählungsstelle eingerichtet. Nach der Volkszählung wandelte die Stadt die Zählstelle in eine kommunale abgeschottete Statistikstelle um. Diese Statistikstelle war nach wie vor im Südflügel des Fuldaer Stadtschlusses untergebracht, in dem auch ein Großteil der übrigen Verwaltung untergebracht war. Im Kellergeschoß im Südflügel war nur die Statistikstelle sowie der Personalrat mit einem Sitzungszimmer untergebracht. Damit war gewährleistet, daß nur Besucher und Bedienstete, die gezielt die Statistikstelle aufsuchen wollen, dies auch taten. Die Tür in den Raum mußte von innen geöffnet werden. Bemerkbar machen konnten sich Besucher durch eine Klingel. Über der Tür war eine Videokamera angebracht, der Monitor befand sich in einem Regal oberhalb des Eingangsbereiches im innen gelegenen Teil der Statistikstelle.

Eine Person betreute das statistische Aufgabenfeld der Stadt. Nach wie vor Gültigkeit hatten die Satzungen über die regelmäßigen

Datenübermittlungen, die besondere Geschäftsanweisung sowie die Zuständigkeitsregelung für Statistiken und Umfragen.

Bei der Fremdenverkehrs- und Agrarstatistik fungierte die Statistikstelle nur als Durchlaufstation. Eigene Auswertungen wurden bisher nicht erstellt. Im Zusammenhang mit der Bevölkerungsfortschreibung wurden die eingehenden Bögen vor der Weitergabe an das Statistische Landesamt auf ihre inhaltliche Plausibilität hin kontrolliert.

Die Geburts-, Eheschließungs- und Sterbefallkarten wurden vom Standesamt an die Statistikstelle weitergeleitet. Auch hier erfolgte nur eine Plausibilitätskontrolle.

Die Bautätigkeitsstatistik wurde seit einiger Zeit ausschließlich durch das Bauamt abgewickelt. Adreßdateien wurden für den Bereich der Fremdenverkehrs- und Agrarstatistik geführt.

Zum Zeitpunkt der Prüfung gab es einen PC im Stand-alone-Betrieb. Ein Zugang zum Verwaltungsrechner der Stadt bestand ebenfalls. Dieser wurde genutzt, um das zentrale Schreibprogramm verwenden zu können. Allerdings war geplant, den PC in ein Windows-NT-Netz, das im Sommer vergangenen Jahres aufgebaut wurde, zu integrieren.

In der Statistikstelle Fulda gab es keine Punkte, die aus datenschutzrechtlicher Sicht hätten geändert bzw. verbessert werden müssen.

20. Straßenverkehr

Name und Adresse im Autofenster

Verkehrsteilnehmer dürfen nicht verpflichtet werden, eine Genehmigung der Straßenverkehrsbehörde, die Name und Anschrift des Inhabers enthält, im Fahrzeug offen auszulegen.

20.1

Stadtverwaltung Flörsheim

Eine Bürgerin aus Flörsheim hat sich an mich gewandt und folgendes gerügt: Sie ist Mitglied in mehreren Naturschutzverbänden und betreut in der Gemarkung ihres Wohnortes diverse Nistkästen heimischer Vögel. Hierzu ist das Befahren von Feldwegen mit dem Auto erforderlich. Gem. § 46 Abs. 1 Straßenverkehrsordnung (StVO) kann die Straßenverkehrsbehörde Ausnahmen genehmigen von Verboten, die durch bestimmte Verkehrszeichen angeordnet sind. Die Stadtverwaltung hat ihr für das Befahren von Feldwegen eine Ausnahmegenehmigung erteilt. Allerdings hat die Behörde sie verpflichtet, die Genehmigung im Gebrauchsfalle im Wageninnern ihres Fahrzeuges, von außen gut sichtbar, vorne rechts an der Windschutzscheibe anzubringen. Die Genehmigung enthält u.a. ihren Namen und ihre Anschrift.

Die Bürgerin wandte sich dagegen, daß auf diese Weise jeder Spaziergänger, der im Feld an ihrem Fahrzeug vorbeigeht, ihren Namen und ihre Anschrift erfahren kann. Vergeblich bat sie die Behörde um Ausstellung einer Bescheinigung, in der nur das Kfz-Kennzeichen aufgeführt ist.

Ich pflichtete der Betroffenen bei und teilte der Stadtverwaltung mit, daß die gewählte Verfahrensweise nicht mit datenschutzrechtlichen Grundsätzen vereinbar ist. Denn mittelbar

wird die Betroffene verpflichtet, jeder das Fahrzeug einsehenden Person alle in der Genehmigung aufgeführten Daten zu offenbaren. Für die Aufgabenerfüllung der Straßenverkehrsbehörde war dies nicht erforderlich, insbesondere nicht zur Kontrolle der Ausnahmegenehmigung und zur Vorbeugung gegen Mißbrauch. Die Straßenverkehrsbehörde hätte z.B. auf eine Auslage ganz verzichten können oder eine Ausnahmegenehmigung ohne Namen und Adresse ausstellen können. Von der letztgenannten Möglichkeit machen die Straßenverkehrsbehörden im allgemeinen bei der Ausstellung von Anwohnerparkausweisen, Schwerbehindertenparkausweisen oder sonstigen mir bekannten Park- oder Zufahrtsausnahmegenehmigungen Gebrauch.

Die Stadtverwaltung Flörsheim änderte die Verfahrensweise zunächst nicht. Sie teilte mir lediglich mit, daß sie den Hessischen Städte- und Gemeindebund um eine Stellungnahme gebeten hat. Als die Ausnahmegenehmigung für die Betroffene zu erneuern war, hat sie jedoch in der neuen Genehmigung Name und Adresse der Betroffenen nicht mehr aufgeführt und mir eine Kopie zukommen lassen.

Damit werden künftig die datenschutzrechtlichen Belange der Betroffenen berücksichtigt.

20.2

Stadtverwaltung Frankfurt

Eine Bürgerin aus Frankfurt-Höchst wandte sich mit dem gleichen Anliegen wie die Flörsheimer Einwohnerin an mich. Ihr war eine Dauerparkerlaubnis nach § 46 Abs. 1 StVO erteilt worden. Die Erlaubnis gestattete ihr, in bestimmten Höchster Straßen zu parken, ohne die Parkscheinautomaten zu bedienen. Auch diese Genehmigung enthält Name und Anschrift der Betroffenen und die

Passage "Beim Verlassen des Fahrzeuges ist die Erlaubnis gut sichtbar im Inneren des Autos abzulegen".

Die Stadtverwaltung Frankfurt sah die Offenbarung von Name und Anschrift an die am Auto vorbeigehenden Passanten nicht als rechtlich geboten an. Personen, die sich gegen die jahrzehntelang geübte Praxis wenden - so die Stadtverwaltung in einer ersten telefonisch eingeholten Stellungnahme - würde gesagt, sie sollten einfach die entsprechende Passage in der Genehmigung ignorieren und den oberen Teil der Genehmigung nach hinten wegnicken. Das Ordnungspersonal wüßte schon Bescheid und würde keine Ordnungsstrafen verhängen.

Auf Grund meiner schriftlichen Stellungnahme sah auch die Stadtverwaltung die Notwendigkeit einer Abänderung der Verfahrensweise. Sie schlug vor, daß die Betroffenen zunächst mittels eines Aufklebers darüber informiert werden, daß das obere Drittel der Genehmigung nach hinten weggeknickt werden darf. Bei der Ende 1999 beabsichtigten Installation eines neuen Datenverarbeitungsverfahrens soll dann Name und Adresse des Betroffenen auf der Rückseite aufgedruckt werden.

Ich habe der Stadtverwaltung mitgeteilt, daß ich gegen diese Verfahrensweise keine Einwände habe.

21. Kammern

Akteneinsicht in Vorgänge der Industrie- und Handelskammer

Dem Betroffenen darf die Einsicht in die zu seiner Person gespeicherten Daten nicht mit der Begründung verweigert werden, daß die Unterlagen lediglich interne Bedeutung haben.

Ein Bürger bat mich zu prüfen, ob die Industrie- und Handelskammer ihm rechtmäßig die Einsicht in ihn betreffende Unterlagen verwehrt.

Der Bürger hatte eine Ausfallbürgschaft bei der Bürgschaftsbank Hessen für eine Existenzgründung beantragt. Die Bürgschaftsbank hatte daher die zuständige Industrie- und Handelskammer gebeten, hierzu Stellung zu nehmen und insbesondere die Pläne und die Marktsituation zu bewerten. Darüber hinaus sollte die fachliche Qualifikation des Antragstellers beurteilt werden. Die Stellungnahme gegenüber der Bürgschaftsbank erfolgte auf Grund der vom Antragsteller eingereichten Unterlagen sowie eines Gesprächs zwischen Industrie- und Handelskammer und Antragsteller.

Da die Bürgschaftsbank die Übernahme einer Ausfallbürgschaft ablehnte, wollte sich der Bürger darüber informieren, welche Gründe hierzu geführt hatten. Zu diesem Zweck wollte er auch die Stellungnahme der Industrie- und Handelskammer einsehen, da er auf Grund des Gesprächsverlaufs den Verdacht hatte, daß gerade diese Stellungnahme dabei maßgeblich war. Die Industrie- und Handelskammer begründete sowohl gegenüber dem Bürger als auch mir gegenüber ihre Ablehnung der Einsicht damit, daß die Stellungnahme lediglich internen Charakter habe.

Diese Rechtsauffassung, daß es sich bei der gegenüber der Bürgschaftsbank Hessen erteilten Stellungnahme um einen internen

Vorgang handelt, teilte ich nicht. Das Hessische Datenschutzgesetz räumt in § 18 jedem Betroffenen das Recht ein, Auskunft über alle zu seiner Person in Akten und Dateien gespeicherten Daten zu verlangen; eine Unterscheidung zwischen internen und allgemeinen Vorgängen ist nicht vorgesehen.

§ 18 HDSG

(1) Werden personenbezogene Daten in einer Datei gespeichert, dann ist dem Betroffenen von der speichernden Stelle auf Antrag gebührenfrei Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten,
2. den Zweck und die Rechtsgrundlage der Verarbeitung sowie
3. die Herkunft der Daten und die Empfänger regelmäßiger Übermittlungen, soweit dies gespeichert ist.

In dem Antrag soll die Art der Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden.

...

(4) Sind personenbezogene Daten in Akten gespeichert, die zur Person des Betroffenen geführt werden, dann kann er bei der speichernden Stelle Einsicht in die von ihm bezeichneten Akten verlangen. Werden die Akten nicht zur Person des Betroffenen geführt, hat er Angaben zu machen, die das Auffinden der zu seiner Person gespeicherten Daten mit angemessenem Aufwand ermöglichen. Die Einsichtnahme ist unzulässig, wenn die Daten des Betroffenen mit Daten Dritter oder geheimhaltungsbedürftigen nicht personenbezogenen Daten derart verbunden sind, daß ihre Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist. In diesem Fall ist dem Betroffenen Auskunft nach Abs. 1 zu erteilen. Im übrigen kann ihm statt Einsicht Auskunft gewährt werden.

Es spielt darüber hinaus auch keine Rolle, ob die Stellungnahme der Industrie- und Handelskammer ausschlaggebend für die Ablehnung der Ausfallbürgschaft war.

Leider hat die Industrie- und Handelskammer zunächst trotz meiner Aufklärung über die Rechtslage auf ihrem Standpunkt beharrt und dem Bürger weiterhin die Einsichtnahme verweigert. Ich sah mich daher gezwungen, mich an die zuständige Aufsichtsbehörde, das Hessische Ministerium für Wirtschaft, Verkehr und Landesentwicklung zu wenden. Kurz darauf teilte mir der Beschwerdeführer und später auch die Industrie- und Handelskammer mit, daß dem Bürger inzwischen Einsicht in die entsprechenden Unterlagen gewährt wurde.

22. Wohnungswesen

22.1

Zweckentfremdung von Wohnraum

Zur Feststellung, ob in einer Liegenschaft Wohnraum leer steht, kann es zulässig sein, daß das Amt für Wohnungswesen als zuständige Behörde für die Verfolgung von Ordnungswidrigkeiten zur Sachverhaltsermittlung Verbrauchsdaten für diesen Wohnraum bei den Stadtwerken erhebt.

Ein Bürger hat sich an meine Dienststelle gewandt und sich darüber beschwert, daß das Amt für Wohnungswesen einer Hessischen Kommune Verbrauchsdaten für eine Liegenschaft bei den Stadtwerken erhoben hatte. Auf Grund der von dort mitgeteilten Daten war der Wohnungsinhaber angeschrieben und die Einleitung eines Ordnungswidrigkeitenverfahrens wegen des Leerstehenlassens von Wohnraum angekündigt worden. Die Verwaltungsbehörde hatte sich dabei auf die Ermittlungsnormen des Ordnungswidrigkeitengesetzes und der Strafprozeßordnung gestützt. Der Bürger war der Auffassung, daß solche Ermittlungen bei Dritten lediglich durch einen Gerichtsbeschluß rechtens seien.

Auf meine Bitte um Stellungnahme teilte mir das Amt für Wohnungswesen mit, daß auf Grund von Hinweisen der Verdacht bestanden habe, daß in der betreffenden Liegenschaft mehrere Wohnungen leerstünden. Da das vermeidbare Leerstehenlassen von Wohnräumen eine Ordnungswidrigkeit ist, sah sich das Amt veranlaßt, entsprechende Sachverhaltsermittlungen vorzunehmen.

Auf Grund der Stellungnahme der Kommune habe ich dem Bürger daraufhin mitgeteilt, daß das Amt als zuständige Verwaltungsbehörde für die Verfolgung von Ordnungswidrigkeiten bei Vorliegen des Verdachts einer Ordnungswidrigkeit verpflichtet ist, den Sachverhalt zu erforschen. Dazu kann sie auch Dritte

befragen, wie in diesem Fall die Stadtwerke, ohne daß eine vorherige Erhebung der Daten beim Betroffenen nach den einschlägigen Vorschriften rechtlich geboten ist. Da im Falle des Leerstehenlassens von Wohnraum die Verbrauchsdaten bei den Stadtwerken regelmäßig wertvolle Hinweise für die Sachverhaltsaufklärung geben können, ist die Datenerhebung bei dieser Stelle auch erforderlich und damit zulässig. Der Vollständigkeit halber sei hier noch erwähnt, daß das eingeleitete Ordnungswidrigkeitenverfahren inzwischen durch einen rechtskräftigen Bußgeldbescheid abgeschlossen wurde.

22.2

Fehlbelegung

Es ist unzulässig, sämtliche Daten von Hauseigentümerinnen und Hauseigentümern mit denen der Mieterinnen und Mieter von Sozialwohnungen im gebundenen Bestand abzugleichen, um festzustellen, ob alle „Sozialwohnungsmieter“ im Verfahren zur Festsetzung der Fehlbelegungsabgabe korrekte Angaben zu ihren Einkommensverhältnissen gemacht haben.

Die Universitätsstadt Gießen hatte zufällig bei Anträgen auf Wohnungsvermittlung bzw. anhand von Mitteilungen des Amtsgerichts über Räumungsklagen festgestellt, daß Haus- bzw. Eigentumswohnungseigentümer in Einzelfällen gleichzeitig Mieter von Sozialwohnungen im gebundenen Bestand (d.h. Wohnungen, die nach dem II. Wohnungsbaugesetz noch einer festen Mietpreisbindung unterliegen) sind und ihre Einkünfte aus Vermietung und Verpachtung bei der Erhebung der Fehlbelegungsabgabe nicht angegeben haben. Da durch die verschwiegenen Einnahmen entweder gar keine oder aber eine zu niedrige Fehlbelegungsabgabe festgesetzt worden war, waren der Stadt Einnahmeausfälle entstanden. Die Stadt beabsichtigte deshalb einen generellen Abgleich der Daten der Haus- und

Wohnungseigentümer mit den Daten der Mieter von öffentlich geförderten Wohnungen, und zwar unabhängig davon, ob im Einzelfall konkrete Anhaltspunkte dafür vorlagen, daß die Mieter unvollständige Angaben zu ihrer Einkommenssituation gemacht hatten.

Auf Anfrage habe ich der Stadt Gießen mitgeteilt, daß ein derartiger Abgleich datenschutzrechtlich nicht zulässig ist. Das Hessische Gesetz zum Abbau der Fehlsubventionen im Wohnungswesen regelt in § 7, daß die Daten zum Einkommen beim Betroffenen selbst zu erheben sind; die Wohnungsinhaber sind danach zur Auskunft verpflichtet.

§ 7 HessAFWoG

Die Inhaberinnen und Inhaber von Wohnungen im Sinne von § 2 müssen auf Verlangen der zuständigen Stelle die zur Festsetzung einer Ausgleichszahlung notwendigen Auskünfte geben, soweit sie dazu in der Lage sind. Sie müssen insbesondere die Höhe ihres Einkommens und des von ihnen gezahlten Entgelts nachweisen sowie die Personen benennen, welche die Wohnung nicht nur vorübergehend benutzen.

Ein genereller Datenabgleich widerspricht diesem Grundsatz und ist aus meiner Sicht auch unverhältnismäßig. Bei der Einkommensermittlung im Verfahren zur Festsetzung einer eventuellen Fehlbelegungsabgabe sollten die Mieter darauf hingewiesen werden, daß auch Einkünfte aus Vermietung und Verpachtung maßgebliches Einkommen i.S. des Hessischen Gesetzes zum Abbau von Fehlsubventionen im Wohnungswesen sind. Sollte die Stadt im Einzelfall Anhaltspunkte haben, daß ein Mieter einer Sozialwohnung im gebundenen Bestand tatsächlich Angaben zu seinem Einkommen verschweigt, die aus vermietetem Haus- oder Wohnungseigentum stammen könnten, so hielte ich die einzelne Nachfrage bei den Ämtern, die über diese Informationen

verfügen - wie etwa das Steueramt oder das Vermessungsamt -
allerdings für zulässig. Die Universitätsstadt Gießen hat auf Grund
meiner Stellungnahme von dem beabsichtigten Datenabgleich
abgesehen.

23. Finanzwesen

23.1

Neue DV-Entwicklung in der Finanzverwaltung

Die regelmäßige Information über den Stand neuer DV-Projekte im Bereich der Finanzverwaltung nimmt mittlerweile eine feste Position innerhalb meiner jährlichen Aufgaben ein. In diesem Berichtsjahr standen für mich die Fortschritte in der Entwicklung der DV-Projekte „FISCUS“ und „GÜP“ im Vordergrund.

23.1.1

FISCUS (Föderales integriertes standardisiertes computerunterstütztes Steuersystem)

FISCUS ist die auf Grund eines Verwaltungsabkommens zwischen Bund und Ländern vom 2. Dezember 1994 entwickelte Neukonzeption eines einheitlichen automatisierten Besteuerungsverfahrens für alle Bundesländer. Das Verfahren setzt sich aus verschiedenen Teilprodukten zusammen, deren Entwicklung auf die verschiedenen Länder verteilt ist. Die jeweiligen Entwicklungsstellen arbeiten in einer einheitlichen Software-Entwicklungsumgebung (Sprache, Methoden, Werkzeuge und Datenbanksystem) und sind untereinander vernetzt. Sie sind mit einem systemtechnischen Zentrum verbunden, das bei dem Rechenzentrum der Finanzverwaltung des Landes Nordrhein-Westfalen eingerichtet wurde. Das Zentrum betreibt die Datenverarbeitungsgeräte, auf denen für die Systementwicklung von den Beteiligten gemeinsam benötigte Daten und Programme vorgehalten werden, und die zentralen Komponenten des erforderlichen Netzwerks. Die Gesamtprojektleitung führt eine Koordinierungsstelle beim Bundesministerium für Finanzen durch (Koordinierungsstelle für die Neukonzeption der Automation in der Steuerverwaltung – KAS). Deren erster Projektbericht 1998 liegt nunmehr vor. Nach der Zeitplanung sollen die neuen Produkte nach

und nach bis zum Jahr 2006 in allen Ländern eingesetzt werden. Jedem Land steht ein Übernahmzeitraum von drei Jahren zur Verfügung, ein fertiges Modul nach seiner Ersteinführung zu implementieren. Die erste Stufe "Vollstreckung" (NRW) läuft seit Mitte 1997 in einigen Finanzämtern Nordrhein-Westfalens in der Erprobungsphase. Die Produkte umfassen zusammen alle Vorgänge des Besteuerungsverfahrens, der steuerlichen Nebenleistungen, Steuerstraf- und Bußgeldverfahren in Finanzämtern, Oberfinanzdirektionen und obersten Finanzbehörden. Hessen ist für die Entwicklung der Komponenten „Betriebsprüfung (Innendienst)“, „Umsatzsteuersonderprüfung“, „Lohnsteueraußenprüfung“, sowie für „Einheitswertbewertung Grundbesitz“ und „Landwirtschaftskammer Umlage“ zuständig. Die Ersteinführung der hessischen Komponenten ist für das Jahr 2000/2001, bzw. 2004 geplant, wobei zu berücksichtigen ist, daß die Umstellung auf den EURO und auf die Jahrtausendwende derzeit erhebliche Arbeitskapazitäten in der Steuerverwaltung binden. Soweit mir das Automations-Konzept jetzt schon vorgestellt werden konnte, habe ich festgestellt, daß die Sicherstellung des Steuergeheimnisses auch die datenschutzrechtlichen Belange ausreichend abdeckt. Ich werde die Weiterentwicklung und Umsetzung des Verfahrens beobachten.

23.1.2

GÜP (Unterstützung der Veranlagungstätigkeiten für Gewerbetreibende, Bezieher von Überschußeinkünften und für die Gewinn-/Verlustfeststellung bei Personengesellschaften)

Im Jahr 1989 stellte die Hessische Finanzverwaltung erste Überlegungen an, wie auf der Grundlage von PC-Arbeitsplätzen die Tätigkeit in den Veranlagungsbereichen unterstützt werden kann. Auf Grund der Ergebnisse von Organisationsuntersuchungen wurde in den 46 hessischen Finanzämtern der Veranlagungsbereich "Überschußeinkünfte" 1992/93 und 1995 in zwei Schritten

aufgelöst und den Bereichen "Arbeitnehmerveranlagung", "Gewerbetreibende" und "Personengesellschaften" angegliedert. Der Bereich "Arbeitnehmerveranlagungen" verfügte mit BEA (Bearbeiter Eingabe Arbeitnehmerveranlagung) bereits über ein EDV-Verfahren, das auf einem Rechner der mittleren Datentechnik mit dem Betriebssystem AMBOSS basierte, an den Terminals angeschlossen waren.

Die 1989 begonnenen Überlegungen wurden der technischen Entwicklung angepaßt. So ergab sich das Konzept einer Client-Server-Architektur. Die schnelle Umsetzung wird aber durch die Ankündigung der Fa. Siemens, die Unterstützung des Betriebssystems AMBOSS zum Ende 1999 einzustellen, unabdingbar. Bis zu diesem Zeitpunkt müssen die hessischen Finanzämter eine neue IT-Infrastruktur mit den erforderlichen Anwendungen besitzen. Es wurde daher das Projekt GÜP: HEFINA (HEFINA: Hessische Finanzamts-Ausstattung) begonnen, dessen Ziel es ist, alle Teilbereiche der Finanzämter mit PC-Anwendungen auszustatten. Die Systeme sollen mit WINDOWS-NT ausgestattet sein. Es sind etwa 7000 Arbeitsplätze betroffen.

Um termingerecht fertig werden zu können, wurden mehrere Vor- und Teilprojekte gestartet. Beispielsweise werden alle Finanzämter und die OFD komplett strukturiert verkabelt, LAN in den Finanzämtern aufgebaut, das Personal in den neuen Systemen geschult und die IT-Betreuung unter Einbeziehung der Hessischen Zentrale für Datenverarbeitung umorganisiert.

Die Verfahren selbst sollen nicht nur der Verwaltung, sondern auch der Bürgerin und dem Bürger direkte Vorteile bringen. Ziel ist es, auf der einen Seite angesichts der immer komplexer werdenden Änderungen im Steuerrecht eine zeitnahe und vollständige Ausschöpfung der Steuerquellen zu erreichen. Auf der anderen Seite soll eine angemessene Bearbeitungszeit, umfassende Beratung und die Gleichmäßigkeit der Rechtsanwendung

gewährleistet werden. Die Verwaltung soll beispielsweise von der Integration einer Textverarbeitung auf Basis von Word, zu der schon mehrere hundert Vorlagen programmiert wurden, und einem Informationssystem profitieren. Für den Bürger erwartet man eine beschleunigte Bearbeitung von Steuererklärungen. Es soll aber auch möglich sein, am Arbeitsplatz die spätere Echt-Verarbeitung zu simulieren. Dadurch können dem Bürger aussagekräftige Zahlen über Steuererstattungen oder Nachzahlungen genannt und Fehler frühzeitig erkannt werden.

Trotz aller Neuerungen wird aber wie bisher auf dem Großrechner der Hessischen Zentrale für Datenverarbeitung die Datenverarbeitung und Datenhaltung überwiegend erfolgen. Dadurch soll das hohe Maß an Datenschutz und Datensicherung erhalten bleiben.

In einem Finanzamt läuft seit Herbst 1997 ein Pilotversuch mit den Funktionalitäten Textverarbeitung und Fallbearbeitung ohne Arbeitnehmerbezirke in einer ersten Ausprägung.

Mit einem zweiten Finanzamt wird seit Anfang 1998 die Ablösung von BEA getestet. Dort beginnen zum Jahresende erste Tests als Echanwendung. Wenn die Tests erfolgreich sind, gehen weitere Ämter Anfang 1999 in Produktion. Parallel zum Test der Software werden die Finanzämter mit der neuen Hardware ausgestattet. Etwa die Hälfte soll bis Ende 1998 ausgestattet sein.

Mitte des Jahres wurde mir der Projektstand von GÜP:HEFINA vorgestellt. Neben einer Demonstration der Software im Testumfeld der Hessischen Zentrale für Datenverarbeitung wurde mir das Zugriffsschutzkonzept erläutert. Wenn es konsequent umgesetzt wird, erfüllt es die datenschutzrechtlichen Anforderungen. Ich werde die Umsetzung im nächsten Jahr prüfen.

23.2

Bestandsaufnahme zur Hundesteuer in Friedrichsdorf

Die auf der Grundlage der erweiterten Hundesteuersatzung durchgeführte Hundebestandsaufnahme war datenschutzrechtlich nicht zu beanstanden.

Im Berichtszeitraum meines 25. Tätigkeitsberichts (Ziff.4) hatte ich das Angebot eines privaten Unternehmens zu beurteilen, das die flächendeckende Erhebung von Hundehalterdaten in einer Stadt zum Zweck der Steuerveranlagung zum Inhalt hatte. Jetzt hat die Stadt Friedrichsdorf eine Erhebung durchgeführt.

Die anbietende Firma ging damals davon aus, daß in jeder Kommune Steuereinnahmen durch nicht gemeldete Hunde verloren gingen. Durch ihr Angebot, einen Abgleich der jeweils bestehenden örtlichen Steuerlisten über Hundehalter mit dem Ergebnis einer persönlichen Befragung aller Haushalte der jeweiligen Kommune durchzuführen, sollten Steuerländer überführt werden. Ich hatte mich seinerzeit gegen die Maßnahme in dieser allgemeinen Form ausgesprochen, da keine ausreichende Rechtsgrundlage für das beschriebene Verfahren vorhanden war. Weder im damals noch geltenden Hessischen Hundesteuergesetz und den entsprechenden Satzungen der Kommunen noch im Hessischen Kommunalabgabengesetz oder in der Abgabenordnung ist die flächendeckende Befragung von Einwohnern ohne konkreten Anlaß zur Ermittlung von Steuerhinterziehungen vorgesehen. Hinzu kam die Problematik, ob Privatunternehmer Daten für die Zwecke der (hoheitlichen) Besteuerung verarbeiten dürfen.

Die Stadt Friedrichsdorf hatte festgestellt, daß zahlreiche Hunde in ihrem Stadtgebiet nicht gemeldet waren und zufällige Einzelfeststellungen den gesamten Bestand nicht erfaßten. Der gemeldete Hundebestand blieb über Jahre mehr oder weniger gleich, während die tatsächliche Anzahl der Hunde im Stadtgebiet

offensichtlich zunahm. Die Stadtverwaltung setzte sich mit dem Angebot der Firma auseinander und fand eine datenschutzrechtlich akzeptable Möglichkeit, durch sie eine Hundebestandsaufnahme verbunden mit einer Rassefeststellung (im Hinblick auf eine etwaige Besteuerung von Kampfhunden) durchzuführen. Die Erforderlichkeit der Maßnahme war durch die Feststellung der Stadt hinreichend begründet. Die Stadt ergänzte ihre bereits bestehende Hundesteuersatzung um einen weiteren Paragraphen, der in bestimmten zeitlichen Abständen die Ermittlung des Hundebestandes, auch mittels privater Helfer, vorsieht. Auf Grund des konkreten Anlasses, der vorgelegten Satzung und unter Heranziehung der über § 4 Kommunalabgabengesetz anwendbaren §§ 85, 93 der Abgabenordnung war die Maßnahme datenschutzrechtlich nicht mehr zu beanstanden. Es war nicht zu befürchten, daß in die Rechte der Beteiligten oder anderer Personen in unzulässiger Weise eingegriffen würde. Die Maßnahme war zur Erreichung des Zwecks geeignet und erforderlich und der Eingriff in die Rechte der Betroffenen verhältnismäßig.

Zur Durchführung der Bestandsaufnahme gab die Stadt Friedrichsdorf auch keine Namenslisten oder Steuerlisten an die Firma heraus, sondern nur alphabetisch geordnete Straßenlisten mit Hausnummern. Die eingesetzten Mitarbeiter der Firma wurden als Verwaltungshelfer tätig. Sie wurden über die strikte Einhaltung der datenschutzrechtlichen Vorschrift belehrt und erhielten genaue Anweisungen über die Vorgehensweise, z.B. durften sie nicht gegen den Willen eines Betroffenen Grundstücke oder Wohnungen betreten oder minderjährige Personen befragen. Von der Stadt erhielten sie Ausweise, die sie für das Handeln im Auftrag der Stadt Friedrichsdorf legitimierten und die sie vor der Befragung vorzeigen mußten. Die Firma unterwarf sich meiner Kontrolle. Eine vorgeschaltete Pressemitteilung machte die Bürger auf die bevorstehende Befragung aufmerksam. Laut Auskunft der Stadtverwaltung kam es zu keinen Beschwerden über das Verfahren oder die Vorgehensweise der Mitarbeiter.

Die Maßnahme erbrachte bereits eine Erhöhung des Hundesteueraufkommens um ca. 25 bis 30%. Die Auswertung ist noch nicht abgeschlossen.

Als Arbeitsergebnis übergab die Firma der Stadt eine Liste, in der anhand der vorgegebenen, alphabetisch geordneten Straßennamen vom jeweiligen Mitarbeiter Ergänzungen eingetragen wurden. Dabei handelte es sich in den meisten Fällen um die von außen an Schildern ersichtlichen Namensangaben der Betroffenen und die Feststellung, ob und ggf. wieviele Hunde welcher Rasse angegeben, gesehen oder auf Grund anderweitiger Umstände vermutet werden konnten, sowie um das Datum des Besuchs. Hinsichtlich der Spalte „Bemerkungen“ mußte ich jedoch Mängel feststellen. Entgegen der vertraglichen Vereinbarung wurden Minderjährige und nicht zum Haushalt gehörende Dritte befragt bzw. deren Auskünfte notiert. Ich habe diese Vorgehensweise gegenüber der Firma kritisiert.

24. Ordnungswidrigkeiten

Der Flughafenschutzdienst leistet keine Amtshilfe

Die routinemäßige Bearbeitung von Ordnungswidrigkeiten, die regelmäßig und massenweise von einer privaten Stelle angezeigt werden, darf nicht dazu führen, daß die Anzeigerstatter der Einfachheit halber per Vordruck „in Amtshilfe“ gehört werden und die Verfahrensakte zur Einsicht erhalten.

Ein Rechtsanwalt aus Frankfurt machte mich darauf aufmerksam, daß die Stadt Frankfurt in Ordnungswidrigkeitenverfahren, die vom Flughafenschutzdienst angezeigt werden, diesen nicht wie eine private Organisation, sondern wie eine Behörde behandelt. In dem mir dann vorgelegten Einzelfall wurde tatsächlich der Anzeigerstatter des Flughafenschutzdienstes vom Ordnungsamt der Stadt Frankfurt ersucht, eine "dienstliche Erklärung" zu dem Vorfall und zu den Einlassungen des Betroffenen abzugeben. Die vollständige Verfahrensakte war dem Anschreiben beigelegt. In dem dabei benutzten Vordruck „Amtshilfe in Ordnungswidrigkeitenverfahren“ war der Flughafenschutzdienst neben Polizei- und Verkehrsbehörden als Adressat aufgeführt und für alle genannten Stellen verschiedene Amtshilfebegehren gleichlautend formuliert, z.B. eine dienstliche Erklärung des anzeigenden Beamten zu übersenden oder den Anzeigenden/Zeugen zur Einlassung des Betroffenen zu hören. Dem Hinweis „Vorgang ist beigelegt (s. Anl.)“ oder „siehe Vorgang“ war zu entnehmen, daß die Verfahrensakte offensichtlich regelmäßig mitversandt wurde. Die Stadtverwaltung hat die Datenschutzverletzung eingeräumt und sich beim Betroffenen entschuldigt.

Es war den Beteiligten schnell klar, daß es sich beim Flughafenschutzdienst nicht um eine Behörde handelt, sondern um eine Einrichtung der Flughafen-AG, und damit um eine private

Stelle. Folglich sind die dortigen Anzeigerstatter keine Amtsträger, sondern allenfalls Zeugen im Verfahren.

Wegen der großen Anzahl der täglich aus dem Flughafenbereich eingehenden Anzeigen wollte die Stadt die Bearbeitung der Verfahren so rationell wie möglich gestalten. Der Flughafenschutzdienst wurde der Einfachheit halber nachträglich als Adressat in den für Behörden vorgesehenen Fragebogen eingesetzt, mit der Folge, daß er - zumindest im vorliegenden Fall - auch ebenso behandelt wurde. Diese Vorgehensweise wurde von der Stadt Frankfurt beendet, indem sie einen neuen Vordruck "Zeugenfragebogen" entwickelte, der an private Stellen und Personen versendet wird, die als Zeuge oder Zeugin in Frage kommen.

Auch eine Versendung der Ermittlungsakte an private Stellen oder Personen ist jetzt ausgeschlossen. Es werden nunmehr vom jeweiligen Sachbearbeiter Fragen an den Zeugen formuliert, wenn der Sachverhalt weitere Aufklärung anhand der Einlassung des Betroffenen erfordert. Dabei sind vom Bearbeiter die datenschutzrechtlichen Belange zu beachten. Die Datenschutzbeauftragte der Flughafen AG hat freundlicherweise die Mitarbeiterinnen und Mitarbeiter des Flughafenschutzdienstes ebenfalls über die Rechtslage informiert.

25. Bilanz

25.1

Ökologischer Landbau

Umsetzung der EWG-Verordnung Nr. 2092/91

(24. Tätigkeitsbericht, Ziff. 10 und 25. Tätigkeitsbericht, Ziff. 21.6)

In den beiden Tätigkeitsberichten hatte ich die datenschutzrechtlichen Probleme im Zusammenhang mit der Umsetzung der Verordnung (EWG) Nr. 2092/91 des Rates vom 24. Juni 1991 über den ökologischen Landbau dargestellt. Insbesondere die Vermischung von staatlicher und privater Kontrolle der Betriebe war unbefriedigend und entsprach nicht den datenschutzrechtlichen Anforderungen.

Seit 1. Januar 1998 erläßt die Kontrollbehörde für den ökologischen Landbau beim Hessischen Landesamt für Regionalentwicklung und Landwirtschaft im Rahmen eines Prüfverfahrens, dem sich potentielle Kontrollstellen zu unterwerfen haben, Zulassungsbescheide. Diese Zulassungsbescheide ermächtigen die private Kontrollstelle, im Auftrag der Kontrollbehörde, also des Hessischen Landesamtes für Regionalentwicklung und Landwirtschaft, staatliche Kontrollen der Betriebe vorzunehmen.

Jede potentielle private Kontrollstelle, die sich beim Landesamt meldet, muß geprüft werden. Dies gilt auch für Stellen, die in einem anderen Bundesland angesiedelt sind. Erfüllt die Stelle die erforderlichen Normen, erfolgt ihre Zulassung durch das Landesamt für das Gebiet des Bundeslandes Hessen. Unabhängig davon kann ein Erzeuger zusätzliche Verbandskontrollen - soweit er einem Verband angehört - vereinbaren. In der Regel bieten die durch das Landesamt zertifizierten Kontrollstellen eine Durchführung auch dieser zusätzlichen Verbandskontrollen an. In

der Vergangenheit fand eine unklare Vermengung dieser einerseits staatlich und andererseits privat initiierten Kontrolle statt.

Um den Betrieben eine klare Unterscheidung zu ermöglichen, wurde in Zusammenarbeit mit dem Landesamt und mir ein Formular "Datenschutzvereinbarung" entwickelt, welches vor jeder staatlichen Kontrolle durch die Kontrollstelle dem zu kontrollierenden Betrieb vorgelegt werden muß. Darin wird die Verwendung und Übermittlung von Daten an Dritte geregelt. U.a. ist in dem Formular vorgesehen, daß der betroffene Betrieb in die Verwendung und Übermittlung der Daten an den privaten Verein bzw. Verband ausdrücklich zustimmen muß. Erfolgt keine Einwilligung, die auf diesem Formular schriftlich festgehalten wird, findet ausschließlich eine staatliche Kontrolle durch die Kontrollstelle statt. Eine Übermittlung der Daten erfolgt dann nur an das Hessische Landesamt für Regionalentwicklung und Landwirtschaft.

Damit ist ein transparentes Verfahren und eine klare Trennung zwischen staatlicher und privater Kontrolle gewährleistet. Entsprechend den Vorgaben des Hessischen Datenschutzgesetzes haben sich die privaten Kontrollstellen verpflichtet, die Bestimmungen des Hessischen Datenschutzgesetzes einzuhalten und sich meiner Kontrolle zu unterwerfen (§ 4 HDSG).

25.2

Europol nimmt die Arbeit auf

(25. Tätigkeitsbericht, Ziff. 2.2)

In diesem Jahr wurden die letzten Voraussetzungen für das Inkrafttreten der Europol-Konvention erfüllt. Alle beteiligten Staaten haben die Konvention ratifiziert.

Das Europäische Polizeiamt - Europol - kann seine Arbeit aufnehmen. Im Unterschied zur bisherigen vorläufigen Phase kann Europol nunmehr selbst Daten über Personen in eigenen Informations- und Analysedateien speichern, auswerten und an andere Stellen weitergeben.

Eine wesentliche Voraussetzung für die Arbeitsaufnahme von Europol ist mit der Einsetzung der Gemeinsamen Kontrollinstanz geschaffen worden. Sie überprüft, ob durch die Verarbeitung von Daten bei Europol die Rechte von Personen verletzt werden. Ihr Beschwerdeausschuß entscheidet verbindlich über Beschwerden der Betroffenen im Zusammenhang mit der Auskunftserteilung, der Überprüfung gespeicherter Daten sowie deren Berichtigung und Löschung.

Die deutschen Datenschutzbeauftragten sind durch den Bundesbeauftragten für den Datenschutz und den Landesbeauftragten von Sachsen-Anhalt in der Gemeinsamen Kontrollinstanz vertreten. Sie haben sich bei den Beratungen der Geschäftsordnung der Gemeinsamen Kontrollinstanz dafür eingesetzt, daß ihre Mitglieder weitgehende Unabhängigkeit genießen, ihr Amt unparteiisch wahrnehmen, die Behandlung von Beschwerden in einem fairen und grundsätzlich öffentlichen Verfahren erfolgt und der Anspruch der Betroffenen auf rechtliches Gehör gewahrt wird. Sie werden auf die Einhaltung dieser Grundsätze bei ihrer Mitarbeit in der Gemeinsamen Kontrollinstanz achten.

Dies ist von besonderer Bedeutung, da es auf der Grundlage der derzeitigen Europol-Konvention keine umfassende Kontrolle durch die ordentliche Gerichtsbarkeit auf nationaler wie europäischer Ebene gibt.

Mit der Speicherung, Nutzung und Übermittlung personenbezogener Daten greift Europol in die Grundrechte der

Betroffenen ein. Sie müssen daher nach deutschem wie europäischem Rechtsverständnis die Möglichkeit haben, Rechtsschutz zu suchen. Dies wird jedenfalls dann unabdingbar sein, wenn Europol künftig eigene Ermittlungsbefugnisse erhält, wie sie im Vertrag von Amsterdam vorgesehen sind.

25.3

HEPOLAS

(25. Tätigkeitsbericht, Ziff. 21.7)

In meinem 25. Tätigkeitsbericht hatte ich den Projektstand von HEPOLAS dargestellt. Mittlerweile wurde die Individualsoftware (ISW), d.h. der erste Teil der Vorgangsbearbeitung, in einer Polizeidienststelle testweise installiert. Daraus resultierten Änderungsanforderungen, die in die Software eingearbeitet werden. Mit der ISW Version 2.2, die für das 1. Quartal 1999 geplant ist, werden die meisten Änderungen umgesetzt. Die für das 2. Quartal 1999 vorgesehene Version 2.3 soll neben der HEPOLIS-Schnittstelle die restlichen Anpassungen umfassen.

Mitte des Jahres stellte mir das Landeskriminalamt die damals aktuelle Programmversion in einer Testumgebung vor. Dabei wurden keine Mängel offenkundig. Eine abschließende Aussage läßt sich aber erst treffen, wenn eine Polizeidienststelle das Verfahren nutzt und das Verfahren in diesem Umfeld geprüft wird. Eine entsprechende Prüfung habe ich für 1999 vorgesehen.

Das von mir geforderte Datensicherheitskonzept wurde zum Jahresende von der Hessischen Zentrale für Datenverarbeitung als Rohfassung fertiggestellt. Bis Ende des 1. Quartals 1999 soll es mit der Polizei und mir abgestimmt werden. Damit ist der Polizei ein Rahmen für die zu ergreifenden Datensicherheitsmaßnahmen gegeben.

Weiterhin ist ab Januar 1999 ein Pilotversuch im Bereich der Polizeidirektion Hanau geplant. An elf Standorten wird die ISW Version 2.2 für einen dienststellenübergreifenden Flächentest installiert. Damit ist ein Technologie-Update und ein Test der Funktion "Einmalerfassung - Mehrfachnutzung" verbunden. Zuerst werden Hard- und Software bereitgestellt sowie mit Testdaten die verschiedenen Funktionen im Zusammenspiel der Dienststellen verifiziert. Daran anschließend wird der Echtbetrieb aufgenommen. Ziele des Tests sind:

- Erkenntnisse gewinnen, ob die eingesetzte Technologie ausreichend ist,
- verifizieren, ob das Schulungs- und Betreuungskonzept adäquat sind und
- Auswirkungen auf die Aufbau- und Ablauforganisation feststellen.

Bei der Verfahrensentwicklung wurde das Augenmerk auf eine möglichst einfache Bedienung gelegt. Die Mitarbeiterinnen und Mitarbeiter der Polizei sollen lediglich eine Einführung von zwei Stunden erhalten und dann das Verfahren nutzen können. Der Test muß zeigen, ob diese Annahmen realistisch sind.

25.4

Verwaltungsvorschriften zum Ausländergesetz

(25. Tätigkeitsbericht, Ziff. 13.1)

Im letzten Tätigkeitsbericht (Ziff. 13.1) hatte ich berichtet, daß das Bundesministerium des Innern nach sechs Jahren einen Entwurf für die nach § 104 Ausländergesetz (AuslG) zu erstellenden Verwaltungsvorschriften vorgelegt hat.

Der überarbeitete Entwurf des Bundesministeriums des Innern vom 30. Juni 1998 hat - was die datenschutzrechtlichen Probleme

betrifft - nur marginale Verbesserungen erfahren. Positiv zu bewerten ist, daß das Hessische Ministerium des Innern und für Landwirtschaft, Forsten und Naturschutz fast alle meine Vorschläge als Abänderungsanträge im Bundesrat eingebracht hat.

25.5

Smart-Card im Asylverfahren

(26. Tätigkeitsbericht, Ziff. 24.4)

In den letzten Tätigkeitsberichten hatte ich von Plänen des Bundesministeriums des Innern berichtet, eine Smart-Card für Asylbewerber einzuführen. Die jedem Asylbewerber auszuhändigende Smart-Card soll eine Reihe von Daten enthalten: u.a. biometrische Daten des Fingerabdrucks, Lichtbild, Daten zum Asylverfahren, sowie Daten über die Berechtigung zum Empfang von Leistungen. Der Einsatz der Karte ist für unterschiedliche Zwecke vorgesehen. Zunächst dient die Karte als Identifikationsnachweis. Vor allem soll sie aber auch die Kommunikation zwischen den am Asylverfahren beteiligten Behörden verbessern, indem die oder der Betroffene die Karte bei der entsprechenden Behörde vorlegt und damit von einem eindeutigen Datensatz ausgegangen werden kann. Genutzt werden soll die Karte im übrigen auch bei der Vergabe von Leistungen und bei der Aufenthaltskontrolle.

Mittlerweile hat die Firma ORGA-CONSULT GmbH in Paderborn die vom Bundesministerium des Innern in Auftrag gegebene Machbarkeitsstudie erstellt. Nach meinen Informationen wurde die Studie Anfang Juli dieses Jahres an das Bundesministerium des Innern und das Bundesamt für die Anerkennung ausländischer Flüchtlinge versandt. Derzeit liegt den zuständigen Landesministerien und den Datenschutzbeauftragten die Machbarkeitsstudie noch nicht vor. Sobald ich die Unterlagen erhalte, werde ich mich dazu äußern.

25.6

Entwurf eines Gesetzes über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Landes Hessen (26. Tätigkeitsbericht, Ziff. 24.5)

Seit sechs Jahren weise ich in fast jedem meiner Tätigkeitsberichte darauf hin, daß das Verfahren der Sicherheitsüberprüfung einer gesetzlichen Grundlage bedarf.

Das Hessische Ministerium des Innern und für Landwirtschaft, Forsten und Naturschutz hat mir nun mitgeteilt, daß die Beratungen über den Entwurf eines Hessischen Sicherheitsüberprüfungsgesetzes nicht zum Abschluß gebracht werden konnten und daher mit einem abschließenden Ergebnis nicht in dieser Legislaturperiode zu rechnen ist.

Ich halte es nicht für akzeptabel, daß in einem Bereich, in dem derart weitgehende Eingriffe in das Recht auf informationelle Selbstbestimmung erfolgen, immer noch ohne konkrete gesetzliche Regelung gearbeitet wird. In dieser Sicht bestärken mich auch verschiedene Eingaben von Bürgerinnen und Bürgern, die sich einer Sicherheitsüberprüfung unterziehen müssen. Auch der Präsident des Landesamtes für Verfassungsschutz hat in einer Rundfunksendung im November 1998 mitgeteilt, daß nach seinem Eindruck zu häufig Sicherheitsüberprüfungen unter übertriebenen Geheimhaltungsstufen veranlaßt werden.

26. Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

26.1

Entschließung der 55. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 19./20. März 1998

Datenschutz beim digitalen Fernsehen

Die Datenschutzbeauftragten des Bundes und der Länder machen darauf aufmerksam, daß bei elektronischen Diensten immer umfangreichere Datenspuren über das Verhalten der einzelnen entstehen. Mit der Digitalisierung der Fernseh- und Hörfunkübertragung entsteht die technische Infrastruktur dafür, daß erstmals auch das individuelle Mediennutzungsverhalten registriert werden kann. Sie bekräftigen deshalb ihre Forderung, daß auch bei der Vermittlung und Abrechnung digitaler Fernsehsendungen eine flächendeckende Registrierung des individuellen Fernsehkonsums vermieden wird. Im digitalen Fernsehen („Free TV“ und „Pay TV“) muß die unbeobachtete Nutzung des Mediums ohne Nachteile möglich bleiben.

Die Datenschutzbeauftragten begrüßen es deshalb, daß die Staats- und Senatskanzleien Vorschläge für die Änderung des Rundfunkstaatsvertrags vorgelegt haben, mit denen Belangen des Datenschutzes Rechnung getragen werden soll. Besonders hervorzuheben sind folgende Punkte:

- Die Gestaltung technischer Einrichtungen muß sich an dem Ziel ausrichten, daß so wenige personenbezogene Daten wie möglich erhoben, verarbeitet und genutzt werden;

- die Rundfunkveranstalter müssen die Nutzung und Bezahlung von Rundfunkangeboten anonym oder unter Pseudonym ermöglichen, soweit dies technisch möglich und zumutbar ist;
- personenbezogene Daten über die Inanspruchnahme einzelner Sendungen dürfen für Abrechnungszwecke nur gespeichert werden, wenn ein Einzelnachweis verlangt wird;
- wie bereits im Mediendienste-Staatsvertrag enthält auch der Entwurf des Rundfunkstaatsvertrags eine Vorschrift zum Datenschutzaudit, d.h. Veranstalter können ihr Datenschutzkonzept und ihre technischen Einrichtungen von unabhängigen Gutachtern prüfen und das Prüfungsergebnis veröffentlichen lassen.

Die Datenschutzbeauftragten halten diese Grundsätze für geeignet, eine datenschutzgerechte Nutzung digitaler Fernsehangebote zu ermöglichen. Die technischen Möglichkeiten, diesen datenschutzrechtlichen Vorgaben zu entsprechen, sind gegeben. Die Datenschutzbeauftragten konnten sich bereits 1996 hiervon praktisch überzeugen. Die Systementscheidung von Veranstaltern für einen Decodertyp, der möglicherweise weniger geeignet ist, die Datenschutzanforderungen zu erfüllen, kann kein Maßstab für die Angemessenheit dieser Anforderungen sein, wenn zugleich andere Geräte ihnen ohne Probleme genügen.

Der Forderung von Inhabern von Verwertungsrechten, einen Nachweis über die Inanspruchnahme von pay-per-view-Angeboten vorzulegen, kann ohne Personenbezug - etwa durch zertifizierte Zähleinrichtungen oder den Einsatz von Pseudonymen - entsprochen werden.

Die Datenschutzbeauftragten bitten deshalb die Ministerpräsidentin und die Ministerpräsidenten der Länder, an den datenschutzrechtlichen Regelungen des Entwurfs festzuhalten.

Damit würden das bisherige Datenschutzniveau für die Fernsehnutzung im digitalen Zeitalter abgesichert und zugleich die Vorschriften für den Bereich des Rundfunks und der Mediendienste harmonisiert.

Die Datenschutzbeauftragten fordern die Rundfunkveranstalter und Hersteller auf, den Datenschutz bei der Gestaltung von digitalen Angeboten schon jetzt zu berücksichtigen.

26.2

Entschließung der 55. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 19./20. März 1998

Datenschutzprobleme der Geldkarte

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wiederholt ihre Forderung aus ihrer Entschließung vom 13.10.1995 nach einem anonymen elektronischen Zahlungsverfahren bei elektronischen Geldbörsen. Dies gilt insbesondere für die Geldkarte des deutschen Kreditwesens, bei der in kartenbezogenen „Schattenkonten“ der Evidenzzentralen nicht nur der Kaufbetrag und ein identifizierbarer Händlerschlüssel, sondern auch der Kaufzeitpunkt gespeichert werden. Mit diesen Daten können sämtliche mit der Geldkarte getätigten Kaufvorgänge jahrelang nachvollzogen werden, wenn die Daten mit den persönlichen Kundendaten zusammengeführt werden. Diese Geldkarte erfüllt nicht die Forderungen der Datenschutzbeauftragten.

Außerdem werden die Kundinnen und Kunden über diese „Schattenkonten“ noch nicht einmal informiert. Die Herausgeber solcher Karten bzw. die Kreditinstitute haben aber die Pflicht, ihre Kundinnen und Kunden über Art und Umfang der im Hintergrund laufenden Verarbeitungsvorgänge zu informieren.

Unabhängig davon müssen bei der Geldkarte des deutschen Kreditwesens sämtliche Umsatzdaten in den Evidenzzentralen und auch bei den Händlern nach Abschluß der Verrechnung (Clearing) gelöscht oder zumindest anonymisiert werden.

Die Datenschutzbeauftragten fordern die Kartenherausgeber und die Kreditwirtschaft erneut dazu auf, vorzugsweise kartengestützte Zahlungssysteme ohne personenbezogene Daten - sog. White Cards - anzubieten. Die Anwendung ist so zu gestalten, daß ein karten- und damit personenbezogenes Clearing nicht erfolgt.

Der Gesetzgeber bleibt aufgerufen sicherzustellen, daß auch in Zukunft die Möglichkeit besteht, im wirtschaftlichen Leben im gleichen Umfang wie bisher bei Bargeldzahlung anonym zu bleiben.

26.3

Entscheidung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998

Fehlende bereichsspezifische Regelungen bei der Justiz

Derzeit werden in allen Bereichen der Justiz - bei Staatsanwaltschaften, Gerichten und Gerichtsvollziehern - im Zuge von Modernisierungsvorhaben umfassende Systeme der automatisierten Datenverarbeitung eingeführt mit der Folge, daß sensible personenbezogene Daten auch hier in viel stärkerem Maße verfügbar werden als bisher. Sogar die Beauftragung Privater mit der Verarbeitung sensibler Justizdaten wird erwogen. Gerade vor dem Hintergrund dieser vollkommen neuen Qualität der Datenverarbeitung in der Justiz wird deutlich, daß die Rechtsprechung des Bundesverfassungsgerichts zum sogenannten Übergangsbonus hier keine tragfähige Grundlage für Eingriffe in

die informationelle Selbstbestimmung mehr darstellen kann. Vielmehr müssen die Entscheidungen des Gesetzgebers den Maßstab für die weitere technische Ausgestaltung der Datenverarbeitung innerhalb der Justiz bilden und nicht umgekehrt. Dabei ist nicht nur für formell ausreichende Rechtsgrundlagen Sorge zu tragen. Auch Fragen der Datensicherheit und der Ordnungsmäßigkeit der Datenverarbeitung bedürfen der Regelung.

Seit dem Volkszählungsurteil des Bundesverfassungsgerichts sind 15 Jahre vergangen. Dennoch werden ausgerechnet im Bereich der Justiz sensible personenbezogene Daten nach wie vor ohne die vom Bundesverfassungsgericht geforderten bereichsspezifischen gesetzlichen Grundlagen erhoben und verarbeitet.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen deshalb im Anschluß an ihren Beschluß der 48. Konferenz vom 26./27.09.1994 in Potsdam ihre wiederholten Forderungen zu bereichsspezifischen Regelungen bei der Justiz.

Zwar hat der Gesetzgeber in der abgelaufenen Legislaturperiode zumindest Regelungen über Datenerhebung, -verarbeitung und -nutzung im Strafvollzug sowie über die Datenübermittlung von Amts wegen durch Gerichte und Staatsanwaltschaften an Gerichte, Behörden und sonstige öffentlichen Stellen geschaffen.

Trotzdem sind in wichtigen Bereichen gesetzliche Regelungen weiterhin überfällig. Ausreichende gesetzliche Regelungen fehlen vor allem für

- weite Bereiche der Datenverarbeitung im Strafverfahren, insbesondere in automatisierten Dateien

namentlich die

- Übermittlung von Strafverfahrensdaten an nicht am Strafverfahren beteiligte dritte Stellen;

- Rechte der Betroffenen (nicht nur der Beschuldigten, sondern auch von Zeugen und sonstigen Personen, deren Daten gespeichert werden) in bezug auf Daten, die im Zusammenhang mit einem Strafverfahren gespeichert werden.
- Aufbewahrung von Akten, Karteien und sonstigen Unterlagen sowie die Dauer der Speicherung in automatisierten Dateien;
- Datenübermittlung zu wissenschaftlichen Zwecken;
- Datenverarbeitung in der Zwangsvollstreckung;
- Datenverarbeitung im Jugendstrafvollzug;
- Datenverarbeitung im Vollzug der Untersuchungshaft.

Der Gesetzgeber sollte daher in der kommenden Legislaturperiode zügig die notwendigen Novellierungen, für die zum Teil ja schon erhebliche Vorarbeiten geleistet worden sind, aufgreifen. Dabei ist nicht die jeweils geübte Praxis zu legalisieren, sondern es muß vorab unter datenschutzrechtlichen Gesichtspunkten geprüft werden, welche Form der Datenerhebung und -verarbeitung in welchem Umfang erforderlich ist. Ferner hat der Gesetzgeber jeweils bereichsspezifisch zu prüfen, inwieweit Aufgaben der Justiz und damit verbundene Datenverarbeitungen Privaten übertragen werden dürfen.

Der Entwurf für ein „StVÄG 1996“ erfüllt diese Voraussetzungen nicht, im Gegenteil fällt er teilweise hinter den bereits erreichten Standard der allgemeinen Datenschutzgesetze und anderer bereichsspezifischer Regelungen (wie z.B. dem Bundeszentralregistergesetz und den Polizeigesetzen der Länder) zurück. Zu kritisieren sind vor allem:

- Mangelnde Bestimmtheit der Voraussetzungen für Maßnahmen der Öffentlichkeitsfahndung
- Unangemessen weite Auskunfts- und Akteneinsichtsmöglichkeiten für nicht Verfahrensbeteiligte
- Unzureichende Regelungen über Inhalt, Ausmaß und Umfang von staatsanwaltlichen Dateien und Informationssystemen.

Die Datenschutzbeauftragten halten es deshalb zum Schutz des Rechts des Einzelnen auf informationelle Selbstbestimmung für geboten, wegen der mit der Datenerhebung, Verarbeitung und Nutzung verbundenen Rechtseingriffe unverzüglich in der neuen Legislaturperiode bereichsspezifische Regelungen der materiellen Voraussetzungen sowie der organisatorischen und verfahrensrechtlichen Vorkehrungen zu schaffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechtes der Bürgerinnen und Bürger entgegenwirken.

26.4

Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998

Dringlichkeit der Datenschutzmodernisierung

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt und unterstützt grundsätzlich die vom 62. Deutschen Juristentag (DJT) im September 1998 in Bremen gefaßten Beschlüsse zum Umgang mit Informationen einschließlich personenbezogener Daten. Von den gesetzgebenden Körperschaften erhofft sich die Konferenz die Berücksichtigung dieser Beschlüsse bei der nunmehr dringend erforderlichen

Umsetzung der EG-Datenschutzrichtlinie in Bundes- und Landesrecht.

Insbesondere betont die Konferenz folgende Punkte:

- Die materiellen Anforderungen des Datenschutzrechts sind angesichts der wachsenden Datenmacht in privater Hand auf hohem Niveau grundsätzlich einheitlich für den öffentlichen wie für den privaten Bereich zu gestalten.
- Die anlaßfreie Aufsicht für die Einhaltung des Datenschutzes im privaten Bereich muß in gleicher Weise unabhängig und weisungsfrei ausgestaltet werden wie die Datenschutzkontrolle bei öffentlichen Stellen.
- Die Rechte der Bürgerinnen und Bürger sind zu stärken; als Voraussetzung für die Ausübung des Rechts auf informationelle Selbstbestimmung der Betroffenen sind die Verpflichtungen zu ihrer Information, Aufklärung und ihren Wahlmöglichkeiten ohne faktische Zwänge auszuweiten.
- Ein modernisiertes Datenschutzrecht hat die Grundsätze der Datenvermeidung, des Datenschutzes durch Technik, der Zweckbindung der Daten und ihres Verwendungszusammenhangs in den Mittelpunkt zu stellen.
- Zur Sicherstellung vertraulicher und unverfälschter elektronischer Kommunikation ist die staatliche Förderung von Verschlüsselungsverfahren geboten, nicht eine Reglementierung der Kryptographie.

26.5

Entschließung der 56. Konferenz der Datenschutzbeauftragten

des Bundes und der Länder vom 5./6. Oktober 1998

Entwicklungen im Sicherheitsbereich

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, daß die Sicherheitsbehörden in den vergangenen Jahren umfangreiche zusätzliche Eingriffsbefugnisse erhalten haben. Demgegenüber fehlen in weiten Teilen Erkenntnisse über die Wirksamkeit und Grundrechtsverträglichkeit der Anwendung dieser Instrumente, wie z.B. bei der Schleppnetzfahndung und der Ausweitung der Telefonüberwachung.

Die Datenschutzbeauftragten des Bundes und der Länder erwarten vom Bundesgesetzgeber und der Bundesregierung, daß die Erforderlichkeit und die Wirksamkeit aller Eingriffsbefugnisse anhand objektiver Kriterien überprüft werden (Evaluierung).

26.6

Entscheidung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998

Verweigerung der Auskunft durch das Bundesamt für Finanzen auf Anfragen Betroffener über ihre Freistellungsaufträge

Die Datenschutzbeauftragten des Bundes und der Länder betonen das Recht der Bürgerinnen und Bürger auf Auskunft über ihre Daten auch gegenüber der Finanzverwaltung (§ 19 BDSG). Die Betroffenen haben Anspruch, von dem Bundesamt für Finanzen Auskunft über die Freistellungsaufträge zu erhalten, die sie ihrer Bank im Zusammenhang mit dem steuerlichen Abzug von Zinsen erteilt haben.

Der Bundesbeauftragte für den Datenschutz hat die Verweigerung der Auskünfte gegenüber dem Bundesministerium der Finanzen beanstandet und dieses aufgefordert, den entsprechenden Erlaß an das Bundesamt aufzuheben. Bisher hat das Ministerium in der Sache allerdings nicht eingelenkt.

Für die Betroffenen ergibt sich hierdurch ein unhaltbarer Zustand. Ihnen wird die Auskunft zu Unrecht vorenthalten.

Die Datenschutzbeauftragten der Länder unterstützen mit Nachdruck die Forderung des Bundesbeauftragten für den Datenschutz gegenüber dem Bundesministerium der Finanzen, seinen Erlaß an das Bundesamt für Finanzen aufzuheben und dieses anzuweisen, dem Auskunftsanspruch der Auftraggeber von Freistellungsaufträgen nachzukommen.

26.7

Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998

Weitergabe von Meldedaten an Adressbuchverlage und Parteien

Bei den Datenschutzbeauftragten des Bundes und der Länder gehen viele Beschwerden ein, in denen deutlicher Unmut über veröffentlichte Daten in Adressbüchern und unverlangt erhaltene Werbesendungen geäußert wird. Vor Wahlen nehmen die Beschwerden noch zu. Überrascht stellten Betroffene fest, daß sie persönlich adressierte Wahlwerbung der Parteien bekommen. Ihnen ist unerklärlich, wie Adressbuchverlage und Parteien an ihre Adressen gekommen sind. Sie erhalten auf Anforderung Daten aus den kommunalen Melderegistern. Damit sind die Adressbuchverlage und Parteien gegenüber anderen gesellschaftlichen Gruppen privilegiert.

Dieser Umgang mit Meldedaten ist weder transparent noch angemessen. Die Konferenz tritt dafür ein, die Rechte der Bürgerinnen und Bürger zu verbessern. Die Information über die Widerspruchsmöglichkeit erreicht die Menschen häufig nicht. Vorzuziehen ist deshalb eine Einwilligungslösung. Sie würde das Grundrecht auf informationelle Selbstbestimmung konsequent umsetzen - erst fragen, dann handeln. Nach der Einwilligungslösung ist eine Erklärung informierter Bürgerinnen und Bürger gegenüber dem Meldeamt nötig, ob sie mit den Datenweitergaben an die genannten Empfänger einverstanden sind oder nicht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder empfiehlt den gesetzgebenden Körperschaften, künftig die Einwilligungslösung vorzusehen.

26.8

Entscheidung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998

Prüfungskompetenz der Datenschutzbeauftragten bei den Gerichten

Die Datenschutzbeauftragten des Bundes und der Länder stellen fest, daß in der Praxis die Abgrenzung ihrer Zuständigkeiten bei den Gerichten immer wieder Anlaß von Unsicherheiten ist. Sie weisen daher darauf hin, daß die Beschränkung der Prüfkompetenz bei den Gerichten einzig und allein den Zweck hat, den grundgesetzlich besonders geschützten Bereich der richterlichen Unabhängigkeit von Kontrollen freizuhalten.

Deshalb erstreckt sich die Kontrolle der Datenschutzbeauftragten bei den Gerichten u.a. auch darauf, ob die erforderlichen

technischen und organisatorischen Maßnahmen zur Datensicherung getroffen und eingehalten werden, insbesondere bei automatisierter Datenverarbeitung.

Die Datenschutzbeauftragten des Bundes und der Länder halten eine gesetzliche Klarstellung für hilfreich, daß Gerichte der Kontrolle des Bundesbeauftragten bzw. der Landesbeauftragten für den Datenschutz unterliegen, soweit sie nicht in richterlicher Unabhängigkeit tätig werden.

Hessisches Datenschutzgesetz (HDSG)

in der Fassung vom Februar 1999¹

Inhaltsübersicht

ERSTER TEIL

Allgemeiner Datenschutz

Erster Abschnitt

Grundsatzregelungen

Aufgabe	§ 1
Begriffsbestimmungen	§ 2
Anwendungsbereich	§ 3
Verarbeitung personenbezogener Daten im Auftrag	§ 4
Behördlicher Datenschutzbeauftragter	§ 5
Verfahrensverzeichnis	§ 6
Zulässigkeit der Datenverarbeitung	§ 7
Rechte des Betroffenen	§ 8
Datengeheimnis	§ 9
Technische und organisatorische Maßnahmen	§ 10

Zweiter Abschnitt

Rechtsgrundlage der Datenverarbeitung

Erforderlichkeit	§ 11
Erheben	§ 12
Zweckbindung	§ 13
Verantwortlichkeit für die Zulässigkeit der Daten- übermittlung	§ 14
Gemeinsame Verfahren	§ 15
Übermittlung an Personen oder Stellen außerhalb des öffentlichen Bereichs	§ 16

¹ Zum Zeitpunkt des Redaktionsschlusses des Tätigkeitsberichts war die Neufassung noch nicht veröffentlicht. Änderungen gegenüber der alten Fassung sind durch Fettdruck gekennzeichnet.

Übermittlung an Empfänger außerhalb des Geltungs- bereichs des Grundgesetzes	§ 17
---	------

Dritter Abschnitt

Rechte des Betroffenen

Auskunft und Benachrichtigung	§ 18
Berichtigung, Sperrung und Löschung	§ 19
Schadensersatz	§ 20

ZWEITER TEIL

Hessischer Datenschutzbeauftragter

Rechtsstellung	§ 21
Unabhängigkeit	§ 22
Verschwiegenheitspflicht	§ 23
Aufgaben	§ 24
Gutachten und Untersuchungen	§ 25
Frist	§ 26
Beanstandungen durch den Hessischen Datenschutz- beauftragten	§ 27
Anrufung des Hessischen Datenschutzbeauftragten	§ 28
Auskunftsrecht des Hessischen Datenschutzbeauftragten	§ 29
Berichtspflicht	§ 30
Personal- und Sachausstattung	§ 31

DRITTER TEIL

Besonderer Datenschutz

Datenverarbeitung für Planungszwecke	§ 32
Datenverarbeitung für wissenschaftliche Zwecke	§ 33
Datenschutz bei Dienst- und Arbeitsverhältnissen	§ 34
Übermittlung an öffentlich-rechtliche Religions- gesellschaften	§ 35
Fernmessen und Fernwirken	§ 36

Datenverarbeitung des Hessischen Rundfunks zu journalistisch-redaktionellen Zwecken	§ 37
--	------

VIERTER TEIL

Rechte des Landtags und der kommunalen Vertretungsorgane

Auskunftsrecht des Landtags und der kommunalen Vertretungsorgane	§ 38
Verarbeitung personenbezogener Daten durch den Landtag und die kommunalen Vertretungsorgane	§ 39

FÜNFTER TEIL

Schlußvorschriften

Straftaten	§ 40
Ordnungswidrigkeiten	§ 41
Übergangsvorschrift	§ 42
Aufhebung bisherigen Rechts	§ 43
Inkrafttreten	§ 44

ERSTER TEIL

Allgemeiner Datenschutz

ERSTER ABSCHNITT

Grundsatzregelungen

§ 1

Aufgabe

(1) Aufgabe des Gesetzes ist es, die Verarbeitung personenbezogener Daten durch **die in § 3 Abs. 1 genannten** Stellen zu regeln, um

1. das Recht des einzelnen zu schützen, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen, soweit keine Einschränkungen in diesem Gesetz oder in anderen Rechtsvorschriften zugelassen sind,
2. das auf dem Grundsatz der Gewaltenteilung beruhende verfassungsmäßige Gefüge des Staates, insbesondere der Verfassungsorgane des Landes und der Organe der kommunalen Selbstverwaltung untereinander und zueinander, vor einer Gefährdung infolge der automatisierten Datenverarbeitung zu bewahren.

(2) Aufgabe der obersten Landesbehörden, Gemeinden und Landkreise sowie der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts ist es, die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz jeweils für ihren Bereich sicherzustellen.

§ 2

Begriffsbestimmungen

(1) Personenbezogene Daten sind Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person (Betroffener).

(2) Datenverarbeitung ist jede Verwendung gespeicherter oder zur Speicherung vorgesehener personenbezogener Daten. Im Sinne der nachfolgenden Vorschriften ist

1. Erheben das Beschaffen von Daten über den Betroffenen,
2. Speichern das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung,
3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten in der Weise, daß die Daten durch die datenverarbeitende Stelle an den Dritten weitergegeben werden oder daß der Dritte zum Abruf bereitgehaltene Daten abrufen,
4. Sperren das Verhindern weiterer Verarbeitung gespeicherter Daten,
5. Löschen das Unkenntlichmachen gespeicherter Daten

ungeachtet der dabei angewendeten Verfahren.

(3) Datenverarbeitende Stelle ist jede der in § 3 Abs. 1 genannten Stellen, die Daten für sich selbst verarbeitet oder durch andere verarbeiten läßt.

(4) Empfänger ist jede Person oder Stelle, die Daten erhält.

(5) Dritter ist jede Person oder Stelle außerhalb der datenverarbeitenden Stelle, ausgenommen der Betroffene oder

diejenigen Personen und Stellen, die innerhalb des Geltungsbereichs der EG-Datenschutzrichtlinie Daten im Auftrag verarbeiten.

(6) Automatisiert ist eine Datenverarbeitung, wenn sie durch Einsatz eines gesteuerten technischen Verfahrens selbsttätig abläuft.

(7) Eine Akte ist jede **der Aufgabenerfüllung** dienende Unterlage, **die nicht Teil der automatisierten Datenverarbeitung ist.**

(8) Soweit andere landesrechtliche Vorschriften den Dateibegriff verwenden, ist Datei

1. eine Sammlung von Daten, die durch automatisierte Verfahren ausgewertet werden kann (automatisierte Datei), oder
2. eine gleichartig aufgebaute Sammlung von Daten, die nach bestimmten Merkmalen geordnet und ausgewertet werden kann (nicht-automatisierte Datei).

§ 3

Anwendungsbereich

(1) Dieses Gesetz gilt für Behörden und sonstige öffentliche Stellen des Landes, der Gemeinden und Landkreise sowie der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und für deren Vereinigungen **ungeachtet ihrer Rechtsform. Dieses Gesetz gilt auch für nicht-öffentliche Stellen, soweit sie hoheitliche Aufgaben unter Aufsicht der in Satz 1 genannten Stellen wahrnehmen.**

(2) Die Vorschriften dieses Gesetzes gehen denen des Hessischen Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

(3) Soweit besondere Rechtsvorschriften über den Datenschutz bei der Verarbeitung personenbezogener Daten vorhanden sind, gehen sie den Vorschriften dieses Gesetzes vor.

(4) Dieses Gesetz gilt nicht für personenbezogene Daten, solange sie in allgemein zugänglichen Quellen gespeichert sind sowie für Daten des Betroffenen, die von ihm zur Veröffentlichung bestimmt sind.

(5) Soweit der Hessische Rundfunk personenbezogene Daten ausschließlich zu eigenen journalistisch-redaktionellen Zwecken verarbeitet, gelten von den Vorschriften dieses Gesetzes nur die §§ 10 und 37. Im übrigen gelten die Vorschriften dieses Gesetzes.

(6) Soweit öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, gelten für sie nur der Zweite Teil sowie die §§ 34 und 36 dieses Gesetzes. Mit Ausnahme der Vorschriften über die Aufsichtsbehörde sind im übrigen die für nicht-öffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes einschließlich der Straf- und Bußgeldvorschriften anwendbar.

§ 4

Verarbeitung personenbezogener Daten im Auftrag

(1) Die datenverarbeitende Stelle bleibt für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz **sowie für die Erfüllung ihrer sich aus § 8 ergebenden Pflichten** auch dann verantwortlich, wenn personenbezogene Daten in ihrem Auftrag durch andere Personen oder Stellen verarbeitet werden. Der Auftragnehmer darf personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Ist der Auftragnehmer der Ansicht, daß eine Weisung des Auftraggebers gegen dieses Gesetz oder andere

Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Zuverlässigkeit und der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen; dabei sind der Gegenstand und der Umfang der Datenverarbeitung, die technischen und organisatorischen Maßnahmen sowie etwaige Unterauftragsverhältnisse festzulegen. Für ergänzende Weisungen gilt Satz 2 entsprechend. Der Auftraggeber hat zu prüfen, ob beim Auftragnehmer die nach § 10 erforderlichen Maßnahmen getroffen **und die erhöhten Anforderungen bei der Verarbeitung von Daten, die besonderen Amts- oder Berufsgeheimnissen unterliegen sowie der in § 7 Abs. 4 genannten Daten eingehalten werden. An nicht-öffentliche Stellen darf ein Auftrag nur vergeben werden, wenn weder gesetzliche Regelungen über Berufs- oder besondere Amtsgeheimnisse noch überwiegende schutzwürdige Belange entgegenstehen.**

(3) Sofern die Vorschriften dieses Gesetzes auf den Auftragnehmer keine Anwendung finden, ist der Auftraggeber verpflichtet, vertraglich sicherzustellen, daß der Auftragnehmer die Bestimmungen dieses Gesetzes befolgt und sich der Kontrolle des Hessischen Datenschutzbeauftragten unterwirft. Der Auftraggeber hat den Hessischen Datenschutzbeauftragten **vorab** über die Beauftragung zu unterrichten.

(4) Abs. 1 bis 3 gelten auch für Personen und Stellen, die im Auftrag Wartungsarbeiten und vergleichbare Hilfstätigkeiten bei der Datenverarbeitung erledigen.

§ 5

Behördlicher Datenschutzbeauftragter

(1) Die datenverarbeitende Stelle hat **schriftlich** einen behördlichen Datenschutzbeauftragten **sowie einen Vertreter** zu bestellen. Bestellt werden dürfen nur Beschäftigte, die dadurch keinem Interessenkonflikt mit sonstigen dienstlichen Aufgaben ausgesetzt werden. Für die Wahrnehmung seiner Aufgaben nach Abs. 2 muß der behördliche Datenschutzbeauftragte die erforderliche Sachkenntnis und Zuverlässigkeit besitzen. **Wegen dieser Tätigkeit, bei der er frei von Weisungen ist, darf er nicht benachteiligt werden. Er ist insoweit unmittelbar der Leitung der datenverarbeitenden Stelle zu unterstellen; in Gemeinden und Gemeindeverbänden kann er auch einem hauptamtlichen Beigeordneten unterstellt werden. Der behördliche Datenschutzbeauftragte ist im erforderlichen Umfang von der Erfüllung anderer Aufgaben freizustellen sowie mit den zur Erfüllung seiner Aufgaben notwendigen räumlichen, personellen und sachlichen Mitteln auszustatten. Die Beschäftigten der datenverarbeitenden Stelle können sich ohne Einhaltung des Dienstweges in allen Angelegenheiten des Datenschutzes an ihn wenden.**

(2) Der behördliche Datenschutzbeauftragte hat die Aufgabe, die datenverarbeitende Stelle bei der Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz zu unterstützen und Hinweise zur Umsetzung zu geben. Zu seinen Aufgaben gehört es insbesondere

- 1. auf die Einhaltung der Datenschutzvorschriften bei der Einführung von Maßnahmen, die das in § 1 Satz 1 Nr. 1 geschützte Recht betreffen, hinzuwirken,**
- 2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den**

**Bestimmungen dieses Gesetzes sowie den sonstigen
Vorschriften über den Datenschutz vertraut zu machen,**

- 3. die datenverarbeitende Stelle bei der Umsetzung der nach den §§ 6, 10 und 29 erforderlichen Maßnahmen zu unterstützen,**
- 4. das nach § 6 Abs. 1 zu erstellende Verzeichnis zu führen und für die Einsicht nach § 6 Abs. 2 bereitzuhalten,**
- 5. das Ergebnis der Untersuchung nach § 7 Abs. 6 zu prüfen und im Zweifelsfall den Hessischen Datenschutzbeauftragten zu hören.**

Soweit keine gesetzliche Regelung entgegensteht, kann er die zur Erfüllung seiner Aufgaben notwendige Einsicht in Akten und die automatisierte Datenverarbeitung nehmen. Vor einer beabsichtigten Maßnahme nach Satz 2 Nr. 1 ist er rechtzeitig umfassend zu unterrichten und anzuhören. Wird er nicht rechtzeitig an einer Maßnahme beteiligt, ist die Entscheidung über die Maßnahme auszusetzen und die Beteiligung nachzuholen.

(3) Die datenverarbeitende Stelle kann einen Beschäftigten ihrer Aufsichtsbehörde mit deren Zustimmung zum Beauftragten für den Datenschutz bestellen. Mehrere datenverarbeitende Stellen können gemeinsam einen ihrer Beschäftigten zum Datenschutzbeauftragten bestellen, wenn dadurch die Erfüllung seiner Aufgabe nicht beeinträchtigt wird. Bestellungen von Personen, die nicht der datenverarbeitenden Stelle angehören, sind dem Hessischen Datenschutzbeauftragten mitzuteilen.

§ 6²

Verfahrensverzeichnis

(1) Wer für den Einsatz eines Verfahrens zur automatisierten Verarbeitung personenbezogener Daten zuständig ist, hat in einem für den behördlichen Datenschutzbeauftragten bestimmten Verzeichnis festzulegen:

- 1. Name und Anschrift der datenverarbeitenden Stelle,**
- 2. die Zweckbestimmung und die Rechtsgrundlage der Datenverarbeitung,**
- 3. die Art der gespeicherten Daten,**
- 4. den Kreis der Betroffenen,**
- 5. die Art regelmäßig übermittelter Daten, deren Empfänger sowie die Art und Herkunft regelmäßig empfangener Daten,**
- 6. die zugriffsberechtigten Personen oder Personengruppen,**
- 7. die technischen und organisatorischen Maßnahmen nach § 10,**
- 8. die Technik des Verfahrens,**
- 9. Fristen für die Löschung nach § 19 Abs. 3,**
- 10. eine beabsichtigte Datenübermittlung nach § 17 Abs. 2,**
- 11. das begründete Ergebnis der Untersuchung nach § 7 Abs. 6 Satz 3.**

(2) Die Angaben des Verfahrensverzeichnisses können bei der datenverarbeitenden Stelle von jeder Person eingesehen werden; dies gilt für die Angaben zu Nr. 7, 8 und 11 nur, soweit dadurch die Sicherheit des Verfahrens nicht beeinträchtigt wird.

Satz 1 gilt nicht für

² § 6 tritt am 1. Juni 1999 in Kraft.

1. Verfahren des Landesamtes für Verfassungsschutz,

**2. Verfahren, die der Gefahrenabwehr oder der
Strafverfolgung dienen,**

3. Verfahren der Steuerfahndung,

**soweit die datenverarbeitende Stelle eine Einsichtnahme im
Einzelfall mit der Erfüllung ihrer Aufgaben für unvereinbar
erklärt.**

§ 7

Zulässigkeit der Datenverarbeitung

(1) Die Verarbeitung personenbezogener Daten ist nur zulässig,
wenn

**1. eine diesem Gesetz vorgehende Rechtsvorschrift sie vorsieht
oder zwingend voraussetzt,**

2. dieses Gesetz sie zuläßt oder

3. der Betroffene ohne jeden Zweifel eingewilligt hat.

(2) Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. **Sie muß sich im Falle einer Datenverarbeitung nach Abs. 4 ausdrücklich auch auf die dort genannten Daten beziehen.** Wird die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt, ist der Betroffene hierauf schriftlich besonders hinzuweisen. Der Betroffene ist in geeigneter Weise über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten, aufzuklären. Die Aufklärungspflicht umfaßt bei beabsichtigten Übermittlungen auch den Empfänger der Daten. Der

Betroffene ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, daß er die Einwilligung verweigern **und jederzeit mit Wirkung für die Zukunft widerrufen kann.**

(3) Unzulässig ist eine zu rechtlichen Folgen oder erheblichen Beeinträchtigungen für den Betroffenen führende Entscheidung, wenn sie auf einer Bewertung einzelner Merkmale seiner Person beruht, die ausschließlich durch eine automatisierte Verarbeitung seiner Daten erstellt wurde. Eine Entscheidung nach Satz 1 kann durch Gesetz zugelassen werden, das die Wahrung der berechtigten Interessen des Betroffenen sicherstellt.

(4) Soweit nicht eine Rechtsvorschrift die Verarbeitung personenbezogener Daten über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben vorsieht oder zwingend voraussetzt, darf eine Verarbeitung nur nach §§ 33 bis 35 und 39 erfolgen. Im übrigen ist eine Verarbeitung auf Grund dieses Gesetzes nur zulässig, wenn sie ausschließlich im Interesse des Betroffenen liegt und der Hessische Datenschutzbeauftragte vorab gehört worden ist.

(5) Wenn der Betroffene schriftlich begründet, daß der rechtmäßigen Verarbeitung seiner Daten auf Grund dieses Gesetzes schutzwürdige, sich aus seiner besonderen persönlichen Lage ergebende Gründe entgegenstehen, ist die Verarbeitung nur zulässig, nachdem eine Abwägung im Einzelfall ergeben hat, daß seine Gründe hinter dem öffentlichen Interesse an der Verarbeitung zurückstehen müssen. Dem Betroffenen ist das Ergebnis mit Begründung schriftlich mitzuteilen.

(6) Wer für den Einsatz oder die wesentliche Änderung eines Verfahrens zur automatisierten Datenverarbeitung zuständig ist, hat vor dem Beginn der Verarbeitung zu untersuchen, ob damit Gefahren für die in § 1 Abs. 1 Nr. 1 geschützten Rechte verbunden sind; dies gilt in besonderem Maße für die in § 7 Abs. 4 genannten Daten. Das Verfahren darf nur eingesetzt werden, wenn sichergestellt ist, daß diese Gefahren nicht bestehen oder durch technische und organisatorische Maßnahmen verhindert werden können. Das Ergebnis der Untersuchung und dessen Begründung sind aufzuzeichnen und dem behördlichen Datenschutzbeauftragten zur Prüfung zuzuleiten.

(7) Die in § 3 Abs. 1 Satz 2 und Abs. 6 genannten Stellen dürfen Daten, die Straftaten betreffen, nur unter behördlicher Aufsicht verarbeiten oder wenn eine Rechtsvorschrift dies vorsieht.

§ 8

Rechte der Betroffenen

(1) Jeder hat nach Maßgabe dieses Gesetzes ein Recht auf

1. Auskunft und Benachrichtigung über die zu seiner Person gespeicherten Daten (§ 18),
2. **Überprüfung der rechtmäßigen Verarbeitung seiner Daten auf Grund von ihm vorgebrachter besonderer persönlicher Gründe (§ 7 Abs. 5),**
3. **Einsicht in das Verfahrensverzeichnis (§ 6 Abs. 2),**
4. Berichtigung, Sperrung oder Löschung der zu seiner Person gespeicherten Daten (§ 19),
5. Schadensersatz (§ 20),
6. Anrufung des Datenschutzbeauftragten (§§ 28 und 37 Abs. 2).

(2) Wenn eine in § 3 Abs. 1 genannte Stelle für die Gewährung einer Leistung, das Erkennen einer Person oder für einen anderen Zweck einen Datenträger herausgibt, auf dem personenbezogene Daten des Inhabers automatisiert, etwa in Form einer Chipkarte, verarbeitet werden, dann hat sie sicherzustellen, daß er dies erkennen und seine ihm nach Abs. 1 Nr. 1 bis 5 zustehenden Rechte ohne unvertretbaren Aufwand geltend machen kann. Der Inhaber ist bei Ausgabe des Datenträgers über die ihm nach Abs. 1 zustehenden Rechte sowie über die von ihm bei Verlust des Datenträgers zu treffenden Maßnahmen und über die Folgen aufzuklären.

§ 9

Datengeheimnis

Den bei der datenverarbeitenden Stelle oder in deren Auftrag beschäftigten Personen, die Zugang zu personenbezogenen Daten haben, ist eine Verarbeitung dieser Daten zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck während und nach Beendigung ihrer Tätigkeit untersagt. Diese Personen sind über die bei ihrer Tätigkeit zu beachtenden Vorschriften über den Datenschutz zu unterrichten.

§ 10

Technische und organisatorische Maßnahmen

(1) Die datenverarbeitende oder in ihrem Auftrag tätige Stelle hat die technischen und organisatorischen Maßnahmen zu treffen, die nach **Abs. 2 und 3** erforderlich sind, um die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz zu gewährleisten. **Erforderlich sind diese Maßnahmen, soweit der damit verbundene Aufwand unter Berücksichtigung der Art**

der personenbezogenen Daten und ihrer Verarbeitung zum Schutz des in § 1 Abs. 1 Nr. 1 genannten Rechts angemessen ist.

(2) Werden personenbezogene Daten automatisiert verarbeitet, ist das Verfahren auszuwählen oder zu entwickeln, welches geeignet ist, so wenig personenbezogene Daten zu verarbeiten, wie zur Erreichung des angestrebten Zwecks erforderlich ist. Außerdem sind Maßnahmen schriftlich anzuordnen, die nach dem jeweiligen Stand der Technik und der Art des eingesetzten Verfahrens erforderlich sind, um zu gewährleisten, daß

- 1. Unbefugte keinen Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, erhalten (Zutrittskontrolle),**
- 2. Unbefugte an der Benutzung von Datenverarbeitungsanlagen und -verfahren gehindert werden (Benutzerkontrolle),**
- 3. die zur Benutzung eines Datenverarbeitungsverfahrens Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können (Zugriffskontrolle),**
- 4. personenbezogene Daten nicht unbefugt oder nicht zufällig gespeichert, zur Kenntnis genommen, verändert, kopiert, übermittelt, gelöscht, entfernt, vernichtet oder sonst verarbeitet werden (Datenverarbeitungskontrolle),**
- 5. es möglich ist, festzustellen, wer welche personenbezogenen Daten zu welcher Zeit verarbeitet hat und wohin sie übermittelt werden sollen oder übermittelt worden sind (Verantwortlichkeitskontrolle),**
- 6. personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),**
- 7. durch eine Dokumentation aller wesentlichen Verarbeitungsschritte die Überprüfbarkeit der**

Datenverarbeitungsanlage und des -verfahrens möglich ist (Dokumentationskontrolle),

8. die innerbehördliche oder innerbetriebliche Organisation den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).

(3) Werden personenbezogene Daten nicht automatisiert verarbeitet, dann sind insbesondere Maßnahmen zu treffen, um den Zugriff Unbefugter bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung zu verhindern.

ZWEITER ABSCHNITT

Rechtsgrundlage der Datenverarbeitung

§ 11

Erforderlichkeit

(1) Die Verarbeitung personenbezogener Daten ist nach Maßgabe der nachfolgenden Vorschriften zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der datenverarbeitenden Stelle liegenden Aufgaben und für den jeweils damit verbundenen Zweck erforderlich ist. **Die Erforderlichkeit einer Datenübermittlung muß bei einer der beteiligten Stellen vorliegen.**

(2) Sind personenbezogene Daten in Akten derart verbunden, daß ihre Trennung nach erforderlichen und nicht erforderlichen Daten nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist, dann sind die Kenntnisnahme, die Weitergabe innerhalb der datenverarbeitenden Stelle und die Übermittlung der Daten, die nicht zur Erfüllung der jeweiligen Aufgabe erforderlich sind, über Abs. 1 hinaus zulässig. Diese Daten unterliegen insoweit einem Verwertungsverbot.

§ 12

Erheben

(1) Personenbezogene Daten sind grundsätzlich bei dem Betroffenen mit seiner Kenntnis zu erheben. **Werden Daten nicht über eine bestimmte Person, sondern über einen bestimmbaren Personenkreis, etwa durch Videoüberwachung, erhoben, dann genügt es, wenn er die seinen schutzwürdigen Belangen angemessene Möglichkeit zur Kenntnisnahme hat.**

(2) Bei öffentlichen Stellen dürfen Daten im Einzelfall ohne seine Kenntnis nur erhoben werden, wenn

1. eine Rechtsvorschrift dies vorsieht, zwingend voraussetzt oder der Betroffene eingewilligt hat,
2. die Bearbeitung eines vom Betroffenen gestellten Antrags ohne Kenntnis der Daten nicht möglich ist oder Angaben des Betroffenen überprüft werden müssen; der Betroffene ist darauf hinzuweisen, bei welchen Personen oder Stellen seine Daten erhoben werden können,
3. die Abwehr erheblicher Nachteile für das Allgemeinwohl oder von Gefahren für Leben, Gesundheit und persönliche Freiheit dies gebietet,
4. sich bei Gelegenheit der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben oder
5. die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte dafür

bestehen, daß schutzwürdige Belange des Betroffenen beeinträchtigt werden können.

(3) Beim Betroffenen und bei Dritten außerhalb des öffentlichen Bereichs dürfen Daten ohne seine Kenntnis nur erhoben werden, wenn der Schutz von Leben und Gesundheit oder die Abwehr einer erheblichen Gefährdung der natürlichen Lebensgrundlagen dies im Einzelfall gebietet oder eine Rechtsvorschrift dies vorsieht **oder, soweit es sich um eine Rechtsvorschrift des Bundes handelt, zwingend voraussetzt.**

(4) Werden Daten beim Betroffenen mit seiner Kenntnis erhoben, dann ist er **von der datenverarbeitenden Stelle** in geeigneter Weise über **deren Anschrift**, den Zweck der Datenerhebung **sowie über seine Rechte nach § 8** aufzuklären. Die Aufklärungspflicht umfaßt bei beabsichtigten Übermittlungen auch den Empfänger der Daten. Werden Daten bei dem Betroffenen auf Grund einer durch Rechtsvorschrift festgelegten Auskunftspflicht erhoben, dann ist er auf die Rechtsgrundlage hinzuweisen. Im übrigen ist er darauf hinzuweisen, daß er die Auskunft verweigern kann. Sind die Angaben für die Gewährung einer Leistung erforderlich, ist er über die möglichen Folgen einer Nichtbeantwortung aufzuklären.

(5) Werden Daten beim Betroffenen ohne seine Kenntnis erhoben, dann ist er davon zu benachrichtigen, sobald die rechtmäßige Erfüllung der Aufgaben dadurch nicht mehr gefährdet wird. Die Benachrichtigung umfaßt die Angabe der Rechtsgrundlage und die in Abs. 4 Satz 1 und 2 vorgesehene Aufklärung.

§ 13

Zweckbindung

(1) Personenbezogene Daten dürfen grundsätzlich nur für den Zweck weiterverarbeitet werden, für den sie erhoben oder gespeichert worden sind.

(2) Sollen personenbezogene Daten zu Zwecken verarbeitet werden, für die sie nicht erhoben oder gespeichert worden sind, dann ist dies nur aus den in § 12 Abs. 2 und 3 genannten Gründen zulässig. Besondere Amts- oder Berufsgeheimnisse bleiben unberührt.

(3) Sind personenbezogene Daten in Akten derart verbunden, daß ihre Trennung nach verschiedenen Zwecken nicht oder nur mit unvertretbar großem Aufwand möglich ist, so tritt an die Stelle der Trennung ein Verwertungsverbot nach Maßgabe von Abs. 2 für die Daten, die nicht dem Zweck der jeweiligen Verarbeitung dienen.

(4) Personenbezogene Daten, die für andere Zwecke erhoben worden sind, dürfen auch zur Ausübung von Aufsichts- und Kontrollbefugnissen sowie zu Ausbildungs- und Prüfungszwecken in dem dafür erforderlichen Umfang verwendet werden.

(5) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nicht für andere Zwecke verwendet werden.

§ 14

Verantwortlichkeit für die Zulässigkeit der Datenübermittlung

Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Ist die Übermittlung zur Erfüllung von Aufgaben **eines in § 3 Abs. 1** genannten Empfängers erforderlich, so trägt auch dieser hierfür die Verantwortung und hat

sicherzustellen, daß die Erforderlichkeit nachträglich überprüft werden kann. Die übermittelnde Stelle hat in diesem Fall die Zuständigkeit des Empfängers und die Schlüssigkeit der Anfrage zu überprüfen. Bestehen im Einzelfall Zweifel an der Schlüssigkeit, so hat sie darüber hinaus die Erforderlichkeit zu überprüfen. Der Empfänger hat der übermittelnden Stelle die für ihre Prüfung erforderlichen Angaben zu machen.

§ 15

Gemeinsame Verfahren

(1) Die Einrichtung eines automatisierten Verfahrens, das mehreren datenverarbeitenden Stellen gemeinsam die Verarbeitung personenbezogener Daten ermöglicht, ist nur zulässig, wenn dies unter Berücksichtigung der schutzwürdigen Belange der Betroffenen und der Aufgaben der beteiligten Stellen angemessen ist. Die Benutzung des Verfahrens ist im Einzelfall nur erlaubt, wenn hierfür die Zulässigkeit der Datenverarbeitung gegeben ist. Vor der Einrichtung oder Änderung eines gemeinsamen Verfahrens ist der Hessische Datenschutzbeauftragte zu hören. Ihm sind die Festlegungen nach Abs. 2 Satz 1, das Verfahrensverzeichnis nach § 6 Abs. 1 und das Ergebnis der Untersuchung nach § 7 Abs. 6 Satz 3 vorzulegen.

(2) Die beteiligten Stellen bestimmen eine Stelle, der die Planung, Einrichtung und Durchführung des gemeinsamen Verfahrens obliegt und legen schriftlich fest

1. die Bezeichnung und die Aufgaben jeder beteiligten datenverarbeitenden Stelle sowie den Bereich der Datenverarbeitung, für deren Rechtmäßigkeit sie im Einzelfall verantwortlich ist und

2. die für die Durchführung des gemeinsamen Verfahrens nach § 10 Abs. 2 getroffenen technischen und organisatorischen Maßnahmen.

Die mit der Durchführung des gemeinsamen Verfahrens betraute Stelle verwahrt ein Doppel des von den beteiligten Stellen nach § 6 Abs. 1 zu erstellenden Verfahrensverzeichnisses und hält es zusammen mit den Angaben nach Satz 1 Nr. 1 zur Einsicht für die Öffentlichkeit bereit; dies gilt auch für die Angaben nach Satz 1 Nr. 2, soweit dadurch die Sicherheit des Verfahrens nicht beeinträchtigt wird. § 6 Abs. 2 gilt entsprechend.

(3) Stellen, auf die dieses Gesetz keine Anwendung findet, können am gemeinsamen Verfahren beteiligt werden, wenn vertraglich sichergestellt ist, daß sie in diesem Verfahren die Bestimmungen dieses Gesetzes beachten und sich der Kontrolle des Hessischen Datenschutzbeauftragten unterwerfen.

(4) Die Betroffenen können ihre Rechte nach § 8 Abs. 1 Nr. 1 bis 5 gegenüber jeder der beteiligten Stellen geltend machen, unabhängig davon, welche Stelle im Einzelfall für die Verarbeitung der betroffenen Daten verantwortlich ist. Die Stelle, an die der Betroffene sich wendet, leitet das Anliegen an die jeweils zuständige Stelle weiter. Das Auskunftsrecht nach § 18 erstreckt sich auch auf die Angaben nach Abs. 2 Satz 1 Nr. 1.

(5) Die Abs. 1, 2 und 4 Satz 3 gelten entsprechend, wenn innerhalb einer datenverarbeitenden Stelle ein gemeinsames automatisiertes Verfahren zur Verarbeitung personenbezogener Daten für verschiedene Zwecke eingerichtet wird.

§ 16

Übermittlung an Personen oder Stellen außerhalb des öffentlichen Bereichs

(1) Die Übermittlung personenbezogener Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs ist über §§ 11 und 13 hinaus zulässig, wenn der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und keine Anhaltspunkte dafür bestehen, daß schutzwürdige Belange des Betroffenen beeinträchtigt werden können.

(2) Der Empfänger darf die übermittelten Daten nur zu dem Zweck verwenden, zu dessen Erfüllung sie ihm übermittelt wurden.

§ 17

Übermittlung an Empfänger außerhalb des Geltungsbereichs des Grundgesetzes

(1) Für die Zulässigkeit der Übermittlung personenbezogener Daten innerhalb des Geltungsbereichs der EG-Datenschutzrichtlinie gelten die Vorschriften dieses Gesetzes.

(2) Eine Übermittlung an Empfänger außerhalb des in Abs. 1 genannten Bereichs ist auf Grund dieses Gesetzes nur zulässig, wenn sie ausschließlich im Interesse des Betroffenen liegt oder beim Empfänger ein angemessener Datenschutz gewährleistet ist. Vor der Entscheidung über die Angemessenheit ist der Hessische Datenschutzbeauftragte zu hören. Sofern beim Empfänger kein angemessener Datenschutz gewährleistet ist, dürfen personenbezogene Daten nur übermittelt werden, wenn

1. der Betroffene seine Einwilligung gegeben hat,

- 2. die Übermittlung für die Wahrung eines überwiegenden öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist,**
- 3. die Übermittlung für die Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist oder**
- 4. die Übermittlung aus einem Register erfolgt, das zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, soweit die gesetzlichen Voraussetzungen im Einzelfall gegeben sind.**

Der Empfänger, an den die Daten übermittelt werden, ist darauf hinzuweisen, daß die übermittelten Daten nur zu Zwecken verarbeitet werden dürfen, die mit den Zwecken zu vereinbaren sind, zu deren Erfüllung sie ihm übermittelt werden.

DRITTER ABSCHNITT

Rechte des Betroffenen

§ 18

Auskunft und Benachrichtigung

(1) Datenverarbeitende Stellen, die personenbezogene Daten automatisiert speichern, haben die Betroffenen von dieser Tatsache schriftlich zu benachrichtigen und dabei die Art der Daten sowie die Zweckbestimmung und die Rechtsgrundlage der Speicherung zu nennen. Die Benachrichtigung erfolgt zum Zeitpunkt der Speicherung oder im Fall einer beabsichtigten

Übermittlung spätestens mit deren Durchführung. Dienen die Daten der Erstellung einer beabsichtigten Mitteilung an den Betroffenen, kann die Benachrichtigung mit dieser Mitteilung verbunden werden.

(2) Eine Pflicht zur Benachrichtigung besteht nicht, wenn

- 1. die Daten beim Betroffenen erhoben oder von ihm mitgeteilt worden sind,**
- 2. die Verarbeitung der personenbezogenen Daten durch Gesetz ausdrücklich vorgesehen ist,**
- 3. der Betroffene auf andere Weise Kenntnis von der Verarbeitung seiner Daten erlangt hat,**
- 4. die Benachrichtigung des Betroffenen unmöglich ist oder einen unverhältnismäßigen Aufwand erfordert.**

(3) Datenverarbeitende Stellen, die personenbezogene Daten automatisiert speichern, haben dem Betroffenen auf Antrag gebührenfrei Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten
2. den Zweck und die Rechtsgrundlage der Verarbeitung sowie
3. die Herkunft der Daten und die **Empfänger übermittelter Daten**, soweit dies gespeichert ist.

In dem Antrag soll die Art der Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden.

(4) Abs. 1 und 3 gelten nicht für personenbezogene Daten, die deshalb gesperrt sind, weil sie auf Grund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, sowie für solche Daten, die ausschließlich zum Zwecke der Datensicherung oder Datenschutzkontrolle gespeichert werden.

(5) Sind personenbezogene Daten in Akten gespeichert, die zur Person des Betroffenen geführt werden, dann kann er bei der speichernden Stelle Einsicht in die von ihm bezeichneten Akten verlangen. Werden die Akten nicht zur Person des Betroffenen geführt, hat er Angaben zu machen, die das Auffinden der zu seiner Person gespeicherten Daten mit angemessenem Aufwand ermöglichen. Die Einsichtnahme ist unzulässig, wenn die Daten des Betroffenen mit Daten Dritter oder geheimhaltungsbedürftigen nicht personenbezogenen Daten derart verbunden sind, daß ihre Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist. In diesem Fall ist dem Betroffenen Auskunft nach Abs. 3 zu erteilen. Im übrigen kann ihm statt Einsicht Auskunft gewährt werden.

(6) Abs. 1 **und 3** gelten nicht, soweit eine Abwägung ergibt, daß die dort gewährten Rechte des Betroffenen hinter dem öffentlichen Interesse an der Geheimhaltung oder einem überwiegenden Geheimhaltungsinteresse Dritter zurücktreten müssen. Die Entscheidung trifft der Leiter der speichernden Stelle oder dessen Stellvertreter. Werden Auskunft oder Einsicht nicht gewährt, ist der Betroffene unter Mitteilung der wesentlichen Gründe darauf hinzuweisen, daß er sich an den Hessischen Datenschutzbeauftragten wenden kann.

(7) Bei Prüfungs- und Berufungsverfahren können die in Abs. 1 bis 6 gewährten Rechte erst nach dem Verfahrensabschluß geltend gemacht werden.

§ 19

Berichtigung, Sperrung und Löschung

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.

(2) Personenbezogene Daten sind zu sperren, wenn

1. ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt,
2. ihre Verarbeitung unzulässig **ist** und **die Löschung den Betroffenen in der Verfolgung seiner Rechte beeinträchtigen würde.**

Bei automatisierten **Verfahren** ist die Sperrung grundsätzlich durch technische Maßnahmen sicherzustellen; im übrigen ist ein entsprechender Vermerk anzubringen. Gesperrte Daten dürfen über die Speicherung hinaus nicht mehr verarbeitet werden, es sei denn, daß die Verarbeitung zur Behebung einer bestehenden Beweisnot oder aus sonstigen im rechtlichen Interesse eines Dritten liegenden Gründen unerlässlich ist oder der Betroffene in die Verarbeitung eingewilligt hat.

(3) Personenbezogene Daten sind unverzüglich zu löschen, sobald feststeht, daß ihre Speicherung nicht mehr erforderlich ist, um die Zwecke zu erfüllen, für die sie erhoben worden sind oder für die sie nach § 13 Abs. 2 und 4 weiterverarbeitet werden dürfen. Wenn bei der Speicherung nicht absehbar ist, wie lange die Daten benötigt werden, ist nach einer auf Grund der Erfahrung zu bestimmenden Frist zu prüfen, ob die Erforderlichkeit der Speicherung noch besteht. Satz 1 findet keine Anwendung, wenn Grund zu der Annahme besteht, daß durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden.

(4) Personenbezogene Daten sind zu löschen, wenn ihre Verarbeitung unzulässig ist.

(5) **Empfänger** personenbezogener Daten sind unverzüglich von der Berichtigung nach Abs. 1 sowie von der Sperrung nach Abs. 2

und der Löschung nach Abs. 4 zu unterrichten. Die Unterrichtung kann unterbleiben, wenn sie einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte bestehen, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden können.

(6) Sind personenbezogene Daten in Akten gespeichert, ist die **Löschung** nach Abs. 3 nur durchzuführen, wenn die gesamte zur Person des Betroffenen geführte Akte zur Erfüllung der dort genannten Aufgaben nicht mehr erforderlich ist. Die Abs. 1 bis 4 gelten nicht für Stellen, die Akten nur vorübergehend beigezogen haben.

§ 20

Schadensersatz

(1) Wird der Betroffene durch eine unzulässige oder unrichtige automatisierte Verarbeitung personenbezogener Daten in seinen Rechten nach § 1 **Abs. 1** Nr. 1 beeinträchtigt, so hat ihm der Träger der datenverarbeitenden Stelle den daraus entstehenden Schaden zu ersetzen. In schweren Fällen kann der Betroffene auch wegen des Schadens, der nicht Vermögensschaden ist, eine billige Entschädigung in Geld verlangen. Der Ersatzpflichtige haftet jedem Betroffenen für jedes schädigende Ereignis bis zu einem Betrag von fünfhunderttausend Deutsche Mark.

(2) Auf das Mitverschulden des Betroffenen und auf die Verjährung sind die §§ 254 und 852 des Bürgerlichen Gesetzbuches entsprechend anzuwenden.

(3) Weitergehende sonstige Schadensersatzansprüche bleiben unberührt.

(4) Der Rechtsweg vor den ordentlichen Gerichten steht offen.

ZWEITER TEIL

Hessischer Datenschutzbeauftragter

§ 21

Rechtsstellung

(1) Der Landtag wählt auf Vorschlag der Landesregierung den Hessischen Datenschutzbeauftragten.

(2) Der Präsident des Landtags verpflichtet den Hessischen Datenschutzbeauftragten vor dem Landtag, sein Amt gerecht zu verwalten und die Verfassung des Landes Hessen und das Grundgesetz für die Bundesrepublik Deutschland getreulich zu wahren.

(3) Der Hessische Datenschutzbeauftragte steht nach Maßgabe dieses Gesetzes in einem öffentlich-rechtlichen Amtsverhältnis. Das Amt kann auch einem Beamten im Nebenamt, einem beurlaubten Beamten oder einem Ruhestandsbeamten übertragen werden.

(4) Der Hessische Datenschutzbeauftragte wird für die Dauer der jeweiligen Wahlperiode des Landtags gewählt; nach dem Ende der Wahlperiode bleibt er bis zur Neuwahl im Amt. Die Wiederwahl ist zulässig. Vor Ablauf der Amtszeit kann er nur abberufen werden, wenn Tatsachen vorliegen, die bei einem Beamten die Entlassung aus dem Dienst rechtfertigen. Er kann jederzeit von seinem Amt zurücktreten. **Er bestellt für den Fall seiner Verhinderung oder für den Fall seines vorzeitigen Ausscheidens aus dem Amt für die Zeit bis zur Wahl seines Nachfolgers einen Beschäftigten seiner Dienststelle zum Vertreter. Als Verhinderung gilt auch,**

wenn im Einzelfall in der Person des Hessischen Datenschutzbeauftragten Gründe vorliegen, die bei einem Richter zum Ausschluß von der Mitwirkung oder zur Ablehnung wegen Besorgnis der Befangenheit führen können.

(5) Der Hessische Datenschutzbeauftragte kann an den Sitzungen des Landtags und seiner Ausschüsse nach Maßgabe der Geschäftsordnung des Landtags teilnehmen und sich zu Fragen äußern, die für den Datenschutz von Bedeutung sind.

(6) Die Vergütung des Hessischen Datenschutzbeauftragten ist durch Vertrag zu regeln.

§ 22

Unabhängigkeit

Der Hessische Datenschutzbeauftragte ist **als oberste Landesbehörde in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen.**

§ 23

Verschwiegenheitspflicht

Der Hessische Datenschutzbeauftragte ist auch nach Beendigung seines Amtsverhältnisses verpflichtet, über die ihm bei seiner amtlichen Tätigkeit bekanntgewordenen Angelegenheiten Verschwiegenheit zu wahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Der Hessische Datenschutzbeauftragte gilt als oberste Dienstbehörde im Sinne des § 96 der Strafprozeßordnung. Er entscheidet entsprechend nach den Bestimmungen über die Vorlage- und Auskunftspflichten von Behörden in den gerichtlichen

Verfahrensordnungen. Er trifft die Entscheidungen nach §§ 75 und 76 des Hessischen Beamtengesetzes für sich und die ihm zugewiesenen Bediensteten in eigener Verantwortung.

§ 24

Aufgaben

(1) Der Hessische Datenschutzbeauftragte überwacht die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz bei den datenverarbeitenden Stellen. Zu diesem Zwecke kann er Empfehlungen zur Verbesserung des Datenschutzes geben; insbesondere kann er die Landesregierung und einzelne Minister sowie die übrigen datenverarbeitenden Stellen in Fragen des Datenschutzes beraten.

Die Gerichte unterliegen der Kontrolle des Hessischen Datenschutzbeauftragten, soweit sie nicht in richterlicher Unabhängigkeit tätig werden. Der Hessische Datenschutzbeauftragte kontrolliert die Einhaltung der Datenschutzvorschriften auch bei den Stellen, die sich und soweit sie sich nach § 4 Abs. 3 Satz 1 seiner Kontrolle unterworfen haben.

(2) Der Hessische Datenschutzbeauftragte beobachtet die Auswirkungen der automatisierten Datenverarbeitung auf die Arbeitsweise und die Entscheidungsbefugnisse der datenverarbeitenden Stellen. Er hat insbesondere darauf zu achten, ob sie zu einer Verschiebung in der Gewaltenteilung zwischen den Verfassungsorganen des Landes, zwischen den Organen der kommunalen Selbstverwaltung und zwischen der staatlichen und der kommunalen Selbstverwaltung führen. Er soll Maßnahmen anregen, die ihm geeignet erscheinen, derartige Auswirkungen zu verhindern.

(3) Der Hessische Datenschutzbeauftragte arbeitet mit den Behörden und sonstigen Stellen, die für die Kontrolle der

Einhaltung der Vorschriften über den Datenschutz im Bund und in den Ländern zuständig sind, zusammen.

(4) Zum Zwecke der Zusammenarbeit kann der Hessische Datenschutzbeauftragte von den nach **den Vorschriften** des Bundesdatenschutzgesetzes in Hessen für **nicht-öffentliche Stellen** zuständigen Aufsichtsbehörden Auskünfte verlangen. Bei der Überprüfung nicht-öffentlicher Stellen kann er mit seiner Zustimmung beteiligt werden. Gibt er der zuständigen Aufsichtsbehörde Verstöße gegen Datenschutzvorschriften bei nicht-öffentlichen Stellen bekannt, unterrichtet ihn die Aufsichtsbehörde von Zeitpunkt, Umfang und Ergebnis der Überprüfung.

§ 25

Gutachten und Untersuchungen

(1) Der Landtag und die Landesregierung können den Hessischen Datenschutzbeauftragten mit der Erstattung von Gutachten und der Durchführung von Untersuchungen in Datenschutzfragen und Fragen des freien Zugangs zu Informationen betrauen.

(2) Der Landtag, der Präsident des Landtags und die in § 38 Abs. 3 genannten Vertretungsorgane können verlangen, daß der Hessische Datenschutzbeauftragte untersucht, aus welchen Gründen Auskunftersuchen nicht oder nicht ausreichend beantwortet wurden.

§ 26

Frist

Soweit der Hessische Datenschutzbeauftragte auf Grund einer Rechtsvorschrift gehört wird, teilt er unverzüglich mit, ob und innerhalb welcher Frist er eine Stellungnahme abgeben wird.

§ 27

Beanstandungen durch den Hessischen Datenschutzbeauftragten

(1) Stellt der Hessische Datenschutzbeauftragte Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Datenschutzbestimmungen oder sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so beanstandet er dies

1. bei der Landesverwaltung gegenüber der zuständigen obersten Landesbehörde,
2. bei den Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie bei Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gegenüber dem Vorstand oder dem sonst vertretungsberechtigten Organ

und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf. In den Fällen von Satz 1 Nr. 2 unterrichtet der Hessische Datenschutzbeauftragte gleichzeitig auch die zuständige Aufsichtsbehörde.

(2) Der Hessische Datenschutzbeauftragte kann von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, **insbesondere** wenn es sich um unerhebliche **oder inzwischen beseitigte** Mängel handelt.

(3) Mit der Beanstandung kann der Hessische Datenschutzbeauftragte Vorschläge zur Beseitigung der Mängel und zur sonstigen Verbesserung des Datenschutzes verbinden.

(4) Die gemäß Abs. 1 abzugebende Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die auf Grund der Beanstandung des Hessischen Datenschutzbeauftragten getroffen worden sind. Die in Abs. 1 Satz 1 Nr. 2 genannten Stellen leiten der zuständigen Aufsichtsbehörde eine Abschrift ihrer Stellungnahme an den Hessischen Datenschutzbeauftragten zu.

§ 28

Anrufung des Hessischen Datenschutzbeauftragten

(1) Jeder kann sich an den Hessischen Datenschutzbeauftragten wenden, wenn er annimmt, bei der Verarbeitung seiner personenbezogenen Daten durch datenverarbeitende Stellen, ausgenommen die Gerichte, soweit sie nicht in Verwaltungsangelegenheiten tätig werden, in seinen Rechten verletzt worden zu sein. Niemand darf dafür gemäßregelt oder benachteiligt werden, daß er sich auf Grund tatsächlicher Anhaltspunkte für einen Verstoß gegen dieses Gesetz oder andere Vorschriften über den Datenschutz an den Hessischen Datenschutzbeauftragten wendet.

(2) Beschäftigte öffentlicher Stellen können sich ohne Einhaltung des Dienstweges an den Hessischen Datenschutzbeauftragten wenden. Die dienstrechtlichen Pflichten der Beschäftigten bleiben im übrigen unberührt.

§ 29

Auskunftsrecht des Hessischen Datenschutzbeauftragten

(1) Alle datenverarbeitenden Stellen und ihre Auftragnehmer sind verpflichtet, den Hessischen Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen. Ihm ist dabei insbesondere

1. Auskunft zu seinen Fragen sowie Einsicht in alle Unterlagen zu gewähren, die in Zusammenhang mit der Verarbeitung personenbezogener Daten stehen,

2. Zutritt zu allen Diensträumen zu gewähren.

(2) Die Rechte nach Abs. 1 dürfen nur vom Hessischen Datenschutzbeauftragten persönlich ausgeübt werden, wenn die oberste Landesbehörde im Einzelfall feststellt, daß die Sicherheit des Bundes oder eines Landes dies gebietet. In diesem Fall müssen personenbezogene Daten eines Betroffenen, dem von der datenverarbeitenden Stelle Vertraulichkeit besonders zugesichert worden ist, auch ihm gegenüber nicht offenbart werden.

(3) Der Hessische Datenschutzbeauftragte ist über Verfahrensentwicklungen und Gesetzesvorhaben im Zusammenhang mit der automatisierten Verarbeitung personenbezogener Daten rechtzeitig und umfassend zu unterrichten.

§ 30

Berichtspflicht

(1) Zum 31. Dezember jeden Jahres hat der Hessische Datenschutzbeauftragte dem Landtag und der Landesregierung einen Bericht über das Ergebnis seiner Tätigkeit vorzulegen. Er gibt dabei auch einen Überblick über die technischen und organisatorischen Maßnahmen nach § 10 und regt Verbesserungen des Datenschutzes an. Zwischenberichte sind zulässig.

(2) Die Landesregierung legt ihre Stellungnahme zu dem Haupt- oder Zwischenbericht dem Landtag vor. Zusammen mit der Stellungnahme zum Hauptbericht gibt sie einen Bericht über die

Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörden.

§ 31

Personal- und Sachausstattung

(1) Dem Hessischen Datenschutzbeauftragten ist vom Präsidenten des Landtags die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen; sie ist im Einzelplan des Landtags in einem eigenen Kapitel auszuweisen.

(2) Die **Beamten** werden auf Vorschlag des Hessischen Datenschutzbeauftragten ernannt. Ihr Dienstvorgesetzter ist der Hessische Datenschutzbeauftragte, an dessen Weisungen sie ausschließlich gebunden sind. **Für sonstige Beschäftigte gelten Satz 1 und 2 entsprechend.**

DRITTER TEIL

Besonderer Datenschutz

§ 32

Datenverarbeitung für Planungszwecke

(1) Für Zwecke der öffentlichen Planung können personenbezogene Daten gesondert verarbeitet werden. Die Verarbeitung soll von der übrigen Verwaltung personell und organisatorisch getrennt erfolgen.

(2) Die zu Planungszwecken gespeicherten personenbezogenen Daten dürfen nicht für andere Verwaltungszwecke genutzt werden. Sobald es der Zweck der Planungsaufgabe erlaubt, sind die zu

diesem Zweck verarbeiteten personenbezogenen Daten so zu verändern, daß sie sich weder auf eine bestimmte Person beziehen noch eine solche erkennen lassen. Eine Übermittlung von Daten, aus denen Rückschlüsse auf Einzelpersonen gezogen werden können, ist unzulässig.

§ 33

Datenverarbeitung für wissenschaftliche Zwecke

(1) Zum Zwecke wissenschaftlicher Forschung dürfen **datenverarbeitende** Stellen personenbezogene Daten ohne Einwilligung des Betroffenen **im Rahmen** bestimmter Forschungsvorhaben **verarbeiten**, soweit dessen schutzwürdige Belange wegen der Art der Daten, ihrer Offenkundigkeit oder der Art ihrer Verwendung nicht beeinträchtigt werden. Der Einwilligung des Betroffenen bedarf es auch nicht, wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Betroffenen überwiegt und der Zweck der Forschung nicht auf andere Weise **oder nur mit unverhältnismäßigem Aufwand** erreicht werden kann. **Im Falle des Satz 2** bedarf die **Verarbeitung** durch Stellen des Landes der vorherigen Genehmigung der obersten Landesbehörde oder einer von dieser bestimmten Stelle. Die Genehmigung muß den Empfänger, die Art der zu übermittelnden personenbezogenen Daten, den Kreis der Betroffenen und das Forschungsvorhaben bezeichnen und ist dem Hessischen Datenschutzbeauftragten mitzuteilen.

(2) Sobald der Forschungszweck dies erlaubt, sind die Merkmale, mit deren Hilfe ein Personenbezug hergestellt werden kann, gesondert zu speichern; die Merkmale sind zu löschen, sobald der Forschungszweck **dies zuläßt**.

(3) Eine Verarbeitung der nach Abs. 1 übermittelten Daten zu anderen als Forschungszwecken ist unzulässig. Die nach Abs. 1 Satz 2 übermittelten Daten dürfen nur mit Einwilligung des Betroffenen weiterübermittelt werden.

(4) Soweit die Vorschriften dieses Gesetzes auf den Empfänger keine Anwendung finden, dürfen personenbezogene Daten nur übermittelt werden, wenn sich der Empfänger verpflichtet, die Vorschriften der Abs. 2 und 3 einzuhalten und sich der Kontrolle des Hessischen Datenschutzbeauftragten unterwirft.

§ 34

Datenschutz bei Dienst- und Arbeitsverhältnissen

(1) Der Dienstherr oder Arbeitgeber darf Daten seiner Beschäftigten nur verarbeiten, wenn dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung innerdienstlicher **planerischer, organisatorischer, sozialer und personeller Maßnahmen erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung es vorsieht. **Die für das Personalaktenrecht geltenden Vorschriften des Hessischen Beamtengesetzes sind, soweit tarifvertraglich nichts anderes geregelt ist, auf Angestellte und Arbeiter im öffentlichen Dienst entsprechend anzuwenden.****

(2) Abweichend von § 16 Abs. 1 ist eine Übermittlung der Daten von Beschäftigten an Personen und Stellen außerhalb des öffentlichen Bereichs nur zulässig, wenn der Empfänger ein rechtliches Interesse darlegt, der Dienstverkehr es erfordert oder der Betroffene eingewilligt hat. Die Übermittlung an einen künftigen Dienstherrn oder Arbeitgeber ist nur mit Einwilligung des Betroffenen zulässig.

(3) Das Auskunftsrecht nach § 18 Abs. 3 umfaßt auch die Art der automatisierten Auswertung der Daten des Beschäftigten. § 18 Abs. 6 findet keine Anwendung.

(4) Im Falle des § 19 Abs. 3 Satz 1 sind die Daten der Beschäftigten zu löschen. Daten, die vor der Eingehung eines Dienst- oder Arbeitsverhältnisses erhoben wurden, sind unverzüglich zu löschen, sobald feststeht, daß ein Dienst- oder Arbeitsverhältnis nicht zustande kommt. Dies gilt nicht, wenn Grund zu der Annahme besteht, daß durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden.

(5) Vor Einführung, Anwendung, Änderung oder Erweiterung eines automatisierten Verfahrens zur Verarbeitung von Daten der Beschäftigten hat die Dienststelle das Verzeichnisse (§ 6) der Personalvertretung im Rahmen des personalvertretungsrechtlichen Beteiligungsverfahrens mit dem Hinweis vorzulegen, daß sie eine Stellungnahme des Hessischen Datenschutzbeauftragten fordern kann. Macht die Personalvertretung von dieser Möglichkeit Gebrauch, beginnt die von ihr einzuhaltende Frist erst mit der Vorlage der von der Dienststellenleitung einzuholenden Stellungnahme.

(6) Daten der Beschäftigten, die im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen nach § 10 Abs. 2 gespeichert werden, dürfen nicht zu Zwecken der Verhaltens- oder Leistungskontrolle ausgewertet werden.

§ 35

Übermittlung an öffentlich-rechtliche Religionsgesellschaften

Die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaften ist in entsprechender

Anwendung der Vorschriften über die Übermittlung an öffentliche Stellen nur zulässig, sofern sichergestellt ist, daß bei dem Empfänger gleichwertige Datenschutzmaßnahmen getroffen werden.

§ 36

Fernmessen und Fernwirken

Wer eine Datenverarbeitungs- oder Übertragungseinrichtung zu dem Zweck nutzt, bei einem Betroffenen, insbesondere in der Wohnung oder in den Geschäftsräumen ferngesteuert Messungen vorzunehmen oder andere Wirkungen auszulösen, bedarf dessen Einwilligung.

§ 37

Datenverarbeitung des Hessischen Rundfunks zu journalistisch-redaktionellen Zwecken

(1) Führt die journalistisch-redaktionelle Verarbeitung personenbezogener Daten zur Veröffentlichung von Gegendarstellungen der Betroffenen, so sind diese Gegendarstellungen zu den gespeicherten Daten zu nehmen und für dieselbe Zeitdauer aufzubewahren wie die Daten selbst.

(2) Der Rundfunkrat bestellt einen Beauftragten für den Datenschutz, der die Ausführung von Abs. 1 und § 10 sowie anderer Vorschriften über den Datenschutz im journalistisch-redaktionellen Bereich frei von Weisungen überwacht. An ihn kann sich jedermann wenden, wenn er annimmt, bei der Verarbeitung personenbezogener Daten zu journalistisch-redaktionellen Zwecken in seinen Rechten verletzt worden zu sein. Beanstandungen richtet der Beauftragte für den Datenschutz an den Intendanten und

unterrichtet gleichzeitig den Rundfunkrat. Die Dienstaufsicht obliegt dem Verwaltungsrat.

(3) Dem nach Abs. 2 zu bestellenden Beauftragten für den Datenschutz können auch die Aufgaben nach § 5 zugewiesen werden.

VIERTER TEIL

Rechte des Landtags und der kommunalen Vertretungsorgane

§ 38

Auskunftsrecht des Landtags und der kommunalen Vertretungsorgane

(1) Die Hessische Zentrale für Datenverarbeitung, die Kommunalen Gebietsrechenzentren und die Landesbehörden, die Datenverarbeitungsanlagen betreiben, sind verpflichtet, dem Landtag, dem Präsidenten des Landtags und den Fraktionen des Landtags die von diesen im Rahmen ihrer Zuständigkeit verlangten Auskünfte auf Grund der gespeicherten Daten zu geben, soweit Programme zur Auswertung vorhanden sind. Die Auskünfte dürfen keine personenbezogenen Daten enthalten. Den Auskünften darf ein gesetzliches Verbot oder ein öffentliches Interesse nicht entgegenstehen; dem Auskunftsrecht des Landtags steht ein öffentliches Interesse in der Regel nicht entgegen. Der Landtag hat Zugriff zu den Daten, soweit durch technische Maßnahmen sichergestellt ist, daß die Grenzen der Sätze 1 bis 3 eingehalten werden.

(2) Der Landtag kann von der Landesregierung Auskünfte über die bestehenden **Verfahren** verlangen, die für Auskünfte oder den

Zugriff nach Abs. 1 geeignet sind. Das Auskunftsverlangen kann sich erstrecken auf

1. den Namen des **Verfahrens** mit kurzer Funktionsbeschreibung,
2. die vorhandenen Verfahren,
3. den Aufbau der Datensätze mit Angaben über den Inhalt und die Ordnungskriterien,
4. die vorhandenen Auswertungsprogramme,
5. die zuständige Behörde

(3) Das Auskunftsrecht nach Abs. 1 steht im Rahmen ihrer Zuständigkeiten den Gemeindevertretungen und den Kreistagen sowie deren Fraktionen und den entsprechenden Organen anderer in § 3 Abs. 1 genannten Körperschaften und Anstalten gegenüber der Hessischen Zentrale für Datenverarbeitung, dem zuständigen Kommunalen Gebietsrechenzentrum und den Behörden der Gemeinden und Gemeindeverbände zu, die Datenverarbeitungsanlagen betreiben. Der Antrag der Fraktionen ist in den Gemeinden über den Gemeindevorstand, in den Kreisen über den Kreisausschuß zu leiten.

§ 39

Verarbeitung personenbezogener Daten durch den Landtag und die kommunalen Vertretungsorgane

(1) Mit Ausnahme der §§ 1 **Abs. 1** Nr. 2, 25 und 38 gelten die Vorschriften dieses Gesetzes für den Landtag nur, soweit er in Verwaltungsangelegenheiten tätig wird, insbesondere wenn es sich um die wirtschaftlichen Angelegenheiten des Landtags, die Personalverwaltung oder die Ausführung von gesetzlichen

Vorschriften, deren Vollzug dem Präsidenten des Landtags zugewiesen ist, handelt. Im übrigen gibt sich der Landtag unter Berücksichtigung seiner verfassungsrechtlichen Stellung eine Datenschutzordnung. Sie findet auf die für die Fraktionen und Abgeordneten tätigen Personen entsprechende Anwendung.

(2) Die Landesregierung darf personenbezogene Daten, die für andere Zwecke erhoben worden sind, zur Beantwortung parlamentarischer Anfragen sowie zur Vorlage von Unterlagen und Berichten im Rahmen der Geschäftsordnung des Hessischen Landtags in dem dafür erforderlichen Umfang verwenden. Dies gilt nicht, wenn die Übermittlung der Daten wegen ihres streng persönlichen Charakters für die Betroffenen unzumutbar ist. Besondere gesetzliche Übermittlungsverbote bleiben unberührt.

(3) Von der Landesregierung übermittelte personenbezogene Daten dürfen nicht in Landtagsdrucksachen aufgenommen oder in sonstiger Weise allgemein zugänglich gemacht werden. Dies gilt nicht, wenn keine Anhaltspunkte dafür bestehen, daß schutzwürdige Belange der Betroffenen beeinträchtigt werden.

(4) Abs. 2 gilt entsprechend für die Verwaltungsbehörden der Gemeinden und Gemeindeverbände im Rahmen ihrer jeweiligen Auskunftspflichten nach der Hessischen Gemeindeordnung und der Hessischen Landkreisordnung.

FÜNFTER TEIL

Schlußvorschriften

§ 40

Straftaten

(1) Wer gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, personenbezogene Daten entgegen den Vorschriften dieses Gesetzes

1. erhebt, speichert, zweckwidrig verwendet, verändert, übermittelt, zum Abruf bereithält oder löscht,
2. abrufen, einsieht, sich verschafft oder durch Vortäuschung falscher Tatsachen ihre Übermittlung an sich oder einen Dritten veranlaßt,

wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Abs. 1 findet nur Anwendung, soweit die Tat nicht in anderen Vorschriften mit Strafe bedroht ist.

§ 41

Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer entgegen § 16 Abs. 2 oder § 33 Abs. 3 Daten nicht nur für den Zweck verwendet, zu dessen Erfüllung sie ihm übermittelt wurden.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Deutsche Mark geahndet werden.

§ 42

Übergangsvorschrift

Auf Akten, die bei Inkrafttreten des Gesetzes vorhanden waren, ist § 19 Abs. 1, 4 und 6 nur anwendbar, wenn die speichernde Stelle

die Voraussetzungen für die Berichtigung, Löschung oder Sperrung bei der Erfüllung ihrer laufenden Aufgaben feststellt.

§ 43

Aufhebung bisherigen Rechts

Das Hessische Datenschutzgesetz vom 31. Januar 1978 (GVBl. I S. 96), geändert durch Gesetz vom 14. Oktober 1980 (GVBl. I S. 377), sowie die Hessische Verordnung über die Veröffentlichung der Angaben über gespeicherte personenbezogene Daten vom 1. November 1978 (GVBl. I S. 553) und die Hessische Verordnung über die vom Hessischen Datenschutzbeauftragten zu führenden Dateienregister vom 8. Dezember 1978 (GVBl. I S. 682) werden aufgehoben.

§ 44³

Inkrafttreten

Dieses Gesetz tritt am 1. Januar 1987 in Kraft.

³ § 44 betrifft das Inkrafttreten des Gesetzes vom 11. November 1986. Das Dritte Gesetz zur Änderung des Hessischen Datenschutzgesetzes ist - mit Ausnahme des § 6 - am Tage nach seiner Verkündung in Kraft getreten. § 6 tritt am 1. Juni 1999 in Kraft.

Vorstehend sind die Änderungen des Artikels 1 des Dritten Gesetzes zur Änderung des Hessischen Datenschutzgesetzes eingearbeitet. Die Änderungen anderer Gesetze (Hessisches Krankenhausgesetz, Hessisches Schulgesetz, Hessisches Privatrundfunkgesetz, Gesetz über das Landesamt für Verfassungsschutz) durch Artikel 3 des Gesetzes sind hier nicht enthalten.

**Orientierungshilfe zu Datenschutzfragen des
Anschlusses von Netzen der öffentlichen Verwaltung
an das Internet (Überarbeitete Fassung vom September
1998)**

**erstellt vom Arbeitskreis Technik der Konferenz der
Datenschutzbeauftragten des Bundes und der Länder**

Epidemiologie und Datenschutz

Deutsche Arbeitsgemeinschaft für Epidemiologie (DAE) ¹⁾ und Arbeitskreis Wissenschaft der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ²⁾

Einleitung

Die epidemiologische Forschung zielt nicht auf personenbezogene, sondern auf bevölkerungsbezogene wissenschaftliche Aussagen. Hierbei stützt sie sich jedoch in der Regel auf personenbezogene Daten zum Gesundheitszustand der Probanden, soziodemographische Angaben, Informationen über Risikofaktoren und oftmals medizinische Untersuchungsbefunde und Ergebnisse aus der Analyse biologischer Materialien. Die individuellen Untersuchungsergebnisse werden üblicherweise den Probanden mitgeteilt. Zur Durchführung der Forschungsprojekte werden vielfach Namen und Anschriften zur Kontaktaufnahme benötigt. Darüber hinaus muß eine korrekte Zuordnung von Follow-up-Ergebnissen sowie die Zusammenführung von Daten aus verschiedenen Quellen sichergestellt werden.

Epidemiologie und Datenschutz stehen traditionell im Spannungsfeld des Schutzes der Persönlichkeitsrechte der von der Datenverarbeitung Betroffenen und dem wissenschaftlichen Anliegen, durch das Auswerten von Gesundheitsdaten zu wichtigen und auf andere Weise nicht erreichbaren Kenntnissen zu gelangen.

-
- 1) vom Vorstand der Deutschen Arbeitsgemeinschaft für Epidemiologie (DAE) in Abstimmung mit der Deutschen Gesellschaft für medizinische Information, Biometrie und Epidemiologie (GMDS), der Deutschen Gesellschaft für Sozialmedizin und Prävention (DGSMP) und der Deutschen Region der Biometrischen Gesellschaft zustimmend zur Kenntnis genommen am 28.05.1998
 - 2) von der Konferenz der Datenschutzbeauftragten zustimmend zur Kenntnis genommen am 08.06.1998

Im Anschluß an eine Diskussion der datenschutzrechtlichen Fragen zwischen der Deutschen Forschungsgemeinschaft und dem Arbeitskreis Wissenschaft der Konferenz der Datenschutzbeauftragten des Bundes und der Länder haben Epidemiologen und Datenschützer versucht, typische Problemfelder zu identifizieren und zu gemeinsamen Lösungsvorschlägen zu kommen. Die folgenden Vorschläge sollen den mit Datenschutzfragen bei epidemiologischen Studien befaßten Wissenschaftlern, Datenschützern, Ethikkommissionen, Behörden und Forschungsförderern zur Information und Orientierung dienen, um Probleme zu vermeiden, die durch fehlende Kenntnis der datenschutzrechtlichen Vorschriften, ungeeignet formulierte Einverständniserklärungen oder durch eine falsche oder übervorsichtige Interpretation der Rechtsvorschriften zur Datenübermittlung für Forschungszwecke etc. bedingt sind.

1.

Rechtliche Rahmenbedingungen für die Forschung mit personenbezogenen Daten

1.1

Forschung mit anonymisierten Daten

Die datenschutzrechtlichen Bestimmungen finden nur Anwendung, wenn für ein Forschungsprojekt personenbezogene Daten benötigt werden. Forschung mit anonymisierten Daten ist jederzeit ohne datenschutzrechtliche Vorgaben möglich. Ob es sich im konkreten Fall um personenbezogene oder um anonymisierte Daten handelt, bedarf allerdings sorgfältiger Prüfung. § 3 Abs. 7 BDSG enthält eine gesetzliche Definition des Anonymisierens. Dieser Definition zufolge ist Anonymisieren das Verändern personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und

Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können (sog. "faktische Anonymisierung"). Anonymisierung wird in der wissenschaftlichen bzw. datenschutzrechtlichen Diskussion ganz überwiegend im Sinne einer faktischen Anonymisierung verstanden. Einzelangaben sind z.B. dann keine anonymisierten Daten, wenn beim Forschungsinstitut bzw. beim Forscher lediglich eine organisatorische Trennung der Hilfsmerkmale von den übrigen Daten vorgenommen wurde oder wenn lediglich Name und Adresse der Betroffenen weggelassen wurden und die Betroffenen anhand der weiteren Angaben noch identifizierbar sind. Auch aggregierte Daten können nicht immer als anonymisiert qualifiziert werden. Im Einzelfall muß eine Risikoanalyse unter Berücksichtigung insbesondere des eventuellen Wertes der in Frage stehenden Daten für potentielle Interessenten sowie der dem Empfänger oder den potentiellen Interessenten zur Verfügung stehenden Ressourcen (Zusatzwissen, technische Möglichkeiten der Datenverarbeitung etc.) durchgeführt werden.

In einigen wenigen Bundesländern wird Anonymisierung im Sinne einer absoluten Anonymisierung verstanden, d.h. Einzelangaben werden nur dann als anonym qualifiziert, wenn sie unter keinen Umständen mehr zuzuordnen sind.

1.2

Forschung mit Einwilligung der Betroffenen

Personenbezogene Daten können im Rahmen der epidemiologischen Forschung auf der Basis einer Einwilligung der Betroffenen verarbeitet werden. Nach den datenschutzrechtlichen Regelungen muß die Einwilligung der Betroffenen bestimmte inhaltliche und formale Voraussetzungen erfüllen, damit sie rechtswirksam ist. Insbesondere müssen die Betroffenen über die vorgesehene Verarbeitung ihrer Daten informiert werden (Träger

und Leiter des Forschungsprojekts, Zweck des Forschungsvorhabens, Art und Weise der Datenverarbeitung, Personenkreis, der von den personenbezogenen Daten Kenntnis erhält, Zeitpunkt der Löschung der personenbezogenen Daten etc.), damit sie die Tragweite ihrer Entscheidung erkennen können. Die Einwilligung muß in der Regel schriftlich erteilt werden, die gesetzlichen Regelungen sehen jedoch Ausnahmen vor. Ferner ist ein Hinweis erforderlich, daß die Einwilligung freiwillig ist, aus der Verweigerung der Einwilligung keine Nachteile entstehen und ein Widerruf der Einwilligung möglich ist. Einzelheiten sind den jeweils einschlägigen Regelungen zu entnehmen.

Verfügt die Forschungsstelle nicht über die Namen und Adressen der Personen, bei denen Einwilligungen eingeholt werden sollen, und kann sie sich diese Daten auf Grund der rechtlichen Regelungen (z.B. Meldegesetz) nicht beschaffen, so kann die Forschungsstelle die Betroffenen in der Weise kontaktieren, daß sie ihre Anschreiben, Merkblätter etc. in verschlossenen Umschlägen der Stelle übergibt, die über die Daten verfügt, damit letztere auf die Umschläge Namen und Adressen schreibt und die Anschreiben dann versendet. Auf diese Weise wird vermieden, daß die Daten Dritten zur Kenntnis gelangen. Dabei sollte für die Betroffenen in dem Anschreiben eindeutig erkennbar sein, daß ihre geschützten Daten von der Stelle, die über die Daten verfügt, nicht an die forschende Stelle weitergegeben wurden.

1.3

Forschung mit personenbezogenen Daten ohne Einwilligung der Betroffenen

Das Grundgesetz gewährleistet das Recht auf informationelle Selbstbestimmung als Bestandteil des allgemeinen Persönlichkeitsrechts im Sinne von Artikel 2 i.V.m. Artikel 1 Grundgesetz. Ebenso gewährleistet das Grundgesetz die Freiheit

von Wissenschaft und Forschung in Artikel 5 Grundgesetz. Diese beiden Grundrechte können bei Forschungsvorhaben, für die - zumindest vorübergehend - personenbezogene Daten benötigt werden, miteinander in Konflikt geraten. In dieser Situation ist es - wie auch bei anderen Grundrechtskonflikten - in erster Linie Aufgabe des Gesetzgebers, diese potentiellen Konflikte so zu regeln, daß beide Grundrechte möglichst weitgehend realisiert werden können. Der Gesetzgeber muß die rechtlichen Rahmenbedingungen festlegen, unter denen personenbezogene Daten zu Forschungszwecken ohne Einwilligung der Betroffenen verwendet werden dürfen. Dabei sind auch die besonderen Schweigepflichten wie z.B. die ärztliche Schweigepflicht i.S.d. Berufsordnung und des § 203 StGB zu beachten. Nach der Rechtsprechung des Bundesverfassungsgerichts ist eine Einschränkung des Rechts auf informationelle Selbstbestimmung nur im überwiegenden Allgemeininteresse und unter Beachtung des Grundsatzes der Verhältnismäßigkeit zulässig. Die Verarbeitung personenbezogener Daten muß für den angestrebten Zweck geeignet und notwendig sein und es darf keine Alternative geben, die die Betroffenen weniger belastet (z.B. Anonymisierungs- bzw. Pseudonymisierungsverfahren, Einwilligung der Betroffenen).

Gesetzliche Forschungsregelungen, die das Recht auf informationelle Selbstbestimmung und die Freiheit von Wissenschaft und Forschung in diesem Sinne zuordnen, sind z.B. in Landeskrankenhausgesetzen, Meldegesetzen, im Sozialgesetzbuch X, Krebsregistergesetzen, im Bundesdatenschutzgesetz und in Landesdatenschutzgesetzen enthalten. Entgegen dem allgemeinen Grundsatz der Zweckbindung personenbezogener Daten können nach diesen Regelungen unter bestimmten Voraussetzungen Daten, die zu einem anderen Zweck als wissenschaftlicher Forschung erhoben wurden, zu Forschungszwecken weiterverwendet werden.

2.

Forschungsansätze in der Epidemiologie, Datenbedarf und Rechtsgrundlagen der Datenverarbeitung

Die Epidemiologie ist die Lehre von der Verteilung der Krankheiten und ihrer Risikofaktoren in der Bevölkerung. Aussagen epidemiologischer Forschung betreffen nicht das Individuum, sondern eine Bevölkerungsgruppe. Daher werden personenbezogene Daten nur für die Datenerfassung und ggf. spätere Kontaktaufnahmen sowie für die Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen benötigt.

Als wichtigste epidemiologische Studientypen sind beispielhaft anzusehen:

- Bei Querschnittserhebungen wird typischerweise einmalig eine Befragung und/oder Untersuchung von Probanden durchgeführt. Diese werden persönlich um ihr Einverständnis gebeten. Die epidemiologische Fragestellung umfaßt z.B. die Charakterisierung von Erkrankungshäufigkeiten in der untersuchten Bevölkerungsgruppe oder den Zusammenhang zwischen dem Auftreten von Erkrankungen und Risikofaktoren. Aus datenschutzrechtlicher Sicht sind hier – wie auch bei den anderen Studienformen – die formalen und inhaltlichen Voraussetzungen der Einwilligungserklärung der Betroffenen zu beachten, ferner die jeweils einschlägigen Vorschriften zur Verarbeitung und Nutzung personenbezogener Daten durch die Forschungseinrichtungen (z.B. § 40 BDSG).
- Als zweiter Studientyp ist die Kohortenstudie zu nennen. Hierbei werden - z.B. ausgehend von einer Querschnittstudie - wiederholt Untersuchungen an denselben Probanden durchgeführt. Für diese Follow-up-Untersuchungen ist es erforderlich, personenbezogene Daten zu speichern,

Anschriften zu aktualisieren etc. Diese Datenverarbeitung muß von den Einwilligungserklärungen umfaßt sein. Als epidemiologische Fragestellungen werden das Auftreten neuer Erkrankungen oder bestimmter Todesursachen im Zusammenhang mit bestimmten Risikofaktoren bearbeitet. Im letzteren Fall ist es zusätzlich erforderlich, über Einwohnermeldeämter und Gesundheitsämter den Vitalstatus sowie im Falle des Versterbens die Todesursache zu erheben. Als Rechtsgrundlage hierfür kommen die gesetzlichen Forschungsregelungen oder die Einwilligung der Betroffenen in Betracht.

- Einen Spezialfall von Kohortenstudien stellen retrospektive Kohortenstudien (mit zurückverlagertem Beginn) dar, die insbesondere im Bereich der Berufsepidemiologie häufig eingesetzt werden. Bei solchen Studien wird typischerweise aufgrund von betrieblichen Unterlagen die Exposition gegenüber bestimmten Arbeitsstoffen am Arbeitsplatz erhoben. Häufig interessiert das Auftreten von Krebserkrankungen oder das Versterben an bestimmten Todesursachen im Zusammenhang mit den beruflichen Expositionen. Hierbei ist es nicht ungewöhnlich, daß die Personen selbst nicht befragt werden, sondern daß ihre Exposition aus den betrieblichen Unterlagen bestimmt wird und die Krebserkrankung oder Todesursache durch Auswertung eines Krebsregisters oder über Einwohnermeldeamt und Gesundheitsamt in Erfahrung gebracht wird. Als Rechtsgrundlage für die Verarbeitung personenbezogener Daten kommen die gesetzlichen Forschungsregelungen oder die Einwilligung der Betroffenen in Betracht.

- Als weiterer epidemiologischer Studientyp ist die Fall-Kontroll-Studie zu nennen. Hierbei werden als Fälle Personen mit bestimmten Erkrankungen bezeichnet, die Kontrollpersonen gegenübergestellt werden. Fälle und

Kontrollen werden im Hinblick auf in der Vergangenheit liegende Risikofaktoren befragt. Häufig ist es sinnvoll, Fälle aus Registern, z.B. Krebsregistern, einzubeziehen. Als Rechtsgrundlage kommen die gesetzlichen Forschungsregelungen, z.B. in Krebsregistergesetzen, oder die Einwilligung der Betroffenen in Betracht.

3.

Typische Problemfelder

3.1

Zweckbindung von personenbezogenen Daten

Problem:

Personenbezogene Daten werden auf der Grundlage einer Einwilligung der Betroffenen oder einer gesetzlichen Forschungsregelung zu einem bestimmten Zweck, d.h. für eine konkrete epidemiologische Studie, erhoben. Aus wissenschaftlicher Sicht kann es allerdings später wichtig werden, diese Daten für die Bearbeitung neuer Fragestellungen zu nutzen, die zum Zeitpunkt der Einwilligungserklärung der Betroffenen bzw. der Übermittlungen der Daten noch nicht bekannt waren und daher in die Angaben zum Zweck der Verwendung der Daten nicht einbezogen wurden. Eine erneute Kontaktierung der Probanden ist häufig nicht möglich oder wäre mit zusätzlichem hohem Aufwand und Kosten verbunden und könnte wegen Umzug, Tod, Desinteresse etc. der Betroffenen auch zu Problemen im Hinblick auf die Repräsentativität der Daten führen.

Lösungsansätze:

- Soweit es sich um anonymisierte Daten handelt, unterliegt eine Zweckänderung der Daten keinen rechtlichen Beschränkungen. Die datenschutzrechtlichen Regelungen sind nicht

anzuwenden. Dies gilt entsprechend für die Verwendung biologischer Materialien.

- Es besteht die Möglichkeit, Einwilligungserklärungen so zu formulieren, daß eine eventuelle inhaltliche Änderung bzw. Ausweitung der Fragestellungen der Studie mit umfaßt ist. Grundsätzlich muß eine Einwilligungserklärung hinreichend bestimmt sein. Die Anforderungen an die Vollständigkeit und Präzision der Einwilligungserklärungen können jedoch je nach der konkreten Verarbeitungssituation variieren. Bei der Verarbeitung personenbezogener Daten für eine wissenschaftliche Studie ist eine weitere Formulierung des Zwecks vertretbar und angemessen. Es ist die Entscheidung der Betroffenen, inwieweit sie auch eine Einwilligungserklärung mit einer weiteren Formulierung des Zwecks der Studie unterschreiben, d.h. es handelt sich um eine Frage der Akzeptanz. Die Einwilligungserklärung kann auch verschiedene Varianten der Verwendung der Daten enthalten, über die die Betroffenen entscheiden.
- Bei einer Übermittlung personenbezogener Daten auf der Grundlage einer gesetzlichen Forschungsregelung ist es vertretbar und angemessen, den Zweck der Übermittlung der Daten (d.h. die Darstellung des Forschungsvorhabens) so zu formulieren, daß eventuelle inhaltliche Änderungen bzw. Ausweitungen der Fragestellungen der Studie mit umfaßt sind.
- In Betracht kommt auch eine Anwendung der datenschutzrechtlichen Regelungen über die Zweckänderung personenbezogener Daten. Die rechtlichen Voraussetzungen für eine Zweckänderung sind im Einzelfall zu prüfen.
- Verfahrensrechtliche Lösungen wie z.B. Einschaltungen von Ethikkommissionen, Datenschutzbeauftragten etc. kommen im Regelfall nur dann in Betracht, wenn Rechtsvorschriften

vorhanden sind, die grundsätzlich eine Zweckänderung der Daten unter bestimmten Voraussetzungen zulassen, denn weder Ethikkommissionen noch Datenschutzbeauftragte können ihre Entscheidung an die Stelle der Entscheidung der Betroffenen setzen.

3.2

Löschung der Daten nach Beendigung des Forschungsvorhabens

Problem:

Es ist offen, in welchem Umfang die Daten nach Beendigung des Forschungsvorhabens gelöscht werden müssen.

Lösungsansätze:

- Soweit die Daten anonymisiert sind, sind die datenschutzrechtlichen Regelungen nicht anzuwenden und die weitere Verarbeitung der Daten unterliegt keinen rechtlichen Beschränkungen.
- Werden personenbezogene Daten verarbeitet, sollte der Zeitpunkt der Löschung der personenbezogenen Daten in dem Text der Einwilligungserklärung bzw. dem Antrag auf Übermittlung der Daten konkret benannt werden. Ist im Einzelfall eine Speicherung anonymisierter Daten für die wissenschaftliche Nachprüfbarkeit der Forschungsergebnisse nach ihrer Publikation nicht ausreichend, so kann eine Speicherung der personenbezogenen Daten für einen bestimmten Zeitraum nach der Publikation der Forschungsergebnisse zur wissenschaftlichen Nachprüfbarkeit der Forschungsergebnisse zulässig sein. Der Zeitpunkt für die Löschung der personenbezogenen Daten sollte in der Einwilligungserklärung bzw. in dem Antrag auf Übermittlung der Daten möglichst konkret benannt werden.

3.3

Weitergabe anonymisierter Daten

Problem:

In einem Forschungsvorhaben erweist es sich als sinnvoll, anonymisierte Daten aus mehreren Studien zu poolen, d.h. zusammenzuführen und gemeinsam statistisch auszuwerten, weil sich für viele Fragestellungen nur dadurch ausreichend große Fallzahlen erreichen lassen. Auch eine Weitergabe von anonymisierten Daten in Form von Public Use Files kann sinnvoll sein, um die Daten anderen Wissenschaftlern für ihre Forschung zugänglich zu machen.

Lösungsansätze:

- Grundsätzlich können anonymisierte Daten ohne rechtliche Beschränkungen weitergegeben werden. Es muß allerdings im Einzelfall geprüft werden, ob es sich tatsächlich um anonymisierte Daten handelt und ob die Daten auch nach der Zusammenführung mit den Daten aus den anderen Studien noch als anonymisiert qualifiziert werden können. Eine Zusammenführung anonymisierter Daten aus mehreren Studien führt häufig dazu, daß eine Deanonymisierung der Daten noch schwieriger wird. Im Einzelfall kann es jedoch durchaus auch die Konstellation geben, daß anonymisierte Daten durch ihre Zusammenführung mit Daten aus anderen Studien leichter deanonymisiert werden können und dann u.U. als personenbezogen qualifiziert werden müssen. In diesem Fall sind die datenschutzrechtlichen Regelungen zu beachten.
- Eine Übermittlung personenbezogener Daten ist nicht in jedem Fall ausgeschlossen. Es gilt das oben unter 3.1 Gesagte entsprechend.

3.4

Optimale Gestaltung der Einverständniserklärung bzw. des Antrags auf Übermittlung der Daten

Problem:

Einerseits sollten in der Einverständniserklärung bzw. in dem Antrag auf Übermittlung der Daten möglichst präzise die zu untersuchende Fragestellung, die Vorgehensweise und die an der Studie beteiligten Institutionen angegeben werden. Andererseits kann es sich im Laufe einer Studie ergeben, daß Kooperationspartner wechseln und sich Fragestellungen erweitern bzw. neue Fragestellungen auftauchen. Wie kann dies in der Einverständniserklärung bzw. in dem Antrag optimal berücksichtigt werden?

Lösungsansätze:

- Die Formulierung des Zwecks der epidemiologischen Studie kann so erfolgen, daß eine evtl. inhaltliche Änderung bzw. Ausweitung der Fragestellungen der Studie mit umfaßt ist (vgl. oben 3.1).

- Die datenverarbeitende Stelle - im Regelfall die Institution (Klinikum, Institut etc.) - muß in der Einwilligungserklärung bzw. in dem Antrag auf Übermittlung personenbezogener Daten konkret und verbindlich benannt werden. Aus datenschutzrechtlicher Sicht ist es von zentraler Bedeutung, daß die Verantwortlichkeit für die personenbezogenen Daten dauerhaft klar geregelt ist und der Bürger eindeutig darüber informiert ist, an wen er sich wo bei Auskunftersuchen, Widerruf seiner Einwilligung etc. wenden kann. Die Namen der Kooperationspartner müssen nur dann konkret aufgeführt werden, wenn sie mit einer eigenständigen Auswertung der personenbezogenen Daten befaßt sind.

- Im Einzelfall ist es auch möglich, eine Klausel dahingehend aufzunehmen, daß Abweichungen von der angegebenen Vorgehensweise und Erweiterungen der Fragestellungen nur nach Rücksprache mit dem zuständigen Datenschutzbeauftragten bzw. der Ethikkommission erfolgen.

3.5

Verknüpfung personenbezogener Datensätze (record linkage), z.B. bei Kohortenstudien

Problem:

Es soll eine Studie durchgeführt werden, bei der ein Abgleich verschiedener Datenbestände vorgenommen wird, die Betroffenen jedoch zu keinem Zeitpunkt direkt kontaktiert bzw. um Einwilligung gebeten werden. Ein Beispiel hierfür ist eine Studie, bei welcher die Expositionsbedingungen am Arbeitsplatz aus betrieblichen Unterlagen der dort tätigen Arbeitnehmer zusammengestellt werden. Die Erhebung der aufgetretenen Erkrankungen erfolgt über vorhandene Krankheitsregister (z.B. Krebsregister) oder über Einwohnermeldeämter und Gesundheitsämter zur Erhebung des Vitalstatus und der Todesursache.

Lösungsansätze:

- In einzelnen gesetzlichen Regelungen wie z.B. Krebsregistergesetzen ist ein Abgleich verschiedener Datenbestände vorgesehen. Im übrigen sehen die bundes- bzw. landesrechtlichen Regelungen - mit Unterschieden im einzelnen - grundsätzlich die Möglichkeit von Datenübermittlungen durch Betriebe, Einwohnermeldeämter, Gesundheitsämter, Krebsregister etc. vor (vgl. z.B. § 28 Abs. 2 Nr. 2 BDSG, Meldegesetze, Gesetze über den öffentlichen Gesundheitsdienst, Krebsregistergesetze, Forschungsregelungen im Bundesdatenschutzgesetz und in den

Landesdatenschutzgesetzen). Die rechtlichen Voraussetzungen dieser Übermittlungsbestimmungen müssen im Einzelfall geprüft werden.

Vor der Durchführung einer Studie sollte der Einsatz eines Treuhänders, d.h. eines vertrauenswürdigen Dritten, geprüft werden, der insbesondere personenbezogene Daten aus verschiedenen Quellen zuordnet, speichert und anonymisiert an die Forschungsinstitution übermittelt. Die Übermittlung personenbezogener Daten an einen Treuhänder bedarf ebenso wie die Übermittlung personenbezogener Daten an die Forschungsinstitution selbst einer Rechtsgrundlage. Der Einsatz eines Treuhänders kann jedoch im Einzelfall den Eingriff in das Recht der Betroffenen auf informationelle Selbstbestimmung minimieren, indem der Kreis derjenigen Personen, die personenbezogene Daten zur Kenntnis erhalten, reduziert wird und die Datensicherheit umfassender gewährleistet wird. Diese Aspekte haben Relevanz für die in vielen Forschungsregelungen vorgesehene Abwägung zwischen den schutzwürdigen Belangen der Betroffenen und dem öffentlichen Interesse an der Durchführung des Forschungsvorhabens.

3.6

Nutzung der amtlichen Statistik

Problem:

Häufig werden von den statistischen Ämtern des Bundes und der Länder in der Praxis nur Daten übermittelt, bei denen eine Mindestzahl auftretender Konstellationen pro Zelle erfüllt ist. Hierdurch werden bestimmte Aussagen unmöglich gemacht, z.B. die Unterteilung einer Untersuchungsgruppe nach Altersklassen oder nach genaueren diagnostischen Einheiten wie Todesursachen.

Lösungsansätze:

Die statistischen Ämter des Bundes und der Länder dürfen faktisch anonymisierte Einzelangaben für wissenschaftliche Vorhaben an Hochschulen und andere Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung übermitteln, wenn die Empfänger Amtsträger, für den öffentlichen Dienst Verpflichtete oder nach § 16 Abs. 7 Bundesstatistikgesetz Verpflichtete sind (§ 16 Abs. 6 BStatG). Die Daten sind zu löschen, sobald das Vorhaben durchgeführt ist, eine verbindliche Löschungsfrist besteht nicht (§ 16 Abs. 8 BStatG).

Es besteht die Möglichkeit, aus bereits vorliegenden Individualdaten faktisch anonymisierte Einzelangaben zu bestellen. Von diesem Weg wird jedoch häufig aus Kostengründen Abstand genommen. Für einige Bereiche sind faktisch anonyme Daten auf Vorrat erstellt worden, z.B. aus dem Mikrozensus 1995 und der Einkommens- und Verbrauchsstichprobe 1993. Einzelangaben aus solchen Beständen können gegen geringe Gebühr bezogen werden, die breite Anwendung dieser Verfahren wird aber durch Geldmangel behindert.

Leichter verfügbar sind statistische Tabellen, die i.a. dadurch anonymisiert sind, daß Felder mit geringen Belegungen so zusammengefaßt wurden, daß Zahlen kleiner als 3 nicht mehr auftreten. Dies ist für Forschungszwecke oft hinderlich. Soweit jedoch die Angaben aus Feldern mit zu geringer Belegung nicht mehr erkennen lassen, als nach § 16 Abs. 6 BStG übermittelt werden darf, und auch die weiteren Bedingungen dieser Vorschrift erfüllt werden, bestehen keine datenschutzrechtlichen Bedenken gegen die Übermittlung auch solcher Tabellen mit faktisch anonymisierten Einzelangaben.

3.7

Aufbewahrung von Daten der amtlichen Statistik

Problem:

Die Löschung älterer Datenbestände kann der epidemiologischen Forschung unwiederbringlich Grundlagen entziehen.

Lösungsansätze:

Abgesehen von den Hilfsmerkmalen (insbesondere Namen und Anschriften) gibt es i.a. keine gesetzlichen Lösungsfristen für statistische Einzelangaben. Die Lösungspraxis richtet sich nach der Einschätzung des zu erwartenden Nutzens aus der weiteren Aufbewahrung im Verhältnis zu deren Kosten.

Datenschutzrechtlich zulässig wäre eine weitere Speicherung statistischer Einzelangaben auch für zukünftig erwartete, aber noch nicht im einzelnen bekannte Zwecke. Vor Löschung der Daten sind diese nach den jeweils geltenden archivrechtlichen Bestimmungen den zuständigen Archiven anzubieten. Zur Dauer der Speicherung der Daten bei den statistischen Ämtern bzw. bei den Archiven sollte aus dem Wissenschaftsbereich der Bedarf dargelegt werden. Die Aufbewahrung der Totenscheine (im Original) richtet sich nach dem jeweiligen Landesrecht.

3.8**Nutzung von Krebsregistern für Fall-Kontroll-Studien****Problem:**

Bei Fall-Kontroll-Studien wird häufig ein (möglichst repräsentativer) Zugang zu bestimmten Erkrankungsgruppen benötigt. Dieser kann unter hohen Kosten auf der Grundlage von Einwilligungen der Betroffenen oder gesetzlichen Forschungsregelungen über Krankenhäuser erfolgen, in denen diese Patienten behandelt werden. Ein effektiverer und vollständigerer Zugang ist aber derjenige über Krankheitsregister (z.B. Krebsregister). Der Zugang über das Register dient dabei nur der Auffindung des Patienten und der Kontaktaufnahme mit ihm,

alles weitere kann durch die Einverständniserklärung der beteiligten Personen abgedeckt werden. Diesen Patienten werden dann Kontrollpersonen aus der Bevölkerung gegenübergestellt, die auf anderem Wege kontaktiert und in die Studie einbezogen werden.

Lösungsansätze:

- Gemäß § 8 des Krebsregistergesetzes des Bundes (KRG) können für Maßnahmen des Gesundheitsschutzes und bei wichtigen und auf andere Weise nicht durchzuführenden, im öffentlichen Interesse stehenden Forschungsaufgaben die zuständigen Behörden der Vertrauensstelle des Krebsregisters die Abgleichung Personen identifizierender Daten mit Daten des Krebsregisters und die Entschlüsselung der erforderlichen verschlüsselten Identitätsdaten und deren Übermittlung im erforderlichen Umfang genehmigen.

Vor der Übermittlung personenbezogener Daten hat die Vertrauensstelle über den meldenden behandelnden Arzt oder Zahnarzt die schriftliche Einwilligung des Patienten einzuholen. Ist der Patient verstorben, hat die Vertrauensstelle vor der Datenübermittlung die schriftliche Einwilligung des nächsten Angehörigen einzuholen, soweit dies ohne unverhältnismäßigen Aufwand möglich ist.

- Die Länder können in ihren Gesetzen zur Ausführung des Krebsregistergesetzes abweichende Regelungen treffen (§ 13 Abs. 5 Nr. 2 KRG). Einige Länder haben vom Krebsregistergesetz des Bundes abweichende datenschutzrechtliche Modelle (z.B. keine Aufgliederung des Registers in Vertrauensstelle und Registerstelle) gewählt. Im Einzelfall sind die einschlägigen Übermittlungsbestimmungen zu prüfen und zu beachten.

3.9

Datenschutzfragen bei bundesweiten Studien

Problem:

Bei Studien, die in mehreren Bundesländern stattfinden, sind häufig die unterschiedlichen datenschutzrechtlichen Regelungen der Bundesländer zu berücksichtigen.

Lösungsansätze:

Zur Vereinfachung des Verfahrens kann der Studienleiter den für ihn zuständigen Datenschutzbeauftragten bzw. denjenigen Datenschutzbeauftragten, in dessen Bundesland die zentrale Speicherung der Daten des Forschungsprojekts erfolgen soll, darum bitten, die Stellungnahmen der anderen Datenschutzbeauftragten (soweit von dem konkreten Forschungsprojekt betroffen) zu koordinieren.

Die Beschlüsse des 62. Deutschen Juristentages Bremen 1998

D. Abteilung Öffentliches Recht

Thema: Geben moderne Technologien und die europäische Integration Anlaß, Notwendigkeit und Grenzen des Schutzes personenbezogener Informationen neu zu bestimmen?

1. Die Erfordernisse der modernen Informationstechnologien und Informationsdienste sowie die EG-Datenschutzrichtlinie mit ihren vereinheitlichenden Schutzstandards geben Anlaß, Datenschutz und Informationsrecht gesetzlich neu zu regeln. Der Inhalt dieser Neuregelung wird maßgeblich durch die informationsfördernden, informationsermöglichenden und informationsbegrenzenden Gehalte des Grundgesetzes bestimmt.

angenommen: 44:0:0

2. Bei der gebotenen Neuorientierung muß der Datenschutz als konstitutiver Teil einer umfassenden Informationsordnung begriffen werden, für die das – auf den Gedanken der Informationsgerechtigkeit ausgerichtete – Informationsrecht den rechtlichen Rahmen bildet.

angenommen: 40:3:1

Geboten ist eine Informationsordnung, die u.a. den Zugang zu Informationen und den Umgang mit Informationen insbesondere im Hinblick auf den Schutz personenbezogener Daten regelt.

angenommen: 38:3:2

Vergleichbar schutzbedürftige Informationen juristischer Personen (insbesondere Betriebs- und Geschäftsgeheimnisse) sind einzubeziehen.

angenommen: 35:10:2

Das Datenrecht ist als Datenverkehrsordnung auszugestalten.

angenommen: 35:6:4

3. Das künftige Informationsrecht sollte einheitliche Schutzstandards anstreben.

angenommen: 38:1:5

Dies schließt Differenzierungen nach den Grundrechtspositionen der Informationshandelnden (z.B. Medienfreiheit, Wissenschaftsfreiheit, Glaubensfreiheit) bzw. nach spezifischen Sachstrukturen (z.B. Gesundheits- und Sozialrecht, Strafprozeßrecht) ein.

angenommen: 35:0:10

4. Die Reformschritte sind zu einem umfassenden Informationsgesetzbuch zusammenzuführen. Zur Vorbereitung soll unverzüglich eine Kommission eingerichtet werden.

angenommen: 36:0:10

5. Es empfiehlt sich, ein grundsätzlich einheitliches materielles Datenschutzrecht für den öffentlichen und den privaten Bereich zu schaffen, dessen innere Differenzierungen sich nach den Unterschieden in der Schutzbedürftigkeit unter Beachtung der Selbstbestimmung (Freiwilligkeit) und des Gefahrenpotentials zu richten haben. (Antrag Hamm)

angenommen: 23:21:1

6. Der Verbreitung strafbarer und jugendgefährdender Informationen ist – unter Beachtung des Zensurverbotes – insbesondere durch gesetzlich geregelte technische Vorkehrungen entgegenzuwirken.

angenommen: 44:1:1

7. Ein Eckpfeiler der Neuregelung sind technischer Selbstschutz und Selbstregulierungen (z.B. Datenschutz-Audit, Codes of conduct).

angenommen: 42:1:2

Voraussetzung ist die nachprüfbar Wirksamkeit derartiger Vorkehrungen.

angenommen: 37:4:5

Dies setzt die Unabhängigkeit der Kontrollinstanzen, einschließlich der internen Datenschutzbeauftragten, voraus.
(Antrag Jaspers)

angenommen: 23:12:9

8. Die Verschlüsselung personenbezogener Daten soll erlaubt bleiben, bei besonderen Gefährdungslagen geboten werden.

angenommen: 43:0:3

- a) Ein gesetzliches Hinterlegungsgebot ist nicht vorzusehen.

angenommen: 37:5:4

- b) Ein gesetzliches Hinterlegungsgebot ist vorzusehen (Antrag Pitschas)

abgelehnt: 4:38:4

- c) Die Fortentwicklung der Informationsgesellschaft verlangt danach, Prinzipien des Datenschutzes und der Sicherheit der Informationsverarbeitung zum integralen Bestandteil der Produkte, Dienstleistungen und Beratungen zu machen.
(Antrag Büllsbach)

angenommen: 40:1:4

Elektronischer Handel kann nur sicher funktionieren, wenn die freie Benutzung von kryptographischen Produkten und

Dienstleistungen gewährleistet ist. (Antrag Büllesbach)

angenommen: 36:1:8

Eine Beschränkung des Gebrauchs von

Verschlüsselungstechniken ist daher abzulehnen. (Antrag

Büllesbach)

angenommen: 35:1:9

9. Das künftige Informationsrecht soll sich wirkungsorientiert u.a. an folgenden Leitlinien ausrichten: Datenvermeidung und Datensparsamkeit, Zweckbindung der Daten, Systemdatenschutz, klare Verantwortlichkeiten im Datenumgang, Anonymisierung und Pseudonymisierung personenbezogener Daten, Datensicherheit durch technische und organisatorische Vorkehrungen, Folgenausgleich.

angenommen: 40:1:4

10. Wirksame Kontrolle ist Voraussetzung eines erfolgreichen Datenschutzes.

angenommen: 46:0:0

Eine wesentliche Bedeutung kommt hierbei den unabhängigen Datenschutzbeauftragten im öffentlichen und privaten Bereich zu.

angenommen: 41:1:4

Die Datenschutzkontrolle durch öffentliche Stellen soll weisungsfrei und verselbständigt durchgeführt werden.

angenommen: 37:6:3

11. Grenzüberschreitende Informationsflüsse und internationale Vernetzungen machen verstärkte internationale Zusammenarbeit und Regelungen unerlässlich.

angenommen: 46:0:0

Organisationsplan des Hessischen Datenschutzbeauftragten

Hessischer Datenschutzbeauftragter

Prof. Dr. Rainer Hamm Tel. (06 11) 14 08 20

Vertretung des Hessischen Datenschutzbeauftragten und Dienststellenleitung

Ute Arlt Tel. (06 11) 14 08 22

Vorzimmer:

Ursula Gegner Tel. (06 11) 14 08 21

Gruppe A

Referat A1

Gruppenleitung, Koordinierung und Grundsatzfragen, interne Verwaltung

Ute Arlt Tel. (06 11) 14 08 22

Mitarbeiter/innen:

Christel Friedmann-Baradel Tel. (06 11) 14 08 14

Bernd Groh Tel. (06 11) 14 08 35

Karin Nitsche Tel. (06 11) 14 08 34

Referat A2

Bildung, Verwaltung von Hochschulen und anderen Wissenschafts- einrichtungen, Schulverwaltung, Schulen einschl. Forschung, Archive

Manfred Weitz Tel. (06 11) 14 08 45

Mitarbeiterin:

Karin Nitsche Tel. (06 11) 14 08 34

Referat A3

Finanzwesen, Einwohnerwesen, Verkehr, Ordnungswidrigkeiten

Cornelia Topp Tel. (06 11) 14 08 38

Mitarbeiter/innen:

Mitarbeiter:

Michael Sobota

Tel. (06 11) 14 08 27

Referat C2

**Verfassungsschutz, Ausländerrecht, Europäische Union,
Schengener Informationssystem**

Angelika Schriever-Steinberg

Tel. (06 11) 14 08 25

Mitarbeiter:

Alfons Schranz

Tel. (06 11) 14 08 32

Referat C3

Justiz, Staatsanwaltschaften, Vollzugsanstalten, Polizei

Barbara Dembowski

Tel. (06 11) 14 08 26

Mitarbeiter:

Alfons Schranz

Tel. (06 11) 14 08 32

Gruppe D

Referat D1

**Gruppenleitung, Gesundheitswesen, Wissenschaft und Forschung,
Betreuungsrecht, Redaktion des Tätigkeitsberichts**

Dr. Rita Wellbrock

Tel. (06 11) 14 08 23

Mitarbeiter:

Rainer Banse

Tel. (06 11) 14 08 33

Referat D2

Personalwesen, Sozialwesen

Dr. Robert Piendl

Tel. (06 11) 14 08 36

Mitarbeiter:

Rainer Banse

Tel. (06 11) 14 08 33

Bernd Groh

Tel. (06 11) 14 08 35

Referat D3

**Kommunen, Vermessungswesen, Gewerberecht, Umwelt,
Landwirtschaft, Forsten und Naturschutz, Öffentlichkeitsarbeit**

Ulrike Müller

Tel. (06 11) 14 08 42

Mitarbeiter/in:

Helga Schaller

Tel. (06 11) 14 08 41

Michael Sobota

Tel. (06 11) 14 08 27

Abkürzungsverzeichnis

ABl.	Amtsblatt des Hessischen Kultusministeriums
Abs.	Absatz
AG	Aktiengesellschaft
AOK	Allgemeine Ortskrankenkasse
ARGE	AOK-Rechenzentrum Mitte
Art.	Artikel
AsylbLG	Asylbewerberleistungsgesetz
AuslG	Ausländergesetz
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BGBI.	Bundesgesetzblatt
BGHZ	Entscheidungen des Bundesgerichtshofs in Zivilsachen
BKAG	Bundeskriminalamtsgesetz
BPersVG	Bundespersönlichkeitsgesetz
BSHG	Bundessozialhilfegesetz
BStatG	Bundestatistikgesetz
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerwG	Bundesverwaltungsgericht
BVK	Börsenverrechnungskonto
BWS	Buchungszentrale der westfälisch-lippischen Sparkassen
bzw.	beziehungsweise
ca.	circa
CDU	Christlich Demokratische Union
CICS	Customer Information Control System
d.h.	das heißt
DJT	Deutscher Juristentag
DNA	Desoxyribonucleinacid (Desoxyribonukleinsäure)
DV	Datenverarbeitung
DV-System	Datenverarbeitungssystem
EG	Europäische Gemeinschaft
E-Mail	Elektronische Post
EU	Europäische Union

FGG	Gesetz über die Angelegenheiten der freiwilligen Gerichtsbarkeit
FISCUS	Föderales integriertes standardisiertes computerunterstütztes Steuersystem
GG	Grundgesetz
ggf.	gegebenenfalls
GhK	Gesamthochschule Kassel
GmbH	Gesellschaft mit beschränkter Haftung
GÜP	Unterstützung der Veranlagungstätigkeiten für Gewerbetreibend, Bezieher von Überschußeinkünften und für die Gewinn-/Verlustfeststellung bei Personengesellschaften
GVBl.	Gesetz- und Verordnungsblatt des Landes Hessen
HBG	Hessisches Beamtengesetz
HbL	Hilfe in besonderen Lebenslagen
HDSG	Hessisches Datenschutzgesetz
HEPOLAS	Hessisches Polizeiarbeitsplatzsystem
HessAFWoG	Hessisches Gesetz zum Abbau der Fehlsubventionen im Wohnungswesen
HessLStatG	Hessisches Landesstatistikgesetz
HEZ	Händlererevidenzzentrale
HGO	Hessische Gemeindeordnung
HKHG	Hessisches Krankenhausgesetz
HLU	Hilfe zum Lebensunterhalt
HSchulG	Hessisches Schulgesetz
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
HWG	Hessisches Wassergesetz
i.S.d.	im Sinne des
IDVS	Informations- und Datenverarbeitungssystem
INPOL	Informationssystem der Polizei
IuKDG	Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste
JMBL	Justizministerialblatt
KAN	Kriminalaktennachweis
KEZ	Kartenevidenzzentrale; auch Börsenevidenzzentrale
Kfz	Kraftfahrzeug

Kfz-Registerbehörden	Kraftfahrzeugregisterbehörden
KIV	Kommunale Informationsverarbeitung
KRG	Krebsregistergesetz
LARGO	Phantasiename für Datenverarbeitungssystem beim Landesamt für Verfassungsschutz
LfV	Landesamt für Verfassungsschutz
LTDrucks.	Landtagsdrucksache
MDSStV	Mediendienstestaatsvertrag
MESTA	Mehrländer-Staatsanwaltschafts-Automation
MVS	Multiple Virtual Storage
NADIS	Nachrichtendienstliches Informationssystem
NJW	Neue Juristische Wochenschrift
NSIS	Nationaler Teil des Schengener Informationssystems
PC	Personal-Computer
PROSOZ	Programm Sozialhilfe
PsychThG	Psychotherapeutengesetz
RACF	Resource Access Control Facility
RVO	Reichsversicherungsordnung
s.	siehe
S.	Seite
s. Anl.	siehe Anlage
SGB	Sozialgesetzbuch
SIRENE-Büro	Supplementary Information Request of the National Entry
SIS	Schengener Informationssystem
sog.	sogenannte(r/s)
StAnz.	Staatsanzeiger
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
StVÄG 1996	Strafverfahrensänderungsgesetz 1996
StVG	Straßenverkehrsgesetz
StVO	Straßenverkehrsordnung
StVollzG	Strafvollzugsgesetz
TDDSG	Teledienststedatenschutzgesetz
TDG	Teledienstegesetz

TSO	Time Sharing Option
u.a.	unter anderem
UVEG	Gesetz zur Einordnung der gesetzlichen Unfallversicherung in das Sozialgesetzbuch
VereinsG-DVO	Durchführungsverordnung zum Vereinsgesetz
VwVfG	Verwaltungsverfahrensgesetz
z.B.	zum Beispiel
ZEVIS	Zentrales Verkehrsinformationssystem
Ziff.	Ziffer
ZKA	Zentraler Kreditausschuß

Sachwortverzeichnis zum 27. Tätigkeitsbericht

ActiveX	8.2, Anhang 2
Adreßbücher	26.7
- Meldedaten	26.7
Adreßmittlungsverfahren	18.3
Akteneinsichtsrecht	21., 26.3
- in Akten der IHK	21.
Aktenzugriff	18.2
Altakten	18.1
Anonymisierung	Anhang 4
Anordnung, richterliche	5.1, 5.2.1
Archivierung	18.1
ARGE-Mitte (Rechenzentrum der AOK)	7.3
- Konzepte	7.3.2
- Prüfung	7.3
- Prüfungsfeststellungen	7.3.3
- technisches Umfeld	7.3.1
Asylverfahren	25.5
Aufbewahrungsfrist	18.1
Auskunft an Betroffene	26.6
- Bundesamt für Finanzen	26.6
Ausländer	11., 25.4
- Abschiebung	11.5
- Akten	11.3
- Ausländerzentralregister	11.1
- Fahndung	11.6
- Gesetz	25.4
- Verein	11.4
- Zusammenarbeit mit der Polizei	11.5
Ausnahmegenehmigung	20.1
- im Straßenverkehr	20.1
Automatisierung	6.1, 6.1.2
- bei der Justiz	6.1, 6.1.2

Benachrichtigung	2.2.2.2
Börsenevidenzzentrale	4.4
Bundesamt für Finanzen	26.6
- Entschließung der Datenschutzbeauftragten	26.6
Bundeskriminalamt	5.1, 5.3
Bundessozialhilfegesetz	7.5, 14.3
Chipkarten	2.2.3.4, 4.
- Geldkarte	4.
Cookies	8.2, Anhang 2
Dateienregister	2.2.2.1
Daten, sensitive	2.2.3.2
Datenerhebung	26.3
- bei der Justiz	26.3
Datenschutz-Audit	Anhang 4
Datenschutzbeauftragter	2.2.1, 2.2.5, 15.1, 15.2, Anhang 4
- behördlicher, interner	2.2.1, 15.1, Anhang 4
- Hessischer	2.2.5
Datenschutzkontrolle	2.1, 26.4, Anhang 4
- anlaßfreie Aufsicht	26.4
- Organisation	2.1
- Unabhängigkeit	26.4, Anhang 4
- Weisungsfreiheit	Anhang 4
Datenschutzkonzept	7.6
Datenschutzmaßnahmen	2.2.3.1
- technische, organisatorische	2.2.3.1
Datenschutzmodernisierung	26.4
- Entschließung der Datenschutzbeauftragten	26.4
Datensparsamkeit	2.2.3.1, Anhang 4
Datenübermittlung	2.2.4
Datenverarbeitung	23.1, 23.2, 25.3
- der Finanzverwaltung	23.1, 23.2

- FISCUS	23.1
- GÜP-HEFINA	23.2
- der Polizei	25.3
- HEPOLAS	25.3
Datenverkehrsordnung	Anhang 4
Datenvermeidung	26.4, Anhang 4
Deutscher Juristentag	26.4
Digitales Fernsehen	26.1
- Entschließung der Datenschutzbeauftragten	26.1
DNA-Analyse	5.1
Dual-homed Gateway	Anhang 2
EG-Richtlinie zum Datenschutz	2., 26.4, Anhang 4
Eingriffsbefugnis	5.2.2, 26.5
- im Sicherheitsbereich	5.2.2, 26.5
Einsatz technischer Mittel	5.2.1
- HSOG-Novelle	5.2.1
Einwilligung	5.1
- DNA-Dateien	5.1
E-Mail	17.2
- im Schulbereich	17.2
Epidemiologie und Datenschutz	Anhang 3
EU-Richtlinie zum Datenschutz	2., 26.4, Anhang 4
Europol	25.2
Evidenzzentralen	4.4
- GeldKarten-System	4.4
Fehlbelegung von Wohnraum	22.2
- Fehlbelegungsabgabe	22.2
- Einkommensnachweis	22.2
Fernmeldegeheimnis	9.3
Fernsehen, digitales	26.1
Firewall-Systeme	8.2, Anhang 2

Flughafenschutzdienst	24.
- Amtshilfe	24.
- Ordnungswidrigkeiten	24.
Forschung	10.
- Forschungsgeheimnis	10.1
Freistellungsaufträge	26.6
- Entschließung der Datenschutzbeauftragten	26.6
Gefahrenabwehr	5.2.4, 13.1
- Wasseraufsicht	13.1
Geldkarte	4., 26.2
- Abgleichsmöglichkeiten	4.5
- Abläufe	4.4.2
- Datenflüsse	4.4.2.6
- Empfehlungen	4.8
- Entschließung der Datenschutzbeauftragten	26.2
- rechtliche Wertung	4.6, 4.7
- Systembeschreibung	4.4
- vertragliche Grundlagen	4.3
Gemeinsame Kontrollinstanz	25.2
Gerichte	6.1, 26.3, 26.8
Gerichtsvollzieher	6.1
Gesundheitsamt	7.6
GÜP-HEFINA	23.2
Händlererevidenzzentrale	4.4
HEPOLAS	25.3
- Datensicherheitskonzept	25.3
HEPOLIS	11.6.2
Herkunftssicherungs- und Informationssystem für Tiere	13.2
Hessisches Datenschutzgesetz	2.1
- Novellierung	2.1
Hundesteuer	23.2
- Bestandsaufnahme	23.2
- Satzung	23.2
Identitätsfeststellung	5.1
- DNA-Dateien	5.1

IDVS II	7.3.2
Informationsgesetzbuch	Anhang 4
INPOL	5.3
Internet	8.1, 8.2, 17.2, Anhang 2
- Benutzungsordnung	17.2
- Orientierungshilfe	8.2, Anhang 2
- Schule	17.2
- Verantwortlichkeit für Links	8.1
Java	8.2, Anhang 2
JavaScript	8.2, Anhang 2
Job	7.3.1.2, 7.3.3.3.2
Jugendamt	14.2
- Zusammenarbeit mit anderen Stellen	14.2
Justizdaten	26.3
Kartenevidenzzentrale s. Börsenevidenzzentrale	
Klassenkonferenzen	17.1
Kommunale Statistikstelle	19.
Kommunen	12., 19.
- Prüfungen und Beratungen	12.3
- Statistikstellen	19.
Kommunikationsdaten	17.2
- bei Internetnutzung	17.2
Kontrolle, verdachtsunabhängige	5.2.2, 5.2.3
Kontrollstelle	5.2.3
Kontrollzuständigkeit	6.1.2, 26.8
Krankenhausbehandlung	7.5
- Arztberichte	7.5
- Epikrisen	7.5
- Krankenakten	7.5
Krankenkasse	7.4

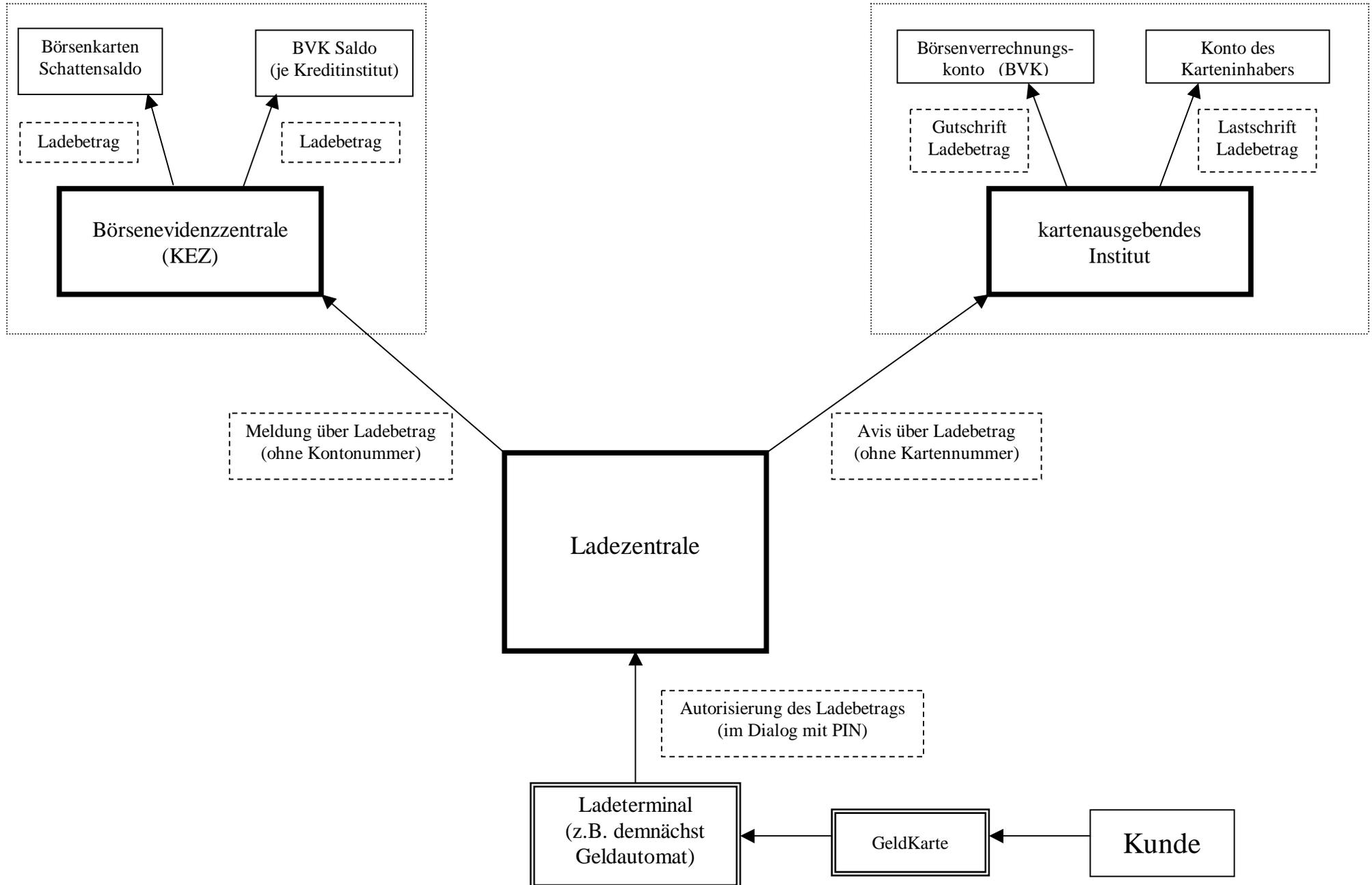
Krebsregister	7.1.
- Anonymisierung der Meldungen	7.1.2.1
- Meldepflicht für Ärztinnen und Ärzte	7.1.2.2
Kriminalaktennachweis (KAN)	5.3.1
Kryptographie	26.4, Anhang 4
Landesamt für Verfassungsschutz	16.1, 16.2
- Arbeitsplan	16.1
- Prüffall	16.1
Landwirtschaftliches Unternehmensverzeichnis	12.4
LARGO	16.1, 16.2
Lauschangriff	5.2
Lebenshaltungskosten eines Ausländers	11.1, 11.2
Marketing	18.3
Mediendienste-Staatsvertrag	8.1.1
Meldedaten	26.7
- Adreßbücher	26.7
- Einwilligung in Datenübermittlung	26.7
- Entschließung der Datenschutzbeauftragten	26.7
MESTA	6.3
Mitarbeiterdatenschutz	7.4
MVS	7.3.1
- Grenzen der Schutzfunktion	7.3.1.3
- Schutzfunktionen	7.3.1.2
Nachrichtendienste	6.1.3
Ökologischer Landbau	25.1
- private und staatliche Kontrolle	25.1
Packet Filter	Anhang 2
Parkerlaubnis	20.2
Parteien	26.7
- Meldedaten	26.7
PERKEO	9.

Personalakten	18.2
Personalaktenrecht	15.2
Personaldatenverarbeitung	15.2, 18.2
Personalrat	15.1
Plug Ins	8.2, Anhang 2
Polizei	5.2, 6.1.3, 11.5
- Zusammenarbeit mit Ausländerbehörde	11.5
Prävention	5.3.1
Private Sicherheitsdienste	5.4
Protokollierung	5.3.2
Prüfungskompetenz	26.8
- der Datenschutzbeauftragten bei Gerichten	26.8
- Entschließung der Datenschutzbeauftragten	26.8
Pseudonymisierung	17.2, Anhang 4
Psychotherapeutengesetz	7.2
RACF	7.3.2.2, 7.3.3
Rechenzentrum der AOK s. ARGE-Mitte	
Regelungen, bereichsspezifische	6.1.1, 26.3
Reihenuntersuchung	5.1
Rundfunkstaatsvertrag	26.1
Sachakten	18.2
Schattensaldo	4.4.2
Schengener Durchführungsabkommen	3.
- Alias-Personalien	3.4
- Fahndungsunterlagen	3.5
- Protokollierung	3.5
- Schengener Informationssystem	3.1, 3.3, 3.5, 3.6
- SIRENE Büro	3.2
Schleierfahndung	5.2.2

Schülervertretung	17.1
Schutz privater Rechte	5.4
Schweigepflicht	7.1.1, 7.2, 10.1
Screened Gateway	Anhang 2
Sicherheitsbehörden - Entschließung der Datenschutzbeauftragten	5.2.2, 6.1.3, 26.5 26.5
Sicherheitsüberprüfung	25.6, 3.2
Smart-Card	25.5
Sozialdatenschutz - verdeckte Ermittlungen	14.4 14.4
Sozialgeheimnis - Großraumbüro	7.4 7.4
Sozialgesetzbuch	14.3
Sozialhilfe - Datenabgleich	14.1 14.1
Sozialhelfemißbrauch	14.3
Speicherung - Dauer der -	5.3.1, 5.3.3 5.2.5, 5.3
Staatsanwaltschaft - Automation	6.1, 6.1.3, 6.3, 26.3 6.3
Stateful Inspection	Anhang 2
Strafverfahren	26.3
Strafverfolgung	5.2.4, 6.1.3
Strafvollzug	6.2
Straßenverkehr	20.
Studentenausweis	18.3
Teledienstegesetz	8.1.1, 9.2
Telefonüberwachung	6.1.3, 26.5
TP-Monitor	7.3.2, 7.3.3.3.2

Übergangsbonus	6.1, 26.3
Verbrechensbekämpfung, vorbeugende	5.3
Verbunddateien	5.3.3
Verdienstausschlag	12.1
- ehrenamtliches Magistratsmitglied	12.1
Verfahren, gemeinsame	2.2.3.3
Verfahrensverzeichnis	2.2.2.1
Verpflichtungserklärung	11.1, 11.2
Verschlüsselung	26.4, Anhang 4
Verschwiegenheitspflicht	17.1
Videoüberwachung	2.2.3.5
Vorabkontrolle	2.2.3.2
Warndatei	11.1
Wassergesetz	13.1
- Gesamtnovelle	13.1
Weitergabe von KfZ-Daten	5.4
Wohnraumüberwachung	5.2.1
ZEVIS	5.4.3
Zweckbindung	26.4, Anhang 4
Zweckentfremdung	22.1
- Ordnungswidrigkeit	22.1
- Wohnraum	22.1

Ladevorgang bei einer GeldKarte



Zahlung mit einer GeldKarte

