16. Wahlperiode

Drucksache **16/3746**

HESSISCHER LANDTAG

07. 03. 2005

Dreiunddreißigster Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

vorgelegt zum 31. Dezember 2004
vom Hessischen Datenschutzbeauftragten
Prof. Dr. Michael Ronellenfitsch
nach § 30 des Hessischen Datenschutzgesetzes vom 7. Januar 1999

Eingegangen am 7. März 2005 · Ausgegeben am 29. März 2005
Druck: Druckerei Chmielorz GmbH, 65205 Wiesbaden · Auslieferung: Kanzlei des Hessischen Landtags, Postfach 3240, 65022 Wiesbaden

INHALTSVERZEICHNIS

Vorwort

Die Zeichen der Zeit stehen nicht günstig für den Datenschutz. Damit soll nicht gesagt werden, dass öffentliche Stellen in Hessen besonders krass gegen das Datenschutzrecht verstoßen würden. Wie der vorliegende Tätigkeitsbericht zeigt, sind sich die öffentlichen Stellen durchaus der Anforderungen bewusst. Was Sorge bereitet, ist die technische Entwicklung, welche die Gefahren für die informationelle Selbstbestimmung exponentiell anwachsen ließ. Mit den Gefahren sind natürlich auch Chancen etwa bei der Verbrechensbekämpfung verbunden. Spektakuläre, besser gesagt: publikumswirksame Erfolge auf diesem Gebiet, wie etwa im Fall Moshammer, wecken die Neigung, das technisch Machbare auch wirklich zu machen. In Ausnahmesituationen berechtigte Datenzugriffe werden als „normal“ empfunden und geraten so zur Normalität. Es tritt ein Gewöhnungsprozess ein bis hin zum moralischen Impetus derjenigen, die „gläserne“ Politiker fordern, aber für sich selbst (noch) vor dem gläsernen Menschen zurückschrecken. Gegen solche Zeitströmungen kommt es darauf an, dass der institutionalisierte Datenschutz seine Wächterrolle ernst nimmt. Dass dies geschehen ist, belegt der Tätigkeitsbericht, der über die Aufgabenwahrnehmung des Hessischen Datenschutzbeauftragten exemplarisch Aufschluss gibt.

Ronellenfitsch

Register der Rechtsvorschriften

AufenthG	Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet (Aufenthaltsgesetz) vom 30. Juli 2004 (BGBl. I S. 1950)
AuslG	Gesetz über die Einreise und den Aufenthalt von Ausländern im Bundesgebiet vom 9. Juli 1990 (BGBl. I S. 1354), zuletzt geändert durch Art. 15 des Gesetzes zur Steuerung und Begrenzung der Zuwanderung und zur Regelung des Aufenthalts und der Integration von Unionsbürgern und Ausländern (Zuwanderungsgesetz) vom 30. Juli 2004 (BGBl. I S. 1950), außer Kraft getreten durch Art. 15 Abs. 3 Zuwanderungsgesetz am 1. Januar 2005 (BGBl. I S. 1950)
BDG	Bundesdisziplinargesetz in der Fassung vom 9. Juli 2001 (BGBl. I S. 1510), zuletzt geändert durch Art. 7 Versorgungsänderungsgesetz 2001 vom 20. Dezember 2001 (BGBl. I S. 3926)
BDSG	Bundesdatenschutzgesetz in der Fassung vom 14. Januar 2003 (BGBl. I S. 66)
BEG	Bundesentschädigungsgesetz in der Fassung vom 29. Juli 1956 (BGBl. I S. 562), zuletzt geändert durch Gesetz vom 26. August 1966 (BGBl. I S. 525)
BSHG	Bundessozialhilfegesetz in der Fassung vom 23. März 1944 (BGBl. I S. 646, 2975), zuletzt geändert durch Art. 68 Gesetz zur Einordnung des Sozialhilferechts in das Sozialgesetzbuch vom 27. Dezember 2003 (BGBl. I S. 3022)
EG	Vertrag zur Gründung der Europäischen Gemeinschaft vom 25. März 1957 (BGBl. II S. 766) in der Fassung des Vertrags über die Europäische Union vom 7. Februar 1992 (BGBl. II S. 1253/1256); zuletzt geändert durch die Akte zum Beitrittsvertrag vom 16. April 2003 (BGBl. II S. 1410)
GG	Grundgesetz für die Bundesrepublik Deutschland vom 23. Mai 1949 (BGBl. S. 1), zuletzt geändert durch Art. 96 Gesetz zur Änderung des Grundgesetzes vom 26. Juli 2002 (BGBl. I S. 2863)
HArchivG	Hessisches Archivgesetz vom 18. Oktober 1989 (GVBl. I S. 270), zuletzt geändert durch Art. 1 ÄndG vom 10. März 2002 (GVBl. I S. 34)
HDO	Hessische Disziplinarordnung in der Fassung der Bekanntmachung vom 11. Januar 1989 (GVBl. I S. 58), zuletzt geändert durch Art. 1 ÄndG vom 3. November 1998 (GVBl. I S. 401)
HDSG	Hessisches Datenschutzgesetz in der Fassung vom 7. Januar 1999 (GVBl. I S. 98)

HessLStatG	Gesetz über die Statistik im Land Hessen vom 19. Mai 1987 (GVBl. I S. 67), zuletzt geändert durch ÄndG vom 24. November 1994 (GVBl. I S. 676)
HKHG	Hessisches Krankenhausgesetz 2002 in der Fassung vom 6. November 2002 (GVBl. I S. 662)
HMG	Hessisches Meldegesetz in der Fassung vom 19. März 1999 (GVBl. I S. 274)
HSchG	Hessisches Schulgesetz in der Fassung vom 2. August 2002 (GVBl. I S. 466)
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung in der Fassung vom 31. März 1994 (GVBl. I S. 174), zuletzt geändert durch das Achte Änderungsgesetz vom 15. Dezember 2004 (GVBl. I S. 444)
IT-Sicherheitsleitlinie	StAnz. 2004, S. 3827
KWG	Kreditwesengesetz vom 10. Juli 1961 (BGBl. I S. 881) in der Fassung vom 9. September 1998 (BGBl. I S. 2776), zuletzt geändert durch Art. 5 Gesetz zur Umsetzung der Richtlinie 2002/47/EG vom 6. Juni 2002 über Finanzsicherheiten und Änderung des Hypothekenbankgesetzes und anderer Gesetze vom 5. April 2004 (BGBl. I S. 502)
MRRG	Melderechtsrahmengesetz in der Fassung vom 19. April 2002 (BGBl. I S. 1342) zuletzt geändert durch Gesetz vom 27. Mai 2003 (BGBl. I S. 742)
ÖPNVG	Gesetz zur Weiterentwicklung des öffentlichen Personennahverkehrs in Hessen in der Fassung vom 19. Januar 1996 (GVBl. I S. 50)
OWiG	Ordnungswidrigkeitengesetz in der Fassung vom 19. Februar 1987 (BGBl. I S. 602), zuletzt geändert durch Art. 18 Gesetz vom 9. Dezember 2004 (BGBl. I S. 3220)
PBefG	Personenbeförderungsgesetz in der Fassung vom 8. August.1990 (BGBl. I S. 1690), zuletzt geändert durch Art. 24 Gesetz vom 29. Dezember 2003 (BGBl. I S. 3076)
PostG	Postgesetz vom 22. Dezember 1997 (BGBl. I S. 3294), zuletzt geändert durch Art. 224 Achte ZuständigkeitsanpassungsVO vom 25. November 2003 (BGBl. I S. 2304)
RSAV	Risikostruktur-Ausgleichsverordnung vom 3. Januar 1994 (BGBl. I S. 55), geändert durch die Vierte Verordnung zur Änderung der Risikostruktur-Ausgleichsverordnung vom 27. Juni 2002 (BGBl. I S. 2286 Nr. 42)

SDÜ	Übereinkommen zur Durchführung des Übereinkommens von Schengen vom 14. Juli 1985 zwischen den Regierungen der Staaten der Benelux-Wirtschaftsunion, der Bundesrepublik Deutschland und der Französischen Republik betreffend den schrittweisen Abbau der Kontrollen an den gemeinsamen Grenzen vom 19. Juli 1990 – Schengener Durchführungsübereinkommen (BGBl. II 1993 S. 1013)
SGB I	Erstes Buch Sozialgesetzbuch – Allgemeiner Teil vom 5. Dezember 1975 ((BGBl. I S. 3015), zuletzt geändert durch Art. 2 Gesetz zur Einordnung des Sozialhilferechts in das Sozialgesetzbuch vom 27. Dezember 2003 (BGBl. I S. 3022)
SGB V	Fünftes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz in der Fassung vom 18. Januar 2001 (BGBl. I S. 130), zuletzt geändert durch Art. 4 Gesetz zur Einordnung des Sozialhilferechts in das Sozialgesetzbuch vom 27. Dezember 2003 (BGBl. I S. 3022)
SGB IX	Neuntes Buch Sozialgesetzbuch – Rehabilitation und Teilhabe behinderter Menschen in der Fassung vom 19. Juni 2001 (BGBl. I S. 1046, 1047), zuletzt geändert durch Art. 1 Gesetz zur Förderung der Ausbildung und Beschäftigung schwer behinderter Menschen vom 23. April 2004 (BGBl. I S. 606)
SGB X	Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz in der Fassung vom 18. Januar 2001 (BGBl. I S. 130), zuletzt geändert durch Art. 9 Gesetz zur Organisationsreform in der gesetzlichen Rentenversicherung vom 9. Dezember 2004 (BGBl. I S. 3242)
StGB	Strafgesetzbuch in der Fassung vom 13. November 1998 (BGBl. I S. 3322), zuletzt geändert durch das Erste Justizmodernisierungsgesetz vom 24. August 2004 (BGBl. I S. 2198)
StPO	Strafprozessordnung in der Fassung vom 7. April 1987 (BGBl. I S. 1074), zuletzt geändert durch das Opferrechtsreformgesetz vom 24. Juni 2004 (BGBl. I S. 1354)
TKG	Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190)
UklaG	Gesetz über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen (Unterlassungsklagengesetz) in der Fassung vom 27. August 2002 (BGBl. I S. 3422, 4346)
UStG	Umsatzsteuergesetz in der Fassung vom 9. Juni 1999 (BGBl. I S. 1270)

UVG	Gesetz zur Sicherung des Unterhalts von Kindern allein stehender Mütter und Väter durch Unterhaltsvorschüsse oder -ausfallleistungen (Unterhaltsvorschussgesetz) in der Fassung vom 2. Januar 2002 (BGBl. S.2 615), geändert durch Art. 10 Nr. 1 Gesetz zur Steuerung und Begrenzung der Zuwanderung und zur Regelung des Aufenthalts und der Integration von Unionsbürgern und Ausländern (Zuwanderungsgesetz) vom 20. Juni 2002 (BGBl. I S. 1946)
VereinsG	Gesetz zur Regelung des öffentlichen Vereinsrechts vom 5. August 1964 (BGBl. I S. 593), zuletzt geändert durch Art. 5 Abs. 2 Vierunddreißigstes StrafrechtsändG vom 22. August 2002 (BGBl. I S. 3390)
VereinsG-DVO	Verordnung zur Durchführung des Gesetzes zur Regelung des öffentlichen Vereinsrechts (VereinsG) vom 28. Juli 1966 (BGBl. I S. 457), zuletzt geändert durch Art. 6 Abs. 1 Vierunddreißigstes StrafrechtsändG vom 22. August 2002 (BGBl. I S. 3390)
Verordnung über die Verarbeitung personenbezogener Daten in Schulen	vom 30. November 1993 (ABl. des Hessischen Kultusministeriums Nr. 2/1994 S. 114)
VOBGM	Verordnung zur Ausgestaltung der Bildungsgänge und Schulformen der Grundstufe (Primarstufe) und der Mittelstufe (Sekundarstufe I) und der Abschlussprüfungen in der Mittelstufe in der Fassung vom 20. März 2003 (ABl. des Hessischen Kultusministeriums Nr. 4/2003 S. 163)
VwVfG	Verwaltungsverfahrensgesetz in der Fassung vom 23. Januar 2003 (BGBl. I S. 102), geändert durch Kostenrechtsmodernisierungsgesetz vom 5. Mai 2004 (BGBl. I S. 718)
ZPO	Zivilprozessordnung in der Fassung vom 12. September 1950 (BGBl. I S. 533), zuletzt geändert durch Erstes Justizmodernisierungsgesetz vom 24. August 2004 (BGBl. I S. 2198)
Zuwanderungsgesetz	Gesetz zur Steuerung und Begrenzung der Zuwanderung und zur Regelung des Aufenthalts und der Integration von Unionsbürgern und Ausländern vom 30. Juli 2004 (BGBl. I S. 1950)

Kernpunkte

1. Die Kontrollzuständigkeit des Hessischen Datenschutzbeauftragten erstreckt sich auf den gesamten Bereich der Daseinsvorsorge, unabhängig davon, ob die Daten verarbeitenden Stellen öffentlich oder privatrechtlich organisiert sind. Dazu gehören z. B. der Rhein-Main-Verkehrsverbund (RMV) und auch die Fraport AG, soweit sie den Flughafen als Verkehrsweg eröffnet und aufrechterhält (Ziff. 2).

2. Die Entscheidungen des Bundesverfassungsgerichts zum Großen Lauschangriff und anderen verwandten Themen haben Konsequenzen für das Instrumentarium der Strafverfolgungs- und Polizeibehörden, die bei den gesetzlichen Regelungen beachtet werden müssen (Ziff. 4.1 und 10.3). Die Novellierung im Polizeirecht des Landes hat diese nicht konsequent genug berücksichtigt und weitere tiefe Eingriffsbefugnisse geschaffen, die datenschutzrechtlicher Prüfung nicht standhalten (Ziff. 5.1.1).

3. Die automatisierte Kennzeichenerkennung (Aufnahme von Kfz-Kennzeichen mit digitalen Kameras im fließenden Verkehr) stellt einen unzulässigen Eingriff in das Recht auf informationelle Selbstbestimmung dar, wenn z. B. Kennzeichen unverdächtiger Personen gespeichert oder Bewegungsprofile erstellt werden (Ziff. 5.1.2).

4. In Planfeststellungsverfahren zum Ausbau des Frankfurter Flughafens dürfen Einwendungen der Bürger, die lediglich allgemeine Argumente ohne persönlichen oder regionalen Bezug enthalten (Jedermann-Einwendungen), nur anonymisiert an die Vorhabenträgerin weitergeleitet werden (Ziff. 5.4.1).

5. Wegen der zunehmenden Analysemöglichkeiten muss die Verwendung von Blut- und Gewebeproben in Krankenhäusern intern klar festgelegt werden. Die Patienten sind über Umfang, Zweck und Dauer der Aufbewahrung und Verwendung ihrer Proben zu informieren. Sollen Proben für den Aufbau einer dauerhaften „Biobank“ für allgemeine Forschungszwecke verwendet werden, ist vorher ihre Einwilligung einzuholen (Ziff. 5.8.1).

6. Die Bemühungen zur Kostenersparnis und Effizienzsteigerung führen vermehrt zur Übertragung von Aufgaben auf private Dienstleister. Dabei sind detaillierte Regelungen zu treffen und Vorschriften zu beachten damit eine datenschutzgerechte Gestaltung gewährleistet wird (Ziff. 5.9.1 und 6.1)

7. Die im E-Government-Konzept des Landes vorgesehenen zentralen IT-Strukturen und Datenbestände und das Ziel des Übergangs auf eine vollständig elektronische Arbeit der Verwaltung stellen hohe Anforderungen an Datenschutz und Datensicherheit. Einige namentlich datenschutzrechtliche Probleme sind noch ungelöst (Ziff. 8.1).

8. Die Radio Frequency Identification-Technik (RFID) wird zunehmend für die verschiedensten Anwendungen (z. B. beim Einkauf, der Zutrittskontrolle und im öffentlichen Nahverkehr) eingesetzt. Wegen der Möglichkeit personenbezogene Daten unbemerkt zu verarbeiten und damit etwa Persönlichkeits- oder Bewegungsprofile zu erstellen ist vor dem Einsatz einer solchen Technik auf die Einhaltung des Datenschutzes besonderes Augenmerk zu legen (Ziff. 8.4 und 10.5).

9. Nach wie vor gibt es Fälle, in denen Bürger ihre Datenschutzrechte nur durch Einschaltung meiner Behörde durchsetzen konnten (Ziff. 5.1.4, 5.1.5, 5.11.2).

10. In der öffentlichen Wahrnehmung muss der Datenschutz wieder einen Stellenwert erlangen, welcher der Bedrohungslage infolge der technischen Entwicklung entspricht (Ziff. 1).

1. Einführung

Der Datenschutz befindet sich in einer paradoxen Situation. Als sich zu Beginn der 1970er Jahre die Risiken einer rechnergestützten massenhaften und schnellen Verarbeitung personenbezogener Daten für die informationelle Selbstbestimmung und die Persönlichkeitsrechte der Betroffenen erst abzeichneten, stand der Datenschutz im Brennpunkt des öffentlichen Interesses. Heute haben sich die Risiken für die informationelle Selbstbestimmung zu realen Gefahren verdichtet. Die Informationsgesellschaft ist Wirklichkeit geworden. In der Informationsgesellschaft besteht nicht nur der Wunsch, sondern auch die Möglichkeit, automatisiert Informationen zu beschaffen und zu verarbeiten, um „Profile“ zu erstellen (Persönlichkeitsprofil, Kundenprofil, Wählerprofil, Täterprofil u. dgl.). Der früher nur als Schlagwort viel beschworene „gläserne Mensch“ nimmt Gestalt an. Nichtsdestoweniger sieht sich der Datenschutz in den Hintergrund gedrängt. Die Sensibilisierung für die Bedeutung des Datenschutzes im Hinblick auf die Persönlichkeitsentfaltung der Bürgerinnen und Bürger, die geleitet von der Rechtsprechung des Bundesverfassungsgerichts (Urteil vom 15. Dezember 1983 – 1 BvR 209, 269, 362, 420, 440, 484/83 – BVerfGE 65,1) zu einer hoch entwickelten und weltweit vorbildlichen Datenschutzkultur in Deutschland geführt hat, droht abzunehmen. Belange der äußeren und inneren Sicherheit, Erfordernisse der Terrorismusbekämpfung, Konsequenzen der Globalisierung, Umbau der Sozialsysteme, Wandel der Staatsaufgaben, Privatisierung und Verwaltungsmodernisierung entwickeln eine Eigendynamik, angesichts derer der Datenschutz vielfach als effektivitätshemmender Störfaktor betrachtet wird.

Dass es gleichwohl, wie der vorliegende Tätigkeitsbericht belegt, mit dem öffentlichen Datenschutz in Hessen nicht schlecht bestellt ist, ist den institutionellen und organisatorischen Vorkehrungen ebenso zu verdanken, wie dem guten Willen der Beteiligten.

Es wächst aber die Sorge vor Fehlentwicklungen, die sich nur vermeiden lassen, wenn die zentrale Bedeutung eines funktionierenden Datenschutzes für unsere freiheitlich demokratische Verfassungsordnung weiterhin im allgemeinen Bewusstsein verhaftet bleibt.

Aus diesem Grund beginnt der vorliegende Tätigkeitsbericht mit einigen allgemeinen Bemerkungen zur Aufgabenstellung und Kontrollzuständigkeit des Hessischen Datenschutzbeauftragten. Daran anschließend wird auf die aktuelle europäische Entwicklung des Datenschutzes eingegangen, die auf den Datenschutz im Land Hessen ebenso ausstrahlt wie die Rechtsentwicklung im Bund. Den Kern des Berichts macht naturgemäß der Datenschutz auf der Ebene des Landes sowie der Kommunen, sonstigen Selbstverwaltungskörperschaften und Kammern aus. Die Entwicklungen und Empfehlungen im Bereich der Technik und Organisation beschäftigen sich im vorliegenden Bericht insbesondere mit dem E-Government-Konzept des Landes. Es folgen der Bilanzbericht und die Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die vom Hessischen Datenschutzbeauftragten mitverantwortet werden. Unter den Materialien ist die praktisch bedeutsame IT-Sicherheitsleitlinie für die Hessische Landesverwaltung aufgeführt.

2. Kontrollzuständigkeit des Hessischen Datenschutzbeauftragten

2.1 Allgemeines

Die Datenschutzkontrolle des öffentlichen Bereichs ist nicht auf die öffentlich-rechtliche Organisationsform, sondern auf die Aufgabenstellung der Daten verarbeitenden Stellen bezogen. Sie umfasst alle Stellen, die bei ihrer Aufgabenerfüllung öffentlich-rechtlichen Bindungen unterliegen.

Die einleitend angedeuteten Entwicklungen namentlich bei der Erfüllung staatlicher Aufgaben sowie im Staatsorganisationsrecht bieten Anlass für wenige klarstellende Bemerkungen zur Aufgabenstellung und Kontrollzuständigkeit des Hessischen Datenschutzbeauftragten.

2.1.1 Öffentlicher Bereich

Gemäß § 24 Abs. 1 Satz 1 HDSG überwacht der Hessische Datenschutzbeauftragte die Einhaltung der datenschutzrechtlichen Vorschriften bei den Daten verarbeitenden Stellen. Daten verarbeitende Stelle ist jede Behörde und sonstige öffentliche Stelle des Landes, der Gemeinden und Landkreise sowie der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen ungeachtet ihrer Rechtsform, die Daten für sich selbst verarbeitet oder durch andere verarbeiten lässt (§ 2 Abs. 3 i. V. m. § 3 Abs. 1 Satz 1 HDSG). Erfasst werden auch nicht-öffentliche Stellen, soweit sie hoheitliche Aufgaben unter Aufsicht der vorstehend aufgeführten Stellen wahrnehmen.

§ 2 Abs. 3 HDSG

Daten verarbeitende Stelle ist jede der in § 3 Abs. 1 genannten Stellen, die Daten für sich selbst verarbeitet oder durch andere verarbeiten lässt.

§ 3 Abs. 1 HDSG

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.

Die komplementäre Regelung findet sich in § 2 Abs. 4 BDSG.

§ 2 Abs. 4 BDSG

Nicht-öffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Absätze 1 bis 3 fallen. Nimmt eine nicht-öffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.

Nach § 2 Abs. 3 BDSG gelten Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder, die Aufgaben der öffentlichen Verwaltung wahrnehmen, ungeachtet der Beteiligung nicht-öffentlicher Stellen als öffentliche Stellen des jeweiligen Landes, wenn sie entweder nicht über den Bereich des Landes hinaus tätig werden oder dem Bund nicht die absolute Mehrheit der Anteile oder Stimmen zusteht.

§ 2 Abs. 3 BDSG

Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder, die Aufgaben der öffentlichen Verwaltung wahrnehmen, gelten ungeachtet der Beteiligung nicht-öffentlicher Stellen als öffentliche Stellen des Bundes, wenn
1. sie über den Bereich eines Landes hinaus tätig werden oder
2. dem Bund die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht.
Andernfalls gelten sie als öffentliche Stellen der Länder.

Bei der Auftragsdatenverarbeitung für öffentliche Stellen durch nicht-öffentliche Stellen haben sich diese der Kontrolle des Hessischen Datenschutzbeauftragten zu unterwerfen (§ 4 Abs. 3 Satz 1 i. V. m. § 24 Abs. 1 Satz 4 HDSG).

§ 4 Abs. 3 Satz 1 HDSG

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.

Die Gesamtschau dieser Bestimmungen ergibt, dass die Datenschutzkontrolle des öffentlichen Bereichs nicht auf die öffentlich-rechtliche Organisationsform, sondern auf die Aufgabenstellung der Daten verarbeitenden Stellen bezogen ist. Erfasst werden alle Stellen, die bei ihrer Aufgabenerfüllung öffentlich-rechtlichen Bindungen unterliegen. Das sind zum einen alle Stellen, die hoheitliche Aufgaben im engeren Sinne wahrnehmen. Handelt es sich um Personen des privaten Rechts, müssen diese ohnehin mit Hoheitsgewalt beliehen werden, so dass sie dann als Behörden nach § 1 Abs. 2 HVwVfG handeln.

§ 1 Abs. 2 HVwVfG

Behörde im Sinne dieses Gesetzes ist jede Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt.

Zum öffentlichen Bereich zählen daher ferner Tätigkeiten zur Erfüllung des öffentlichen Daseinsvorsorgeauftrags.

Die Zuordnung der Daseinsvorsorgeaufgaben zum öffentlichen Bereich folgt nicht nur aus einfachem Recht, sondern ist auch verfassungsrechtlich geboten. Das Grundgesetz und die Hessische Verfassung haben sich für den Staat als Organisationsform des sozialen Zusammenlebens entschieden. Die Selbstqualifizierung der Bundesrepublik Deutschland als sozialer Rechtsstaat zwingt dazu, hieraus die gebotenen verfassungsrechtlichen Konsequenzen zu ziehen. Der Staat wird im Innenverhältnis durch seine Zwecke und Aufgaben definiert. Hierbei gibt es Aufgaben, die der Staat selbst erfüllen muss, und Aufgaben, deren Erfüllung er jedenfalls zu ermöglichen und zu gewährleisten hat. So mögen Versorgungs-, Transport-, Kommunikations- und Entsorgungsnetze dank privater Initiative entstehen. Zwangsweise durchsetzen können Private solche Netze nicht. Sie sind darauf angewiesen, dass der Staat in ihrem Interesse enteignet, weil sie auf die Mitbenutzung fremden Eigentums angewiesen sind. Eine Enteignung ist dann aber nur zum Wohl der Allgemeinheit zulässig. Wo obendrein Private generell nicht in der Lage sind, eine flächendeckende Infrastruktur aufzubauen und dem Markt zu öffnen, besteht eine entsprechende unmittelbare Einstandspflicht des Staats. Der Staat bzw. die kommunalen und sonstigen Selbstverwaltungskörperschaften müssen kraft Verfassungsauftrags Aufgabenträger der Daseinsvorsorge sein. Das bedeutet freilich nur, dass der Staat die Leistungsaufgaben der Daseinsvorsorge nicht dem freien Spiel der Kräfte überlassen darf. Für die Daseinsvorsorge gelten öffentlich-rechtliche Grundsätze. Öffentlich-rechtlich sind nicht nur die Regelungen, die das hoheitlich-obrigkeitliche Verwaltungshandeln betreffen. Öffentlich-rechtlich sind vielmehr die Regelungen, die den Interessen des Staates und der Allgemeinheit dienen, während privatrechtlich die Regelungen sind, die das Verhalten Privater in deren eigener Interessensphäre betreffen. Da vielfach eine kongruente Interessenlage besteht, sind Überschneidungen nicht ausgeschlossen. Auch eine unternehmerische Betätigung kommt bei der Daseinsvorsorge in Betracht. Erforderlich ist dann aber, dass sich im Wettbewerb eine ausreichende Erfüllung der Daseinsvorsorgeaufgabe sicherstellen lässt. Auch bei den „wirtschaftlichen Leistungen im öffentlichen Interesse“ nach Art. 16 des Vertrags zur Gründung der Europäischen Gemeinschaft (EG) ist der Wettbewerb nur Mittel der optimalen Leistungserbringung und nicht Selbstzweck. Das Vorliegen einer Daseinsvorsorgeaufgabe hat somit die rechtliche Konsequenz, dass die Aufgabe dem öffentlichen Bereich zuzuordnen ist. Dieses Verständnis der „Daseinsvorsorge“ liegt der Rechtsprechung namentlich des Bundesverfassungsgerichts zugrunde (vgl. BVerfG-Urteil vom 10. Dezember 1974 – 2 BvK 1/73; 2 BvR 902/73, BVerfGE 38, 258 (270 f.); Beschluss vom 7. Juni 1977 – 1 BvR 108, 424/73 und 226/4, BVerfGE 45, 63 (78); Beschluss vom 20. März 1984 – 1 BvL 26/82 – BVerfGE 66, 248 (258); Beschluss vom 14. April 1987 – 1 BvR 775/84, BVerfGE 75,192 (199f.); Kammerbeschluss vom 23. September 1994 – 2 BvR 1547/85, NVwZ 1995, 370; Kammerbeschluss vom 7. Januar 1999 – 2 BvR 927/97, NVwZ 1999, 520; Kammerbeschluss vom18. Februar 1999 – 1 BvR 1367/88, 146 und 147/91, NVwZ 1999, 1103). Gegen den Rechtsbegriff der Daseinsvorsorge wird zwar gelegentlich eingewandt, er sei zu unbestimmt. Darin liegt aber gerade seine Stärke, denn auf diese Weise ist er in der Lage, mit der technischen und sozialen Entwicklung Schritt zu halten. Im Übrigen lassen sich die Anwendungsfelder der Daseinsvorsorge an Hand einer reichhaltigen judiziellen Kasuistik induktiv abstecken. Erfasst werden Bereiche der Versorgungswirtschaft (Ver- und Entsorgung), des Verkehrswesens (Infrastruktur, Verkehrswirtschaft), des Rundfunks („Grundversorgung“), der Telekommunikation („Universaldienste“) und des Kreditwesens ferner Bildungs-, Sozial-, Gesundheits-, Kultur- und Freizeiteinrichtungen.

2.1.2 Gerichte

Die Kontrollbefugnis des Hessischen Datenschutzbeauftragten erstreckt sich nicht funktionell auf die Recht sprechende Gewalt, die allein den Richtern zusteht (Art. 92 GG). Die Gerichte unterliegen jedoch der Kontrolle des Hessischen Datenschutzbeauftragten, soweit sie nicht in richterlicher Unabhängigkeit tätig werden (§ 24 Abs. 1 Satz 3 HDSG).

2.1.3 Kontrolle der Kontrolleure?

Die Aufsicht über den nicht-öffentlichen Bereich obliegt dem Regierungspräsidium, das seinerseits der Fachaufsicht des Hessischen Ministeriums des Innern und für Sport untersteht. Eine Kontrollzuständigkeit des Hessischen Datenschutzbeauftragten im Hinblick auf die Datenschutzaufsicht durch die für nicht-öffentliche Stellen zuständigen Aufsichtsbehörden besteht nicht. Mit diesen Behörden hat der Hessische Datenschutzbeauftragte indessen zusammenzuarbeiten (§ 24 Abs. 3 HDSG). Zum Zwecke der Zusammenarbeit kann er auch von diesen Aufsichtsbehörden Auskünfte verlangen (§ 24 Abs. 4 Satz 1 HDSG). Als unabhängige oberste Landesbehörde hat der Hessische Datenschutzbeauftragte darüber hinaus darauf zu achten, dass die der parlamentarischen Kontrolle unterliegenden Staatsorgane, ihre datenschutzrechtliche Aufgaben nach Gesetz und Recht wahrnehmen (vgl. § 24 HDSG). Eine derartige mittelbare Kontrolle des nicht-öffentlichen Bereichs wird freilich nur in Extremfällen in Betracht kommen, die der Gefährdung des verfassungsmäßigen Staatsgefüges vergleichbar sind, auf die der Hessische Datenschutzbeauftragte gemäß § 24 Abs. 2 Satz 2 HDSG ohnehin zu achten hat.

§ 24 HDSG

(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.

2.2 Fraport AG

Soweit die Fraport AG Aufgaben der öffentlichen Daseinsvorsorge wahrnimmt, ist sie öffentliche Stelle nach dem Hessischen Datenschutzgesetz und unterliegt meiner Kontrolle.

Die Fraport AG wird in wesentlichen Teilen auf dem Gebiet der Daseinsvorsorge tätig und unterliegt insoweit der Kontrolle des Hessischen Datenschutzbeauftragten. Die gegenteilige Ansicht, von der uns das Hessischen Ministerium des Inneren und für Sport mit Schreiben vom 28. Dezember 2004 „nach eingehender Prüfung der Sach- und Rechtslage“, jedoch ohne nähere Begründung nachrichtlich in Kenntnis gesetzt hat, halte ich für unzutreffend. Die Fraport AG ist zwar auch ein nicht-öffentliches Unternehmen, das sich in verschiedenen Bereichen ausschließlich marktorientiert betätigt. In diesem Zusammenhang untersteht es der Datenschutzaufsicht des Regierungspräsidiums Darmstadt. Der Frankfurter Flughafen ist jedoch in erster Linie Flughafen und nicht Shopping Center. Angesichts des Flugplatzzwangs lässt sich der Gemeingebrauch am Luftraum nur durch Nutzung von Verkehrsflugplätzen verwirklichen. Verkehrsflughäfen sind damit unverzichtbarer Bestandteil der Verkehrsinfrastruktur. Alle Tätigkeiten, die in unmittelbarem Zusammenhang mit der Planung, Errichtung, Erweiterung und dem Betrieb von Verkehrsflughäfen stehen, erfolgen in Erfüllung einer öffentlichen Aufgabe. In der Startbahn-West-Entscheidung vom 7. Juli 1978 (BVerwG 4 C 79.76 u. a., BVerwGE 56,110) ging das Bundesverwaltungsgericht ebenfalls davon aus, dass die Errichtung und der Betrieb von Verkehrsflughäfen eine unternehmerische Betätigung ist. Es qualifizierte Verkehrsflughäfen gleichwohl als Einrichtungen, mit denen öffentliche Zwecke verfolgt werden, zu deren Gunsten somit eine gemeinnützige Planung betrieben werden kann. Da der Fraport AG Eingriffe in entgegenstehende Rechte Dritter zugebilligt werden, ist für deren planfeststellungsbedürftige Vorhaben eine Planrechtfertigung erforderlich. Planungsrechtlich erfüllt die Fraport AG als Vorhabenträger eine öffentliche Aufgabe. Es wäre inkonsequent, die öffentliche Aufgabenerfüllung der Fraport AG planungs- und datenschutzrechtlich unterschiedlich zu behandeln.

2.3 Anwendbarkeit des Hessischen Datenschutzgesetzes auf hessische Verkehrsverbünde

Die Nahverkehrsverbünde in Hessen fallen in den Anwendungsbereich des Hessischen Datenschutzgesetzes und damit auch unter meine datenschutzrechtliche Kontrolle. Anlass für meine Stellungnahme war eine Umfrage zu dieser Fragestellung in den einzelnen Bundesländern.

Für die hessischen Verkehrsverbünde gilt das Landesdatenschutzgesetz, weil es sich um Vereinigungen von öffentlichen Stellen des Landes Hessen i. S. v. § 3 Abs. 1 HDSG handelt. So sind Mitglieder im Rhein-Main-Verkehrsverbund (RMV) elf hessische Städte, fünfzehn Kreise sowie das Land selbst. Weitere Mitglieder gibt es nicht. Schon allein deshalb ist der Anwendungsbereich des HDSG eindeutig zu bejahen. Im Übrigen nehmen die Verbünde auch nicht am Wettbewerb teil. Ablesbar ist dies aus dem Gesetz zur Weiterentwicklung des öffentlichen Personennahverkehrs in Hessen i. d. F. vom 19. Januar 1996 (ÖPNVG). Danach ist der öffentliche Personennahverkehr in Hessen eine Selbstverwaltungsaufgabe der Aufgabenträger. Aufgabenträger sind die Landkreise, kreisfreien Städte und Sonderstatusstädte. Nach § 2 Abs. 1 ÖPNVG ist der öffentliche Personennahverkehr eine Aufgabe der Daseinsvorsorge, die durch die genannten Aufgabenträger sicherzustellen ist. Nach § 5 Abs. 1 ÖPNVG erfüllen die Aufgabenträger ihre Aufgaben im Regionalverkehr gemeinsam in Verkehrsverbünden. Das sind derzeit der RMV und der NVV (Nordhessischer Verkehrsverbund). Für Mittelhessen könnte ein zusätzlicher Verbund gegründet werden. Hinsichtlich der Versorgung im ÖPNV besteht damit nach der gesetzlichen Aufgabenzuweisung praktisch eine Monopolstellung des Verbundes, sodass man eine wettbewerbliche Betätigung verneinen muss. Auch deshalb gilt für die Verbünde, soweit sie personenbezogene Daten verarbeiten, das HDSG.

3. Europa

3.1 Schengener Durchführungsübereinkommen

Auch im vergangenen Jahr nahm der Hessische Datenschutzbeauftragte – vertreten durch eine Mitarbeiterin – zugleich für die anderen Landesdatenschutzbeauftragten an den Sitzungen der Gemeinsamen Kontrollinstanz für das Schengener Informationssystem in Brüssel teil. Der Beitrag stellt die Arbeitsschwerpunkte dar.

3.1.1 Allgemeines

Die Gemeinsame Kontrollinstanz hat sich durch den Beitritt der neuen Mitgliedstaaten zum 1. Mai 2004 um zehn weitere Delegationen vergrößert. Diese haben allerdings noch einen Beobachterstatus, da das Schengener Durchführungsübereinkommen (SDÜ) für diese Staaten noch nicht in Kraft gesetzt wurde.
Der Vorsitz der Gemeinsamen Kontrollinstanz wechselte im Dezember 2003 von Italien zu dem Niederländer Ulco van de Pol. Als Vertreterin wurde die portugiesische Delegierte Isabell Cruz gewählt.
Im April 2004 erschien der bereits seit Dezember 2003 in Englisch vorliegende Tätigkeitsbericht der Gemeinsamen Kontrollinstanz für die Jahre 2003 und 2004 endlich in deutscher Sprache. Er kann beim BfD oder mir bezogen werden.
Im September d. J. fand erstmals im Anschluss an die regulären Sitzungen in Brüssel eine gemeinsame Sitzung der Kontrollgremien für Schengen, Europol, Eurojust und das Zollinformationssystem in Anwesenheit des Europäischen Datenschutzbeauftragten Peter Hustinx und seines Vertreters statt. Ziel dieser erneut geplanten Zusammenkunft war eine bessere Zusammenarbeit der vier Kontrollinstanzen. Diese ist vor dem Hintergrund umso wichtiger, als die Überlegungen zur Zusammenlegung der Kontrollinstanzen aber auch der Harmonisierung des für sie geltenden materiellen Rechts konkreter werden. An dieser Entwicklung wird sich die Gemeinsame Kontrollinstanz für Schengen durch Stellungnahmen und Diskussionen aktiv beteiligen.

3.1.2 Entwicklungen des Schengener Informationssystems

Wichtigstes Thema in der Gemeinsamen Kontrollinstanz war die Auseinandersetzung mit Plänen zu einer Erweiterung des Schengener Informationssystems (SIS), dem so genannten SIS II (32. Tätigkeitsbericht, Ziff. 3.2).
Die Schaffung einer neuen Generation des Schengener Informationssystems mit einer neuen Technik ist notwendig, weil das jetzige SIS nur für 18 Staaten ausgelegt ist, der Kreis der Teilnehmer sich aber auf 25 erhöht hat.

Allerdings wird dies auch zum Anlass genommen, das System effizienter auszubauen und den Wünschen bestehender oder potenzieller Nutzer entgegenzukommen. Aus dem Zusammenspiel der diskutierten Änderungsvorschläge geht jedenfalls hervor, dass sich das SIS von einem reinen Abfragesystem (ist die betroffene Person im SIS registriert oder nicht?) zu einem Analyseinstrument für die Polizeibehörden und andere Stellen entwickelt.

3.1.2.1 Bereits feststehende Änderungen

Im letzten Tätigkeitsbericht (Ziff. 3.2.1) hatte ich von einigen Änderungen des SDÜ berichtet, die demnächst erfolgen sollten. Dies betraf u. a.

- die Tätigkeit der SIRENE-Büros (Suplimentary Information Request at the National Entry) und der Verarbeitung der dort anfallenden Unterlagen. In Deutschland betrifft dies das Bundeskriminalamt, das als nationale Stelle für die Verarbeitung der Daten im SIS zuständig ist,
- neue Zugriffsrechte für EUROPOL (das Europäische Polizeiamt), EUROJUST (die Europäische Stelle zur justiziellen Zusammenarbeit) und nationale Justizbehörden,
- die Protokollierung von Abrufen aus dem SIS.

Mittlerweile ist die entsprechende Verordnung des Rates der Europäischen Union über die Einführung neuer Funktionen für das Schengener Informationssystem in Kraft getreten (ABl. der Europäischen Gemeinschaften L 162 vom 30. April 2004), sie wird aber – auch wegen der fehlenden technischen Vorkehrungen – noch nicht angewandt. Der Beschluss des Rats zum gleichen Thema (ABl. C 160 vom 4. Juli 2002) konnte wegen eines Parlamentsvorbehalts Schwedens noch nicht vom Rat angenommen werden, andere Hinderungsgründe stehen dem aber nicht entgegen.

3.1.2.2 In der Diskussion befindliche Vorschläge

Aus neueren Unterlagen der Kommission und des Rats ergibt sich, dass SIS II ein so genanntes flexibles Instrument werden soll, das sich neuen Gegebenheiten anpassen und das innerhalb eines vertretbaren zeitlichen Rahmens und ohne größere Kosten und Anstrengungen Benutzeranfragen gerecht werden kann. Diese Erweiterungsmöglichkeit betrifft zum einen den Zugriff weiterer Behörden und öffentlicher Stellen. Beispielsweise gibt es einen Vorschlag der Kommission, wonach Fahrzeugzulassungsstellen auf das SIS zugreifen sollen. Derzeit nicht mehr in der Diskussion scheint der Zugriff privater Stellen zu sein.

Zum anderen geht es um zusätzliche in das SIS aufzunehmende Datenkategorien. Im letzten Tätigkeitsbericht (Ziff. 3.2.2) hatte ich von der Übernahme der Daten aus dem europäischen Haftbefehl berichtet (ABl. L 190 vom 18. Juli 2002). Es geht aber auch um Daten aus anderen EU-Datenbanken wie z. B. EUROPOL oder dem Zollinformationssystem. In der Diskussion sind weiterhin biometrische Daten wie Lichtbilder und Fingerabdrücke.

Die Gemeinsame Kontrollinstanz hat sich in einer Stellungnahme vom 24. Mai 2004 mit den Plänen für ein so genanntes „flexibles“ System auseinander gesetzt und hat auf verschiedene Probleme hingewiesen. Ein derartiges flexibles System sei für eine schleichende Funktionserweiterung anfälliger, weil die Realisierung der Wünsche unterschiedlichster Interessenten dazu führen könne, dass das System Informationen für Zwecke verarbeite, die ursprünglich gar nicht vorgesehen waren. Zum anderen sei eine angemessene Beurteilung der potenziellen Auswirkungen eines derartigen „flexiblen“ Systems kaum denkbar, weil seine endgültige Form nicht absehbar sei. Die Gemeinsame Kontrollinstanz warnte vor einer Entwicklung dahingehend, dass vermeintliche technische Sachzwänge über die Art und Weise der Rechtsetzung mitbestimmen. Sie regte an, in einem ersten Schritt eine Datenschutzfolgenabschätzung durchzuführen, um festzustellen, welche Auswirkungen bestimmte Funktionserweiterungen des SIS auf die Rechte Einzelner haben. Auf der Grundlage einer derartigen Folgenabschätzung sollte dann ein neuer rechtlicher Rahmen erarbeitet werden.

3.1.3 Gemeinsame Überprüfung der Ausschreibungen zu Drittausländern

Im letzten Tätigkeitsbericht (Ziff. 3.3) hatte ich berichtet, dass die Gemeinsame Kontrollinstanz eine Überprüfung der Ausschreibungen von Drittausländern zur Einreiseverweigerung in allen Schengenstaaten beschlossen hat. Deutschland hat die Überprüfung abgeschlossen (die Prüfung in Hessen wird unter Ziff. 3.2 dargestellt). Auch die meisten anderen Länder haben ihre Prüfberichte erstellt und dem Sekretariat übermittelt. Derzeit wird vom Sekretariat der Gemeinsamen Kontrollinstanz eine Synthese der Ergebnisse erstellt, um dann Verbesserungsvorschläge auszuarbeiten.

3.2 Europaweit koordinierte Prüfung von Ausschreibungen zur Einreiseverweigerung in das Schengen-Gebiet

In über 10 % der von mir geprüften hessischen Ausschreibungen im Schengener Informationssystem lagen die Ausschreibungsvoraussetzungen nicht vor. Ausschreibungen die älter als drei Jahre waren, waren überwiegend unrechtmäßig, weil die nach dreijähriger Datenspeicherung vorgeschriebene Prüfung der weiteren Erforderlichkeit unterblieb. Dort wo sie nicht unterblieb, erging sie weitgehend nicht ordnungsgemäß oder falsch.

3.2.1 Vorbemerkung und Anlass der Prüfung

Nach Abschaffung der Personenkontrollen an den Binnengrenzen der so genannten Schengen-Vertragsstaaten wurde als Kompensationsmaßnahme das Schengener Informationssystem (SIS) eingeführt. Es hat u. a. zum Ziel, Personen, die schon einmal z. B. nach einem abgelehnten Asylantrag abgeschoben oder ausgewiesen worden sind, vorläufig nicht erneut ins Schengengebiet einreisen zu lassen, um gegebenenfalls erneut Asyl zu beantragen. Die Rechtsgrundlage ist Art. 96 Schengener Durchführungsübereinkommen (SDÜ).

Art. 96 SDÜ

(1) Die Daten bezüglich Drittausländern, die zur Einreiseverweigerung ausgeschrieben sind, werden aufgrund einer nationalen Ausschreibung gespeichert, die auf Entscheidungen der zuständigen Verwaltungsbehörden und Gerichten beruht, wobei die Verfahrensregeln des nationalen Rechts zu beachten sind.

(2) Die Entscheidungen können auf die Gefahr für die öffentliche Sicherheit und Ordnung oder die nationale Sicherheit, die die Anwesenheit eines Drittausländers auf dem Hoheitsgebiet der Vertragspartei bedeutet, gestützt werden. …

(3) Die Entscheidungen können ebenso darauf beruhen, dass der Drittausländer ausgewiesen, zurückgewiesen oder abgeschoben worden ist, wobei die Maßnahme nicht aufgeschoben oder aufgehoben worden sein darf, ein Verbot der Einreise oder des Aufenthaltes enthalten oder davon begleitet sein muss und auf der Nichtbeachtung des nationalen Rechts über die Einreise oder den Aufenthalt von Ausländern beruhen muss.

Mit „Drittausländer“ sind Ausländer gemeint, die keinem der Schengenstaaten angehören. Bei Abschiebe- und Ausweisungsverfügungen deutscher Ausländerbehörden handelt es sich um Entscheidungen nach Abs. 3 dieser Vorschrift, denn sie sind gemäß § 8 Abs. 2 AuslG[1] von einem Einreiseverbot in die Bundesrepublik begleitet.

§ 8 Abs. 2 AuslG

Ein Ausländer der ausgewiesen oder abgeschoben worden ist, darf nicht erneut ins Bundesgebiet einreisen und sich darin aufhalten. Ihm wird auch beim Vorliegen der Voraussetzungen eines Anspruches nach diesem Gesetz keine Aufenthaltsgenehmigung erteilt. Die in den Sätzen 1 und 2 bezeichneten Wirkungen werden auf Antrag in der Regel befristet. Die Frist beginnt mit der Ausreise.

Datenschutzinstanz für das Schengener Informationssystem ist die Gemeinsame Kontrollinstanz aller Schengenstaaten (s. Ziff. 3.1). Dieser Stelle lagen verschiedene Hinweise vor, dass es auch Ausschreibungen im Schengener Informationssystem zu solchen Personen geben soll, die die Voraussetzungen von Art. 96 SDÜ nicht erfüllen (s. 6. Tätigkeitsbericht der Gemeinsamen Kontrollinstanz Schengen vom 5. April 2004, Kapitel 2, Ziff. II; www.bfd.bund.de/informationen/schengen.html). Auch mein Amtsvorgänger hatte in den Jahren 2001 und 2002 an dieser Stelle über fehlerhafte Datenspeicherungen im Schengener Informationssystem berichtet (29. Tätigkeitsbericht, Ziff. 12.1; 30. Tätigkeitsbericht, Ziff. 17). Die Gemeinsame Kontrollinstanz beschloss, jede nationale Datenschutzbehörde möge nach bestimmten feststehenden Kriterien überprüfen, ob die Eingaben personenbezogener Daten durch die Behörden des jeweiligen Landes entsprechend Art. 96 SDÜ erfolgt sind.

3.2.2 Der Prüfungsansatz

Da es sich bei den Ausschreibungen nach Art. 96 SDÜ in der Praxis weit überwiegend um Entscheidungen gemäß Abs. 3 der Regelung handelt und diese Entscheidungen von den Ausländerbehörden als Behörden des Landes getroffen worden sind, ergab sich für die Bundesrepublik Deutschland die Zuständigkeit der Landesdatenschutzbeauftragten. Diese gingen nach einem identischen Prüfraster vor, das den in der Gemeinsamen Kontrollinstanz aufgestellten Kriterien entsprach.

Das Raster umfasste folgende Fragen:

1. Enthält die Ausländerakte ein Formular, das die Ausschreibung gemäß Art. 96 SDÜ im SIS betrifft?
   (Liegt eine Entscheidung i. S. d. Art. 96 SDÜ vor.)

2. Handelt es sich bei dem Betroffenen um einen Drittausländer?

3. Liegt der Ausschreibung ein Ausschreibungsgrund zu Grunde?

4a. Wird die Erforderlichkeit der Ausschreibung, wie in Art. 112 Abs. 1 SDÜ vorgesehen, überprüft?

4b. Wird diese Prüfung dokumentiert und wie werden die Gründe für eine weitere Speicherung in den Unterlagen festgehalten?

4c. Wie hoch ist der Anteil der geprüften Ausschreibungsfälle mit mehr als sechs Jahren und mehr als neun Jahren Ausschreibungsdauer?

[1] Jetzt sinngemäß § 11 Abs. 1 AufenthG

5. Wird die Ausschreibungsfrist im SIS an das nach § 8 Abs. 2 AuslG unbefristet wirkende nationale Einreiseverbot gekoppelt oder wird differenziert?
6. Werden im Falle einer Löschung im SIS die zugrunde liegenden Unterlagen vernichtet? Falls nicht, wofür werden sie noch aufbewahrt?

Die in Ziff. 4 angeführte Rechtsgrundlage lautet wie folgt:

Art. 112 Abs. 1 SDÜ

Die zur Personenfahndung in dem Schengener Informationssystem aufgenommenen personenbezogenen Daten werden nicht länger als für den verfolgten Zweck erforderlich gespeichert. Spätestens drei Jahre nach ihrer Einspeicherung ist die Erforderlichkeit der weiteren Speicherung von der ausschreibenden Vertragspartei zu prüfen. …

Zur Sicherstellung dieser Prüfung wertet das Bundeskriminalamt den nationalen Datenbestand des SIS regelmäßig aus und informiert die Ausländerbehörden mit einem Formularschreiben in jedem Einzelfall von dem bevorstehenden Ablauf der Dreijahresfrist.

Da der beim BKA geführte deutsche Datenbestand im SIS ca. 200.000 Datensätze umfasst, konnte nicht der Gesamtbestand überprüft werden. Das BKA hat auf Veranlassung des Bundesbeauftragten für den Datenschutz eine Liste von Fällen nach einem Zufallsgenerator erstellen lassen, die jede 500. Ausschreibung als Prüffall auswies. Daraus ergaben sich ca. 400 Prüffälle, die nun von den jeweils zuständigen Landesdatenschutzbeauftragten geprüft werden sollten.

3.2.3 Das Prüfergebnis

Von den insgesamt ca. 400 Prüffällen entfielen 47 auf hessische Behörden. Knapp die Hälfte stammte von der Ausländerbehörde Frankfurt; der Rest verteilte sich auf 19 weitere Ausländerbehörden. Eine Ausländerakte war unauffindbar. Das nachfolgende Ergebnis bezieht sich also auf 46 Prüffälle.

Nach Einsicht in die Ausländerakten konnte ich die Fragen wie folgt beantworten:

zu 1. Die hessischen Ausländerbehörden schreiben obligatorisch nach Ausweisungen und Abschiebungen die Betroffenen mit einem bestimmten, ansonsten bei der Polizei Verwendung findenden Vordruck aus. Eine bestimmte Stelle im LKA nimmt die Dateneingabe ausschließlich anhand dieses Vordruckes vor. Es liegt also immer eine förmliche Entscheidung nach Art. 96 SDÜ vor. In zehn Fällen war zu beanstanden, dass die Ausschreibung nicht wie in einer Verwaltungsvorschrift zum SDÜ vorgesehen „unverzüglich“, sondern erst verzögert nach der ausländerrechtlichen Entscheidung erfolgte. Da die Ausschreibungsdauer nicht an den Zeitpunkt der ausländerrechtlichen Entscheidung, sondern am Ausschreibungsdatum anknüpft, führte dies zu entsprechenden Verzögerungen um mehrere Monate, teilweise mehrere Jahre bei der Löschung der Daten.

zu 2. In allen geprüften 46 Fällen handelte es sich wie vorgeschrieben bei den Betroffenen um Drittausländer und nicht etwa um EU-Angehörige.

zu 3. In 41 Fällen waren die Betroffenen ausgewiesen oder abgeschoben, lag also die in Art. 96 Abs. 3 genannte materielle Voraussetzung vor. In fünf Fällen war dies nicht der Fall. Diese fünf Betroffenen hätten nicht zum Einreiseverbot ausgeschrieben werden dürfen.

zu 4. Diese Prüfung entfiel in 22 der 46 Fälle, weil die Ausschreibung nicht länger als drei Jahre zurücklag.

zu 4a. In den geprüften 24 Fällen erfolgte die Prüfung nach Art. 112 Abs. 1 SDÜ nur in elf Fällen. 13-mal gab es keinerlei Dokumentation. Auch das Schreiben des Bundeskriminalamtes, dass rechtzeitig vor Fristablauf in jedem Einzelfall erstellt wird und die Sachbearbeitung unterstützen soll, war der Ausländerakte nicht zu entnehmen schien also nicht bearbeitet worden zu sein.

zu 4b. Die elf durch diverse Bearbeitungsnotizen wie Stempel, Häkchen oder Handzeichen dokumentierten Prüfungen führten nur in einem Fall zur Löschung der Daten. In den verbleibenden zehn Fällen wurde in einem Fall mit der Notiz „§ 47 AuslG“ (§ 47 Ausländergesetz behandelt Ausweisungen wegen besonderer Gefährlichkeit [2]) auch der Grund für die Verlängerung der Datenspeicherung dokumentiert. In den restlichen neun Fällen waren die Gründe nicht genannt. Dabei lagen materiell in einigen Fällen auch gar keine Gründe vor.

[2] Jetzt sinngemäß § 53 AufenthG

zu 4c. Der Anteil der geprüften Ausschreibungsfälle mit mehr als sechs Jahren Ausschreibungsdauer lag bei vier von 46 Fällen. Der Anteil der geprüften Ausschreibungsfälle mit mehr als neun Jahren Ausschreibungsdauer lag bei einem von 46 Fällen.

zu 5. Die Ausschreibung ergeht nie unbefristet. Es ist technisch sichergestellt, dass spätestens nach sechs Jahren der Datensatz automatisch gelöscht wird, es sei denn, die Speicherung wird aufgrund einer Einzelfallentscheidung verlängert.

zu 6. Die Ausschreibungsunterlagen werden zur Ausländerakte genommen und dienen der Dokumentation. Sie teilen das Schicksal der Akte.

Dieses Ergebnis habe ich dem Bundesbeauftragten für den Datenschutz zum Zusammentragen mit den Prüfergebnissen aus den anderen Bundesländern und zum Vortrag in der Gemeinsamen Kontrollinstanz zur Verfügung gestellt. Auch das Hessische Innenministerium habe ich über das Ergebnis informiert.

3.2.4 Konsequenzen

In den Fällen, in denen die Ausschreibungsvoraussetzungen fehlten, waren die Datenspeicherungen zu löschen. Bei den Ausschreibungen die älter als drei Jahre waren, war in 13 Fällen die Prüfung der Erforderlichkeit zur Fortdauer des Einreiseverbotes nach Art. 112 SDÜ nachzuholen. In den Fällen, in denen diese Prüfung erfolgt war, war in einigen Fällen die Dokumentation der Gründe für die Fortdauer der Datenspeicherung vorzunehmen. Dort wo keine Gründe vorlagen, musste das Ergebnis der Prüfung korrigiert werden. Die erforderlichen Korrekturen in den geprüften Einzelfällen wurden mir seitens der Ausländerbehörden sämtlich bestätigt. Die Behörde, bei der die verzögerten Ausschreibungen vorkamen, hat mir nachvollziehbar dargelegt, dass die Verzögerungen auf Grund eines mittlerweile abgestellten organisatorischen Mangels aufgetreten waren. Einige Ausländerbehörden habe ich gebeten, ihre Praxis zu korrigieren. Die Ausländerbehörde der Stadt Frankfurt hat in einer internen Dienstanweisung alle Mitarbeiterinnen und Mitarbeiter der Ausländerbehörde auf die aufgezeigten Mängel hingewiesen und konkrete Hinweise zu deren Begegnung erlassen.

Weitere evtl. erforderliche Korrekturen am Verfahren der Ausschreibung zur Einreiseverweigerung in das Schengengebiet und an der Prüfung der Erforderlichkeit dieser Datenspeicherung nach drei Jahren, entsprechend Art. 112 Abs. 1 SDÜ, werden derzeit von den Datenschutzbeauftragten des Bundes und der Länder diskutiert. In meinem nächsten Bericht werde ich das Thema wieder aufgreifen und über die weitere Entwicklung berichten.

4. Bund

4.1 Die Entscheidung des Bundesverfassungsgerichts zum Großen Lauschangriff und die Konsequenzen für das Instrumentarium von Strafverfolgungsbehörden

Das Bundesverfassungsgericht hat mit seinem Urteil vom 3. März 2004 zum großen Lauschangriff Maßstäbe formuliert. Die Anwendung dieser Maßstäbe macht eine Überprüfung und ggf. Überarbeitung aller Regelungen zur heimlichen Datenerhebung erforderlich.

4.1.1 Kernbereich und Menschenwürdegehalt

Das BVerfG hat mit Urteil am 3. März über die Grundlagen der Wohnraumüberwachung in der Verfassung bzw. die Umsetzung in der Strafprozessordnung entschieden (1 BvR 2378/98, 1084/99, BVerfGE 109, 279). Dabei hat es u. a. als Leitsätze formuliert:

- Zur Unantastbarkeit der Menschenwürde gemäß Art. 1 GG gehört die Anerkennung eines absolut geschützten Kernbereichs privater Lebensgestaltung. In diesen Bereich darf die akustische Überwachung von Wohnraum zu Zwecken der Strafverfolgung (Art. 13 Abs. 3 GG) nicht eingreifen. Eine Abwägung nach Maßgabe des Verhältnismäßigkeitsgrundsatzes zwischen der Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) und dem Strafverfolgungsinteresse findet insoweit nicht statt.

- Die auf die Überwachung von Wohnraum gerichtete gesetzliche Ermächtigung muss Sicherungen der Unantastbarkeit der Menschenwürde enthalten sowie den tatbestandlichen Anforderungen des Art. 13 Abs. 3 GG und den übrigen Vorgaben der Verfassung entsprechen.

- Führt die auf eine solche gesetzliche Ermächtigung gestützte akustische Wohnraumüberwachung gleichwohl zur Erhebung von Informationen aus dem absolut geschützten Kernbereich privater Lebensgestaltung, muss sie abgebrochen werden und Aufzeichnungen müssen gelöscht werden; jede Verwertung solcher Informationen ist ausgeschlossen.

Mit Beschluss vom gleichen Datum hat das BVerfG im Zusammenhang mit Regelungen des Außenwirtschaftsgesetzes auch für die Telekommunikationsüberwachung ausgesprochen, dass der Gesetzgeber die Grundsätze der Lauchangriffentscheidung zu beachten habe (1 BvF 3/92, NJW 2004, 2213).

Das BVerfG bekräftigt damit den hohen Rang des Grundrechts auf Unverletzlichkeit der Wohnung und des Rechts auf informationelle Selbstbestimmung. Bei der Interpretation von Art. 1 GG durch das Gericht lassen sich unterschiedliche Ansätze erkennen. In einer ersten Dimension definiert der Senat den Schutzbereich von Art. 1 GG quasi räumlich. Die Selbstentfaltung verlange einen Rückzugsraum. Die Privatwohnung wird als Raum höchstpersönlicher Lebensgestaltung, als letztes Refugium in einer von technischen Entwicklungen vielfältig bedrohten Umwelt interpretiert. In diesem Privatraum spreche eine Vermutung dafür, dass jede staatliche Maßnahme den Kernbereich und den Menschenwürdegehalt von Art. 13 GG berühre.

Eine zweite Dimension des Menschenwürdebegriffs im Urteil ist nicht räumlich, sondern funktional. Der Senat legt dar, dass auch in der Privatwohnung nicht jede Äußerung durch Art. 1 GG geschützt ist und lässt sich damit auf die Beurteilung der Art, des Inhalts und der Partner der Kommunikation ein. Anhaltspunkte sind etwa die Höchstpersönlichkeit von Äußerungen, Ausdrucksformen der Sexualität, personelle Vertrautheit der Kommunikationspartner (insbesondere der Familienmitglieder usw.).

Mit diesen Entscheidungen hat das Gericht eine intensive Debatte ausgelöst, die weit über die Neuordnung der Regelungen in der StPO zum Großen Lauschangriff hinausgehen. Als erste Reaktion auf diese Entscheidungen hat auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung vom 25./26. März 2004 (s. Ziff. 10.3) auf die notwendigen Folgerungen durch den Gesetzgeber hingewiesen.

4.1.2 Folgerungen für die staatlichen Überwachungsmaßnahmen

Die Entscheidung zum Lauschangriff selbst bezieht sich unmittelbar nur auf die Strafverfolgung. Geht es aber um die Definition eines unantastbaren Bereichs privater Lebensführung, dann richtet sich der Schutz gegen jegliche staatliche Gewalt, also auch gegen polizeiliche Präventivmaßnahmen. In der Entscheidung zum Außenwirtschaftsgesetz hat das Gericht dies ausdrücklich ausgesprochen.

Selbstverständlich muss bei der Umsetzung in den einzelnen Bereichen differenziert vorgegangen werden. So ergeben sich für die Prävention, insbesondere bei der Abwehr von Gefahren für die Rechtsgüter Leben und Gesundheit andere Maßstäbe als bei der Repression. Desgleichen sind die unterschiedlichen Eingriffsmaßnahmen – mit unterschiedlicher Eingriffsintensität – ggf. anderes zu bewerten. Als Rahmen lässt sich festhalten:

- Bei jeder Maßnahme hängt deren Verfassungsmäßigkeit von einer Feststellung der Intensität und Intimität der beobachteten Kommunikation ab.

- Bei bestimmten Privaträumen – anders als bei Geschäftsräumen – spricht eine Vermutung für die durch die Menschenwürde geschützte Intimsphäre und damit gegen die Verfassungsmäßigkeit akustischer Maßnahmen.

- Dasselbe gilt, wenn der Betroffene allein oder mit einem „privilegierten“ Kommunikationspartner (Ehepartner, Kinder, Geschwister aber auch Rechtsanwälte und Priester) sich im geschützten Raum der Privatwohnung aufhält.

4.1.3 Umsetzung durch den Gesetzgeber

Das BVerfG hat für die Neuregelung des Lauschangriffs in der StPO dem Gesetzgeber eine Frist bis zum 30. Juni 2005 gesetzt. Um diese Frist einhalten zu können, hat die Bundesregierung zunächst einen Gesetzentwurf vorgelegt, der sich auf den Bereich der Wohnraumüberwachung beschränkt.

Dieser löste eine ausführliche öffentliche Debatte aus. Dabei wurde die Notwendigkeit dieses Instrumentes zur Strafverfolgung ebenso thematisiert wie die Frage, ob alle vom BVerfG formulierten Anforderungen erfüllt seien. Schwerpunkt war dabei die Rolle der Berufsgeheimnisträger aber auch die Frage, ob und wie in der Praxis das Abhören/Aufzeichnen von Gesprächen, die dem Kernbereich der privaten Lebensführung zuzurechnen sind, gehandhabt werden soll.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich ebenfalls damit beschäftigt und in einer Entschließung vom 28./29. Oktober nochmals auf die Notwendigkeit einer sorgfältigen Umsetzung der Entscheidung hingewiesen (vgl. Ziff. 10.7*)*.

In Hessen finden sich die ersten Konsequenzen im HSOG für die akustische Wohnraumüberwachung und – soweit die Fragen der Benachrichtigung usw. betroffen sind – für alle verdeckten Erhebungsmethoden, da dieses Gesetz zum Zeitpunkt der Entscheidung gerade auch aus anderen Gründen überarbeitet wurde (zu den Details vgl. Ziff. 5.1.1).

4.2 Neues Telekommunikationsgesetz

Das neue Telekommunikationsgesetz bringt keine datenschutzrechtlichen Verbesserungen, sondern führt eher zur Absenkung des Datenschutzniveaus.

Am 26. Juni 2004 ist das neue Telekommunikationsgesetz (TKG) in Kraft getreten (BGBl. I S. 1190). Es ersetzt das Telekommunikationsgesetz vom 25. Juli 1996. Die Telekommunikations-Datenschutzverordnung vom 18. Dezember 2000 (BGBl. I S. 1740) wurde aufgehoben und in das TKG integriert. Datenschutzrechtlich bringt das neue Gesetz keine Verbesserungen, es führt eher zu einer Absenkung des Datenschutzniveaus. Wäre der Bundesgesetzgeber den Vorstellungen des Bundesrates ausnahmslos gefolgt, stünde es um den Datenschutz in der Telekommunikation allerdings schlechter. Dessen wiederholt erhobene Forderung nach Einführung einer Vorratsdatenspeicherung, gegen die sich sowohl die Datenschutzbeauftragten des Bundes und der Länder als auch die Wirtschaft gewandt haben, wurde vorerst nicht umgesetzt. Leider blieb die auch von den TK-Diensteanbietern und der Internetwirtschaft unterstützte Anregung der Datenschutzbeauftragten, die Datenschutzvorschriften aus dem Telekommunikationsgesetz auszugliedern und mit den Datenschutzbestimmungen für Tele- und Mediendienste in einem Gesetz zusammenzuführen, unberücksichtigt.

4.2.1 Vorratsdatenspeicherung

Der Bundesrat verlangt seit Jahren eine Vorratsspeicherung für Verkehrsdaten in der Telekommunikation und bei Tele- und Mediendiensten. Er möchte erreichen, dass für eine gewisse Zeit nachvollziehbar ist, wer wann mit wem telefoniert hat, wer wann welche E-Mails oder SMS abgeschickt oder erhalten hat und wer wann welche Seiten im Internet aufgerufen hat. Die Datenschutzbeauftragten des Bundes und der Länder sehen darin eine unverhältnismäßige Datenspeicherung. Alle Fraktionen im Bundestag haben die Forderungen des Bundesrates immer wieder abgelehnt. In seiner Stellungnahme zum Gesetzentwurf der Bundesregierung schlug der Bundesrat erneut vor, alle Anbieter von Telekommunikationsdiensten zu verpflichten, die Verkehrsdaten sechs Monate zu speichern, und bei Bedarf den Strafverfolgungs-, Gefahrenabwehr- und Sicherheitsbehörden zur Verfügung zu stellen (BTDrucks. 15/2316 S. 120 f.). Auch diesmal lehnte der Bundestag den Vorschlag ab. Im Vermittlungsausschuss von Bundestag und Bundesrat konnte sich der Bundesrat ebenfalls nicht durchsetzen. Damit bleibt es zunächst bei der Regelung, dass Anbieter von Telekommunikationsdiensten Verkehrsdaten maximal 6 Monate für Abrechnungszwecke speichern können. Die meisten Unternehmen schöpfen diesen Zeitrahmen jedoch nicht aus.

Dennoch ist das Thema Vorratsdatenspeicherung damit keinesfalls erledigt. Im Gegenteil – über EU-Vorgaben könnte es auch in Deutschland zu einer Einführung dieses Instruments kommen. Nach dem Terroranschlag in Madrid im März 2004 haben Frankreich, Irland, Schweden und Großbritannien dem EU-Ministerrat den Entwurf eines Rahmenbeschlusses vorgelegt, der vorsieht, dass alle Anbieter von Telekommunikations- und Internetdiensten zur Speicherung sämtlicher Daten über Nutzer dieser Dienste für einen Zeitraum von mindestens einem Jahr verpflichtet werden können. (Entwurf eines Rahmenbeschlusses über die Vorratsspeicherung von Daten, die in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, oder von Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für die Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus vom 28. April 2004 – Ratsdokument 8958/04). Die Datenschutzbeauftragten des Bundes und der Länder haben in einer gemeinsamen Presseerklärung vom 21. Juni 2004 die Bundesregierung aufgefordert, den Entwurf der vier EU-Mitgliedstaaten abzulehnen (siehe www.datenschutz.hessen.de).
Gegenüber der Europäischen Kommission hat der Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Stellungnahme vom 8. September 2004 im Rahmen der von der EU-Kommission durchgeführten öffentlichen Konsultation zur Speicherung von Verkehrsdaten (European Commission's DG InfSo – DG JAI consultation document, July 30th, 2004) die Vorratsdatenspeicherung kritisiert.

4.2.2 Vorausbezahlte (Prepaid-)Karten

Durchsetzen konnte sich der Bundesrat dagegen mit seiner Forderung, die Mobilfunkdiensteanbieter zu verpflichten, auch von Kunden, die ein Gerät mit vorausbezahlter Karte erworben haben, Rufnummer, Namen und Anschrift des Rufnummerninhabers, Datum des Vertragsbeginns und Geburtsdatum zu erheben und den Sicherheits- und Strafverfolgungsbehörden im Rahmen ihrer strafprozessualen, polizei- und sicherheitsgesetzlichen Befugnisse zugänglich zu machen. Der Bundesrat reagierte damit auf ein Urteil des Bundesverwaltungsgerichts vom 22. Oktober 2003 (Az. 6 C 23.02). Das Gericht hatte entschieden, dass die Anbieter von vorausbezahlten Karten nicht verpflichtet seien, personenbezogene Daten ihrer Kunden zu erheben und in eine Kundendatei einzustellen, da diese Daten für die Begründung und Abwicklung des Vertragsverhältnisses nicht erforderlich seien. Der Gesetzgeber hat nunmehr angeordnet, dass Anbieter von Prepaid-Produkten künftig diese Daten allein für Sicherheits- und Strafverfolgungszwecke erheben und speichern müssen. Eine Nacherhebung für beim Inkrafttreten des TKG bereits bestehende Vertragsverhältnisse ist allerdings nicht vorgeschrieben.

Ob diese Maßnahme geeignet und erforderlich ist, um das von den Sicherheits- und Strafverfolgungsbehörden beklagte Problem, Nutzer von Mobilfunkgeräten nicht identifizieren zu können, zu beheben, darf bezweifelt werden. Für Straftäter gibt es jedenfalls genügend Ausweichstrategien, um sich einer Identifizierung zu entziehen.

4.2.3 Inverssuche

Das Verbot der Inverssuche wird durch das neue TKG aufgehoben. Auskunftsdienste durften bislang nur Telefonnummer und Anschrift zum Namen eines Teilnehmers mitteilen. Künftig kann man bei der Auskunft zu einer Telefonnummer auch Name und Anschrift des Teilnehmers erfragen. Anders als die Werbung mancher Diensteanbieter suggeriert, ist diese Inverssuche freilich nicht uneingeschränkt erlaubt. Sie ist nur zulässig, wenn der Teilnehmer im Telefonbuch oder einem öffentlichen elektronischen Kundenverzeichnis eingetragen ist und der Möglichkeit der Inverssuche nicht widersprochen hat. Sein TK-Diensteanbieter muss ihn auf das Widerspruchsrecht hinweisen. Der Widerspruch ist nicht fristgebunden, er kann jederzeit erklärt werden. Der Auskunftsdienst darf Anfragenden nur die in den Telefonbüchern und öffentlichen elektronischen Kundenverzeichnissen enthaltenen Daten mitteilen.

4.2.4 Überwachung

Das neue TKG verpflichtet Betreiber einer Telekommunikationsanlage, mit der Telekommunikationsdienste für die Öffentlichkeit erbracht werden, technische Einrichtungen zur Umsetzung gesetzlich vorgesehener Überwachungsmaßnahmen vorzuhalten. Die Einschränkung dieser Verpflichtung auf Betreiber von TK-Anlagen, mit der Dienste für die Öffentlichkeit erbracht werden, geht nicht zuletzt auf die Kritik der Datenschutzbeauftragten zurück. Im Gesetzentwurf der Bundesregierung war sie nicht vorgesehen. Ohne diese Einschränkung hätten sämtliche Betreiber von Nebenstellenanlagen in Behörden und Betrieben, die den Mitarbeitern die private Nutzung gestatten oder im Fall von Hotels und Krankenhäusern, ihren Gästen bzw. Patienten die Nutzung der TK-Anlage anbieten, Abhöreinrichtungen installieren müssen.

Ausgeweitet wurde der Kreis der Stellen, die Zugriff auf die von TK-Diensteanbieter nach dem TKG zu führenden Kundendateien haben. Wer Telekommunikationsdienste für die Öffentlichkeit erbringt, hat Kundendateien zu führen, in denen u. a. Rufnummern, Name und Anschrift des Rufnummerninhabers, Datum des Vertragsbeginns und Geburtsdatum der Kunden einzutragen sind. Auf diese Dateien kann eine Vielzahl von Stellen zugreifen. Der Zugriff erfolgt über die Regulierungsbehörde für Telekommunikation und Post, die die Daten aus den Kundendateien abruft. Die Diensteanbieter müssen durch technische und organisatorische Maßnahmen sicherstellen, dass ihnen die Abrufe nicht zur Kenntnis gelangen können. Auf die Dateien konnten bislang Gerichte und Strafverfolgungsbehörden, Polizeibehörden des Bundes und der Länder, Zollbehörden, Verfassungsschutzbehörden, MAD und BND zugreifen. Hinzugekommen sind durch die TKG-Novellierung Notrufabfragestellen, die Bundesanstalt für Finanzdienstleistungsaufsicht und die für die Verfolgung und Ahndung von Schwarzarbeit zuständigen Stellen der Länder.

Das TKG räumt den Strafverfolgungsbehörden, der Polizei und den Nachrichtendiensten einen relativ unbeschränkten Zugriff auf solche Daten ein, mittels derer der Zugriff auf andere Daten geschützt wird. Dazu gehören z. B. die Passwörter, die PIN (Personal Identification Number) und der PUK (Personal Unblocking Key), mit dessen Hilfe sich eine Kartensperre nach dreimaliger Falscheingabe der PIN wieder aufheben lässt. Der Forderung des Bundesrates, den Kreis der Zugriffsberechtigten um die Hauptzollämter und Finanzämter zu erweitern, ist der Bundesgesetzgeber nicht gefolgt. Die Kritik der Datenschutzbeauftragten wendet sich dagegen, dass hier ohne Bindung an einen Straftatenkatalog und ohne Richtervorbehalt die Behörden im Rahmen ihrer allgemeinen Ermittlungsbefugnisse von den Telekommunikationsunternehmen Auskunft über diese Daten verlangen können.

5. Land

5.1 Polizei und Strafverfolgung

5.1.1 Novellierung im Polizeirecht

Im Rahmen der diesjährigen Novellierung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung erfolgten eine Vielzahl von Änderungen mit zum Teil weit reichenden neuen Eingriffsbefugnissen für die Polizei.

5.1.1.1 Überblick

Schon seit dem vergangenen Jahr lagen erste Entwürfe vor, das Hessische Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) um neue Eingriffsbefugnisse zu ergänzen. Darin enthalten waren u. a. – soweit das Recht auf informationelle Selbstbestimmung betroffen war – Regelungen zur automatisierten Kennzeichenerkennung, Änderungen im Bereich des Einsatzes von Videoüberwachungsmaßnahmen, die präventive Überwachung des Telekommunikationsverkehrs und der Einsatz der DNA-Analyse bei Kindern. Nach den Entscheidungen des Bundesverfassungsgerichtes vom 3. März 2004 zur

akustischen Wohnraumüberwachung und zum Außenwirtschaftsgesetz wurde der Entwurf nochmals überarbeitet, um die notwendigen Folgerungen für das Polizeirecht aus diesen Entscheidungen zu treffen (vgl. auch Ziff. 4.1).

Die Änderungen sind zum 1. Januar 2005 in Kraft getreten. Nicht in allen Bereichen sind die aus meiner Sicht notwendigen Überarbeitungen – die in weiten Teilen auch bei einer Anhörung vor dem Innenausschuss des Hessischen Landtages durch verschiedene Experten geäußert worden waren – erfolgt.

5.1.1.2 Konsequenzen aus den Entscheidungen des Bundesverfassungsgerichtes vom 3. März 2004

Grundsätzlich begrüße ich es ausdrücklich, dass der Hessische Gesetzgeber für das Polizeirecht Konsequenzen aus den Entscheidungen des Bundesverfassungsgerichtes vom 3. März 2004 zu heimlichen Überwachungsmaßnahmen nach der Strafprozessordnung und dem Außenwirtschaftsgesetz nicht nur für den Bereich der Wohnraumüberwachung getroffen hat. Dabei fehlt zum Teil jedoch eine konsequente Umsetzung und die dafür im Gesetzgebungsverfahren genannten Begründungen sind rechtlich angreifbar.

5.1.1.2.1 Straftaten mit erheblicher Bedeutung

In einem wesentlichen Punkt ergibt sich durch die Neufassung des Gesetzes ein Rückschritt, der m. E. mit den verfassungsrechtlichen Vorgaben schwerlich zu vereinbaren ist. Das Gesetz definiert den Begriff der Straftat mit erheblicher Bedeutung neu.

§ 13 Abs. 3 HSOG

Straftaten mit erheblicher Bedeutung im Sinne dieses Gesetzes sind
1. *Verbrechen und*
2. *Vergehen, die im Einzelfall nach Art und Schwere geeignet sind, den Rechtsfrieden besonders zu stören, soweit sie*
   a. *sich gegen Leib, Leben oder Freiheit einer Person oder bedeutende Sach- oder Vermögenswerte richten,*
   b. *auf den Gebieten des unerlaubten Waffen- oder Betäubungsmittelverkehrs, der Geld- und Wertzeichenfälschung oder des Staatsschutzes (§§ 74a und 120 des Gerichtsverfassungsgesetzes) begangen werden oder*
   c. *gewerbs-, gewohnheits-, serien- oder bandenmäßig oder sonst organisiert begangen werden.*

In der Regel mag es sinnvoll sein, innerhalb eines Gesetzes einen einheitlichen Maßstab für die Verwendung von Begriffen wie den einer „Straftat mit erheblicher Bedeutung“ durch eine Legaldefinition vorzugeben. Allerdings ergeben sich aus einer Legaldefinition nicht unmittelbare Rechtsfolgen. Vielmehr muss dann bei den einzelnen Normen, die die entsprechende Definition verwenden, sorgfältig geprüft werden, ob nicht zusätzlicher Regelungsbedarf besteht. Auch „Straftaten mit erheblicher Bedeutung“ rechtfertigen daher im Geltungsbereich des HSOG nicht automatisch jeden Grundrechtseingriff. Je erheblicher der Grundrechtseingriff ist, desto erheblicher muss vielmehr die den Eingriff legitimierende Straftat sein.

Diese, schon aus dem Grundsatz der Verhältnismäßigkeit folgende, Proportionalregel gilt aus meiner Sicht mindestens für die akustische Wohnraumüberwachung, aber auch für die präventive Telekommunikationsüberwachung.

Das BVerfG hat für den Lauschangriff im repressiven Bereich dargelegt, dass aus verfassungsrechtlichen Gründen die Anwendung auf solche Straftaten zu beschränken ist, die jedenfalls mit einer höheren Freiheitsstrafe als fünf Jahre bewehrt sind. Zwar folgt bereits aus dem Gesetzeswortlaut, dass die Anforderungen an den Einsatz des Lauschangriffes im präventiven Bereich gemäß Art. 13 Abs. 4 GG mit dem Einsatz im repressiven Bereich gemäß Art. 13 Abs. 3 GG nicht völlig deckungsgleich sind.

Art. 13 Abs. 3 und 4 GG

(3) Begründen bestimmte Tatsachen den Verdacht, dass jemand eine durch Gesetz einzeln bestimmte besonders schwere Straftat begangen hat, so dürfen zur Verfolgung der Tat auf Grund richterlicher Anordnung technische Mittel zur akustischen Überwachung von Wohnungen, in denen der Beschuldigte sich vermutlich aufhält, eingesetzt werden, wenn die Erforschung des Sachverhalts auf andere Weise unverhältnismäßig erschwert oder aussichtslos wäre. Die Maßnahme ist zu befristen. Die Anordnung erfolgt durch einen mit drei Richtern besetzten Spruchkörper. Bei Gefahr im Verzuge kann sie auch durch einen einzelnen Richter getroffen werden.

(4) Zur Abwehr dringender Gefahren für die öffentliche Sicherheit, insbesondere einer gemeinen Gefahr oder einer Lebensgefahr, dürfen technische Mittel zur Überwachung von Wohnungen nur auf Grund richterlicher Anordnung eingesetzt werden. Bei Gefahr im Verzuge kann die Maßnahme auch durch eine andere gesetzlich bestimmte Stelle angeordnet werden; eine richterliche Entscheidung ist unverzüglich nachzuholen.

Andererseits ist nach Art. 13 Abs. 4 GG der Einsatz nur zur Abwehr dringender Gefahren, insbesondere einer gemeinen Gefahr oder Lebensgefahr zulässig. Daraus ergibt sich der Wille des verfassungsändernden Gesetzgebers, dass diese dringende Gefahr eine drohende Beeinträchtigung für hochrangige Rechtsgüter voraussetzen muss. Diese Schwelle wird sich nicht allein auf die Androhung einer mehr als fünfjährigen Freiheitsstrafe – so wie dies das BVerfG für die repressive Wohnraumüberwachung ausspricht – beziehen lassen. Insoweit ist – schon durch den Gesetzgeber – eine Abwägung zu treffen zwischen den durch Art. 13 GG geschützten Rechtsgütern und den besonders hochrangigen Schutzgütern, die den Anforderungen einer dringenden Gefahr im Sinne des Art. 13 Abs. 4 GG genügen. Bei dieser Abwägung steht dem Gesetzgeber ein Gestaltungsspielraum zu, den er freilich auch nutzen muss. Das ist bislang nicht in hinreichender Weise geschehen. Insbesondere wird nach meiner Einschätzung die nunmehr in § 13 Abs. 3 HSOG getroffene Definition – die u. a. alle Verbrechen allein anknüpfend an das Mindeststrafmaß (1 Jahr) gemäß § 12 StGB umfasst – nicht gerecht. Hier wäre – ausgehend vom bislang definierten Katalog – eine entsprechende Abwägungsentscheidung durch den Gesetzgeber vorzunehmen. Es kann nicht der Entscheidung der Polizei vor dem jeweiligen konkreten Einsatz überlassen bleiben, ob die Einsatzschwelle des Instrumentariums wirklich erreicht ist. Für eine Abwägung, wie diese Schwelle zu definieren ist, wäre dies auf jeden Fall nicht der geeignete Zeitpunkt. In einer konkreten Gefahrensituation muss sich im Sinne des Verhältnismäßigkeitsprinzips die Entscheidung aus den Vorgaben des Gesetzgebers für Eingriffe in Grundrechte direkt ableiten lassen.

5.1.1.2.2 Akustische Wohraumüberwachung

Als Reaktion auf die Entscheidungen des BVerfG spricht das HSOG für Erkenntnisse aus dem Bereich privater Lebensgestaltung ein Verwertungsverbot aus. Das ist in dieser Form ebenfalls nicht ausreichend.

Das BVerfG hat ausgeführt, dass dem Einzelnen ein unantastbarer Bereich privater Lebensführung zusteht, der der öffentlichen Gewalt entzogen ist. Dies gilt auch für den Einsatz der präventiven Wohnraumüberwachung. Anderseits sind Gespräche, die unmittelbaren Bezug zu der abzuwehrenden Gefahr aufweisen, nie diesem Kernbereich zuzuordnen, unabhängig vom Gesprächspartner oder Ort des geführten Gesprächs. Soweit der Kernbereich betroffen ist, hat das BVerfG für die repressive Wohnraumüberwachung ein absolutes Erhebungsverbot ausgesprochen. Ein Verwertungsverbot greift nur insoweit, als im Einzelfall doch solche Gespräche erfasst worden sind.

Die Gesetzesbegründung (LTDrucks. 16/2353 S. 17) tritt insoweit zu, als der Kernbereich des Störers nicht betroffen sein kann, soweit der Störer in die geschützte Sphäre eines anderen eingreift. Allerdings wird sich nicht jede Äußerung/jedes Gespräch während einer laufenden Überwachungsmaßnahme des dabei Betroffenen auf die abzuwehrende Gefahr beziehen, so dass auch beim Einsatz der Wohnraumüberwachung im präventiven Bereich die Anforderungen des BVerfG zum Schutz des Kernbereichs privater Lebensführung entsprechend anzuwenden sind. Das gilt erst recht, soweit es sich um Gespräche anderer Betroffener in der überwachten Wohnung ohne direkte Beteiligung des zu überwachenden Störers handelt. Für solche müsste sowohl die Erhebung als auch die Aufzeichnung verhindert werden.

5.1.1.2.3 Präventive Telekommunikationsüberwachung

Nunmehr ist der Polizei auch präventiv ein Eingriff in das Telekommunikationsgeheimnis des Art. 10 GG möglich. Im Gegensatz zu einigen anderen Bundesländern erfolgt allerdings eine Beschränkung dieses Instrumentes auf Fälle der Gefahrenabwehr.

§ 15a HSOG

(1) Die Polizeibehörden können von einem Dienstanbieter, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, verlangen, dass er die Kenntnisnahme des Inhalts der Telekommunikation ermöglicht und die näheren Umstände der Telekommunikation einschließlich des Standorts aktiv geschalteter nicht ortsfester Telekommunikationsanlagen übermittelt, wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person unerlässlich ist.

Insoweit entspricht die Eingriffsschwelle der des Lauschangriffes in § 15 Abs. 4 HSOG. Neben dem Auskunftsanspruch gegenüber den Providern auf Inhalt und Umstände der Telekommunikation kann die Polizei zudem mit Hilfe des sog. IMSI-Catchers den Standort von Handys ermitteln lassen. Dies soll ausweislich der Gesetzesbegründung vor allem zum Auffinden von Personen eingesetzt werden, die über ein Handy den bevorstehenden Suizid angekündigt haben.
Diese Maßnahmen stehen außer bei Gefahr im Verzug unter einem Richtervorbehalt.

Zu kritisieren ist jedoch das Fehlen von Regelungen, die den Kernbereich privater Lebensführung schützen. Insoweit ist die Gesetzesbegründung – die allein auf Erkenntnisse abstellt, die die besondere Gefahr begründen (LTDrucks. 16/2352 S. 20) – nicht überzeugend. Bei der präventiven Wohnraumüberwachung, für die die gleiche Eingriffsschwelle gilt und zu der in der Begründung auch mehrmals Parallelen gezogen werden, hat der Gesetzgeber solche Regelungen geschaffen. Geschützt werden müssen Gespräche, die keinen Bezug zu der abzuwehrenden Gefahr haben. Da nicht sichergestellt werden kann, dass die Überwachung immer direkt erfolgt, sondern auch Gespräche aufgenommen werden, um sie (alsbald)

auszuwerten, muss es Regelungen geben, die diesen Kernbereich schützen. Zu beachten ist dabei, dass auch Nichtstörer Inhaber der überwachten Anschlüsse sein können und von den Überwachungsmaßnahmen insbesondere auch die Gesprächspartner betroffen sind.

5.1.1.2.4 Kennzeichnung und weitere Verwendung mittels verdeckter Datenerhebung erlangter Daten

Nach der Novellierung werden nunmehr alle die Daten, die durch einen Eingriff in das Telekommunikationsgeheimnis oder durch Maßnahmen der Wohnraumüberwachung erhoben werden einer besonderen Kennzeichnungspflicht unterworfen. Für die weitere Verwendung dieser Daten, insbesondere die Übermittlung an andere Stellen ist der vom Gesetz gesteckte Rahmen jedoch zu weit.

§ 21 Abs. 3 Satz 3 HSOG

Personenbezogene Daten, die nach § 20 Abs. 6 Satz 2 zu kennzeichnen sind, dürfen nur übermittelt werden, wenn dies zur Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist.

Durch die Kennzeichnung soll sichergestellt werden, dass eine weitere Verwendung nur unter den gleichen Einschränkungen erfolgen kann wie die Erhebung der Daten selbst. So verlangt § 15a HSOG für die dort vorgesehenen Eingriffe in das Telekommunikationsgeheimnis einschließlich der Verwertung von Zufallsfunden, dass dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person unerlässlich ist. Dann muss dies auch für Übermittlungen im Rahmen des § 21 Abs. 3 HSOG gelten, und zwar grundsätzlich für jegliche gekennzeichneten Daten, unabhängig von der konkreten Erhebung.

5.1.1.2.5 Rechte der Betroffenen

Die Neufassung dieser Vorschriften ist im Wesentlichen gelungen. Im Interesse der betroffenen Bürgerinnen und Bürger ist es auch zu begrüßen, dass die entsprechenden Regelungen nunmehr für alle Formen der verdeckten Datenerhebung und der Rasterfahndung identisch sind. Das Verfahren bei der Zurückstellung der Benachrichtigung halte ich in dieser Form allerdings nicht für ausreichend, um den Anforderungen der Verfassung in vollem Umfang Genüge zu tun. Hier sieht das Gesetz zwar die Unterrichtung des Hessischen Datenschutzbeauftragten nicht aber die Kontrolle durch einen Richter vor.

Das BVerfG hat für die Zurückstellung der Benachrichtigung eine gerichtliche Kontrolle gefordert. Grund ist die Gewährleistung eines effektiven Rechtsschutzes (Art. 19 Abs. 4 GG). Unterschiedliche Anforderungen für Maßnahmen im repressiven oder präventiven Bereich sind nicht ersichtlich. Zwar ist der Landesdatenschutzbeauftragte ebenfalls eine unabhängige Instanz. Seine Möglichkeiten sind mit einer Rechtsschutzgewährung durch die Gerichte aber nicht zu vergleichen. Da die entsprechenden Maßnahmen insbesondere die Wohnraumüberwachung und die Eingriffe in das Telekommunikationsgeheimnis – außer bei Gefahr im Verzuge – ebenso wie im repressiven Bereich auch einer richterlichen Anordnung bedürfen, ist mir ein sachlicher Grund für eine unterschiedliche Behandlung im Rahmen der Zurückstellung der Benachrichtigung nicht erkennbar.

5.1.1.3 DNA-Identifizierungsmuster von Kindern

Einen völlig neuen Weg geht das HSOG mit der Ermöglichung des Einsatzes der DNA-Analyse für strafunmündige Kinder in § 19 Abs. 3 HSOG. Damit sollen vor allem Kinder erfasst werden, die bandenmäßig oder organisiert Straftaten begehen. Die Analyse soll es ermöglichen, Spuren von Tatorten beteiligten Kindern zuzuordnen (LTDrucks. 15/2352, S. 21).

§ 19 HSOG
Erkennungsdienstliche Maßnahmen, DNA-Analyse
…
(3) Ist eine noch nicht vierzehn Jahre alte Person verdächtig, eine Straftat mit erheblicher Bedeutung begangen zu haben, und besteht wegen der Art oder Ausführung der Tat die Gefahr, dass sie künftig eine Straftat mit erheblicher Bedeutung begehen wird, können die Polizeibehörden zu Zwecken der vorbeugenden Bekämpfung von Straftaten Körperzellen entnehmen. § 36 Abs. 5 Satz 2 bis 5 gilt entsprechend. Zur Feststellung des DNA-Identifizierungsmusters können die entnommenen Körperzellen molekulargenetisch untersucht werden. § 81f der Strafprozessordnung und § 36 Abs. 5 Satz 3 gelten entsprechend. Die entnommenen Körperzellen sind unverzüglich nach der Analyse zu vernichten, es sei denn, ihre weitere Aufbewahrung ist nach anderen Rechtsvorschriften zulässig.

Dabei wird übersehen, dass Kinder – da nicht strafmündig – keine Straftat begehen können.

Ich habe schon in unterschiedlichen Zusammenhängen darauf hingewiesen, dass die DNA-Analyse aus meiner Sicht nicht kurzerhand mit den klassischen erkennungsdienstlichen Maßnahmen gleichzusetzen ist. Schon im Laufe des Gesetzgebungsverfahrens habe ich deshalb mehrmals meine erheblichen Bedenken geäußert.

Zunächst stellt sich allerdings die Frage, ob hier überhaupt eine Gesetzgebungskompetenz des Landes gegeben ist. Soweit diese Maßnahme den Zwecken des Erkennungsdienstes dient und damit der Erforschung und Aufklärung von Straftaten, ist die Regelung der StPO abschließend. Das Landesrecht kann nicht zum Lückenschluss der StPO herangezogen werden, mögen solche Lücken auch kriminalpolitisch zu bedauern sein. Im Landesrecht kann es somit Regelungen nur für Fälle geben, in denen nicht Beschuldigte im Zusammenhang mit einem möglichen Strafverfahren betroffen sind. Strafmündige Kinder fallen zwar nicht unter diesen Personenkreis. Gleichwohl ergeben sich kompetenzrechtliche Bedenken, weil die Strafunmündigkeit auf einer Entscheidung des Bundesgesetzgebers beruht. Da sie nie Beschuldigte in einem Strafverfahren sein können, würde es einen Wertungswiderspruch bedeuten, wenn gerade deshalb auf sie die verschärften Normen des Polizeirechts anwendbar sein sollen. Die Anknüpfung des § 19 Abs. 3 HSOG an „Verdächtige einer Straftat“ ist daher kompetenzrechtlich problematisch. Darüber hinaus stellt sich die Datenerhebung bei strafunmündigen Kindern im Rahmen der vorbeugenden Verbrechensbekämpfung als ein Mittel mit generalpräventiver Wirkung dar. Damit werden gegenüber Kindern intensivere Mittel eingesetzt als im Jugendstrafrecht, wo die Generalprävention keinen zulässigen Sanktionszweck darstellt.

Ordnet man gleichwohl die Maßnahmen der polizeilichen Aufgabenstellung der Gefahrenabwehr zu, ist zweifelhaft ob die DNA-Analyse, die nicht mit den klassischen erkennungsdienstlichen Maßnahmen gleichgesetzt werden kann, mit dem Grundsatz der Verhältnismäßigkeit vereinbar ist. Denn dann bleibt immer noch die Tatsache, dass DNA-Analysen bei Strafmündigen nur nach den strengeren Maßstäben der StPO für tatsächlich einer Straftat Verdächtige durchgeführt werden dürfen, während die weitergehenden Regelungen des HSOG nur für Kinder gelten.

Darüber hinaus habe ich erhebliche Zweifel, ob diese Norm in der Praxis sinnvoll umgesetzt werden kann. Es ist zwar geregelt, wie die Körperzellen zu behandeln sind und in welchem Verfahren die Auswertung erfolgen soll. Es fehlen aber Regelungen, wie die dann gefundenen Ergebnisse – das DNA-Muster – weiter verwendet werden dürfen bzw. wo sie zu speichern sind. Der Verweis auf die Behandlung erkennungsdienstlicher Unterlagen erscheint mir nicht ausreichend, weil schon die Begründung darauf verweist, dass eine Speicherung im Rahmen der DNA-Datenbank beim BKA, die Grundlage des Einsatzes dieses Instrumentariums auch für zukünftige Sachverhalte ist, aus rechtlichen Gründen nicht erfolgen darf.

5.1.1.4 Kennzeichenerfassung

Wie unter Ziff. 5.1.2 beschrieben, beschränkt sich die Neuregelung in § 14 Abs. 5 HSOG auf die Erhebungsbefugnis zum Zwecke des Abgleichs mit den Fahndungsdateien. Diese Befugnis darf dann zur Anwendung kommen – wie jede Ermittlungsmaßnahme – wenn der Grundsatz der Verhältnismäßigkeit gewahrt wird. Nach der Begründung des Gesetzes (LTDrucks. 16/2352 S. 15) soll das Instrumentarium vor allem eingesetzt werden, um polizeiliche Kontrollen zu effektivieren. In der Begründung wird auf den Sachfahndungsbestand als Abgleichsdatei verwiesen. Der Gesetzestext lässt jedoch auch einen Abgleich mit anderen Fahndungsdateien zu, soweit in diesen (auch) Kfz-Kennzeichen enthalten sind. Daher wird die zukünftige Praxis sorgfältig zu beobachten sein.

Dies gilt verstärkt auch für die technische Ausgestaltung der einzusetzenden Überwachungsgeräte. Da das Gesetz nur vorschreibt, dass Daten, die nicht im Fahndungsbestand enthalten sind, unverzüglich zu löschen sind, bleiben für die konkrete Ausgestaltung einige Fragen offen. Nicht in allen denkbaren Varianten geschieht die Löschung so schnell wie im beschriebenen Modellversuch, d. h. durch Überschreiben durch das jeweils nächste erkannte Kennzeichen.

5.1.1.5 Online-Zugriff der Gefahrenabwehrbehörden

Im HSOG gibt es detaillierte Regelungen zum Informationsaustausch innerhalb der Polizei und zu den Gefahrenabwehrbehörden. Bisher war jedoch ein direkter Zugriff auf die Dateien der Polizei nur für (andere) Polizeibehörden zulässig. Mit der Neuregelung ist vor allem angestrebt, dass in bestimmten Konstellationen auch Gefahrenabwehrbehörden einen Online-Zugriff haben können. Vorgesehen ist dies hauptsächlich im Bereich von Zuverlässigkeitsüberprüfungen. Dabei soll eine Beschränkung auf die erforderlichen Datenzugriffe vor allem dadurch gewährleistet sein, dass der Zugriff nur eine Negativauskunft zulässt. Sind bei der Polizei Daten zur abgefragten Person vorhanden, muss wie bisher eine Anfrage erfolgen, die von der Polizei beantwortet wird, nachdem sie bewertet hat, welche davon konkret für die anfragende Behörde erforderlich sind.

Nach der Neufassung ist ein solcher Zugriff auch erlaubt für die Polizeischule bzw. die Verwaltungsfachhochschule. Nach der Begründung sollen diese Zugriffsmöglichkeiten die Ausbildung mit dem in der Polizei zum Einsatz kommenden Instrumentarium ermöglichen. Zwar ist grundsätzlich auch die Verarbeitung von Daten zu Zwecken der Aus- und Fortbildung zulässig, § 20 Abs. 7 HSOG.

§ 20 Abs. 7 HSOG

Die Polizeibehörden, die Polizeieinrichtung und die Verwaltungsfachhochschule können gespeicherte personenbezogene Daten zur polizeilichen Aus- oder Fortbildung oder zu statistischen Zwecken verarbeiten. Die Daten sind zum frühestmöglichen Zeitpunkt zu anonymisieren. Abs. 1 bis 6 finden insoweit keine Anwendung.

Im Gesetzgebungsverfahren habe ich jedoch Bedenken geäußert, dass im Rahmen des § 24 Abs. 1 der Neufassung keinerlei Beschränkungen oder Rahmenbedingungen zur Wahrung des Grundsatzes der Erforderlichkeit formuliert worden sind. Die zulässige Verwendung von personenbezogenen Daten gemäß § 20 Abs. 7 HSOG, wie sie in der Begründung angeführt ist, kann nicht Grundlage eines jederzeitigen umfassenden Zugriffs auf alle Datenbestände sein. Beschränkungen sind aber im Gegensatz zum Zugriff der Gefahrenabwehrbehörden aus der Norm selbst nicht ersichtlich.

5.1.2 Automatisierte Kennzeichenerkennung

Der Einsatz von Kennzeichenlesegeräten stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung dar, der nur bei sorgfältiger Abwägung und Beachtung des Verhältnismäßigkeitsprinzips zulässig ist.

5.1.2.1 Möglichkeiten der Technik

Versuche, im fließenden Verkehr Kfz-Kennzeichen mit digitalen Kameras aufzunehmen und mit vorhandenen Datenbeständen abzugleichen, gibt es seit einiger Zeit. Als mögliches Anwendungsfeld wurde dazu u. a. die Feststellung von Lenkzeitverstößen bei Bussen oder LKW genannt. Aber auch als Hilfsinstrument im Rahmen von Fahndungsmaßnahmen sollen entsprechende Instrumente eingesetzt werden. Zu diesem Thema gab es in den letzten Jahren mehrmals Gespräche zwischen meinen Mitarbeitern und Vertretern der Polizei, um die rechtlichen Rahmenbedingungen für solche Versuche abzustecken.

Im Herbst 2003 fand dann auch ein solcher Versuch statt, um die Leistungsfähigkeit der Technik, insbesondere die Zuverlässigkeit bei der Erkennung der Kennzeichen zu erproben. Dazu wurde am Elzer Berg eine Kamera montiert. Diese war mit einem Geschwindigkeitsmessgerät gekoppelt und nahm die Kennzeichen der Fahrzeuge auf, die die dort geltenden Geschwindigkeitsbegrenzungen nicht eingehalten hatten. Die aufgenommenen Kennzeichen wurden in einem PC mit einer Kopie der bundesweiten Sachfahndungsdatei abgeglichen. Zusätzlich waren auch einige Beamte mit ihren privaten Fahrzeugen sowie Dienstfahrzeugen an diesen Versuchen beteiligt. Die Abgleichsdatei war ergänzt um die entsprechenden Kennzeichen. Ergab sich dabei ein Treffer, wurde eine Meldung erzeugt, die im Echteinsatz z. B. an die nächste Autobahnpolizeistation übertragen werden könnte. Dort würde dann ein Alarm ausgelöst.

Kennzeichen, für die es keinen Treffer in der Abgleichsdatei gab, wurden sofort vom nächsten aufgenommenen Kennzeichen überschrieben.

Grundsätzlich bewegte sich dieser Versuch in einem zulässigen Rahmen, da er die Erfassung der Kennzeichen auf die Fahrzeuge mit einer Geschwindigkeitsübertretung beschränkte. Diese Daten wurden im Zusammenhang mit den Ordnungswidrigkeiten – Geschwindigkeitsverstöße – erhoben und durften gemäß § 25 Abs. 1 HSOG dann von der Polizei im Rahmen ihrer Aufgaben verwendet werden. Deshalb war ein Abgleich mit dem Fahndungsbestand zulässig.

§ 25 Abs. 1 Satz 3 HSOG

Die Polizeibehörden können ferner im Rahmen ihrer Aufgabenerfüllung erlangte personenbezogene Daten mit dem Fahndungsbestand abgleichen.

5.1.2.2 Eingriff in das Recht auf informationelle Selbstbestimmung

Gleichwohl ist die Zulässigkeit des Einsatzes solcher Lesegeräte unter dem Gesichtpunkt des Eingriffs in das Recht auf informationelle Selbstbestimmung umstritten. Wenn die Kennzeichen aller Fahrzeuge, die an dem Erfassungsgerät vorbeifahren, anlassfrei ausgelesen und – wie lange auch immer – gespeichert werden, stellt sich die Frage der Verhältnismäßigkeit des Eingriffes. Einerseits kann diese Erfassung dazu führen, dass gesuchte Fahrzeuge gefunden werden, anderseits wird eine Vielzahl von Verkehrsteilnehmern erfasst, ohne dass sie dazu Veranlassung geben.

Um den Anforderungen des Verhältnismäßigkeitsprinzips gerecht zu werden, muss der Einsatz der Kennzeichenerfassung an Rahmenbedingungen geknüpft werden. Dazu gehören der Ausschluss von Bewegungsprofilen und die Verhinderung der Speicherung von Daten über unverdächtige Personen. In diesem Sinne hat sich auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder geäußert (vgl. dazu Ziff. 10.4).

5.1.2.3 Schaffung einer Rechtsgrundlage im hessischen Polizeirecht

Um den Einsatz solcher Lesegeräte zu ermöglichen, hat die Landesregierung eine Änderung des HSOG vorgeschlagen. Dabei hat sie sich darauf beschränkt, eine Erhebungsnorm zu schaffen, die lediglich den Zweck der Erhebung – einen Abgleich mit dem Fahndungsbestand – sowie die Anordnung der unverzüglichen Löschung der Daten, die nicht Bestandteil der Fahndungsdatei sind, enthält. Entsprechend den obigen Ausführungen habe ich gegen eine solche Regelung keine grundsätzlichen Bedenken geltend gemacht. Weitere Details zur Regelung siehe unter Ziff. 5.1.1.4.

5.1.3 Prüfung polizeilicher Datenbestände bei den Polizeipräsidien Südhessen und Frankfurt am Main

Eine Prüfung bei den Polizeipräsidien Südhessen und Frankfurt, ob Hinweise in den polizeilichen Informationssammlungen auf Betäubungsmittelkonsum rechtmäßig vergeben wurden, ergab keine Beanstandung.

Die Datensätze in den polizeilichen Informationssammlungen enthalten nicht nur die Personalien von Personen, die verdächtigt werden, Straftaten begangen zu haben und Angaben zu den jeweils zugehörigen Kriminalfällen, sie enthalten auch so genannte personengebundene Hinweise. Solche personengebundenen Hinweise dienen u. a. der Eigensicherung der einschreitenden Beamten, der Einleitung gezielter Fahndungsmaßnahmen und der Unterstützung der Ermittlungen. Sie lauten z. B. „Bewaffnet“, „Gewalttätig“ oder „BtM-Konsument“ (Betäubungsmittel-Konsument). Die Hinweise sind Bestandteil des jeweiligen Verfahrensverzeichnisses nach § 28 HSOG. Soweit sie im Einzelfall zutreffend sind, ist ihre Speicherung zur Aufgabenerfüllung der Polizei erforderlich und damit von § 20 Abs. 1 HSOG – der allgemeinen Zulässigkeitsnorm für die Datenspeicherungen der Polizei – erfasst.

§ 20 Abs. 1 HSOG

Die Gefahrenabwehr und Polizeibehörden können erhobene personenbezogene Daten speichern oder sonst verarbeiten, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. …

Ein anderer Landesdatenschutzbeauftragter hatte festgestellt, in seinem Bundesland werde u. a. der personengebundene Hinweis „BtM-Konsument“ leichtfertig vergeben. Ziel meiner Prüfung war es festzustellen, ob der dort beschriebene Mangel auch in Hessen besteht. Ich bat das Präsidium für Technik, Logistik und Verwaltung der hessischen Polizei um eine Auswertung der Datenbank POLAS. Ausgewählt wurden alle Datensätze, in denen u. a. der personenbezogene Hinweis „BtM-Konsument“ gespeichert war.
Aus der so entstandenen und nach Polizeipräsidien sortierten Liste nahm ich eine Stichprobe von 100 Fällen. Bei 40 Datensätzen des Polizeipräsidiums Südhessen und 60 des Polizeipräsidiums Frankfurt prüften meine Mitarbeiter die Rechtmäßigkeit der Vergabe des personengebundenen Hinweises. Das Ergebnis war eindeutig: Nur in einem dieser 100 Einzelfälle konnte ich mich mit dem Polizeipräsidium Südhessen nicht einigen, ob die Vergabe des Hinweises rechtmäßig war. Meiner Ansicht nach war nicht ausreichend gesichert, dass der Betroffene als „BtM-Konsument“ bezeichnet werden konnte. Das Polizeipräsidium Südhessen war anderer Ansicht. Letztlich habe ich die kriminalfachliche Beurteilung hingenommen. Alle anderen Fälle waren auch aus meiner Sicht nicht zu beanstanden; dort war der personengebundene Hinweis „BtM-Konsument“ auch aus meiner Sicht offensichtlich rechtmäßig. Ich gehe davon aus, dass das Ergebnis in den anderen hessischen Polizeipräsidien ähnlich ausfallen würde. Ein Vorwurf der leichtfertigen Vergabe dieses Hinweises kann in Hessen nicht erhoben werden.

5.1.4 Löschung polizeilicher Daten im Einzelfall

Datenspeicherungen bei der Polizei müssen im Einzelfall für die polizeiliche Aufgabenerfüllung erforderlich sein. Das ist auch bei der Festsetzung der Aufbewahrungsfrist zu beachten. Einem Betroffenen konnte ich erst nach Einschaltung der Aufsichtsbehörde zu seinem Recht verhelfen.

Ein hessischer Bürger erlangte davon Kenntnis, dass die Polizei Daten zu seiner Person gespeichert hatte. Auf seine Frage, wie er Näheres dazu in Erfahrung bringen könne, wies ich ihn auf sein Auskunftsrecht nach § 29 Abs. 1 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) hin.

§ 29 Abs. 1 HSOG

Der betroffenen Person ist auf Antrag gebührenfrei Auskunft zu erteilen über

1. die zu ihrer Person gespeicherten Daten,

2. die Herkunft der Daten und die Empfängerinnen oder die Empfänger von Übermittlungen, soweit dies festgehalten ist,

3. den Zweck und die Rechtsgrundlage der Speicherung und sonstigen Verarbeitung.

In dem Antrag soll die Art der Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Bei einem Antrag auf Auskunft aus Akten kann erforderlichenfalls verlangt werden, dass Angaben gemacht werden, die das Auffinden der Daten ohne einen Aufwand ermöglichen, der außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse steht. Kommt die betroffene Person dem Verlangen nicht nach, kann der Antrag abgelehnt werden.

Als bereichspezifische Vorschrift für das Polizeirecht geht diese Vorschrift dem weitgehend identischen Auskunftsrecht im allgemeinen Datenschutzrecht in § 18 Abs. 3 HDSG bei Auskunftsverlangen an die Polizeibehörden des Landes vor. Nach einer polizeiinternen Regelung ist für solche Auskunftsverlangen das Landeskriminalamt (LKA) zuständig. Also empfahl ich dem Betroffenen sich dorthin zu wenden.

Die Auskunft, die ihm auf seine Anfrage das LKA erteilte, umfasste eine Auflistung von 15 Ermittlungsverfahren, beginnend mit dem Jahr 1986 bis zu einem noch laufenden Verfahren. Mitgeteilt wurden jeweils das Delikt, Tatort und Tatzeit. In einigen Fällen war ergänzt, dass und unter welchem Aktenzeichen ein Verfahren bei der Staatsanwaltschaft anhängig geworden war. Soweit bekannt – dies war in sieben der 15 Verfahren der Fall – war auch der Verfahrensausgang ergänzt.

Der Betroffene bat mich um eine Stellungnahme, ob die Datenspeicherungen rechtmäßig sind und von ihm hingenommen werden müssen. Daraufhin nahm ich Einsicht in die zu seiner Person geführte und mit den automatisierten Datenspeicherungen korrespondierende Kriminalakte des zuständigen Polizeipräsidiums Nordhessen. Dabei machte ich einige Feststellungen, die dafür sprachen, dass die Datenspeicherungen nicht bzw. nicht mehr zur Aufgabenerfüllung der Polizei erforderlich sind.

Aus meiner Sicht stellte sich der Sachverhalt wie folgt dar:
Gegen den Betroffenen wurde 15-mal ermittelt. Er wurde einmal, und zwar im Jahre 1993, wegen Beleidigung zu einer Geldstrafe von zehn Tagessätzen verurteilt. Ein weiteres Verfahren wegen Beleidigung war noch nicht rechtskräftig abgeschlossen. Sechs Verfahren aus den Jahren 1986 bis 1999 wegen Beleidigung, Verstoß gegen das Tierschutzgesetz, Unterschlagung und Bedrohung waren aus unterschiedlichen Gründen eingestellt worden. In sieben Verfahren aus den Jahren 1987 bis 1998 wegen Sachbeschädigung, Beleidigung, Nötigung, gefährlicher Körperverletzung, Bedrohung und unerlaubtem Umgang mit gefährlichen Abfällen war der Polizei der Verfahrensausgang nicht bekannt.

Dass diese sehr umfangreiche auch automatisiert vorgehaltene Datensammlung zur Aufgabenerfüllung der Polizei erforderlich sein sollte, erschien nicht plausibel. Sie betraf u. a. sehr alte und von der Justiz eingestellte oder als geringfügig eingeordnete Ermittlungsverfahren. Ich bat deshalb das Polizeipräsidium Nordhessen, eine Einzelfallbearbeitung i. S. v. § 27 Abs. 2 Nr. 2 HSOG vorzunehmen und festzustellen, ob und inwieweit die Kenntnis der Daten zur Aufgabenerfüllung nach wie vor erforderlich ist.

§ 27 Abs. 2 Nr. 2 HSOG

Automatisiert gespeicherte personenbezogene Daten sind zu löschen und die dazugehörigen Unterlagen sind zu vernichten, wenn

1. ihre Speicherung unzulässig ist oder

2. bei der nach bestimmten Fristen vorzunehmenden Überprüfung oder aus Anlass einer Einzelfallbearbeitung festgestellt wird, dass ihre Kenntnis für die speichernde Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.

Zu Unrecht kam das Polizeipräsidium Nordhessen zu dem Ergebnis, dass sämtliche Daten aufgehoben werden müssten und weiterhin zur Aufgabenerfüllung der Polizei erforderlich seien. Zwar ist klar, dass es sich bei dieser Feststellung um eine fachliche Beurteilung handelt, die von der Polizei selbst und nicht von mir getroffen werden muss. Doch die Zweifel lagen auf der Hand. In mehreren Fällen hatten bereits die Ermittlungen ergeben, dass der ursprünglich erhobene strafrechtliche Vorwurf nicht aufrechterhalten bleiben konnte. Z. B. war in einem Fall wegen Verstoß gegen das Tierschutzgesetz aus dem Jahre 1998 ein Veterinär als Sachverständiger beigezogen. In einem Vermerk der Polizei wurde ausdrücklich festgehalten, dass ein Verstoß gegen das Tierschutzgesetz nicht festzustellen war. In diesem Fall – wie geschehen – unter Festsetzung einer Aufbewahrungsdauer von zehn Jahren einen „Verstoß gegen das Tierschutzgesetz“ im polizeilichen Informationsregister zu speichern, war von Anfang an falsch. In einem anderen gespeicherten Verfahren hatten Polizeibeamte beim Passieren des Grundstückes des Betroffenen festgestellt, dass dort mehrere abgemeldete Schrottfahrzeuge abgestellt waren. In einem Vermerk wurde u. a. festgehalten, die nachfolgende Kontrolle habe ergeben, dass unter den Fahrzeugen keine Ölschlieren festgestellt werden konnten und dass dem ersten Anschein nach der Boden nicht mit Öl oder sonstigen boden- und wassergefährdenden Stoffen verunreinigt sei. Trotzdem wurde der "Fall" der vorhandenen Datenspeicherung mit Angabe des Tatvorwurfes „unerlaubter Umgang mit gefährlichen Abfällen“ zugespeichert. Die Feststellung, dass aus heutiger Sicht die

weitere Aufbewahrung dieser Daten zur Aufgabenerfüllung der Polizei erforderlich sei, war offensichtlich ermessensfehlerhaft. Ähnlich verhielt es sich – nicht bei allen – aber bei einer ganzen Reihe der weiteren Verfahren. Auch war nicht nachvollziehbar, dass Informationen aus Ermittlungsverfahren, die über zehn Jahre zurückliegen und die von der Justiz als geringfügig eingestuft wurden, heute noch zur polizeilichen Aufgabenerfüllung erforderlich sein sollten. Ich bat deshalb das Landespolizeipräsidium, die Entscheidung des Polizeipräsidiums Nordhessen zu überprüfen und zu korrigieren. Das Landespolizeipräsidium betraute das LKA mit dieser Aufgabe. Als dieses dann beim Polizeipräsidium Nordhessen die Akten anforderte, zeigte die Kasseler Behörde Einsicht. Sie löschte die Daten über 14 der insgesamt 15 Ermittlungsverfahren. Es blieb bei der Datenspeicherung über das anfangs als nicht abgeschlossen bezeichnete Ermittlungsverfahren. Dieses war mittlerweile vom Landgericht Marburg gegen Zahlung einer Geldbuße von 300 € nach § 153a Abs. 2 StPO eingestellt. Die Speicherung dieser Daten für einen Zeitraum von drei Jahren, ausgehend von der Tatzeit, war nicht zu beanstanden. Die ursprünglich vorgesehene Aufbewahrungsdauer wurde von zehn auf drei Jahre reduziert. Damit kann der Betroffene, den ich über meine Bemühungen auf dem Laufenden gehalten habe, ab Ende des Jahres 2005 wieder mit einer „weißen Weste“ bei der Polizei rechnen.

5.1.5 Verwechselt: Datenschutzinteresse trotz „weißer Weste“

Durch einen Ermittlungsfehler wurde eine unbeteiligte Person als Beschuldigter in einem Strafverfahren geführt. Die Fehlerbehebung durch die Behörde muss in solchen Fällen einen sicheren Ausschluss der Weiterverarbeitung der fehlerhaften Daten in Akten und die Berichtigung in den Informationssystemen von Polizei und Justiz sicherstellen.

Dr. Albert Ernst[3] , Bürger einer hessischen Kleinstadt, wunderte sich über Post von der Staatsanwaltschaft. Er erhielt von der Arbeitsgruppe Ärzte – eine von der Staatsanwaltschaft beim Oberlandesgericht (OLG) Frankfurt eingerichtete Organisationseinheit – eine Vorladung, wonach er in einer gegen ihn geführten Strafsache wegen Betruges vernommen werden soll. Er rief sofort dort an und teilte mit, er sei überhaupt kein Arzt. Deshalb wisse er nicht worüber er vernommen werden solle. Nach kurzer Prüfung bestätigte ihm sein Gesprächspartner seine Vermutung: Er wurde mit einer anderen Person verwechselt. Er erhielt die Auskunft, er könne die Vorladung ignorieren. Da die Vorladung jedoch die Passage „Falls Sie ohne genügende Entschuldigung ausbleiben, kann Ihre Vorführung angeordnet werden“ enthielt, schrieb er vorsichtshalber die Behörde auch noch an und hoffte, die Sache sei damit erledigt. Leider war das nicht der Fall.

Einige Monate später erhielt er erneut Post von der Staatsanwaltschaft. Nun hieß es „das gegen Sie geführte Verfahren wegen Betruges wurde mit Zustimmung des Gerichts vorläufig eingestellt“. Dem öffentlichen Interesse an der Verfolgung der Straftat sei Genüge getan, wenn er 4.000 € an eine bestimmte gemeinnützige Einrichtung und weitere 4.000 € an die Staatskasse überweise. Nun schon leicht verärgert schrieb er erneut an die Staatsanwaltschaft und bat darum, die Angelegenheit zu berichtigen. Er habe keine Straftat begangen und habe auch nicht die Absicht eine Geldauflage zu erfüllen. Als er dann kurz darauf eine Zahlungsaufforderung der Gerichtskasse erhielt, wandte er sich Hilfe suchend an mich.

Ich nahm Einsicht in die Akte der Staatsanwaltschaft. Danach wurde das Verfahren gegen drei Personen geführt, die gemeinsam eine Arztpraxis betrieben haben. Sie firmierten unter der Bezeichnung „Gemeinschaftspraxis Dr. Susanne und Gerhard Schimmel und A. Ernst“. Diese Praxisbezeichnung war den Unterlagen entnommen, die in einem Labor beschlagnahmt worden waren. So war auch die Akte gekennzeichnet. Nach einem Aufkleber lauteten die Namen der Beschuldigten Dr. Susanne Schimmel, Dr. Gerhard Schimmel und A. Ernst. Auch die Strafanzeige wurde so ausgefertigt. Die weiteren Adressangaben in der Strafanzeige zu den ersten beiden Beschuldigten waren zutreffend bezeichnet. Die Angabe zu dem dritten Beschuldigten lautete ursprünglich nur „A. Ernst“. Sie war handschriftlich ergänzt zu „Dr. Albert Ernst“, es folgten Geburtsdatum und Anschrift des Betroffenen, der sich an mich gewandt hatte. Diese Angaben waren zum Zeitpunkt meiner Akteneinsicht korrigiert. Zu diesem Zeitpunkt stand dort „Alfons Ernst“, es folgte die Anschrift in einer anderen Stadt der Region und ein Korrekturvermerk, der angebracht worden war, nachdem ich gegenüber der Behörde meine Überprüfung angekündigt und darum gebeten hatte, die Vermeidung von Wiederholungsfällen sicherzustellen. Die Verwechslung von Dr. Albert Ernst mit Alfons Ernst zog sich durch das ganze Verfahren. Allerdings waren nicht alle falsch ausgefertigten Schriftstücke falsch zugestellt worden, denn Alfons Ernst wurde von demselben Anwaltsbüro verteidigt wie die anderen beiden Beschuldigen und Schriftstücke wurden mal mit richtiger, mal mit falscher Namensgabe, mal mit richtiger, mal mit falscher Adresse ausgefertigt und mal an die Beschuldigten direkt und mal an das Anwaltsbüro zugestellt. Korrekturnotizen und -verlangen fanden sich von der Polizei, der Staatsanwaltschaft selbst, dem fälschlich angeschriebenen Dr. Albert Ernst und auch vom Verteidiger von Alfons Ernst in der Akte. Ursache der Wiederholung des Fehlers war eine im Alltag übliche Verfahrensweise, wonach der bearbeitende Beamte z. B. nur verfügt „Ladung an Beschuldigte – wie Blatt 1 der Akte“ oder „Kostenrechnung an Beschuldigte – wie Blatt 1 der Akte“. Auf Blatt 1 der Akte stand aber damals der falsche Adressat und die aus den später entstandenen Aktenstücken hervorgehenden Korrekturen wurden beim Ausfertigen der Verfügungen nicht zur Kenntnis genommen. Erst die Korrektur auf Blatt 1 verhinderte weitere Wiederholungen.

Nach Angaben der ermittelnden Polizeibeamten kam die Verwechslung durch einen Ermittlungsfehler zustande. Ursprünglich war nur die Praxisanschrift und im Falle von Herrn Ernst das Vornamensinitial „A“ bekannt. Eine überregionale Aus-

[3] Die Namen sind in diesem Beitrag sinngemäß verändert.

wertung des Einwohnerdatenbestandes erbrachte bei den ersten beiden Beschuldigten die zutreffenden Adressen. Im Falle von „A. Ernst“, männlich und vom Alter her in Frage kommend, gab es eine ganze Reihe von möglichen Beschuldigten. Allerdings führte nur einer den akademischen Grad eines Doktors. Es handelte sich um Dr. Albert Ernst, der auf diese Weise für kurze Zeit als Beschuldigter ins Auge gefasst worden war. Nachfolgende Ermittlungen in der Arztpraxis erbrachten natürlich die richtige Angabe „Alfons Ernst“ und den Wohnsitz in einer anderen Stadt. Bis dahin war die Strafanzeige aber schon mit den falschen Angaben ergänzt und der Fehler hatte sich in der Akte verfestigt.

Dabei war das Interesse auf Berichtigung der Daten durch § 19 Abs. 1 HDSG begründet.

§ 19 Abs. 1 HDSG

Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.

Mit der Korrektur an der entsprechenden Stelle in der Akte wurde eine Wiederholung des Fehlers weitgehend ausgeschlossen. Doch der Berichtigungsanspruch nach § 19 HDSG ist noch weitergehend. So sieht § 19 Abs. 5 HDSG vor, dass auch die Empfänger personenbezogener Daten von einer Berichtigung informiert werden müssen.

§ 19 Abs. 5 HDSG

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.

Auch diesen Anspruch hatte die Staatsanwaltschaft zum Zeitpunkt meiner Akteneinsicht erfüllt. Der Gerichtskasse und einer gemeinnützigen Einrichtung, denen mitgeteilt worden war, von wem und in welcher Höhe sie eine Geldauflage überwiesen bekommen, wurden korrigierende Mitteilungen gemacht.

Doch der Berichtigungsanspruch nach § 19 HDSG bezieht sich nicht nur auf die manuellen Unterlagen der Behörde. Auch die automatisierten Informationssysteme der beteiligten Behörden waren zu korrigieren. Bei der Polizei sah ich das Informationssystem POLAS ein. Auch dort waren die gleichen falschen Daten enthalten: Mit einer vorgesehenen Aufbewahrungsdauer von zehn Jahren, zu präventiven Zwecken und zum bundesweiten polizeilichen Zugriff gekennzeichnet wurden dort Name, Adresse und weitere Daten zu Dr. Albert Ernst, der verwechselten Person, mit der Berufsangabe „Arzt“ und der Deliktsbezeichnung „Abrechnungsbetrug“ gespeichert. Die Polizei hat mir die sofortige Korrektur zugesagt und danach auch bestätigt. Bei der Justiz habe ich das System MESTA eingesehen. Dort lautete die Datenspeicherung zwar auf Alfons Ernst. Als Geburtsdatum und Adresse fanden sich aber die Daten von Dr. Albert Ernst wieder. Auch hier wurde sofortige Korrektur zugesagt und bestätigt.

Die datenschutzrechtlichen Belange von Herrn Dr. Albert Ernst sind verletzt worden. Die Staatsanwaltschaft sah dies ebenso. Sie hat sich bei ihm schriftlich entschuldigt. Von einer Beanstandung nach § 27 HDSG habe ich abgesehen. Herrn Dr. Albert Ernst habe ich informiert.

5.2 Justiz

5.2.1 Auskunftsverhalten der Staatsanwaltschaften

Erneut wandten sich Bürger an mich, deren Auskunftsverlangen an Justizbehörden nicht erfüllt wurden. Die Auskünfte in den mir bekannt gewordenen Fällen wurden nur zögerlich und nicht im gesetzlich geforderten Umfange erfüllt.

In meinem 31. Tätigkeitsbericht, Ziff. 3.4 hatte ich über Einzelfälle und teilweise über Defizite berichtet, wie in den Bereichen Strafverfolgung, Justizvollzug, Ausländerrecht, Verfassungsschutz, Polizei und Finanzverwaltung mit dem Recht auf Auskunft über Datenspeicherungen zur eigenen Person umgegangen wurde. In ihrer Stellungnahme zu diesem Bericht (LTDrucks. 16/1679) führte die Landesregierung aus, meine Feststellung, es käme "recht häufig" vor, dass Bürgern das Recht auf Auskunft über eigene Daten verweigert werde, entbehre einer statistischen Erhebung. In der Tat erfüllen meine Feststellungen zu diesem Sachverhalt nicht den Anspruch einer Erhebung im statistisch wissenschaftlichen Sinne. Dennoch sind sie erheblich, zumal ich im Berichtszeitraum erneut berechtigten Beschwerden Betroffener zur Auskunftserteilung nachgehen musste.

5.2.1.1 Staatsanwaltschaft bei dem Landgericht Kassel

Ein Bürger aus Nordhessen wandte sich an die Staatsanwaltschaft bei dem Landgericht Kassel und bat um Auskunft über die zu seiner Person gespeicherten Daten. Er bat um die Aufführung, wer ihn wann und wegen welchen Deliktes angezeigt hatte. Nachdem ihn die angeschriebene Behörde zehn Wochen lang warten ließ, wandte er sich an mich. Ich schrieb die

Behörde an und bat sein Auskunftsverlangen, gestützt auf § 491 Abs. 1 StPO, zu erfüllen, ihm gemäß § 19 BDSG Auskunft zu erteilen und mich über die Auskunftserteilung zu informieren.

§ 491 Abs. 1 StPO

Dem Betroffenen ist, soweit die Erteilung oder Versagung von Auskünften in diesem Gesetz nicht besonders geregelt ist, entsprechend § 19 BDSG Auskunft zu erteilen.

Solche besonderen Regelungen sieht die Strafprozessordnung in zahlreichen Fallsituationen vor, z. B. während des laufenden Strafverfahrens an den Verteidiger, das Opfer oder an Geschädigte. Nach Abschluss des Verfahrens und ohne Vorliegen von Besonderheiten im Einzelfall, ist die hier zitierte Norm diejenige, die das Recht auf Auskunft über die eigenen Daten sichert. Der Umfang der Auskunft orientiert sich aufgrund des Verweises an § 19 BDSG.

§ 19 Abs. 1 BDSG

(1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,

2. die Empfänger oder Kategorien von Empfängern, an die die Daten weitergeben werden und

3. den Zweck der Speicherung.

In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Sind die personenbezogenen Daten weder automatisiert noch in nicht automatisierten Dateien gespeichert, wird die Auskunft nur erteilt, soweit der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht. Die verantwortliche Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.

Nach meiner Intervention reagierte die Staatsanwaltschaft beim Landgericht Kassel prompt aber nicht ausreichend: Sie schrieb ihm: "Folgende Verfahren waren gegen Sie anhängig…". Es folgte eine Auflistung von fünf Justizaktenzeichen. Bei zwei Verfahren war zusätzlich das Delikt genannt und dass sie an die zuständige Verwaltungsbehörde abgegeben wurden. Weitere Angaben fehlten. Der Betroffene wandte sich erneut an mich. Ich wies die Staatsanwaltschaft auf den Beitrag in meinem 31. Tätigkeitsbericht und den Auskunftsumfang nach § 19 BDSG hin und bat um Nachbesserung. Nun erteilte ihm die Behörde ausführlich die gewünschten Auskünfte und informierte mich entsprechend.

5.2.1.2 Staatsanwaltschaft bei dem Landgericht Marburg

Mit einem fast identischen Auskunftsverlangen wandte sich ein Bürger an die Staatsanwaltschaft bei dem Landgericht Marburg. Nachdem er etwa zehn Wochen lang keine Antwort erhalten hatte, wandte er sich an mich. Auf meine Intervention hin erhielt er eine Aufstellung mit justiziellen Aktenzeichen, Delikten und dem jeweiligen Verfahrensausgang. Dies entsprach zwar ebenfalls nicht dem Auskunftsumfang nach § 19 BDSG, doch der Betroffene verlangte keine Nachbesserung. Ich habe die Sache deshalb auf sich beruhen lassen.

5.2.1.3 Staatsanwaltschaft bei dem Landgericht Frankfurt

Nachdem die Staatsanwaltschaft bei dem Landgericht Frankfurt das Auskunftsverlangen eines Frankfurter Bürgers knapp ein Jahr lang unbeantwortet ließ, wandte er sich an mich. Da die Fragen des Betroffenen sich alle im Rahmen des Auskunftsrechts nach § 19 Abs. 1 hielten, schrieb ich die Staatsanwaltschaft an und fragte, ob der Vorhalt des Betroffenen zutreffe. Die Staatsanwaltschaft bei dem Landgericht Frankfurt bestätigte den Sachverhalt. Wegen permanenter Überlastung sei die zuständige Staatsanwältin nicht dazu gekommen, sich dem Auskunftsverlangen zu widmen. Auch jetzt ließe es die Arbeitsbelastung nicht zu, die Fragen des Betroffenen zu beantworten. Die Antwort könne nicht anhand des Registers erteilt werden, sondern erfordere eine Auseinandersetzung mit der Materie und sei deshalb sehr zeitaufwändig. Der Betroffene habe daher vorläufig einen Ausdruck über die zu seiner Person automatisiert gespeicherten Daten erhalten. Die Beantwortung seiner Fragen wurde in Aussicht gestellt, sobald es die Arbeitsbelastung zulasse.

Diese Verfahrensweise ist mit dem Recht nach § 491 Abs. 1 StPO nicht vereinbar. Zwar nennt weder § 491 Abs. 1 StPO noch § 19 BDSG eine Frist in der ein Auskunftsverlangen zu erfüllen ist. Auch ist es akzeptabel, wenn eine Behörde in einer besonderen Belastungsphase zur Erfüllung eines Auskunftsverlangens länger als üblich benötigt. Ist aber mehr als ein Jahr seit der Anfrage verstrichen, so ist die Pflicht, Auskunft nach § 491 Abs. 1 StPO zu erteilen, verletzt. Ich habe dies

der Staatsanwaltschaft bei dem Landgericht Frankfurt mitgeteilt und sie aufgefordert, das Verlangen zu erfüllen. Den Betroffenen habe ich informiert.

5.2.1.4 Fazit

Ich kann nach wie vor nicht beurteilen, ob es sich bei den mir bekannt gewordenen Fällen um die "Spitze eines Eisberges" oder um seltene Ausnahmefälle handelt. Die beiden ersten Fälle zeigen aber, dass einzelnen Staatsanwaltschaften offenbar der Umfang des Auskunftsrechts nicht bekannt ist. Hier sehe ich Nachbesserungsbedarf. Auch die hohe Arbeitsbelastung darf nicht dazu führen, dass verbriefte Rechte auf der Strecke bleiben.

5.3 Ausländerrecht

5.3.1 Digitales Einbürgerungssystem

Unter Federführung des Hessischen Ministeriums des Innern wird das Einbürgerungsverfahren automatisiert. Ich wurde an dem Projekt frühzeitig beteiligt.

Die bisherigen Pläne für das Digitale Einbürgerungssystem (DiE Hessen) sehen vor, dass die Daten zu den entsprechenden Einbürgerungsverfahren aller in Hessen lebenden Antragsteller in einer Zentraldatei gespeichert werden. Zugriff auf diese Datei sollen die am Einbürgerungsverfahren beteiligten Stellen in differenzierter Weise erhalten.

Der Antrag auf Einbürgerung wird nach wie vor bei den unteren Verwaltungsbehörden (also den Gemeinden bzw. Landkreisen) gestellt. Die unteren Verwaltungsbehörden erfassen die Stammdaten des Antrags und legen diese in der zentralen Einbürgerungsdatei ab. Zugriff auf diese Stammdaten haben dann die jeweils zuständigen Regierungspräsidien. Bisher haben diese die erforderlichen Auskünfte z. B. bei den Polizeibehörden, dem Landesamt für Verfassungsschutz oder dem Bundeszentralregister im schriftlichen Verfahren eingeholt. Das Verfahren DiE soll solche Auskunftsanträge als elektronische Formulare bereits automatisiert mit den Stammdaten füllen und den beteiligten Stellen automatisiert zur Bearbeitung zur Verfügung stellen.

Soweit die auf diese Weise um Auskunft ersuchte Stelle keine Erkenntnisse über die betroffene Person hat, ergänzt sie das vorbereitete Formular entsprechend und schickt es automatisiert an das Regierungspräsidium zurück. Liegen der Behörde Informationen zu dem Betroffenen vor, so übermittelt die Polizei diese konventionell an das Regierungspräsidium, im Fall des Landesamtes für Verfassungsschutz gehen die Informationen an das Hessische Ministerium des Innern. Die Erkenntnisse zu der betroffenen Person werden dann vom Regierungspräsidium bzw. vom Hessischen Ministerium des Innern in DiE gespeichert. Das Ministerium verfolgt mit diesem Projekt das Ziel, die Zusammenarbeit der verschiedenen Behörden zu vereinfachen und zu beschleunigen.

Die Rechtsgrundlage für das digitale Einbürgerungssystem soll in Artikel 4 des Gesetzes zur Kommunalisierung der Landrätin oder des Landrats sowie der Oberbürgermeisterin oder des Oberbürgermeisters als Behörden der Landesverwaltung geschaffen werden.

Auf meine Anregung wurden im Gesetzentwurf durch einen Verweis auf § 15 Abs. 1 und 2 HDSG die erforderliche Beteiligung des Hessischen Datenschutzbeauftragten sowie Einzelheiten des Verfahrensverzeichnisses und der Vorabkontrolle festgeschrieben. Ein weiteres Problem war die vorgesehene Verarbeitung sensitiver Daten.

§ 7 Abs. 4 HDSG

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 Einbürgerungsverfahren können beispielsweise Informationen des Verfassungsschutzes über die politische Auffassung oder die philosophische Überzeugung eine Rolle spielen.

Da die jeweiligen Vorschriften für das Einbürgerungsverfahren – früher in § 86 Nr. 2 Ausländergesetz, seit dem In-Kraft-Treten des Zuwanderungsgesetzes (BGBl. I, S. 1950) zum 1. Januar 2005 in § 11 Nr. 2 Staatsangehörigkeitsgesetz – eine Rechtsgrundlage im Sinne von § 7 Abs. 4 HDSG darstellen, ist die Verarbeitung zulässig.

Derzeit laufen in verschiedenen Kommunen und im Regierungspräsidium Darmstadt Pilotprojekte, die ich kritisch begleite.

5.3.2 Auskunftspflicht nur bei tatsächlichen Ausländervereinen

Zur Feststellung ob ein Verein ein so genannter Ausländerverein ist, dürfen nur die hierfür erforderlichen Informationen erhoben werden.

Der Vorsitzende des eingetragenen Vereins Christlich-Islamische Gesellschaft bat mich, dazu Stellung zu nehmen, ob er verpflichtet sei, der Ordnungsbehörde des Kreises bestimmte Informationen (Mitgliederliste bestehend aus Namen, Anschriften und Geburtsdaten der Mitglieder; Übersicht über den aktuellen Vorstand; gültige Satzung) über den Verein mitzuteilen. Die Behörde begründete ihr Informationsbegehren damit, dass sie prüfen müsse, ob es sich bei dem oben genannten Verein um einen Ausländerverein handele. Der Vorsitzende hatte der Behörde im Vorfeld schon mitgeteilt, dass von den 32 Mitgliedern nur fünf Mitglieder nicht die deutsche Staatsangehörigkeit besitzen.

Ausländervereine sind nach § 14 des Gesetzes zur Regelung des öffentlichen Vereinsrechts (VereinsG) solche Vereine, deren Mitglieder oder Leiter sämtlich oder überwiegend Ausländer sind. Darunter können auch Religionsgemeinschaften und andere Weltanschauungsvereinigungen fallen, da das VereinsG durch Gesetz vom 8. Dezember 2001 insoweit geändert wurde (BGBl. I, S. 3319). Im Unterschied zu Vereinen von Deutschen kann gegen Ausländervereine beispielsweise unter einfacheren Voraussetzungen ein Vereinsverbot nach § 14 Abs. 2 VereinsG ausgesprochen werden.
Die Differenzierung ist vor dem Hintergrund zu sehen, dass das Grundgesetz in Artikel 9 Abs. 1 und 2 die Vereinsfreiheit speziell für Deutsche besonders garantiert.

Ausländervereine unterliegen darüber hinaus einer besonderen Auskunftspflicht nach § 20 der Durchführungsverordnung zum VereinsG.

§ 20 Abs. 1 Durchführungsverordnung zum VereinsG

Ausländervereine … haben auf Verlangen Auskunft zu geben
1. über ihre Tätigkeit
2. wenn sie sich politisch betätigen,
a) über Namen und Anschrift ihrer Mitglieder,
b) über Herkunft und Verwendung ihrer Mittel.

Die Auskunftsverpflichtung besteht allerdings nur dann, wenn feststeht, dass es sich um einen Ausländerverein handelt.
Im vorliegenden Fall hat die Behörde – wohl aufgrund des Namens des Vereins – Anhaltspunkte für einen Ausländerverein gesehen.
Die Behörde kann in diesem Fall zwar bei dem Vorsitzenden anfragen, ob die Voraussetzungen des § 14 Abs. 1 VereinsG erfüllt sind, also die Mitglieder oder Leiter vorwiegend Ausländer sind. Insoweit hatte der Vereinsvorsitzende die erforderlichen Auskünfte bereits gegeben, aus denen zu schließen war, dass es sich nicht um einen Ausländerverein handelt. Es ist der Behörde aber verwehrt, solche Auskünfte zu verlangen, die sie nach § 14 Abs. 1 VereinsG nur bei Ausländervereinen erheben darf.

Ich habe diese Rechtsauffassung der Behörde mitgeteilt und um Auskunft gebeten, wie sie in ähnlich gelagerten Fällen verfährt.

5.4 Landesplanung und Planfeststellung

5.4.1 Behandlung von Einwendungen im Planfeststellungsverfahren

Anlässlich des anstehenden Planfeststellungsverfahrens zum Ausbau des Frankfurter Flughafens tauchte erneut die Frage nach dem Umgang mit den personenbezogenen Daten der Einwender auf. Ich habe das Regierungspräsidium Darmstadt darauf hingewiesen, dass Einwendungen von Bürgern, die lediglich allgemeine Argumente gegen den Flughafenausbau vortragen, generell anonymisiert an die Flughafenbetreiberin weiterzugeben sind.

Bereits im 32. Tätigkeitsbericht, Ziff. 9.1 hatte ich mich zur Frage der Weitergabe personenbezogener Einwenderdaten an die Flughafenbetreiberin Fraport geäußert. Im Rahmen des Planfeststellungsverfahrens zum Bau einer neuen Landebahn war dieses Thema erneut Gegenstand von Erörterungen zwischen dem Wirtschaftsministerium als Planfeststellungsbehörde, dem Regierungspräsidium Darmstadt als Anhörungsbehörde und meiner Dienststelle.

Grundsätzlich gibt es drei Kategorien von Einwenderdaten, die jeweils unterschiedlich zu behandeln sind:

5.4.1.1 Behandlung der Daten von Einwendern, die persönliche Nachteile befürchten

Wie ich bereits in meinem 32. Tätigkeitsbericht ausführlich dargelegt habe, sind potenzielle Einwender im Vorfeld darauf hinzuweisen, dass sie eine anonymisierte Weitergabe ihrer Einwendungen an die Fraport AG verlangen können, wenn Gründe vorgetragen werden, die gegen eine personenbezogene Weitergabe sprechen (z. B. Beschäftigte bei Fraport/Lufthansa etc.). Diese Information sollte, wie im Verfahren zum Bau der A 380-Wartungshalle, Eingang in den Text über die ortsübliche Bekanntmachung der Planauslegung finden. Der Hinweis ist deshalb erforderlich, da betroffene Einwender ein ihnen zustehendes Recht nur geltend machen können, wenn sie über dieses Recht auch informiert sind.

5.4.1.2 Behandlung von so genannten „Jedermann-Einwendungen“

Einwendungen, in denen nur pauschal Argumente gegen den Flughafenausbau vorgetragen werden (z. B. Zerstörung der Umwelt, stetige Erhöhung der Lärmbelastung der Region etc.), die aber keinen konkreten Bezug zur Person des Einwenders haben, sind generell anonymisiert an die Fraport AG weiterzugeben. Die Fraport AG muss sich nämlich mit diesen Argumenten nicht an Hand einzelner Personen auseinander setzen, so dass eine personenbezogene Weitergabe nicht erforderlich und damit unzulässig ist.

5.4.1.3 Behandlung von Einwendungen, die sich auf individuelle Betroffenheiten beziehen

Diese Einwendungen werden prinzipiell personenbezogen an die Fraport AG weitergegeben, da der Betreiberin Gelegenheit gegeben werden muss, sich mit dem Einzelargument auseinander zu setzen und ggf. Abhilfe zu schaffen. Eine anonymisierte Weitergabe findet nur aus den Gründen statt, die unter Ziff. 5.4.1.1 angeführt wurden.

5.5 Schulverwaltung, Schulen und sonstige Bildungseinrichtungen

5.5.1 Pilotprojekt EDUNITE

Das Pilotprojekt EDUNITE des Hessischen Kultusministeriums habe ich datenschutzrechtlich begleitet.

5.5.1.1 Allgemeines

EDUNITE ist ein E-Government-Projekt, das von dem HKM initiiert und gefördert wird. Hierbei handelt es sich um eine neue Generation von Schulkommunikations- und Schulverwaltungssoftware. Auf der einen Seite soll es den Pädagogen ihre administrativen Aufgaben erleichtern und auf der anderen Seite die Kommunikation zwischen Lehrern, Schülern und Eltern fördern. Die Datenverarbeitung erfolgt zentral auf einem Hostrechner. Auf dieser über das Internet erreichbaren Plattform können alle am Schulleben Beteiligten, also Schüler, Eltern und Lehrkräfte, Informationen speichern, die dem schulischen Interesse der verschiedenen Beteiligten dienen und dauerhaft zur Verfügung stehen. Damit soll allen Beteiligten schulisch umfassend angelegtes Wissen zur Verfügung gestellt werden, die Klassenverwaltung der Lehrkräfte optimiert und die schnelle Kommunikation per E-Mail unterstützt werden.

In weiteren Ausbaustufen soll es später möglich sein, übergeordnete Verwaltungseinheiten (Schulamt, Ministerium) einzubinden.

Schon frühzeitig wurde ich in das Projekt einbezogen, um datenschutzrechtliche Belange sowohl in rechtlicher wie auch in technischer Sicht von Anfang an zu berücksichtigen.

Insgesamt unterstützt das Programm zurzeit die automatisierte Erfassung von
- nicht personenbezogenen Daten
- unterrichtsbezogenen Sachdaten
- personenbezogenen Daten von Schülern, Lehrern und Eltern aus dem Schulverwaltungsbereich.

Weiterhin ist eine direkte elektronische Kommunikation zwischen Lehrkräften untereinander und zwischen Schule und Eltern möglich.

Für die datenschutzrechtliche Wertung wurden zwei Fragenkomplexe untersucht:

a) dürfen personenbezogene Daten überhaupt von den jeweiligen Daten verarbeitenden Personen oder Stellen verarbeitet werden? (s. Ziff. 5.5.1.2 Rechtliche Wertung)

b) Wenn ja: Ist die Datensicherheit gewährleistet? (s. Ziff. 5.5.1.3 Technische Wertung)

5.5.1.2 Rechtliche Wertung

Soweit es um personenbezogene Daten geht, ist von dem rechtlichen Grundsatz auszugehen, dass deren Erhebung, Speicherung und weitere Datenverwendung einer rechtlichen Befugnisnorm bedürfen.

Folgende Phasen der Datenverarbeitung kommen bei EDUNITE in Betracht:

- **Erstmalige Datenspeicherung**

  Die rechtliche Befugnis, schulbezogene Verwaltungsdaten der von der Schulverwaltung betroffenen Personen, also Eltern, Lehrkräfte und Schüler, zu erheben und zu speichern, ergibt sich generell aus den einzelnen, für den konkreten Fall anzuwendenden Vorschriften des Schulgesetzes, der „Verordnung über die Verarbeitung personenbezogener Daten in Schulen“ vom 30. November 1993 und ergänzend dem HDSG.
  Da EDUNITE zunächst nur eine technische Plattform darstellt, muss der Benutzer, der personenbezogene Daten erstmals speichert, in jedem Einzelfall prüfen, ob die einschlägige Vorschrift erfüllt ist. Soweit keine besondere Rechtsvorschrift gilt, ist generell zu prüfen, ob die Datenspeicherung für die schulische Aufgabenerfüllung erforderlich ist.

  Soweit EDUNITE bestimmte Datenarten der Eltern und Schüler vorstrukturiert, halten diese sich im Rahmen der o. g. Vorschriften. Insbesondere die in § 1 der o. g. Verordnung katalogartig aufgezählten Daten gelten auf Grund ihrer Bedeutung generell als für die Schulverwaltung erforderlich. Sie werden entweder über die Schnittstelle zum Standardschulprogramm LUSD eingespeist oder von dem Benutzer von EDUNITE direkt erhoben und eingegeben.

- **Weitere Verwendung von Daten innerhalb der Schule**
  Auch die weitere Datenverwendung im Wege lesenden oder schreibenden Zugriffs durch den EDUNITE-Benutzer innerhalb der Schule, vor allem Lehrkräfte und Schulverwaltungsangestellte ist datenschutzrechtlich nur zulässig, wenn und soweit dies für die jeweilige konkrete Aufgabenerfüllung erforderlich ist. Die Zugriffsberechtigung zu den einzelnen Datenbereichen muss also der Art der dienstlichen Aufgabenerfüllung zugeordnet sein.
  Die in EDUNITE festgelegten und den einzelnen Benutzergruppen zugeordneten Zugriffsrechte entsprechen diesen Aufgabenbereichen. So können Lehrkräfte nur auf die Daten der von ihnen betreuten Schüler zugreifen; die ausschließlich für andere Lehrkräfte relevanten Daten stehen technisch nur diesen zur Verfügung.
  Dreh- und Angelpunkt solcher Verwaltungsprogramme ist also das vorweg festzulegende Berechtigungskonzept, das den Änderungen von schulischen Aufgaben auch permanent angepasst werden muss.

- **Verarbeitung der Daten außerhalb der Schule**

  - EDUNITE ermöglicht den Zugriff der Schüler auf sie betreffende Daten der Schulverwaltung über das Internet. Insoweit unterstützt das Programm die behördlichen Auskunftspflichten, etwa nach § 18 Abs. 3 HDSG.

  - Um eine Übermittlung der Daten an Dritte handelt es sich, wenn z. B. die Eltern die in EDUNITE gespeicherten Schuldaten ihrer Kinder einsehen können, wie etwa die Schulnoten oder Fehlzeiten. Hierbei handelt es sich um eine Datenübermittlung an eine Stelle außerhalb des öffentlichen Bereichs, deren Zulässigkeit nach § 16 HDSG zu beurteilen ist. Die Eltern haben bis zur Volljährigkeit des Kindes das Personensorgerecht, wozu die schulischen Belange gehören.

  - Das begründet das erforderliche berechtigte Interesse an der Datenübermittlung.

Nach einer ersten Durchsicht der Datenfelder, der Struktur der Zugriffsberechtigungen auf der Grundlage der allgemeinen Aufgabenverteilung und Auswertungsmöglichkeiten konnte – vorbehaltlich einer systematischen Einzelprüfung aller Details – festgestellt werden, dass keine datenschutzrechtlich unzulässigen Verarbeitungen mit EDUNITE unterstützt werden. Der einzelne Benutzer von EDUNITE trägt jedoch die Verantwortung, die Nutzung rechtlich im Einzelfall begründen zu können.

5.5.1.3 Technische Wertung

Es wurde untersucht, ob die Datensicherheit im Sinne der Anlage 5 der oben genannten Verordnung in Verbindung mit § 10 HDSG gegeben ist.

Die nachstehende Beurteilung erfolgte auf Grund des vorgelegten Exposés für Pilotschulen, des Sicherheitskonzeptes und einer Präsentation in der Freiherr-vom-Stein-Schule in Frankfurt. Die anhand der vorgeschlagenen Sicherheitsmaßnahmen erkennbare angedachte technische Lösung ist positiv zu bewerten. Sie entspricht in den untersuchten Punkten der IT-

Sicherheit (Vertraulichkeit, Integrität und Verfügbarkeit) dem Stand der Technik und schließt einige der seit Jahren bemängelten Schwachstellen in der üblichen Schulverwaltungs-Software. Hervorzuheben ist die verschlüsselte Übertragung der Daten vom Nutzer zum Server ebenso wie deren schulspezifisch verschlüsselte Ablage in einer Datenbank. Ohne Beanstandung in der derzeitigen Realisierung blieb das Rollen- und Berechtigungskonzept.

5.5.1.4 Ausblick

Wenn eine datenschutzrechtliche Umsetzung der konzeptionellen Möglichkeiten von EDUNITE in den einzelnen Schulen und die Berücksichtigung von Datenschutzgesichtspunkten bei der Konzeption der weiteren Ausbaustufen sichergestellt ist, kann das Projekt und dessen Weiterführung unter datenschutzrechtlichen Aspekten befürwortet werden. Ich werde das Pilotprojekt EDUNITE weiterhin beratend begleiten.

5.5.2 Ergebnisse der Prüfung einer Schule

Die hessischen Schulen haben nach wie vor Probleme bei der Umsetzung der Datenschutzbestimmungen.

Im Rahmen meiner Prüftätigkeit besuchte ich ein Gymnasium in einer hessischen Stadt.

Als Gesamteindruck der Prüfung lässt sich zunächst festhalten, dass sich die datenschutzrechtlichen Defizite an hessischen Schulen oft ähneln, jede Schule hat hier jedoch eigene Schwerpunkte. Ein Katalog zentraler datenschutzrechtlicher Mängel an Schulen ist über meine Homepage (www.datenschutz.hessen.de) abrufbar unter dem Suchbegriff „Schule“.

Bei der hier geprüften Schule waren u. a. folgende Punkte zu bemängeln:

5.5.2.1 Mangelhafte Sicherheitsmaßnahmen beim Einsatz der Informationstechnik

Bei der Prüfung des Gymnasiums fanden meine Bediensteten zwar moderne Rechner vor, aber die einfachsten Sicherheitsmaßnahmen waren nicht umgesetzt. Nicht jeder Nutzer besaß ein eigenes Passwort. Die Rechner hatten keinen aktuellen Virenscanner. Der Anschluss an das Internet erfolgte ohne Firewall und die gesamte Dokumentation des Netzes fehlte. Die Antwort wie diese Missstände beseitigt werden, steht noch aus.

5.5.2.2 Nutzung des Privat-PC ohne Genehmigung der Schulleitung

Nach allgemeiner Lebenserfahrung nutzt ein Teil der Lehrerschaft regelmäßig den Privat-PC zu Hause zur Verarbeitung von Schülerdaten, etwa bei der Verwaltung der Noten oder bei der Vorbereitung des Zeugnisses. Möchte die Lehrkraft ihren Privat-PC für solche schulischen Zwecke nutzen, bedarf es nach § 83 Abs. 5 HSchG einer entsprechenden schriftlichen Genehmigung durch die Schulleitung.

§ 83 Abs. 5 HSchG

Personenbezogene Daten von Schülerinnen und Schülern, deren Eltern und Lehrerinnen und Lehrern dürfen in der Regel nur in der Schule verarbeitet werden. Die automatisierte Verarbeitung personenbezogener Daten darf nur auf schuleigenen Datenverarbeitungsgeräten erfolgen. Die Schulleiterin oder der Schulleiter kann in begründeten Ausnahmen gestatten, dass Lehrerinnen und Lehrer Daten von Schülerinnen und Schülern auf Datenverarbeitungsgeräten außerhalb der Schule verarbeiten.

Der Zweck dieses Verfahrens liegt vor allem darin, der Lehrkraft ins Bewusstsein zu bringen, dass sie bei der dienstlichen Nutzung des privaten PC dem öffentlichen Recht, also auch dem Datenschutzrecht unterliegt. Sie trägt deshalb insbesondere auch dafür die Verantwortung, dass die gespeicherten Daten nicht Unbefugten zur Kenntnis gelangen können. Aus diesem Grund sieht das landesweit einheitliche Antragsformular Angaben zur Frage vor, welche Sicherheitsmaßnahmen getroffen wurden, etwa den Einsatz von mobilen Datenträgern, verschlüsselter Speicherung und Ähnliches. Problematisch wird der PC-Einsatz vor allem dann, wenn die Lehrkraft mit ihrem PC auch das Internet nutzt. Berichtet wird mir zunehmend von Fällen, in denen Schüler versuchen, diesen PC zu hacken. Fatal wird es auch dann, wenn die Lehrkraft dort den Entwurf für Abiturarbeiten gespeichert hat.

Von der geprüften Schule waren keine Genehmigungen erteilt worden. Es gab auch keine Anträge aus der Lehrerschaft. Ich habe die Schule aufgefordert, die Lehrkräfte zunächst über die Rechtslage zu informieren und aufzufordern, ggf. diesen Antrag zu stellen.

5.5.2.3 Fehlen eines stellvertretenden Datenschutzbeauftragten

Nach § 5 Abs. 1 Satz 1 HDSG hat jede Behörde auch einen Stellvertreter für den behördlichen Datenschutzbeauftragten zu bestellen.

§ 5 Abs. 1 Satz 1 HDSG

Die Daten verarbeitende Stelle hat schriftlich einen behördlichen Datenschutzbeauftragten sowie einen Vertreter zu bestellen.

Der Zweck liegt vor allem darin, das kontrollierende Auge des Datenschutzbeauftragten auch dann in der Behörde zu erhalten, wenn der hauptamtliche Datenschutzbeauftragte nicht anwesend ist. Sinnvoll ist natürlich zusätzlich eine Zusammenarbeit zwischen dem oder der Datenschutzbeauftragten und der Vertretung, um gemeinsame Positionen einzunehmen und sich wechselseitig zu beraten.

Die hier geprüfte Schule hatte keinen Stellvertreter bestellt. Deshalb habe ich verlangt, dies umgehend nachzuholen.

5.5.2.4 Aussonderung der schulischen Verwaltungsunterlagen

In Ausführung des § 10 HArchivG verlangen die „Richtlinien über die Führung, Aufbewahrung und Archivierung von Schriftgut in Schulen“ (ABl. des Hessischen Kultusministeriums 1993, S. 522) in Abschnitt B die Festlegung von genau vorbestimmten Aufbewahrungsfristen für alle standardmäßig in der Schulverwaltung vorkommenden Unterlagen. Die Fristen sind gestaffelt; die Mindestfrist liegt bei zwei Jahren.

Nach Ablauf der Aufbewahrungsfrist sind die Unterlagen auszusondern, soweit sie nicht dem in dem Erlass genannten Ausnahmekatalog zuzuordnen sind, und dem örtlich zuständigen Staatsarchiv anzubieten zur evtl. Archivierung. Erst wenn dieses entscheidet, die Archivierung abzulehnen, muss die Schule die Unterlagen unverzüglich vernichten.

Bei der hier geprüften Schule waren für zahlreiche vorhandene Unterlagen keine Fristen festgelegt oder sie waren abgelaufen, z. B. bei Klassenbüchern von 1985. Es war deshalb zu fordern, die drei geschilderten Schritte baldmöglichst nachzuholen.

Bei der Besprechung dieses Punktes erwähnte die Schulleitung, in früheren Jahren die Unterlagen dem öffentlichen Archiv des zuständigen Schulträgers angeboten zu haben, der einen Teil der Unterlagen auch übernommen hatte. Das war fehlerhaft. Für die Übernahme ist allein das Staatsarchiv zuständig, denn das öffentliche Archiv des Schulträgers ist nur zuständig für dessen eigene Verwaltungsunterlagen. Darauf habe ich hingewiesen.

5.6 Hochschulen

5.6.1 Prüfung der Universität Marburg

Hochschulverwaltungen haben immer noch Probleme mit der Umsetzung des seit 1999 geltenden Hessischen Datenschutzgesetzes.

Im Berichtsjahr prüfte ich verschiedene Abteilungen der Philipps-Universität Marburg. Im Hinblick auf die vorgefundenen Mängel sind zwei geprüfte Bereiche erwähnenswert:

5.6.1.1 Studentensekretariat

5.6.1.1.1 Fehlende Informationen in Antragsformularen

Das Studentensekretariat verwendet in verschiedenen Zusammenhängen Formulare, durch die es erstmals personenbezogene Daten verschiedener Personengruppen, insbesondere der Studenten, erhebt, z. B. das Antragsformular für die Immatrikulation. Im Rahmen der Datenerhebung bei Betroffenen verlangt § 12 Abs. 4 HDSG die dort spezifizierte Aufklärung der Betroffenen über den Zweck der Datenverarbeitung usw.

§ 12 Abs. 4 HDSG

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.

Ein Teil dieser Informationen fehlte jedoch bei den mir vorgelegten Formularen, z. B. der Hinweis auf § 8 HDSG.

5.6.1.1.2 Überflüssige Information in Antragsformularen

Das Studentensekretariat weist in den jetzt verwendeten Formularen immer noch auf die Tatsache der automatisierten Verarbeitung der erhobenen Daten hin. Dies verlangten die bis 1998 geltenden Vorschriften des HDSG so (vgl. § 18 Abs. 1 HDSG alte Fassung). Inzwischen ist die automatisierte Datenverarbeitung die Regel. Betroffene, bei denen Daten erhoben werden, gehen davon aus, dass diese automatisiert verarbeitet werden. Deshalb sieht die seit 1999 geltende Fassung dieser Vorschrift keinen Hinweis mehr auf die Tatsache der automatisierten Verarbeitung vor. Eine Benachrichtigung über die erhobenen Daten ist seitdem entbehrlich, wenn die Daten bei den Betroffenen erhoben werden (§ 18 Abs. 2 Nr. 1 HDSG).

§ 18 HDSG

(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.
…

Da die betroffenen Daten durch Direkterhebung gewonnen wurden, konnte also der Hinweis auf die automatisierte Verarbeitung der Daten entfallen.

5.6.1.1.3 Vorabkontrolle der Verfahren HIS-POS und HIS-ZUL

Das Studentensekretariat setzt seit ca. zwei Jahren die für die Verwaltung der Studentendaten entwickelten Verwaltungsprogramme HIS-POS und HIS-ZUL ein. Bevor zur Verarbeitung personenbezogener Daten vorgesehene Verwaltungsprogramme eingesetzt werden dürfen, muss nach § 7 Abs. 6 HDSG die so genannte Vorabkontrolle erfolgen.

§ 7 Abs. 6 HDSG

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.

Ziel der Vorabkontrolle ist es sicherzustellen, dass nur Verfahren zum Einsatz kommen, bei denen aus rechtlicher und technischer sicht kein Grund besteht, eine Gefährdung des Rechts auf informationelle Selbstbestimmung anzunehmen. Eine Vorabkontrolle war vor Einsatz des Verfahrens nicht erfolgt. Mir wurde zugesagt, dass sie nachträglich durchgeführt und dokumentiert wird.

5.6.1.1.4 Behandlung von Studentendaten nach Ablauf der Aufbewahrungsfristen

Die im Studentensekretariat manuell und automatisiert gespeicherten Studentendaten werden nach bestimmten schriftlich festgelegten Fristen regelmäßig zunächst verwahrt. Nach Ablauf dieser Fristen sind sie, wie alle sonstigen Verwaltungsdaten der Hochschulverwaltung auch, nach § 10 HArchivG dem örtlich zuständigen Staatsarchiv in Marburg zur Entscheidung über die Archivierung anzubieten. Zwar verlangt § 19 Abs. 3 Satz 1 HDSG grundsätzlich eine Löschung der Daten, wenn ihre Erforderlichkeit für die Aufgabenerfüllung entfallen ist. § 10 HArchivG geht dem § 19 Abs. 3 Satz 1 HDSG aber als Sondervorschrift vor.

§ 10 HArchivG

(1) Die in § 6 genannten Stellen sind verpflichtet, alle Unterlagen, die zur Erfüllung ihrer Aufgaben nicht mehr erforderlich sind, unverzüglich auszusondern und dem zuständigen Archiv zur Übernahme anzubieten. Dies soll im Regelfall dreißig Jahre nach Entstehung der Unterlagen erfolgen. Anzubieten sind auch Unterlagen, die besonderen Rechtsvorschriften über Geheimhaltung oder über den Datenschutz unterworfen sind. Unberührt bleiben gesetzliche Vorschriften über die Löschung oder Vernichtung unzulässig erhobener oder verarbeiteter Daten oder Unterlagen.

(2) Die in § 6 genannten Stellen dürfen Unterlagen nur vernichten oder Daten nur löschen, wenn das zuständige öffentliche Archiv die Übernahme abgelehnt oder nicht binnen eines Jahres über die Archivwürdigkeit angebotener Unterlagen entschieden hat. Von dem Anbieten und Vorhalten von Unterlagen von offensichtlich geringer Bedeutung kann im Einvernehmen mit dem zuständigen öffentlichen Archiv abgesehen werden. Ausgesonderte Unterlagen, deren Übernahme von den öffentlichen Archiven abgelehnt wird, sind im Regelfall zu vernichten, sofern kein Grund zu der Annahme besteht, da durch die Vernichtung schutzwürdige Belange von Betroffenen beeinträchtigt werden.

(3) Die in § 6 genannten öffentlichen Stellen sollen ein Exemplar der von ihnen herausgegebenen Druckschriften dem zuständigen Archiv zur Übernahme anbieten.

Erst nach Ablehnung der Archivierung müssen die Verwaltungsunterlagen endgültig vernichtet bzw. gelöscht werden. Das Studentensekretariat hatte die hiervon betroffenen Verwaltungsunterlagen bisher jedoch dem Staatsarchiv nicht angeboten. Mir wurde zugesagt, dies umgehend nachzuholen.

5.6.1.2 Juristisches Dekanat

5.6.1.2.1 Bescheinigungen über Studienleistungen

Das Dekanat sieht für Studenten, die die zum Semesterschluss vorgesehene Klausur erfolgreich geschrieben haben, die Ausgabe einer entsprechenden schriftlichen Bescheinigung vor. Manche Studenten holen diese Bescheinigungen – aus verschiedenen Gründen – jedoch nicht ab, sodass sie im Dekanatsbüro zunächst liegen bleiben. Nicht geklärt war durch entsprechend klare interne Anweisung, wie lange solche Scheine aufzubewahren sind, ehe sie dem Staatsarchiv zur evtl. Archivierung überlassen oder zur Vernichtung freigegeben werden können. Mir wurde zugesagt, die Frage umgehend zu klären und die Verfahrensweise in einer internen Anordnung klarzustellen.

5.6.1.2.2 Mitarbeiterdaten auf der Homepage

Die Homepage der Hochschule enthält auch unterschiedliche Informationen über den Fachbereich Rechtswissenschaften. Neben einzelnen Professoren, die persönlich mit Bild vorgestellt werden, sind auch die Namen der ihnen zugeordneten Mitarbeiter genannt.

Die allgemeine Problematik der Erwähnung von Mitarbeiter-Daten auf der Homepage einer Behörde habe ich bereits im 25. Tätigkeitsbericht, Ziff. 8.3 erörtert. Diesen Grundsätzen entsprechend hatte das Hessische Ministerium für Wissenschaft und Kunst in einem Erlass vom 27. Februar 2002 die allgemeinen Voraussetzungen der Veröffentlichungen solcher Hochschulmitarbeiter-Daten festgelegt. Danach können Name und Kontaktdaten von Hochschuldozenten einschließlich ihrer Forschungsgebiete und Schwerpunkte auf der Homepage auch ohne ihre Einwilligung erwähnt werden. Zu diesem Kreis gehören aber nicht alle ihre Mitarbeiter. Mir wurde daher zugesagt, deren schriftliche Einwilligung in die Veröffentlichung einzuholen, soweit eine solche personenbezogene Darstellung weiterhin gewünscht wird.

5.6.2 Beratung der Hochschule für Musik und Darstellende Kunst in Frankfurt am Main

Es kann nicht Aufgabe von Entwicklern und Verkäufern von Verwaltungsprogrammen sein, in dieser Rolle gleichzeitig auch eine Vorabkontrolle zu fertigen für die Behörde, die das Programm einsetzen will.

Die Hochschule für Musik und Darstellende Kunst bat mich um datenschutzrechtliche Beratung im Zusammenhang mit der Einführung eines so genannten Informations- und Kommunikationsservers. Dieser soll dem internen und externen Dokumenten- und Datenaustausch folgender Benutzergruppen in der Hochschule dienen:

- zentrale Verwaltung
- Fachbereichsverwaltung
- Hochschullehrer
- Lehrbeauftragte
- Studierende.

Mit der Aufgabe, die Einrichtung einer solchen Kommunikationsplattform zu planen und vorzubereiten, hat die Hochschule ein Unternehmen beauftragt.

Bislang gab es nur ein internes Rechnernetz, jedoch ohne einen Zentralserver, auf dem entsprechend einem gemeinsamen, allgemein gültigen Aktenplan Dokumente und Informationen abgelegt werden konnten. Auch fehlte damit eine zentrale Steuerung der Software-Updates einschließlich der Sicherheitsprogramme und Datensicherungen.

Unter dem Gesichtspunkt der Datensicherheit war die Einrichtung zentraler E-Mail und Dateiserver zu begrüßen, die die zentrale Verwaltung von Benutzerprofilen und eine entsprechende Datensicherung ermöglichen.

Beim Einsatz dieser neuen Software werden auch unterschiedliche personenbezogene Daten verarbeitet. Neben den persönlichen Daten der Systemnutzer wie persönliche Notizen, Termine und E-Mails sind auch zahlreiche Inhalte mit Personenbezug vorgesehen.

Vor Einführung des Systems war daher die Anfertigung einer Vorabkontrolle nach § 7 Abs. 6 HDSG durchzuführen.

§ 7 Abs. 6 HDSG

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.

Den mir vorgelegten ersten Entwurf der Vorabkontrolle hatte der Auftragnehmer erstellt, der die Kommunikationsplattform planen und vorbereiten sollte. Dieses Verfahren ist nicht akzeptabel. Die Vorabkontrolle nach § 7 Abs. 6 HDSG ist von der für den Einsatz des Verfahrens verantwortlichen Stelle durchzuführen. Das bleibt die Hochschule als Auftraggeber auch dann, wenn sie sich für die Konzeption oder sogar für den Betrieb des Verfahrens eines Auftragnehmers bedient. Die Vorabkontrolle soll gerade die datenschutzrechtlichen Schwächen und Risiken sowie die technischen und organisatorischen Maßnahmen zur Vermeidung solcher Risiken aufzeigen und auf dieser Basis bewerten, ob Gefahren für den Datenschutz durch den Einsatz des Verfahrens bestehen. Der Auftragnehmer hat das wirtschaftliche Interesse, seine Dienstleistungen und die von ihm vorgeschlagenen Produkte im guten Licht erscheinen zu lassen. Führt er die Vorabkontrolle durch, besteht eine klare Interessenkollision.

Ich habe der Hochschule meine Bedenken mitgeteilt und sie auf
die Notwendigkeit ergänzender Darstellungen und eigener Bewertungen in der Vorabkontrolle hingewiesen. Die letzte Fassung der Vorabkontrolle, in der auch meine inhaltliche Kritik an der Vorversion Berücksichtigung fand, wurde daher von der Verwaltungsleitung der Hochschule selber konzipiert und verantwortet, bevor sie vom internen Datenschutzbeauftragten abschließend geprüft wurde.

5.7 Forschung und Statistik

5.7.1 Aufbau eines Forschungsdatenzentrums der Statistischen Landesämter

Das Datenschutzkonzept des Forschungsdatenzentrums ist von den Datenschutzbeauftragten des Bundes und der Länder ganz überwiegend nicht akzeptiert worden. Für den vorläufigen Testbetrieb sind detaillierte restriktive Rahmenbedingungen formuliert worden. Für den zukünftigen Echtbetrieb müssen neue Rechtsgrundlagen erarbeitet werden. Eine Verwaltungsvereinbarung zwischen Bund und Ländern über die Zusammenarbeit der Statistischen Ämter des Bundes und der Länder genügt dazu nicht.

5.7.1.1 Aufgabe und Ziel des Forschungsdatenzentrums

Im Oktober 2001 erfolgte die Einrichtung des Forschungsdatenzentrums des Statistischen Bundesamtes. Um der Wissenschaft auch den Zugang zu den dezentral erhobenen Statistiken zu ermöglichen und die regionale Erreichbarkeit zu verbessern, haben die Statistischen Landesämter im März 2002 beschlossen, ein Forschungsdatenzentrum der Statistischen Landesämter einzurichten. Die Leitung erfolgt durch einen Lenkungsausschuss, in dem mehrere Statistische Landesämter vertreten sind und dessen Vorsitz zunächst beim Bayerischen Landesamt für Statistik und Datenverarbeitung liegt. Die Verwaltungs- und Koordinationsaufgaben werden von einer Geschäftsstelle wahrgenommen, die im Landesamt für Datenverarbeitung und Statistik Nordrhein-Westfalen eingerichtet wurde. Ziel des Forschungsdatenzentrums ist es, den Zugang der empirisch arbeitenden Wissenschaft zu den Mikrodaten der amtlichen Statistik in enger Kooperation und unter Berücksichtigung

der gegebenen Zuständigkeiten der Statistischen Ämter des Bundes und der Länder weiter auszubauen; etwa 90 % der Mikrodaten befinden sich bei den Landesämtern. Um dieses Ziel zu realisieren, soll eine wesentliche Aufgabe der Forschungsdatenzentren darin bestehen, ausgewählte Mikrodaten über unterschiedliche Nutzungswege für länderübergreifende wissenschaftliche Analysen zugänglich zu machen. Um eine möglichst zeitnahe Datenbereitstellung zu gewährleisten, soll eine fachlich zentralisierte Datenhaltung in mehreren Statistischen Landesämtern eingerichtet werden (s. auch www.forschungsdatennetzwerk.de).

5.7.1.2 Datenschutzkonzept

Das Datenschutzkonzept für das Forschungsdatenzentrum der Statistischen Landesämter ist Gegenstand der Diskussion zwischen den Statistischen Landesämtern und den Datenschutzbeauftragten des Bundes und der Länder gewesen. Gegenstand der Diskussionen waren insbesondere Fragen der rechtlichen Grundlagen einer Zentralisierung der Statistiken bei einzelnen Landesämtern und des Bereitstellens von Mikrodaten für die Wissenschaft (s. 32. Tätigkeitsbericht, Ziff. 10.1). Aufgrund der Diskussionen wurde das Konzept überarbeitet. Die direkte Nutzung von Mikrodaten durch die Wissenschaft wurde auf faktisch anonymisierte Mikrodaten beschränkt und das Konzept für die Einrichtung einer fachlich zentralisierten Datenhaltung konkretisiert. Gleichwohl wurde das Datenschutzkonzept weiter kontrovers diskutiert. Von den Datenschutzbeauftragten des Bundes und der Länder wurden ganz überwiegend folgende Positionen vertreten:

- Ein Echtbetrieb ist nur möglich, wenn die damit verbundene zentrale Verarbeitung von Statistikdaten auf normenklare Rechtsgrundlagen gestützt werden kann.
- Der Testbetrieb – für den ebenfalls die Rechtsgrundlage fehlt – wird während der Testphase nicht beanstandet, sofern
  - der Betrieb des Forschungsdatenzentrums während der Testphase auf wenige Regionalstellen, maximal fünf, beschränkt wird,
  - die Dauer des Testbetriebs auf längstens zwei Jahre verkürzt wird,
  - parallel ein Modell getestet wird, bei dem eine zusätzliche zentrale Speicherung auf Vorrat nicht erforderlich ist, und
  - die Verwendung des Begriffs „faktische Anonymisierung“ der Definition in § 16 Abs. 6 BDSG entspricht.

Der Bayerische Landesbeauftragte für den Datenschutz hat sich hierbei der Stimme enthalten. Ich habe gegen diese Anforderungen gestimmt, weil mir insbesondere die detaillierten Begrenzungen des Testprojekts zu restriktiv erschienen, um valide Testergebnisse erhalten zu können. Für den künftigen Echtbetrieb müssen allerdings auch aus meiner Sicht neue rechtliche Grundlagen geschaffen werden, da es sich um eine umfassende Änderung der Infrastruktur der amtlichen Statistik handelt, die dauerhaft etabliert werden soll.

5.7.1.3 Ämterübergreifende Aufgabenerledigung

Das Pilotprojekt „Forschungsdatenzentrum“ soll nach den aktuellen Vorstellungen der Statistikämter in eine sehr viel umfassendere Arbeitsteilung münden. Die Statistischen Landesämter und das Statistische Bundesamt beabsichtigen, ihre bereits bei der Softwareentwicklung und -pflege praktizierte Zusammenarbeit auf andere statistische Arbeiten auszudehnen. Die Anregung dazu gab eine Empfehlung der Rechnungshöfe des Bundes und der Länder vom November 2002. Um die Effizienz bei der Aufgabenerledigung zu steigern und Kosten zu senken, sollen nach dem Prinzip „Einer oder einige für alle“ einzelne Statistikämter künftig auch die Statistikaufbereitung und weitere Arbeiten für andere Ämter erledigen. Alle Statistiken, die bundesweit und in Zusammenarbeit zwischen dem Statistischen Bundesamt und den Statistischen Ämtern der Länder bearbeitet werden (dazu zählen die Bundesstatistiken, einschließlich der auf EU-Recht basierenden Statistiken, und die sog. „koordinierten Länderstatistiken“), sollen in Zukunft arbeitsteilig erstellt werden. Bund und Länder beabsichtigten zunächst, die Zusammenarbeit in einer Verwaltungsvereinbarung zu regeln. Zu dem Entwurf einer „Verwaltungsvereinbarung über eine ämterübergreifende Aufgabenerledigung in der amtlichen Statistik“ vom 2. August 2004 bat mich das Hessische Statistische Landesamt um Stellungnahme.

Der Entwurf ging in § 3 Abs. 2 davon aus, dass die Aufbereitungsarbeiten für andere Statistische Ämter datenschutzrechtlich als Datenverarbeitung im Auftrag zu charakterisieren seien. Zwangsläufig wiederholte sich daher die bereits im Zusammenhang mit der Einrichtung der Forschungsdatenzentren geführte Kontroverse, ob es sich bei der geplanten Zusammenarbeit um Datenverarbeitung im Auftrag oder um eine Funktionsübertragung handelt. Letzteres hätte zur Folge, dass eine bereichsspezifische gesetzliche Regelung notwendig wäre.

Das Hessische Landesstatistikgesetz erlaubt dem Statistischen Landesamt, bei der Durchführung amtlicher Statistiken einzelne Arbeiten an Dritte zu übertragen, sofern sichergestellt ist, dass die Vorschriften zum Schutz personenbezogener Daten und der statistischen Geheimhaltung eingehalten werden. Die Übertragung der Arbeiten sämtlicher Verarbeitungsphasen

einer Statistik, von der Vorbereitung über die Datenerhebung bis zur Aufbereitung, auf ein anderes Statistikamt kann wohl kaum noch als Durchführung einzelner Arbeiten durch Dritte gewertet werden. Bei einer Datenverarbeitung im Auftrag dürften darüber hinaus den anderen Statistikämtern nur Arbeiten übertragen werden, die mit technischen oder organisatorischen Ermessensentscheidungen, nicht aber mit Entscheidungen über das Ob und Wie der Datenverarbeitung, verbunden sind. Bei Plausibilitätsprüfungen könnte diese Grenze leicht überschritten werden, sodass in diesem Fall von einer Funktionsübertragung auszugehen wäre. Funktionsübertragungen sind jedoch nach dem Landesstatistikgesetz unzulässig.

Für jede Statistik, die das Hessische Statistische Landesamt durch ein anderes Statistisches Landesamt (teilweise) bearbeiten lassen möchte, müsste geprüft werden, ob die Anforderungen des Landesstatistikgesetzes erfüllt sind. Allein dieser Umstand spricht schon gegen die geplante Verwaltungsvereinbarung. Da es um Bundes- und EU-Statistiken geht, müsste die Rechtmäßigkeitsprüfung bei der Übertragung statistischer Arbeiten auf eine anderes Landesamt in jedem Bundesland nach den dort geltenden landesrechtlichen Vorschriften, die keineswegs bundeseinheitlich sind, erfolgen. Rechtliche Hindernisse in einem Bundesland würden das Konzept „Einer für alle“ zunichte machen.

In Hessen kommt hinzu, dass sich im Fall der Auftragsdatenverarbeitung die vom Hessischen Statistischen Landesamt mit statistischen Arbeiten betrauten Ämter anderer Bundesländer gem. § 4 Abs. 3 HDSG der Kontrolle des Hessischen Datenschutzbeauftragten unterwerfen müssten. Unabhängig davon, ob die Statistikämter dazu rechtlich befugt wären, könnte die Umsetzung dieser landesgesetzlichen Anforderung zu Konflikten mit den Ämtern und mit den für sie zuständigen Datenschutzkontrollbehörden führen.

Ich habe mich daher gegenüber dem Hessischen Statistischen Landesamt für eine einheitliche gesetzliche Regelung der ämterübergreifenden Aufgabenerledigung ausgesprochen. Inzwischen scheint auch die amtliche Statistik von der Notwendigkeit einer gesetzlichen Regelung auszugehen.

5.8 Gesundheitswesen

5.8.1 Aufbewahrung und Verwendung von Blut- und Gewebeproben in hessischen Krankenhäusern

Künftig sollte in Krankenhäusern intern konkret festgelegt und für die Patientinnen und Patienten transparent sein, wie lange Blut- und Gewebeproben für welche Zwecke aufbewahrt und verwendet werden. Werden die Proben nicht mehr für die Behandlung benötigt, sondern für allgemeine Forschungszwecke aufbewahrt (Biobanken), sollte künftig die Einwilligung der Betroffenen eingeholt werden.

Infolge der ständig zunehmenden Möglichkeiten, Blut- und Gewebeproben genetisch zu analysieren, ist die Gewinnung, Aufbewahrung und Verwendung von Blut- und Gewebeproben in den letzten Jahren zunehmend Gegenstand öffentlicher Diskussionen gewesen. Das Thema tangiert neben Aspekten des Arztrechts, des Zivilrechts und des Strafrechts auch datenschutzrechtliche Aspekte: Die Aufbewahrung und Verwendung von Proben, die mit den Identitätsdaten der Patienten beschriftet sind oder mit einem Pseudonym, das einem einzelnen Patienten zugeordnet werden kann, fällt unter den Anwendungsbereich der Datenschutzgesetze (s. hierzu z. B. auch BTDrucks. 14/8256). Ich habe mich 2003 und 2004 stichprobenartig in verschiedenen Kliniken in Hessen über die derzeitige Praxis des Umgangs mit Blut- und Gewebeproben informiert. Im Vordergrund stand dabei die Praxis in den Universitätskliniken, in denen besonders viele Proben entnommen, untersucht und aufbewahrt werden. Auf Grund der von mir gewonnenen Informationen bin ich zu der Auffassung gelangt, dass die rechtlichen Rahmenbedingungen und die Verfahrensweise bei der Gewinnung, Aufbewahrung und Verwendung von Blut- und Gewebeproben weiterer Klärung und Festlegung bedürfen. Nach Abschluss der Diskussionen über die Praxis in den Universitätskliniken wird zu klären sein, in welchem Umfang die Diskussionsergebnisse auf andere Krankenhäuser zu übertragen sind.

5.8.1.1 Behandlungsproben und Forschungsproben

Bei der Verwendung von Proben sind grundsätzlich zu unterscheiden

- Proben, die zur medizinischen Diagnostik und Behandlung entnommen und aufbewahrt werden („Behandlungsproben“)
  Sie können auf der Grundlage des Behandlungsvertrages und der Einwilligung in den körperlichen Heileingriff aufbewahrt und verwendet werden. Eine spezielle gesonderte Einwilligung des Patienten ist hierfür nicht erforderlich.

- Proben, die speziell zu Forschungszwecken entnommen und verwendet werden („Forschungsproben“).
  Eine gesonderte schriftliche Information und Einwilligung der Spender ist erforderlich, soweit eine (Teil-) Probenentnahme ausschließlich zu Forschungszwecken erfolgt.

Im Vordergrund der von mir geführten Gespräche standen die Proben, die (zunächst) zur medizinischen Diagnostik und Behandlung in den Kliniken entnommen und verwendet werden. Dabei ging es um die Fragen, wie lange und für welchen

Zweck Proben aufbewahrt werden und inwieweit die Patienten über die Verwendung informiert sind bzw. um Einwilligung gebeten werden.

5.8.1.2 Dauer der Aufbewahrung der Proben für Behandlungszwecke

Künftig sollte in einer Dienstanweisung intern klar festgelegt sein, wie lange die Proben für Behandlungszwecke aufbewahrt werden. Mit Unterstützung aller Beteiligten konnte zwar im Gespräch die Praxis der Aufbewahrung für die verschiedenen Bereiche weitgehend ermittelt werden, die Klärung der Aufbewahrungsfristen war jedoch teilweise sehr aufwändig und sowohl die Dauer der Aufbewahrung als auch die Gründe für die vorgesehene Dauer der Aufbewahrung waren nicht immer vollständig nachvollziehbar. Konkrete einheitliche Empfehlungen der Fachgesellschaften liegen offenbar auch nicht immer vor bzw. decken sich nicht immer mit der Praxis.

Es ist in erster Linie eine Frage der fachlichen Bewertung, wie lange eine Aufbewahrung von Proben in den jeweiligen Klinikbereichen aus medizinischen Gründen erforderlich ist. Allerdings kann z. B. die abstrakte Möglichkeit, dass im Einzelfall nach Jahren eine Anfrage von einer Versicherung bzw. eine Anfrage eines Angehörigen nach dem Tod des Betroffenen kommen könnte, keine systematische pauschale langfristige Aufbewahrung von Proben zu Behandlungszwecken begründen. Selbstverständlich sind auch evtl. spezialgesetzliche Regelungen (z. B. bei Blutspenden) zu berücksichtigen.

Die Dauer der Aufbewahrung der Proben für Behandlungszwecke sollte auch für die Patientinnen und Patienten transparent sein. § 12 Abs. 1 HKG (Hessisches Krankenhausgesetz) i. V. m. § 12 Abs. 4 HDSG legt verbindlich fest, dass die Patienten über die Verarbeitung ihrer Daten und ihre Rechte i. S. v. § 8 HDSG informiert werden müssen (s. a. Art. 3 Abs. 1 EU-Richtlinie).

§ 12 Abs. 1 HKG

Für Krankenhäuser gelten die Bestimmungen des Hessischen Datenschutzgesetzes vom 11. November 1986 (GVBl. I S. 309) in der jeweils geltenden Fassung ohne die Einschränkung für öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen, nach Maßgabe der folgenden Vorschriften.

§ 12 Abs. 4 HDSG

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.

Zur Umsetzung dieser Vorschriften enthalten die Aufnahmeverträge der hessischen Kliniken im Regelfall unter Hinweis auf diese Vorschriften allgemeine Informationen für die Patienten zur Verarbeitung ihrer Daten in der Klinik. Diese Informationen treffen allerdings bisher keine konkreten Aussagen über die Gewinnung, Aufbewahrung und Verwendung von Proben. Die allgemeinen Informationen sind auch im Regelfall inhaltlich nicht zutreffend bezüglich der Proben. Vor dem Hintergrund der zunehmenden Verwendungsmöglichkeiten der Proben sehe ich es als notwendig an, dass die Patienten künftig auch Informationen bezüglich der Verfahrensweise mit ihren Proben erhalten. Für die Patienten eines Klinikums könnten diese Informationen als zusätzlicher Passus in die nächste Auflage des Aufnahmeformulars aufgenommen oder als getrenntes Merkblatt Interessierten ausgehändigt werden. Für die Patienten, deren Proben von externen Stellen an ein Klinikum zur Untersuchung übersandt werden, könnten die Informationen in ein Merkblatt aufgenommen werden, das die externe Stelle an die Patienten weitergibt.

Für Blutspender sollten Informationen über die Dauer der Aufbewahrung der Proben in dem speziell für Blutspender vorgesehenen Formular enthalten sein.

Da in einem Klinikum in den verschiedensten Zusammenhängen Proben entnommen und verwendet werden, kann es sich bei der allgemeinen Patienteninformation nur um eine pauschalierte Darstellung der generellen Verfahrensweise handeln. Darüber hinaus sollte die Patienteninformation für interessierte Patientinnen und Patienten das Angebot enthalten, zusätzliche Informationen zum Umgang mit ihrer individuellen Probe bei einem benannten Ansprechpartner zu erhalten.

Vorgeschlagen für die Patienteninformation wurde von den Universitätskliniken auch der Hinweis, dass die Proben den Patientinnen und Patienten gehören und von ihnen – soweit sie nicht für Behandlungszwecke verbraucht wurden – herausverlangt werden können. Dies entspricht auch der Rechtsauffassung der Landesärztekammer in Hessen. Die Frage, wer Eigentümer der Proben ist, ist primär keine datenschutzrechtliche, sondern eine eigentumsrechtliche Frage. Allerdings wirkt sich die Frage auf die datenschutzrechtlichen Fragestellungen aus.

5.8.1.3 Gewinnung, Aufbewahrung und Verwendung von Proben im Bereich der Humanmedizin

Im Bereich der Humangenetik werden langfristig angelegte DNA-Banken aufgebaut. Die besonderen Bedingungen der Humangenetik (insbesondere handelt es sich um Fragen der langfristigen gesundheitlichen Entwicklung und aus den Analysen ergeben sich vielfach Informationen auch über Angehörige) erfordern es, in diesem Bereich künftig Umfang und Zweck der Verwendung der Daten und Proben mit den Patientinnen und Patienten konkret schriftlich zu vereinbaren. Dies gilt gerade auch im Hinblick auf die derzeit in der Praxis zum Teil vorgesehene zeitlich unbegrenzte Aufbewahrung von Proben und auch im Hinblick auf immer wieder vorkommende Anfragen von Angehörigen bezüglich einer erneuten Analyse der Proben für ihre Behandlungszwecke.

5.8.1.4 Verwendung der für Behandlungszwecke gewonnenen und aufbewahrten Proben für konkrete Forschungsvorhaben

Nach meinen Feststellungen werden für Behandlungszwecke gewonnene und aufbewahrte Proben vielfach für interne oder externe Forschungszwecke verwendet, teils in personenbezogener, teils in pseudonymisierter oder – selten – in anonymisierter Form.

Nach der gegenwärtigen Rechtslage in Hessen ist eine Verwendung von für die Behandlung entnommenen und aufbewahrten Proben für die Forschung in bestimmtem Umfang zulässig. Der Patient stimmt der Entnahme, Untersuchung und Aufbewahrung der Proben für Behandlungszwecke im Behandlungsvertrag und in der Einwilligung in den körperlichen Heileingriff zu. Diese Proben dürfen grundsätzlich nur zweckgebunden, d. h. für die Behandlung, verwendet werden. Nach den Regelungen der §§ 12 Abs. 3 HKG, 33 HDSG dürfen die Proben aber auch darüber hinausgehend im Einzelfall unter bestimmten Voraussetzungen ohne Einwilligung der Patienten für konkrete Forschungsvorhaben durch interne oder externe Forscher verwendet werden.

§ 12 Abs. 3 HKG

Abs. 2 und § 33 des Hessischen Datenschutzgesetzes gelten in Krankenhäusern mit Behandlungseinrichtungen verschiedener Fachrichtungen (Fachabteilungen) auch zwischen diesen.

§ 33 Abs. 1 und 2 HDSG

(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. …

(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.

Im Hinblick auf die umfassenden Möglichkeiten der Analyse von Proben sind diese Voraussetzungen allerdings besonders sorgfältig zu prüfen und zu dokumentieren. Die genannten Vorschriften beziehen sich in jedem Fall auf konkrete (d. h. insbesondere inhaltlich und zeitlich begrenzte) Forschungsvorhaben und können eine Weitergabe/Verwendung der Proben für allgemeine Forschungs-/Probendatenbanken (Biobanken) nicht rechtlich legitimieren.

5.8.1.5 Verwendung der für Behandlungszwecke gewonnenen und aufbewahrten Proben für allgemeine Forschungszwecke („Biobanken“)

Durch den Behandlungsvertrag und die Einwilligung in den Heileingriff ist eine Aufbewahrung und Verwendung der Proben rechtlich legitimiert, solange die Aufbewahrung und Verwendung für Behandlungszwecke erforderlich ist (vgl. oben Ziff. 5.8.1.2). Proben werden allerdings nach meinen Feststellungen zum Teil auch erheblich länger ausschließlich für allgemeine Forschungszwecke aufbewahrt bzw. verwendet, wenn sie für die Durchführung der Behandlung nicht mehr erforderlich sind.

Weder das Hessische Archivgesetz noch das Hessische Krankenhausgesetz enthalten eine Regelung für die langfristige Verwendung von Proben/Daten für den Aufbau von Biobanken für allgemeine Forschungszwecke.

§ 10 Abs. 1 Hessisches Archivgesetz (HArchivG), der für die gesamte öffentliche Verwaltung in Hessen gilt, legt fest, dass Unterlagen nach Ablauf der festzulegenden Aufbewahrungsfrist dem örtlich zuständigen Staatsarchiv zur Archivierung anzubieten sind. Alternativ kann die Anbietung gegenüber dem eigenen öffentlichen Archiv erfolgen, falls der Rechtsträger

der Klinik darüber verfügt. Wenn die Daten nicht als archivwürdig eingestuft und übernommen werden, sind sie zu vernichten. Personenbezogene Proben sind zwar kein typisches Archivgut, sie können aber auch als Informationsträger i. S. v. § 1 Abs. 2 S. 2 HArchivG angesehen werden. In Archive werden nur archivwürdige Unterlagen aufgenommen (§§ 10 ff. HArchivG). Als archivwürdig werden Unterlagen angesehen, die aufgrund ihrer politischen, wirtschaftlichen, sozialen und kulturellen Bedeutung für die Erforschung und das Verständnis von Geschichte und Gegenwart von bleibendem Wert sind (§ 1 Abs. 4 HArchivG). Diese Formulierungen sehen eine **systematische** allgemeine Aufbewahrung von Proben aus Kliniken nicht vor und werden den medizinischen Forschungsinteressen wohl nicht gerecht; jedenfalls haben auch – soweit ersichtlich – staatliche Archive in Hessen bisher in keinem Fall Proben als archivwürdige Unterlagen übernommen. Auch soweit z. B. Universitätskliniken nach den Bestimmungen des Archivgesetzes ein eigenes Archiv unterhalten, sehen die Bestimmungen eine systematische allgemeine Aufbewahrung von Proben nicht vor (s. o.).

Das Hessische Krankenhausgesetz enthält derzeit lediglich Regelungen hinsichtlich der Verwendung von für die Behandlung der Patienten noch erforderlichen Daten/Proben für konkrete, inhaltlich und zeitlich begrenzte Forschungsvorhaben (s. o.).

Wenn die Universitätskliniken künftig unabhängig von der Behandlung Sammlungen von Proben/Daten für allgemeine Forschungszwecke (Biobanken) aufbewahren bzw. aufbauen wollen, sollte künftig die schriftliche Einwilligung der Patienten zur Verwendung ihrer Proben für den Aufbau von Biobanken eingeholt werden. Es liegt im Interesse der Patienten und Ärzte, aber auch und gerade der Forschung, dass die künftige Verwendung von Proben für allgemeine Forschungszwecke mittels Einwilligungserklärungen auf eine klare und verlässliche rechtliche Grundlage gestellt und die Verfahrensweise klar strukturiert wird.

Dies entspricht der Stellungnahme des Nationalen Ethikrats zum Aufbau und Betrieb von Biobanken vom März 2004. Der Nationale Ethikrat hat sich in dieser Stellungnahme u. a. mit der Verwendung von Proben, die im Behandlungszusammenhang gewonnen wurden, auseinander gesetzt und hierzu die Auffassung vertreten, dass es trotz gewisser rechtlicher Spielräume vorzuziehen sein kann, künftig „eine Nutzung von Proben und personenbezogenen Daten in der Forschung in größerem Umfang als bisher an eine ausdrückliche Einwilligung der Betroffenen zu binden“ (www.ethikrat.org; Biobanken für die Forschung, S. 35). Formularmäßige Einwilligungen hält er für zulässig.

Zu den Informationen, die in der Einwilligungserklärung hinsichtlich der künftigen Verwendung der Proben in einer Biobank enthalten sein sollten, haben sich die Datenschutzbeauftragten bereits 2001 in ihren Vorschlägen zur gesetzlichen Regelung von genetischen Untersuchungen geäußert (30. Tätigkeitsbericht, Ziff. 27.14). Der Hamburger Datenschutzbeauftragte hat dem Hamburger Universitätsklinikum einen Anforderungskatalog zu „Datenschutzrechtlichen Anforderungen an Biobanken“ unterbreitet (www.hamburg.datenschutz.de). Auch in der Stellungnahme des Nationalen Ethikrates sind detaillierte Ausführungen zum Inhalt der Einwilligungserklärungen enthalten, die allerdings zum Teil über datenschutzrechtliche Aspekte hinausgehen.

Im Einzelnen sollte die Einwilligung aus datenschutzrechtlicher Sicht insbesondere die folgenden Angaben enthalten:

- die für die Proben und Daten dauerhaft verantwortliche Stelle,
- das Ziel der Forschung,
- Dauer und Art und Weise der Speicherung/Aufbewahrung (pseudonymisiert/anonymisiert),
- Umfang der gespeicherten Daten,
- Kreis der Personen/Stellen, die von den personenbezogenen, pseudonymisierten und/oder anonymisierten Daten/Proben Kenntnis erhalten können,
- bei pseudonymer Speicherung/Aufbewahrung: mögliche Anlässe für eine Reidentifizierung der Spender,
- Hinweis auf die Freiwilligkeit der Einwilligung und darauf, dass den Betroffenen durch die Ablehnung der Einwilligung keine Nachteile entstehen,
- Hinweis auf das Recht des Spenders, die Einwilligung für die Zukunft zu widerrufen und eine Herausgabe oder Vernichtung seiner Probe zu verlangen,
- Informationen zur evtl. Unterrichtung des Spenders über Forschungsergebnisse.

Die Information kann formularmäßig erfolgen. Die Einwilligungserklärung muss sich auf die o. a. Informationen beziehen und getrennt von der Bio-/Datenbank aufbewahrt werden.

Wegen der Sensitivität des Datenbestandes bedarf eine Biobank strikter Zweckbindung und angemessener organisatorisch-technischer Datensicherheitsmaßnahmen. Die Proben und Daten sind gegen einen unberechtigten Zugriff Dritter sicher zu

schützen. Insbesondere sind die Proben von den Behandlungsdaten bzw. -proben zu trennen und sicher zu pseudonymisieren, d. h. die Identifikationsmerkmale (Name, Geburtsdatum, Adresse etc.) sind durch ein Pseudonym zu ersetzen, das ausschließlich berechtigte Personen in vorher festgelegten Bedarfsfällen mit Hilfe einer Schlüsselliste dem Patienten/Spender wieder zuordnen können.

Je nach Sensitivität des Proben-/Datenbestandes kann eine externe Pseudonymverwaltung durch einen schweigeverpflichteten Datentreuhänder geboten sein.

Ich habe die Universitätskliniken um Stellungnahme gebeten und die künftige Verfahrensweise in den Universitätskliniken wird in den nächsten Monaten Gegenstand von Gesprächen zwischen den Kliniken und mir sein.

5.8.2 Zusammenarbeit des Medizinischen Dienstes der Krankenversicherung Hessen mit dem Medizinischen Dienst der Krankenversicherung Sachsen-Anhalt

Der Medizinische Dienst der Krankenversicherung Hessen kann die Archivierung seiner Aktenbestände sowie deren Bereitstellung in elektronischer Form auf den Medizinischen Dienst der Krankenversicherung Sachsen-Anhalt übertragen. Die rechtlichen Voraussetzungen des § 80 SGB X müssen hierzu eingehalten werden und die Datensicherheit beim Auftragnehmer entsprechend § 78a SGB X gewährleistet sein.

5.8.2.1 Grundlage der Zusammenarbeit – Datenverarbeitung im Auftrag

Gemäß § 276 Abs. 2 SGB V ist der Medizinische Dienst der Krankenversicherung (MDK) verpflichtet, seine Gutachtenakten aus dem medizinischen Bereich für fünf Jahre zu archivieren. Dabei handelt es sich um Krankenversicherten-Akten, Pflegegutachten sowie neurologische und psychiatrische Begutachtungen. Der MDK Sachsen-Anhalt hat in Form einer Auftragsdatenverarbeitung gemäß § 80 Abs. 2 SGB X für den MDK Hessen die zentrale Archivierung der in den dortigen Geschäftsstellen befindlichen Gutachtenakten übernommen. Dabei handelt es sich um etwa 800.000 in Papierform vorliegende Akten, die bislang hessenweit bei den verschiedenen Geschäftsstellen des MDK gelagert waren. Die Akten wurden im Verlauf des Jahres 2004 Geschäftsstellenweise nach Magdeburg verbracht und in einem zentralen Archiv eingelagert. Auf Anforderung des MDK Hessen bzw. dessen Gutachter werden einzelne Akten dem Archiv entnommen und diesem auf elektronischem Weg per E-Mail zur Verfügung gestellt. Die Papierakte wird im Anschluss an die Übermittlung, deren Erfolg dem Versender automatisch quittiert wird, vernichtet. Sollte ein Fehler zu einer unvollständigen Übermittlung geführt haben, erfolgt eine Wiederholung. Erfolgt danach noch immer keine Meldung über die Vollständigkeit des Datentransfers, greift der Systemadministrator in den Verfahrensablauf ein.

5.8.2.2 Organisation beim MDK Sachsen-Anhalt

Die Akten der einzelnen Geschäftsstellen wurden in Stahlschränken und anderen Behältnissen sukzessive von zwei beauftragten Transportunternehmen von Hessen nach Magdeburg transportiert. Dort wird der erste Stock einer ehemaligen Fabrik als Lager und für die Datenerfassung genutzt. Die Anforderung von Akten durch die Geschäftsstellen erfolgt per E-Mail und geht bei der Datenerfassungsstelle als Auftrag ein. Von dort wird das Archivpersonal beauftragt, die angeforderte Akte aus dem Lagerbestand herauszusuchen und der Datenerfassung zuzuführen. Die Akte wird in der Folge eingescannt und verschlüsselt (Lotus-Notes-Verschlüsselung) auf den zentralen Server der MDK-Hauptstelle in Oberursel übermittelt. Nach der erfolgreichen Übermittlung werden die temporär auf dem Server des Archivs gespeicherten Dateien gelöscht und die eingescannten Akten zunächst in abschließbaren Containern abgelegt. Sie werden im weiteren Verfahrensablauf dann von einem hierzu beauftragten Unternehmen vernichtet.

5.8.2.3 Rechtliche Zulässigkeit der Auftragsdatenverarbeitung

Datenverarbeitung im Auftrag ist im Regelfall mit der Kenntnisnahme personenbezogener Daten durch den Auftragnehmer verbunden. Der Gesetzgeber hat das zwar zugelassen, in § 80 SGB X jedoch strikte Vorgaben für die Auftragsdatenverarbeitung festgelegt, weil es sich bei den Sozial- bzw. Gesundheitsdaten um besonders sensitive, dem Sozialgeheimnis nach § 35 SGB I unterliegende Daten handelt.

§ 80 SGB X

…

(2) Eine Auftragsdatenverarbeitung für die Erhebung, Verarbeitung oder Nutzung von Sozialdaten ist nur zulässig, wenn der Datenschutz beim Auftragnehmer nach der Art der zu erhebenden, zu verarbeitenden oder zu nutzenden Daten den Anforderungen genügt, die für den Auftraggeber gelten. Der Auftrag ist schriftlich zu erteilen, wobei die Datenerhebung, -verarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind. Der Auftraggeber ist verpflichtet, erforderlichenfalls Weisungen zur Ergänzung der beim Auftragnehmer vorhandenen technischen und organisatorischen Maßnahmen zu erteilen. Die Auftragserteilung an eine nicht-öffentliche Stelle setzt außerdem voraus, dass der Auftragnehmer dem Auftraggeber schriftlich das Recht eingeräumt hat,

1. Auskünfte bei ihm einzuholen,
2. während der Betriebs- oder Geschäftszeiten seine Grundstücke oder Geschäftsräume zu betreten und dort Besichtigungen oder Prüfungen vorzunehmen und
3. geschäftliche Unterlagen sowie die gespeicherten Sozialdaten und Datenverarbeitungsprogramme einzusehen, soweit es im Rahmen des Auftrags für die Überwachung des Datenschutzes erforderlich ist.

…

(4) Der Auftragnehmer darf die zur Datenverarbeitung überlassenen Sozialdaten nicht für andere Zwecke verarbeiten oder nutzen und nicht länger speichern, als der Auftragnehmer schriftlich bestimmt.

Die Übertragung der Archivleistung sowie die elektronische Aufbereitung der Akten durch den MDK Sachsen-Anhalt entsprechen den Vorgaben einer Datenverarbeitung im Auftrag. Rechte und Pflichten von Auftragnehmer und Auftraggeber sind als Anlage zum Dienstleistungsvertrag in einem Datenschutzvertrag schriftlich dokumentiert. Danach hat der MDK Sachsen-Anhalt ausschließlich auf schriftliche Weisung des MDK Hessen hin die Daten zu verarbeiten. Er hat außerdem die Gewähr dafür zu leisten, dass die erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der Sozialdaten getroffen sind.

5.8.2.4 Datensicherheitsmaßnahmen beim MDK Sachsen-Anhalt

Werden Sozialdaten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Die zu erreichenden Schutzziele ergeben sich aus der Anlage zu § 78a SGB X.

§ 78a SGB X

Die in § 35 des Ersten Buches genannten Stellen, die selbst oder im Auftrag Sozialdaten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen einschließlich der Dienstanweisungen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzbuches, insbesondere die in der zu dieser Vorschrift genannten Anforderungen, zu gewährleisten. Maßnahmen sind nicht erforderlich, wenn ihr Aufwand in keinem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Folgende Maßnahmen zum Schutz der Sozialdaten hat der MDK Sachsen-Anhalt getroffen:

5.8.2.4.1 Gewährung der Zutrittskontrolle

Grundsätzlich haben zum Archiv nur die unmittelbar dort Beschäftigten Zutritt. Dritte können nach vorheriger Anmeldung und nur in Begleitung Berechtigter bzw. autorisierter Personen das Archiv betreten.

5.8.2.4.2 Einhaltung der Zugangskontrolle

Die Zugangskontrolle wird durch verschiedene organisatorische und technische Maßnahmen gewährleistet:

- Kontrolle des Zutritts zum Archiv durch Mitarbeiter am Empfang,
- Anmeldung am System mit Benutzerkennung und Passwort,
- Einsatz von passwortgeschützten Bildschirmschonern an den einzelnen PC-Arbeitsplätzen im Archiv,
- Nutzung einer Firewall zur Abschottung des Intranets gegen unbefugte Eingriffe von außen durch Dritte sowie
- Nutzung einer passwortgeschützten Punkt-zu-Punkt-Verbindung auf PC-Ebene bei Aktenanfragen durch den MDK Hessen.

5.8.2.4.3 Sicherstellung der Zugriffskontrolle

Folgende Maßnahmen sollen die Zugriffskontrolle beim Archiv des MDK Sachsen-Anhalt sicherstellen und gewährleisten:

- die Aufbewahrung der beschriebenen Datenträger (nur einmal beschreibbare CDs) in einem Tresor,
- die automatische Erstellung von Konsolprotokollen,
- ein eigener Archiv-Server,
- die Trennung von Test- und Produktionsbetrieb bei Wartungsarbeiten,
- der Einsatz von Verschlüsselungsverfahren, insbesondere im Rahmen des Datentransfers,

– die Zulassung nur lesender Zugriffe für die Nutzerinnen und Nutzer des Archivs bei Recherchen.

5.8.2.4.4 Gewährleistung der Weitergabekontrolle

Die Auftragserteilung erfolgt unter Angabe der Identifizierungsmerkmale (Patienten-Name, Anschrift, Geburtsdatum) einzelfallbezogen. Im Zusammenhang mit der elektronischen Erfassung sowie dem Versand der Akte als Mail werden Verschlüsselungen vorgenommen (128 Bit). Die Kommunikation zwischen den hessischen Stellen und der Altakten-Scan-Stelle beim MDK Sachsen-Anhalt erfolgt ausschließlich über das Programm ISmed-Notes.

5.8.2.4.5 Sicherstellung der Eingabekontrolle

Die Eingabekontrolle erfolgt durch Systemprotokolle über Zugriffe- und/oder Änderungen auf Benutzerinnen- bzw. Benutzerebene. Damit wird sichergestellt, dass feststellbar ist, wer welche Daten wann in die Anwendung eingestellt hat.

5.8.2.4.6 Gewährleistung der Auftragskontrolle

Die Auftragskontrolle wird durch die Vorgaben im Dienstleistungs- sowie im Datenschutzvertrag sichergestellt. Außerdem sind regelmäßige Kontrollen des Datenschutzbeauftragten des MDK-Hessen avisiert.

5.8.2.4.7 Gewährleistung der Verfügbarkeitskontrolle

Gegen den Verlust oder die Zerstörung der Daten (vornehmlich der eingelagerten Akten) sind an verschiedenen Stellen des Gebäudes Feuerlöscher platziert. Es erfolgt eine regelmäßige Datensicherung (eingescannte Akten) und Lagerung der Datenträger in einem getrennten Brandschutzabschnitt sowie einem feuersicheren Tresor.

5.8.2.4.8 Gewährleistung der Organisationskontrolle

Die getrennte Verarbeitung der zu unterschiedlichen Zwecken erhobenen Sozialdaten wird durch die Anlage mehrerer getrennter Archiv-Datenbanken auf physikalisch getrennten Servern und durch die physikalische Trennung der Inhouse-Netze des MDK Sachsen-Anhalt und der Altakten-Scan-Stelle beim MDK Sachsen-Anhalt gewährleistet.

5.8.2.5 Datenschutzrechtliche Probleme im Bereich des Archivs

Die Auftragsdatenverarbeitung durch den MDK Sachsen-Anhalt, die von mir im Rahmen eines Prüfbesuchs in Magdeburg in Augenschein genommen wurde, entsprach bis auf wenige Ausnahmen den Anforderungen, die sich aus der Anlage zu § 78a SGB X ergeben. Allerdings habe ich folgende Änderungen gefordert:

5.8.2.5.1 Standort des Servers

Der Standort des Servers entspricht nicht den Anforderungen an die Zutrittskontrolle gemäß § 78a Nr. 1 SGB X. Zum Problem kann die potenzielle Gefährdung der Hardware durch äußere Einflüsse ebenso werden, wie der jederzeit mögliche Zutritt des gesamten Archivpersonals. Der Server muss daher in einem abgeschlossenen, nur durch befugte Personen zugänglichen Raum untergebracht werden.

5.8.2.5.2 Aufbewahrungsfrist für die Akten

Gemäß § 276 Abs. 2 SGB V sind die Sozialdaten nach fünf Jahren zu löschen. Es gab jedoch keine schriftliche Vereinbarung zwischen dem MDK Hessen und dem MDK Sachsen-Anhalt, die eine regelmäßige und dem gesetzlichen Erfordernis Rechnung tragende Vernichtung hessischer Akten sicherstellt. Eine entsprechende Vereinbarung und Verfahrensweise, die sich an den gesetzlichen Löschfristen orientiert, ist daher unabdingbar. Dies wurde vom MDK inzwischen durch eine Zusatzvereinbarung umgesetzt.

5.8.2.5.3 Vernichtung der Akten nach der elektronischen Übermittlung

Es lag keine Regelung darüber vor, zu welchem Zeitpunkt nach dem Scan-Vorgang und der elektronischen Übermittlung zum MDK-Server in Hessen die Papierakten zu vernichten sind. Ich habe vorgeschlagen, eine zweiwöchige Frist hierfür vorzusehen. Damit werden gegebenenfalls erforderliche „Nachbesserungen“ bei der Übermittlung oder ein eventuell sogar erforderliches abermaliges Scannen der Papierakte berücksichtigt. Die Umsetzung in Form einer Vereinbarung zwischen dem MDK Hessen und dem MDK Sachsen-Anhalt wurde mittlerweile bestätigt.

5.8.2.5.4 Passwortgestaltung/-regelung

Die Anmeldeprozedur im Zusammenhang mit den Vorgaben zur Passwortgestaltung genügte nicht den Anforderungen, die sich aus dem Grundschutzhandbuch des Bundesamtes für die Sicherheit in der Informationstechnologie ergeben. Hierbei handelt es sich um Mindestanforderungen bei der Verarbeitung personenbezogener Daten. Danach sollte ein Passwort mindestens acht Stellen lang sein und möglichst alphanumerisch generiert werden. Auch ist ein regelmäßiger Passwortwechsel vorzunehmen. Dieser Punkt wurde ebenfalls durch die beteiligten Stellen inzwischen korrigiert.

5.8.2.6 Datenverarbeitung beim MDK Hessen

Auch die Datenverarbeitung beim MDK Hessen selbst war Gegenstand meiner Prüfungen. Die zentrale Zusammenführung der Aktenbestände aller hessischen Geschäftstellen und deren (auf Anforderung) elektronische Übermittlung durch den MDK Sachsen-Anhalt zum zentralen Archivserver der Hauptstelle in Oberursel hat einige datenschutzrechtliche Fragestellungen aufgeworfen.

5.8.2.6.1 Verfahrensablauf

Wenn eine Krankenkasse ein Gutachterauftrag an eine Geschäftsstelle des MDK Hessen erteilt, wird der Auftrag in das EDV-System ISmed eingestellt. Im ISmed-Archiv erfolgt eine Recherche über mögliche Vorakten zum Versicherten. Bei einem positiven Rechercheergebnis wird in ISmed automatisiert eine Anforderungsmail für die Vorakte bei der Altakten-Scan-Stelle nach Magdeburg geschickt. Nach dem Scan-Vorgang der dort gelagerten Akte wird per Mailverschlüsselungsverfahren (Lotus-Notes) der Inhalt der Akte in das elektronische Archivsystem des MDK Hessen übermittelt. Danach wird eine Papierlaufakte für den anfordernden Gutachter erstellt, die als Papierausdruck Teile der angeforderten und elektronisch übermittelten Akte beinhalten kann. Es erfolgt die Begutachtung, an deren Ende die Entscheidung des Gutachters steht, welche zusätzlich entstandenen Unterlagen (z. B. das aktuell gefertigte Gutachten) eingescannt werden sollen. Die Prüfung und Freigabe des Gutachtens in seiner elektronischen Form im ISmed erfolgt durch den Gutachter. Die Authentifizierung erfolgt mittels eines Noteszertifikats, das individuell einem bestimmten Gutachter zugeordnet ist. Ein unterschriebenes Papierexemplar wird nicht mehr erstellt. Mit der Freigabe wird das elektronische Exemplar automatisch in das zentrale Archiv auf dem MDK-Server der Hauptstelle übertragen. Die Papierlaufakte geht an den zuständigen Scannerarbeitsplatz der jeweiligen Beratungsstelle (Pflege- oder Krankenversicherung). Dort wird die Laufakte gescannt, indexiert und an den Archivserver übermittelt, wo eine Zuordnung zu den bereits gespeicherten Unterlagen erfolgt. Außerdem wird ein Papierausdruck (des Gutachtens) gefertigt, der (nicht unterschrieben) an die Krankenkasse versandt wird.

5.8.2.6.2 Datenschutzrechtliche Probleme beim MDK Hessen

5.8.2.6.2.1 Anforderung von Akten (Gutachterauftrag)

Jeder Gutachterauftrag wird in einer für die jeweilige Geschäftsstelle einsehbaren Auftragsdatei abgelegt. Es gibt sieben Beratungsstellen, die über ISmed grundsätzlich nur auf ihre „eigenen“ Gutachten zugreifen können. Darüber hinaus kann jedoch jede Beratungsstelle über die Funktion „neuen Fall anlegen“ Informationen über die Gutachteraufträge aller anderen Beratungsstellen aufrufen, die in einer so genannten zentralen Verweisdatei gespeichert sind. Die zentrale Verweisdatei ermöglicht einen hessenweiten Überblick über alle in Auftrag gegebenen Gutachten.

Das datenschutzrechtliche Problem ist, dass durch das „Neu-Anlegen“ eines Falles (unter der Voraussetzung, dass Name und Geburtsdatum eines Betroffenen bekannt sind) jeder Mitarbeiter, der die Berechtigung zum Anlegen eines neuen Falles hat, über die Verweisdatei auf das Zentralarchiv des Servers in Oberursel zugreifen könnte. Dort sind alle zu dem Betroffenen vorhandenen Dokumente abgelegt und wären in der Folge einsehbar.

Die Anzahl der Personen, die die Berechtigung zum Anlegen eines neuen Falles haben, betrug im Juni 2004 etwa 410 Personen (Gutachter und Assistenzkräfte). Allerdings soll durch eine geplante Umstrukturierung innerhalb des MDK die Zahl der Personen auf ca. 340 Personen reduziert werden. Dennoch bleibt die große Zahl der potenziell Zugriffsberechtigten problematisch. Um eine Kontrolle zu erreichen, wer MDK-seitig die Unterlagen eines in der Datenbank gespeicherten Patienten sich zunächst hat zur Verfügung stellen lassen, diese dann aber doch nicht für die Erstellung eines Gutachtens nutzt, wird eine so genannte „Löschliste“ angelegt. In diese Liste wird der Name des Betroffenen, der Zeitpunkt der Löschung des Auftrags sowie der Verantwortliche, nicht aber der Grund für die Löschung, aufgenommen. Ohne Zweifel kann es vorkommen, dass man versehentlich einen falschen Namen verwendet hat oder eine Falscheingabe aus anderen Gründen erfolgt ist, was eine Löschung erforderlich macht. Eine möglicherweise gezielte Falscheingabe mit dem Zweck, unbefugt (also ohne Auftrag) an Daten eines Betroffenen zu gelangen, wird allerdings nicht verhindert. Um das Problem bei der Zugriffskontrolle dennoch lösen zu können, wurde im Zusammenhang mit der Prüfung des Verfahrens in der Geschäftsstelle des MDK Hessen in Offenbach vereinbart, dass der Datenschutzbeauftragte des MDK die Listen regelmäßig auf ihre Plausibilität hin überprüft und ggf. gezielte Nachfragen zu einzelnen Löschvorgängen vornimmt. Einträge in der Löschliste, die älter als ein Jahr sind, werden automatisch gelöscht.

5.8.2.6.2.2 Konzeption der Zugriffsberechtigungen

Das Konzept über die Vergabe der Zugriffsberechtigungen konnte zum Zeitpunkt der Prüfung in der Geschäftsstelle Offenbach nicht befriedigend geklärt werden. Auf meine Anforderung hat der MDK Hessen eine Aufstellung der Nutzergruppen und deren Zugriffsberechtigungen erstellt. Daraus geht hervor, welche Gruppen (Gutachter, Assistenzkräfte, Administratoren) welche Berechtigungen im Einzelnen haben. Mittlerweile gibt es weitergehende Beschreibungen des Vergabeverfahrens. Damit konnten meine Bedenken in diesem Punkt ausgeräumt werden.

5.8.2.6.2.2.1 Zugriffe der Gutachter

Die Gutachter haben einen lesenden und schreibenden Zugriff auf alle offenen Aufträge ihrer Beratungsstelle. Es besteht jedoch kein Zugriff auf evtl. zu den Aufträgen gehörende Gutachten (es sei denn, es wären eigene Gutachten). Allerdings kann das Recht hierzu eingeräumt werden, wenn der Systemverwalter den Gutachter in die entsprechende persönliche ISmed-Gruppe eines jeweils anderen Gutachters einträgt. Dies muss jedoch mit schriftlichem Antrag und über den Dienstvorgesetzten erfolgen.

5.8.2.6.2.2.2 Zugriffsrechte innerhalb der Datenbanken

ISmed ist in einer Notes-eigenen Scriptsprache programmiert und arbeitet intern mit einer großen Anzahl von Notes-Datenbanken. Diese Datenbanken sind so genannte dokumentenorientierte Datenbanken. Die Datensätze dieser Einheiten sind ganze Dokumente und bestehen aus einer Reihe von Feldern, die auch einzeln angesprochen werden können. Notes unterscheidet primär öffentliche Dokumente, die jedem gehören, der das Recht hat, mit der Datenbank zu arbeiten und normale Dokumente, die demjenigen gehören, der sie erstellt hat (so genannte Zugriffsart: Autor).

Der Zugriff auf Notes-Datenbank-Dokumente wird differenziert über so genannte Zugriffskontrolllisten (ACL = Access-Control-List) gesteuert. Auch wenn z. B. ein öffentliches Dokument allen gehört, kann über diese Zugriffskontrolllisten einem Nutzer oder einer Nutzergruppe das Recht, öffentliche Dokumente zu lesen, entzogen werden. Die Zugriffsrechte erhält man durch eine Gruppenzugehörigkeit und seine Rolle (Gutachter, Sekretärin, Administrator etc.). Die Vergabe der Rechte erfolgt durch den Systemverwalter.

5.8.2.7 Weitere Verfahrensweise

Ich habe dem MDK Hessen meinen Prüfbericht übermittelt und die Beseitigung der datenschutzrechtlichen Defizite gefordert. Über die Umsetzung der erforderlichen Maßnahmen hat mich der Geschäftsführer des MDK Hessen informiert.

5.8.3 Durchführung strukturierter Behandlungsprogramme durch die AOK Hessen

Mit der Einführung der strukturierten Behandlungsprogramme erhalten die Krankenkassen erstmals in bestimmten Bereichen detaillierte medizinische Patientendaten. Ich habe mich stichprobenhaft bei der AOK Hessen über die Weiterverarbeitung der Daten zu Diabetes mellitus Typ 2 informiert. Die Behebung der von mir festgestellten Mängel, die sich im Wesentlichen auf den Zugriff und die Protokollierung der Datenbestände beschränken, ist zugesagt worden.

5.8.3.1 Strukturierte Behandlungsprogramme: eine Kurzbeschreibung

Strukturierte Behandlungsprogramme (Disease-Management-Programme, kurz DMP) haben zum Ziel, den Behandlungsablauf und die Qualität der medizinischen Versorgung chronisch kranker Patienten zu verbessern. Denn im Gegensatz zur Akutversorgung wird die Betreuung chronisch Kranker in Deutschland im internationalen Vergleich als verbesserungsbedürftig bewertet.

Mit dem am 1. Januar 2002 in Kraft getretenen Gesetz zur Reform des Risikostrukturausgleichs in der gesetzlichen Krankenversicherung hat die Bundesregierung die gesetzlichen Grundlagen für Disease-Management-Programme geschaffen. Krankenkassen, die sich gezielt um chronisch Kranke kümmern, soll daraus im Kassenwettbewerb kein finanzieller Nachteil entstehen.

DMP müssen gesetzlich festgelegten Qualitätskriterien entsprechen. Zuständig für Prüfung und Zulassung der einzelnen Programme ist das Bundesversicherungsamt in Bonn. Die strukturierten Behandlungsprogramme der AOK heißen Curaplan.

Die Kooperation zwischen Ärzten, Krankenhäusern und der Krankenkasse in Form von DMP ist derzeit für drei Diagnosen realisiert: Diabetes mellitus Typ 2, Brustkrebs und koronare Herzkrankheit.

5.8.3.2 Gesetzliche Grundlagen für die Durchführung strukturierter Behandlungsprogramme

Der gesetzliche Rahmen der neuen strukturierten Behandlungsprogramme ist in den §§ 137f ff. SGB V festgelegt. Auf der Grundlage des § 266 Abs. 7 Nr. 3 SGB V regelt das Bundesministerium für Gesundheit und Soziale Sicherung (BMGS) durch Änderungsverordnungen zur Risikostruktur-Ausgleichsverordnung (RSAV) u. a. die Krankheiten, die Gegenstand der DMP sein können, die Anforderungen an die Zulassung dieser Programme sowie die für die jeweiligen Krankheiten erforderlichen personenbezogenen Daten für Patienten (s. 31. Tätigkeitsbericht Ziff. 17.3). Das BMGS erlässt die Rechtsgrundlagen zur Umsetzung von DMP als Änderungsverordnungen zur RSAV. Die Verordnungen basieren seit dem 1. Januar 2004 auf Empfehlungen des Gemeinsamen Bundesausschusses, in dem u. a. Ärzte, die Krankenkassen und der Krankenhäuser vertreten sind. Der Gemeinsame Bundesausschuss empfiehlt dem BMGS Diagnosen, für die DMP erarbeitet werden sollen. Für die vom Ministerium dann festgelegten Krankheitsbilder gibt der Ausschuss Empfehlungen zu den Anforderungen an die inhaltliche Ausgestaltung der Behandlungsprogramme. Das BVA prüft, ob die Programme den gesetzlichen Kriterien entsprechen und erteilt nach positiver Entscheidung seine Zulassung. Der Weg der Zulassung ist in § 137g SGB V festgelegt.

Die Risikostruktur-Ausgleichsverordnung (RSAV) in ihrer derzeit gültigen Fassung bildet die rechtliche Grundlage der Disease-Management-Programme. In den §§ 28 ff. und den darin enthaltenen Anlagen 1 bis 8b sind die Vorgaben enthalten, die für die derzeit realisierten Programme Gültigkeit haben.

Das DMP Diabetes mellitus Typ 2 wurde durch die 4. Verordnung zur Änderung der Risikostruktur-Ausgleichsverordnung rechtlich verankert. Darin enthalten sind die Anforderung an das Programm, darunter zum Beispiel die Behandlung nach evidenzbasierten Leitlinien, und eine Übersicht der Daten, die der Arzt bei der Einschreibung eines Patienten in das Programm erfassen muss (Erstdokumentation).

5.8.3.3 Zielsetzung der DMP, die Beteiligten und die datenschutzrechtliche Problemstellung

DMP verfolgen verschiedene Ziele: zunächst geht es darum, Behandlungsziele zu formulieren. Danach muss die Therapie festgelegt werden. Schließlich gilt es, die Kooperation der Versorgungsträger untereinander zu beschreiben. Am Ende soll eine gezieltere und damit bessere Versorgung der chronisch Kranken erreicht werden. Dies sollen auch zusätzliche, qualitätssichernde Maßnahmen ermöglichen.

Der Gesetzgeber hat beschlossen, dass die DMP von den Krankenkassen durchgeführt werden sollen. Dies hat zur Folge, dass die Krankenkassen in diesen Bereichen detaillierte medizinische personenbezogene Patientendaten zur Steuerung der DMP erhalten. Die individuelle Therapieentscheidung soll allerdings nach wie vor dem behandelnden Arzt obliegen. Aus datenschutzrechtlicher Sicht stellt sich die Frage, wie in diesen Bereichen die Aufgaben der Ärzte zur Verarbeitung personenbezogener Patientendaten einerseits und die Aufgaben der Krankenkassen zur Verarbeitung personenbezogener Patientendaten andererseits künftig voneinander abgegrenzt werden und in welchem Umfang und auf welche Art und Weise die Krankenkassen künftig die erstmals bei ihnen vorhandenen detaillierten medizinischen Patientendaten weiterverarbeiten. Diese Frage ist weder in den neuen gesetzlichen Regelungen noch in der RSAV detailliert geregelt. Vor diesem Hintergrund habe ich mich 2004 stichprobenhaft über die Weiterverarbeitung der Patientendaten bei der AOK Hessen informiert, insbesondere bei einem Prüfbesuch bei der DMP-Kopfstelle in Pohlheim.

5.8.3.4 Organisation des DMP Diabetes mellitus Typ 2

Verschiedene Krankenkassen innerhalb Hessens, darunter auch die AOK Hessen, haben eine Arbeitsgemeinschaft (ARGE) gebildet, der auch der Verband der Hausärzte in Hessen angehört. Die ARGE vertritt die Interessen der sie bildenden Gruppen und tritt rechtlich als Empfänger der ärztlichen Dokumentationen auf, welche die Hausärzte erstellen. Allerdings hat die ARGE die Datenverarbeitung selbst an eine so genannte Datenstelle abgegeben, die im Auftrag der ARGE die Bearbeitung der Daten, die Übermittlung an im DMP-Vertrag festgelegte Stellen sowie die Speicherung der Daten übernimmt. Außerdem wickelt die Datenstelle die Vergütungsregelungen mit den am DMP teilnehmenden Hausärzten ab. Datenempfänger sind zum einen die Krankenkassen, die einen im Umfang festgelegten Datensatz erhalten, sowie eine Gemeinsame Einrichtung, in der Maßnahmen zur Qualitätssicherung festgelegt werden.
Der DMP-Vertragsarzt muss zunächst den Patienten über Möglichkeiten und Inhalte des DMP informieren. Hat sich der Patient bereit erklärt, am DMP teilzunehmen, hat er eine Teilnahmeerklärung zu unterschreiben. Zusätzlich muss der Betroffene in die Datenübermittlung der Erst- sowie der jeweiligen Folgedokumentation (darin werden alle weiteren Behandlungsschritte aufgeführt) einwilligen. Die Dokumentation sowie die beiden Erklärungen werden vom Arzt an die Datenstelle übermittelt. Dort wird der Inhalt des Bogens (soweit es sich um einen Beleg handelt; im Übrigen kann der Arzt auch einen Datenträger nutzen oder eine elektronische Übermittlung als Mail vornehmen) erfasst und in Teildatensätze aufgetrennt. Ein Teildatensatz (in dem unter anderem die Namen des Arztes sowie der Versicherten enthalten ist) geht zusammen mit der Teilnahme- sowie der Einwilligungserklärung an die Krankenkasse. Einen anderen Teil erhält die Gemeinsame Einrichtung. Die Gemeinsame Einrichtung erhält von der Datenstelle pseudonymisierte Daten des Arztes und des Versicherten. Daraus

folgen Maßnahmen zur Qualitätssicherung, die auf den Verfahrensablauf des DMP Einfluss nehmen sollen. Die Speicherung der Komplett-Daten erfolgt für einen Zeitraum von sieben Jahren bei der Datenstelle.

5.8.3.5 Ablauforganisation bei der AOK Hessen

5.8.3.5.1 Standort der Datenverarbeitung

Die AOK Hessen hat am Standort eines ihrer Call-Center in Pohlheim (bei Gießen) die zentrale Organisationseinheit angesiedelt, die das DMP Diabetes mellitus Typ 2 betreut und als Kopfstelle für die anderen beteiligten Krankenkassen fungiert. Die dort eingesetzten Mitarbeiterinnen und Mitarbeiter (etwa 18) sind technisch-organisatorisch vom Call-Center abgekoppelt und ausschließlich mit dem DMP befasst.

5.8.3.5.2 Teilnahme- und Einwilligungserklärungen

Die Teilnahme- und Einwilligungserklärungen der Betroffenen werden in der AOK Geschäftsstelle in Groß-Gerau gescannt. Die Bögen gehen anschließend zur AOK nach Darmstadt. Dort werden diese eingelagert bzw. archiviert. Derzeit haben sich etwa 27.500 Personen in das DMP eingeschrieben, von 20.500 Personen liegt eine gültige Erstdokumentation vor.

5.8.3.5.3 Datenverarbeitung bei der AOK Hessen

Von der Datenstelle erhält die AOK etwa zwei Mal wöchentlich gebündelt die Teilnahme- und Einwilligungserklärungen, die nach Groß-Gerau zur Erfassung gehen. Außerdem erhält sie den so genannten Teildatensatz 2b, der inhaltlich in der Risikostruktur-Ausgleichsverordnung festgelegt ist und medizinische Daten über aktuelle Befunde bzw. die Medikation des Patienten enthält. Die zu einem großen Teil als E-Mail ankommenden Daten werden vor dem Versand von der Datenstelle verschlüsselt und nach Eingang bei der AOK entschlüsselt. Monatlich erstellt die Datenstelle für den Datenempfänger eine Übersicht der verschickten Datensätze. Die Erstdokumentation wird von der Krankenkasse nur dann als „korrekt“ akzeptiert und verwendet, wenn die Erklärungen des Patienten vorliegen. Das führt dazu, dass derzeit mehr Einschreibungen als gültige Erstdokumentationen vorliegen.

Mit dem Programm DIMAS können die Sachbearbeiter die Datensätze bearbeiten. Als Ordnungsmerkmale für eine erfolgreiche Suche nach einem Patienten stehen die Krankenversicherungs-Nummer, der Name oder das Geburtsdatum zur Verfügung. Zwar ist der DMP-Arzt für die Angaben über die Diagnose sowie der fortlaufenden Behandlung inhaltlich verantwortlich. Die Mitarbeiterinnen und Mitarbeiter der AOK haben jedoch sowohl lesenden als auch schreibenden Zugriff auf die Datensätze.

Die Inhalte der Datensätze führen dazu, dass der Patient oder der Arzt zu konkreten Verhaltensmaßnahmen durch die AOK aufgefordert werden. Dies geschieht in Form von Arzt-Feedback-Briefen oder einer Erinnerung gegenüber dem Patienten, eine z. B. zeitlich anstehende Untersuchung durchführen zu lassen.

5.8.3.5.4 Fallbearbeitung durch die Beschäftigten der AOK

Zur Fallbearbeitung stehen den Beschäftigten der AOK unterschiedliche Eingabemasken zur Verfügung. Auf einer ist zunächst das „Profil“ des Patienten abgebildet ist (Adresse, Bankverbindung, Versicherungszeiten, Versicherungsarten etc.). In einer weiteren Maske kann die DMP-Einschreibung bearbeitet werden. So ist hier u. a. der einschreibende Arzt vermerkt. Bei einem Arztwechsel des Versicherten müssen diese Angaben entsprechend korrigiert werden. Eine andere Maske zeigt eine Vorgangsliste an. Darin werden u. a. die Zeitpunkte der Erst- und Folgedokumentationen sowie die Diagnosesicherung des Arztes festgehalten. Die Liste kann bei Bedarf, also z. B. dem Eingang einer Folgedokumentation, ergänzt werden. In einer weiteren Maske wird der DMP-Fall dargestellt mit den Hinweisen, ob z. B. ein Mailing verschickt oder das DMP durch den Versicherten abgelehnt wurde. Beim so genannten Mailing handelt es sich um Hinweisbriefe für den Versicherten bzw. den Arzt, die den Betroffenen zu bestimmten Verhaltensänderungen bei der Behandlung (Arzt) oder Wahrnehmung von Untersuchungsterminen (Patient) anhalten soll. Bei der Ein- oder Umschreibung des Versicherten wird der einschreibende Arzt festgehalten sowie Angaben zur Vollständigkeit und der Dokumentation vermerkt. Die Einschreibung in das DMP-Programm erfolgt durch die Abgabe der Teilnahmeerklärung des Patienten durch den Arzt bei der Datenstelle. Die Abgabe der Erklärung wird im Patientendatensatz festgehalten. Dies geschieht ebenso bei der Umschreibung. Darunter versteht man den während der Behandlung erfolgten Wechsel des Arztes durch den Patient.
Schließlich werden medizinische Daten des Patienten in einer weiteren Bearbeitungsmaske vermerkt.

Die medizinischen Inhalte der Eingabemasken basieren sämtlich auf den Angaben, die der Arzt im Wege der Erstdokumentation bzw. der Folgedokumentation an die Datenstelle weitergibt. Die Daten werden in der Datenstelle in einen Datensatz eingegeben, der entweder neu erstellt wird (Ersteinschreibung des Patienten, Erstdokumentation) oder im Wege einer Folgedokumentation zwar bereits erstellt ist, jedoch um zusätzliche Angaben der Folgedokumentation ergänzt wird. In eine der „Karteikarten“ der Maske werden Daten zur Messmethodik des Blutzuckers eingegeben sowie einzelne Blutzucker-Werte

festgehalten. In einer anderen Karteikarte sind Angaben zur Anamnese enthalten. Eine weitere Speicherung umfasst so genannte „relevante Ereignisse der letzten 12 Monate“. Dokumentiert wird in diesem Fall, ob der Patient in diesem Zeitraum z. B. einen Schlaganfall oder Herzinfarkt erlitten hat oder von einer Amputation betroffen war. Schließlich werden aktuelle Befunddaten und Laborwerte zum Betroffenen hinterlegt. Die gespeicherten Informationen haben zur Konsequenz, dass entsprechend des Behandlungsablaufs, den die Kasse nun zur Kenntnis hat, gezielte Anschreiben an den Patienten erfolgen. Darin wird z. B. daran erinnert, anstehende Arzttermine oder Schulungsangebote wahrzunehmen.

Es ist durch technische Vorkehrungen sichergestellt, dass die AOK-Mitarbeiter in den Eingabemasken die dort eingetragenen und vom Arzt erstellte Diagnosen sowie daraus resultierende Behandlungsabläufe nicht beeinflussen können. Die Einflussnahme der Krankenkasse erfolgt ausschließlich durch Informationsschreiben an den Arzt, in dem Hinweise auf eine mögliche Optimierung, z. B. der Medikation, hingewiesen wird. Verantwortlich für die Durchführung der medizinischen Maßnahme bleibt also stets der behandelnde Arzt. Allerdings kann die Krankenkasse über den Zugriff auf die medizinischen Daten die Behandlungsabläufe nachvollziehen und daraus Schlussfolgerungen ziehen. Diese werden in der Folge dem Arzt in Form von Empfehlungen zur Kenntnis gegeben.

5.8.3.6 Datenschutzrechtliche Bewertung

Der Zweck der Verarbeitung medizinischer Daten durch die Krankenkasse steht im Einklang mit den vom Gesetzgeber getroffenen rechtlichen Regelungen.

Kritikwürdig ist jedoch die Ausgestaltung der Zugriffsmöglichkeiten im Programm DIMAS. Dass alle 18 DMP-Mitarbeiter der AOK Hessen sowohl einen lesenden als auch einen schreibenden Zugriff auf die Daten haben, ist von der Sache her nicht zu begründen. Ein wesentlicher Teil der – medizinischen – Daten sind durch Untersuchungsergebnisse festgelegte Parameter, die Grundlage für entsprechende Aktionen der Krankenkasse (Erinnerungen, Feed-back etc.) bilden. Hierzu ist es nicht erforderlich, weitgehende Schreibrechte dem gesamten Personal gegenüber einzuräumen. Dies muss denjenigen Befugten vorbehalten bleiben, die mit der Eingabe von Verlaufswerten zur Diabetes des Versicherten oder dem Versand von Briefen an Arzt oder Versicherten befasst sind. Hinzu kommt, dass mit der Protokollierung nur nachvollzogen werden kann, wer zuletzt auf den Datenzusatz zugegriffen hat. Nicht protokolliert werden dagegen vorgenommene Änderungen. Damit ist keine effektive Zugriffskontrolle i. S. v. § 78a SGB X umgesetzt.

Die AOK Hessen hat zugesagt, die Schreibzugriffe auf die erforderliche Anzahl von Personen zurückzunehmen und die Ausgestaltung der Protokollierung zu prüfen.

5.9 Sozialwesen

5.9.1 Modellprojekt Wiesbaden / Unterhaltsvorschussgesetz

Im Rahmen eines Modellversuchs ist es mit dem Sozialdatenschutz vereinbar, dass die Stadt Wiesbaden sich der Hilfe eines privaten Inkassounternehmers bedient, um von ihr gezahlte Unterhaltsvorschüsse von säumigen Vätern erstattet zu bekommen.

Die Stadt Wiesbaden hat mich um datenschutzrechtliche Begleitung eines einjährigen Modellprojekts (Dauer bis März 2005) gebeten, mit dem unter Einbindung des Hessischen Sozialministeriums und des kommunalen Datenschutzbeauftragten die Kooperation mit einem privaten Inkassounternehmen getestet werden soll.

Vor dem Hintergrund allgemeiner finanzieller Konsolidierungsbemühungen ist die Stadt Wiesbaden bestrebt, die auf der Grundlage des Unterhaltsvorschussgesetzes (UVG) vorab gewährten finanziellen Leistungen wesentlich stärker als bisher gelungen von den an sich unterhaltspflichtigen säumigen Vätern (selten Müttern) zurückzufordern. Die von der Stadt Wiesbaden ausgezahlten Vorschüsse liegen bei jährlich über drei Millionen Euro, die Rückholquote liegt bei etwa 20%; angestrebt ist eine Quote von mindestens einem Drittel der gewährten Leistungen.

Falls durch die Hinzuziehung des Inkassounternehmers eine signifikante Erhöhung der Rückholquote erzielt wird, könnte die datenschutzrechtliche Erforderlichkeit einer Information des Inkassounternehmens über unterhaltssäumige Väter bejaht werden; freilich werden im Rahmen der im nächsten Jahr anstehenden Evaluation auch die Kosten des Inkassounternehmens zu berücksichtigen sein.

Im Rahmen des Projekts hat sich der Inkassounternehmer meiner datenschutzrechtlichen Kontrolle vertraglich unterworfen, und ist über die Zweckbindung und Geheimhaltungspflicht im Sozialdatenschutzrecht belehrt worden (§ 78 SGB X).

§ 78 SGB X

(1) Personen, denen Sozialdaten übermittelt worden sind, dürfen diese nur zu dem Zweck verarbeiten oder nutzen, zu dem sie ihnen befugt übermittelt worden sind. Die Dritten haben die Daten in demselben Umfang geheim zu halten wie die in § 35 des ersten Buches genannten Stellen.

Unterstützt wird das Projekt zusätzlich dadurch, dass die Stadt Wiesbaden im Rahmen der oft erforderlichen Adressenermittlung säumiger Schuldner auch die Adressendatei der Schufa nutzt, wenn andere öffentliche Register die aktuelle Adresse der unterhaltspflichtigen Väter nicht wiedergeben. Auch die Erforderlichkeit dieser Datenerhebung bei der Schufa wird ein Gegenstand der im nächsten Jahr mit den Projektbeteiligten vereinbarten Evaluation sein.

5.9.2 Zusammenarbeit Sozialamt und Polizei

Die Zulässigkeit der Bekanntgabe von Sozialdaten an die Polizei beurteilt sich nach dem Sozialdatenschutzrecht.

Ein Sozialamt bat mich um Auskunft, ob die Polizei zulässigerweise Einsicht in Sozialhilfeakten nehmen könne.

Die Zulässigkeit der in der Gewährung von Akteneinsicht liegenden Bekanntgabe von Sozialdaten richtet sich nach dem Sozialdatenschutzrecht.

§ 73 SGB X erlaubt die Übermittlung von Sozialdaten zur Durchführung eines Strafverfahrens, verlangt aber einen die Übermittlung anordnenden richterlichen Beschluss.

§ 73 SGB X

(1) Eine Übermittlung von Sozialdaten ist zulässig, soweit sie zur Durchführung eines Strafverfahrens wegen eines Verbrechens oder wegen einer sonstigen Straftat von erheblicher Bedeutung erforderlich ist.

(2) Eine Übermittlung von Sozialdaten zur Durchführung eines Strafverfahrens wegen einer anderen Straftat ist zulässig, soweit die Übermittlung auf die in § 72 Abs. 1 Satz 2 genannten Angaben und die Angaben über erbrachte oder demnächst zu erbringende Geldleistungen beschränkt ist.

(3) Die Übermittlung nach den Absätzen 1 und 2 ordnet der Richter an.

Ohne richterlichen Beschluss ist nach § 68 SGB X nur die Übermittlung abschließend aufgezählter Daten zur Erfüllung von Aufgaben der Polizeibehörden auf deren Ersuchen hin zulässig.

§ 68 SGB X

(1) Zu Erfüllung von Aufgaben der Polizeibehörden ist es zulässig, im Einzelfall auf Ersuchen Name, Vorname, Geburtsdatum, Geburtsort, derzeitige Anschrift des Betroffenen, seinen derzeitigen oder zukünftigen Aufenthalt sowie Namen und Anschriften seiner derzeitigen Arbeitgeber zu übermitteln, soweit kein Grund zur Annahme besteht, dass dadurch schutzwürdige Interessen des Betroffenen beeinträchtigt werden, und wenn das Ersuchen nicht länger als sechs Monate zurückliegt.

Eine spezielle Situation ist gegeben, wenn das Sozialamt selbst durch Straftaten betroffen ist (etwa Sozialhilfebetrug); in diesem Fall ist das Sozialamt auch ohne Ersuchen der Polizei im Rahmen eigener Entscheidungskompetenz zur Weitergabe von erforderlichen Sozialdaten an die Polizei befugt (§ 69 Abs. 1 Nr. 1 SGB X), da die Bekämpfung von Sozialleistungsmissbrauch zu den gesetzlichen Aufgaben der Sozialverwaltung zählt.

Ich habe das Sozialamt über die rechtlichen Rahmenbedingungen bei der Zusammenarbeit mit der Polizei informiert.

5.9.3 Unverschlüsselte Sozialdatenübermittlung per E-Mail

Es ist datenschutzrechtlich unzulässig, wenn Sozialhilfeträger mittels unverschlüsselten E-Mails Informationen über Sozialhilfeempfänger austauschen.

Durch einen Hinweis bin ich darauf aufmerksam geworden, dass einzelne Sozialämter sich mit unverschlüsselten E-Mails über Sozialhilfeempfänger informieren, um mehrfachen Sozialhilfebezug durch diese Personen zu verhindern.

Ungerechtfertigtem Sozialhilfebezug entgegenzuwirken, ohne dass im Einzelnen ein Missbrauchsverdacht belegt werden müsste, ist auf der Grundlage von § 117 Abs. 2 BSHG möglich, der einen verdachtsunabhängigen Datenabgleich zwischen den Sozialämtern vorsieht.

§ 117 Abs. 2 BSHG

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. Hierfür dürfen die erforderlichen Daten … anderen Sozialhilfeträgern … 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.

Allerdings dürfen Datenabgleiche, wenn sie mittels E-Mails über das Internet durchgeführt werden, nur in verschlüsselter Form stattfinden. Denn gerade auch im Bereich des Sozialdatenschutzes (§§ 35 SGB I, 67 ff. SGB X) haben die Behörden die erforderlichen technischen Maßnahmen zu treffen, damit Sozialdaten nicht unbefugt zur Kenntnis genommen und verwendet werden können (§ 78a SGB X).

§ 78a SGB X

Die in § 35 des Ersten Buches genannten Stellen, die selbst oder im Auftrag Sozialdaten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen einschließlich der Dienstanweisungen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzbuches, insbesondere die in der Anlage zu dieser Vorschrift genannten Anforderungen, zu gewährleisten.

Nach Nr. 4 der Anlage zu § 78a SGB X ist zu gewährleisten, dass Sozialdaten bei der elektronischen Übertragung nicht unbefugt gelesen, verändert oder entfernt werden können. Eine Übermittlung im Wege einer unverschlüsselten E-Mail via Internet, die dem Versand einer Postkarte gleichzusetzen ist, erfüllt diese Anforderungen nicht.

Unter Hinweis auf diese sozialdatenschutzrechtlichen Bestimmungen habe ich die Sozialhilfeträger aufgefordert, Sozialdaten nicht unverschlüsselt per E-Mails zu übermitteln.

5.9.4 Datenübermittlung nach Israel

Die Übermittlung von personenbezogenen Daten nach Israel wegen Rentenzahlungen nach dem Bundesentschädigungsgesetz ist zulässig, wenn die Übermittlung ausschließlich im Interesse der betroffenen Personen liegt oder wenn die Betroffenen ihre Einwilligung für die Übermittlung erteilt haben.

Das Hessische Sozialministerium hat mich um Stellungnahme gebeten, ob im Hinblick auf Rentenzahlungen nach dem Bundesentschädigungsgesetz ein Abgleich mit israelischen Meldedaten zulässig ist. Konkret geht es darum, dass die hessische Entschädigungsbehörde an unter das Bundesentschädigungsgesetz fallende Personen in Israel lebenslange Renten als Wiedergutmachung für in der Zeit des Nationalsozialismus erlittene Verfolgungsschäden zahlt. Einmal im Jahr werden die Rentenbezieher aufgefordert, öffentlich beglaubigte Lebensbescheinigungen vorzulegen. Geschieht dies trotz Erinnerung nicht, wird unterstellt, dass der Berechtigte verstorben ist. Dieses Verfahren verursacht einen hohen Aufwand und führt sowohl zu Überzahlungen, die zurückgefordert werden müssen, als auch zur Notwendigkeit von Nachzahlungen, wenn Lebensbescheinigungen doch noch mit Verspätung vorgelegt werden.

Die hessische Entschädigungsbehörde und ebenso die Entschädigungsbehörden anderer Bundesländer suchen nach einer Lösung, den in der Regel hoch betagten und zunehmend gebrechlichen Rentenbeziehern die jährliche Beibringung der Lebensbescheinigungen zu ersparen. Für die in Israel lebenden Rentenempfänger bietet sich Abgleich mit den israelischen Meldedaten über das vom Bund getragene OPC (Office for Personal Compensation of Abroad) in Israel an. Es sollen nur die Rentenbezieher in den zukünftigen Datenabgleich einbezogen werden, die zuvor für dieses Verfahren ihre Einwilligung erteilt haben; für diejenigen, die ihre Einwilligung nicht erteilen möchten, bleibt es bei dem bisherigen Verfahren.

Die rechtliche Zulässigkeit der in Ausführung des Bundesentschädigungsgesetzes beabsichtigten Datenübermittlung bestimmt sich für die hessische Entschädigungsbehörde nach dem Hessischen Datenschutzgesetz, da das Bundesentschädigungsgesetz rechtssystematisch nicht dem Sozialgesetzbuch zugeordnet ist.

Da Israel nicht in den Geltungsbereich der EG-Datenschutzrichtlinie fällt, richtet sich die Zulässigkeit der beabsichtigten Datenübermittlung folglich nach § 17 Abs. 2 HDSG, der die Übermittlungen von personenbezogenen Daten in Staaten außerhalb der Europäischen Union betrifft.

§ 17 Abs. 2 HDSG

Eine Übermittlung an Empfänger außerhalb des in Abs. 1 genannten Bereichs ist aufgrund 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,
…

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.

Da das angestrebte Verfahren im Hinblick auf die für die Rentenbezieher angestrebte Entlastungsfunktion ausschließlich im Interesse der Betroffenen liegt und da unabhängig davon vorgesehen ist, die Einwilligung der Betroffenen für die Übermittlung einzuholen, ist eine Übermittlung nach § 17 Abs. 2 HDSG zulässig. Mit Blick auf die Einwilligungen braucht nach § 17 Abs. 2 HDSG auch nicht entschieden zu werden, ob und inwieweit in Israel ein angemessener Datenschutz gewährleistet ist. Allerdings muss das OPC darauf hingewiesen werden, dass die übermittelten Daten nur zum Abgleich mit israelischen Meldedaten verwendet werden dürfen.

Ich habe gegenüber dem Hessischen Sozialministerium eine dementsprechende Stellungnahme abgegeben; was die Ausgestaltung der Übermittlung im Einzelnen betrifft, insbesondere die technischen Randbedingungen, ist das Abstimmungsverfahren mit dem Sozialministerium noch nicht abgeschlossen.

5.9.5 Zusammenarbeit Kindergarten und Schule

Kindergärten und Schulen dürfen über Kinder, deren Einschulung ansteht, grundsätzlich nur mit Einwilligung der Eltern personenbezogene Informationen austauschen.

In Wiesbaden hatten sich Eltern beim behördlichen Datenschutzbeauftragten darüber beschwert, dass ohne ihr Einverständnis zwischen dem Kindergarten und der Grundschule Informationen über ihr Kind ausgetauscht worden seien. Der behördliche Datenschutzbeauftragte hatte daraufhin zwecks datenschutzrechtlicher Würdigung Kontakt mit mir aufgenommen.

Weder das hessische Schul- noch das bundesrechtliche Kinder- und Jugendhilfegesetz regelt explizit, dass kooperative Gespräche zwischen Kindergarten und Schule über die Einschulung von Kindern nur mit Einwilligung der Eltern zulässig sind.

Allerdings ist vor dem Hintergrund des sowohl die Kinder als auch die Eltern schützenden Rechts auf informationelle Selbstbestimmung (Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG) ein grundrechtskonformer Informationsaustausch zwischen Kindergarten und Grundschule grundsätzlich nur mit Einwilligung der Eltern möglich. In diesem Sinne regelt der die Zusammenarbeit zwischen Kindergärten und Schulen betreffende § 15 Abs. 3 der hessischen Verordnung zur Ausgestaltung der Bildungsgänge und Schulformen der Grundstufe (Primarstufe) und der Mittelstufe (Sekundarstufe I) und der Abschlussprüfungen in der Mittelstufe (VOBGM), die auf der Grundlage des Hessischen Schulgesetzes erlassen wurde (§ 20 HSchG), dass die Entgegennahme von Informationen über einzelne Kinder seitens der Schule voraussetzt, dass die entsprechende Einwilligung der Eltern gegenüber dem Kindergarten erklärt worden ist.

§ 15 Abs. 3 VOBGM

Besuche von Kindergartengruppen in der Schule sind geeignet, Kindergartenkinder mit der Schule vertraut zu machen. Die Schulleiterin oder der Schulleiter sowie die Lehrerinnen und Lehrer der zukünftigen Jahrgangsstufe 1 nehmen möglichst frühzeitig Kontakt mit der Leiterin oder Leiter der Kindergartengruppe auf, aus der die Kinder in die jeweils zuständige Schule übergehen werden. Der Austausch zwischen Erzieherinnen oder Erziehern und Lehrerinnen oder Lehrern kann zu einer besseren Beurteilung des Entwicklungsstandes der Kinder beitragen und die individuelle Beratung der Eltern vertiefen. Die Entgegennahme von Informationen über einzelne Kinder setzt voraus, dass eine entsprechende Einwilligung der Eltern gegenüber dem Kindergarten erklärt worden ist.

Diesen rechtlichen Vorgaben entspricht auch die schulpolitische Entwicklung, Kindergarten und Schule zwecks besserer Förderung der Kinder unter Einbindung der Eltern zunehmend zu verzahnen. Regelmäßig dürfte von den Eltern die Einwilligung erteilt werden, da auch den Eltern im Sinne einer kontinuierlichen Entwicklung ihrer Kinder daran gelegen ist, Brüche in deren Förderung zu vermeiden.

Wird ausnahmsweise die Einwilligung versagt und ist dadurch in besonders gelagerten Fällen das Wohl des Kindes gefährdet, kann der Kindergarten oder die Schule mit dem Jugendamt Kontakt aufnehmen, um weitere Schritte zu besprechen.

Mit dem behördlichen Datenschutzbeauftragten und dem Staatlichen Schulamt der Stadt Wiesbaden ist vereinbart worden, zukünftig stärker auf die Einbindung der Eltern in die Kooperation von Kindergarten und Schule zu achten.

5.10 Finanzwesen

5.10.1 „FinanzServiceCenter“ in hessischen Finanzämtern

Bei der Einrichtung von „FinanzServiceCentern“ in Finanzämtern müssen sich Bürgerfreundlichkeit und Datenschutz nicht ausschließen, solange eine Balance zwischen der Transparenz des Raumes und der Diskretion für das Einzelgespräch gefunden wird.

Bürger einer hessischen Stadt hatten darauf hingewiesen, dass sie in einem neu eingerichteten „FinanzServiceCenter“ Gespräche anderer Steuerzahler mit den Sachbearbeitern des Finanzamtes ungewollt mithören konnten.

Ich habe daraufhin das Finanzamt aufgesucht und Folgendes festgestellt:
Die Finanzverwaltung richtet in den hessischen Finanzämtern „FinanzServiceCenter“ ein, um die Bürgerfreundlichkeit zu erhöhen. Neben längeren Öffnungszeiten sollen dem Bürger kompetente Ansprechpartner ohne große Wartezeiten angeboten werden und das Suchen des zuständigen Sachbearbeiters in den häufig weitläufigen Gebäuden erspart werden. Gleichzeitig sollen die Sachbearbeiter ohne Ablenkung durch Steuerpflichtige die Bearbeitung der Steuerakten ungestörter und damit effektiver durchführen können. Im „FinanzServiceCenter“ sollen jedoch nur einfachere Steuerangelegenheiten wie z. B. Fragen zur Einkommensteuererklärung etc. geklärt werden. Jeder Bürger hat nach wie vor die Möglichkeit einen individuellen Termin mit seinem zuständigen Sachbearbeiter telefonisch zu vereinbaren. Brisantere Vorgänge wie z. B. Vollstreckungen, Steuerstrafsachen etc. werden im „FinanzServiceCenter“ nicht bearbeitet.

In dem von mir aufgesuchten Finanzamt wurde das Erdgeschoss komplett umgebaut und den neuen Anforderungen entsprechend gestaltet. Vor dem „FinanzServiceCenter“ muss jeder Besucher eine Bearbeitungsnummer ziehen und dann im Wartebereich warten, bis seine Bearbeitungsnummer aufgerufen wird. In dem großen Raum, der durch mehrere Säulen gegliedert wird, befinden sich 6 Sachbearbeiterplätze. Jeder Arbeitsplatz ist durch eine relativ niedrige Barriere vom Nachbarschreibtisch getrennt. Auf jedem Schreibtisch steht neben dem Namensschild des Sachbearbeiters ein Hinweisschild, dass auf Wunsch auch Einzelgespräche in einem gesonderten Zimmer geführt werden können. Das Finanzamt hat zwei Räume für solche Einzelgespräche eingerichtet. Zwischen den Säulen wurden größere Pflanzen gestellt, um den Wartebereich und die Sachbearbeiterarbeitsplätze optisch und akustisch zu trennen.

Eine Überprüfung ergab, dass ein Mithören nur an zwei Warteplätzen, die sich relativ dicht neben einem Sachbearbeiterarbeitsplatz befanden, ohne Anstrengungen möglich war. Es wurde vorgeschlagen, diese beiden Stühle zu entfernen und zwischen Wand und Säule den Sachbearbeiterplatz durch ein Regal abzuschirmen. Darüber hinaus habe ich angeregt, durch akustische oder visuelle Informationsangebote die wartenden Bürger von den Sachbearbeitergesprächen abzulenken. Außerdem sollte der Hinweis auf die Möglichkeit eines Einzelgespräches bereits im Wartebereich erfolgen. Hier haben die Betroffenen Zeit darüber nachzudenken, ob sie dieses Angebot nutzen möchten.

Der Leiter des Finanzamtes betonte, dass die überwiegende Mehrzahl der Finanzamtsbesucher von dem neuen Serviceangebot begeistert ist und bisher nur sehr wenige Bürger von der Möglichkeit zur Nutzung eines separaten Raumes Gebrauch gemacht haben. Seit Eingang der ersten Beschwerde weisen die Sachbearbeiter vor Beginn eines Gespräches auch mündlich auf die Möglichkeit eines Einzelgespräches hin. Aus datenschutzrechtlicher Sicht ergeben sich keine Gründe, die Einrichtung von bürgerfreundlichen Servicestellen abzulehnen, solange die räumlichen Gegebenheiten die Wahrung der Diskretion zulassen. Es wurde mir zugesagt, meine Anregungen kurzfristig umzusetzen.

Ein kurzer Einblick bei zwei anderen Finanzämtern zeigte, dass ähnliche Mängel auch dort vorliegen. Ich werde daher die datenschutzrechtliche Beratung bei der Einrichtung der „FinanzServiceCenter“ im nächsten Jahr verstärkt fortsetzen.

5.11 Personalwesen

5.11.1 Entwurf eines hessischen Disziplinargesetzes

Der Entwurf eines hessischen Disziplinargesetzes sollte aus datenschutzrechtlicher Sicht strikter dem Bundesdisziplinargesetz angepasst werden.

Das Ministerium des Innern und für Sport hat mir den Entwurf eines Gesetzes zur Neuordnung des Disziplinarrechts (EHDG) zwecks datenschutzrechtlicher Stellungnahme übersandt.

Wie in der Begründung des Entwurfs zunächst einleitend betont wird, soll sich der Entwurf stark an das Disziplinargesetz des Bundes vom 9. Juli 2001 anlehnen, was auch aus datenschutzrechtlicher Perspektive zu begrüßen ist, da einheitliche Regelungen die datenschutzrechtliche Transparenz fördern.

Was § 19 des Entwurfs betrifft, so wird anstelle der Tilgung in § 110 HDO ein Verwertungsverbot ausdrücklich normiert. Dadurch ist noch klarer als bisher, dass ab dem Zeitpunkt des einsetzenden Verwertungsverbotes die Disziplinarmaßnahmen bei Personalentscheidungen nicht mehr berücksichtigt werden dürfen.

§ 19 Abs. 1 EHDG

Ein Verweis darf nach zwei Jahren, eine Geldbuße und eine Kürzung der Dienstbezüge oder eine Kürzung des Ruhegehalts dürfen nach drei Jahren und eine Zurückstufung darf nach sieben Jahren bei weiteren Disziplinarmaßnahmen und bei sonstigen Personalmaßnahmen nicht mehr berücksichtigt werden (Verwertungsverbot). Die Beamtin oder der Beamte gilt nach dem Eintritt des Verwertungsverbots als von der Disziplinarmaßnahme nicht betroffen.

Andererseits ist die Bundesregelung (§ 16 Abs. 3 BDG), wonach Eintragungen in der Personalakte über Disziplinarmaßnahmen nach Eintritt des Verwertungsverbotes von Amts wegen zu entfernen und zu vernichten sind, nicht vollständig übernommen. Nach § 19 Abs. 3 EHDG soll in der Personalakte der Tenor der eine Kürzung des Ruhegehalts oder eine Zurückstufung aussprechenden rechtskräftigen Entscheidung verbleiben.

§ 19 Abs. 3 EHDG

Eintragungen in der Personalakte über die Disziplinarmaßnahme – ausgenommen der Tenor der eine Kürzung des Ruhgehalts aussprechenden unanfechtbaren Entscheidung oder der Tenor der eine Zurückstufung aussprechenden rechtskräftigen Entscheidung – sind nach Eintritt des Verwertungsverbots von Amts wegen zu entfernen und zu vernichten. …

In der Begründung des Entwurfs wird dazu erklärt, eine gänzliche Entfernung aus der Personalakte scheide aus, jeder Versorgungsfall müsse nachvollziehbar und prüfbar, Hinterbliebenenversorgung festsetzbar und das Beamtenverhältnis anhand der Personalakte nachzeichenbar sein. Dies muss aber auch im Bundesbereich der Fall sein. Gleichwohl hat der Bund in der Parallelvorschrift § 16 Abs. 3 BDG eine solche Einschränkung der Entfernung aus der Personalakte, wie sie § 19 Abs. 3 EHDG vorsieht, nicht für erforderlich gehalten. Probleme in Verbindung mit der Bundesregelung sind mir bisher nicht bekannt geworden. Die Abweichung zu Lasten des Datenschutzes der Bediensteten ist deshalb nicht nachvollziehbar. Sie widerspricht auch der in der Entwurfsbegründung betonten Absicht, sich am Bundesdisziplinargesetz zu orientieren.

Da das Personalaktenrecht auch im Beamtenrechtsrahmengesetz des Bundes vorgezeichnet ist, sind Abweichungen beim Inhalt der Personalakten zu Lasten der Bediensteten aus datenschutzrechtlicher Sicht erst recht zu vermeiden.

Ich habe das Innenministerium um Stellungnahme gebeten, die aber bislang noch nicht vorliegt.

5.11.2 Rechtswidrige Aufbewahrung von Lebensläufen

Bewerbungsunterlagen dürfen nicht gegen den Willen der Betroffenen von der Dienststelle aufbewahrt werden, wenn ein Dienst- oder Arbeitsverhältnis nicht zustande kommt.

Eine erfolglose Bewerberin um eine Stelle im öffentlichen Dienst beschwerte sich bei mir darüber, dass sie ihren eingereichten Lebenslauf von der betreffenden Kommune trotz Aufforderung nicht zurückerhalten hatte; stattdessen wurde sie vom Personalamt belehrt, die Aufbewahrung von Lebensläufen sei „bewährte und gängige Praxis“.

Diese Praxis verstößt gegen das geltende Datenschutzrecht, denn die in Rede stehende Aufbewahrung wäre nur dann zulässig, wenn dies durch eine Rechtsvorschrift oder die Einwilligung der betroffenen Person gedeckt wäre, § 7 Abs. 1 HDSG.

§ 7 Abs. 1 HDSG

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.

Im vorliegenden Fall hatte die Bewerberin nicht nur keine Einwilligung für die Aufbewahrung des Lebenslaufs gegeben, sondern ausdrücklich die Zurücksendung gefordert. § 34 HDSG, der den Datenschutz bei Dienst- und Arbeitsverhältnissen betrifft, kommt als Rechtsgrundlage für die Aufbewahrung nicht in Betracht. Im Gegenteil sieht diese Vorschrift sogar grundsätzlich die Löschung der Daten erfolgloser Bewerbungen vor (§ 34 Abs. 4 Satz 2 HDSG).

§ 34 Abs. 4 Satz 2 HDSG

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.

Vor diesem gesetzlichen Hintergrund habe ich die Aufbewahrung des Lebenslaufs entgegen des ausdrücklich erklärten Willens der erfolglosen Bewerberin, und nachdem ich mehr als zwei Monate erfolglos auf eine Stellungnahme der Gemeinde in der Angelegenheit gewartet hatte, wegen Verstoßes gegen §§ 7, 34 HDSG nach § 27 HDSG beanstandet.

Die Kommune hat daraufhin eingeräumt, dass die beanstandete Aufbewahrung durch das Personalamt rechtswidrig ist und sich mit der betreffenden Bewerberin auf eine Vernichtung des Lebenslaufs, der im Bewerbungsverfahren mit handschriftlichen Bemerkungen durch das Personalamt versehen worden war, verständigt.

5.11.3 Informationsrechte der Schwerbehindertenvertretung

Es ist datenschutzrechtlich zulässig, dass die Dienststelle die Schwerbehindertenvertretung über behinderte Bedienstete namentlich informiert.

Eine Schwerbehindertenvertretung bat mich um Auskunft, ob sie von ihrer Dienststelle eine Liste auch solcher behinderter Mitarbeiter verlangen könne, die einen Grad der Behinderung (GDB) von weniger als 50 % aufweisen und Schwerbehinderten noch nicht gleichgestellt sind. Die Dienststelle hatte hiergegen datenschutzrechtliche Bedenken, da die Schwerbehindertenvertretung für diesen Personenkreis nicht zuständig sei, sondern nur für diejenigen, deren GDB 50 % oder mehr betrage sowie für diejenigen, die einen GDB von weniger als 50 % hätten und Schwerbehinderten bereits gleichgestellt worden seien.

Wäre die im Sozialgesetzbuch IX (Rehabilitation und Teilhabe behinderter Menschen) verankerte Schwerbehindertenvertretung nur für diesen Personenkreis zuständig, wäre die darüber hinausgehende Information datenschutzrechtlich unzulässig; § 95 Abs. 1 Satz 3 SGB IX zeigt jedoch, dass der Aufgabenbereich der Schwerbehindertenvertretung weiter gefasst ist.

§ 95 Abs. 1 Satz 3 SGB IX

Die Schwerbehindertenvertretung unterstützt Beschäftigte auch bei Anträgen an die … zuständigen Behörden auf Feststellung einer Behinderung, ihres Grades und einer Schwerbehinderung sowie bei Anträgen auf Gleichstellung an das Arbeitsamt.

Die Vorschrift geht also explizit davon aus, dass die Schwerbehindertenvertretung nicht erst ab Gleichstellung behinderter Personen zuständig wird, sondern schon im Vorfeld unterstützende Funktion hat. Die Zuständigkeit der Schwerbehindertenvertretung ist demnach von der Dienststelle zu eng gesehen worden; die Namen behinderter Bediensteter, die einen Grad der Behinderung von weniger als 50 % aufweisen und Schwerbehinderten noch nicht gleichgestellt sind, müssen der Schwerbehindertenvertretung auf Anfrage von der Dienststelle ebenfalls mitgeteilt werden.

Ich habe die Dienststelle und deren Schwerbehindertenvertretung entsprechend informiert.

6. Kommunen

6.1 Outsourcing bei der Stadt Wiesbaden

Die Landeshauptstadt Wiesbaden hat aus Gründen der Kostenersparnis und Effizienzsteigerung die Aufgaben der eigenen IT-Abteilung an einen privaten Dienstleister übertragen. Die datenschutzgerechte Umsetzung dieses Projekts wurde in einem umfangreichen Vertrag fixiert und mit meiner Dienststelle abgestimmt.

In der Vergangenheit hatte sich die Landeshauptstadt Wiesbaden im Bereich der Datenverarbeitung der Dienstleistung durch das Kommunale Gebietsrechenzentrum (KGRZ) Wiesbaden bedient. Daneben hatte die Stadt aber immer auch eine eigene Datenverarbeitungsabteilung. Vor einigen Jahren wurde dann eine umfassende Neustrukturierung der DV-Landschaft mit dem Ziel geplant, die Datenverarbeitung komplett auszulagern. Von der Beauftragung eines privaten Dienstleisters erhofft man sich, Kosten einzusparen und die Effizienz zu steigern. Der private Partner soll dann unter den rechtlichen Vorgaben der Datenverarbeitung im Auftrag nach § 4 HDSG diese Aufgabe übernehmen. Er ist insofern an die Vorgaben der Landeshauptstadt Wiesbaden gebunden, so wie das in der Vergangenheit auch das KGRZ Wiesbaden als Auftragnehmer gewesen ist.

6.1.1 Rechtlicher Rahmen

Unter welchen Bedingungen sich eine solche Datenverarbeitung im Auftrag durch eine private Firma durchführen lässt, wurde in verschiedenen Gesprächen mit Beschäftigten meiner Dienststelle erörtert. Insbesondere wurde problematisiert, wie Bereiche zu behandeln sind, in denen auf Grund gesetzlicher Vorgaben besondere Geheimhaltungspflichten bestehen. Im Ergebnis wurden Kategorien definiert, in die die Verfahren einzuordnen sind. Es waren die Kategorien

- Unkritische Verfahren
  Es handelt sich dabei um Verfahren, bei denen keine personenbezogenen oder anderweitig besonders schutzwürdige Daten verarbeitet werden.

- Verfahren normaler Sensibilität
  Hier geht es um solche Verfahren, bei denen personenbezogene Daten verarbeitet werden und bei deren Betrieb eine etwaige Kenntnisnahme der Daten durch Mitarbeiter der IT-GmbH zulässig ist.

- Verfahren hoher Sensibilität
  Erfasst werden solche Verfahren, bei denen personenbezogene Daten verarbeitet werden und bei denen die Möglichkeit einer Kenntnisnahme der verarbeiteten oder gespeicherten Daten durch die IT-GmbH, ihre Mitarbeiter oder Dritte ausgeschlossen sein soll.

- Abgeschottete Verfahren
  Einzelne Verfahren stellen Sicherheitsanforderungen, die über die der Verfahren mit besonders hoher Sensibilität hinausgehen. Für diese Verfahren ist nicht nur die Möglichkeit einer Kenntnisnahme der Daten durch die IT-GmbH, sondern auch die Möglichkeit des Zugangs der IT-GmbH zum Rechnersystem zu unterbinden.

- Verfahren mit Sozialdaten
  Derartige Verfahren werden nachstehend gesondert betrachtet, weil für sie besondere Anforderungen gelten.

Für die Verarbeitung der Sozialdaten sah man auf Grund der Anforderungen des § 80 Abs. 5 SGB X ebenfalls die Notwendigkeit, besondere organisatorische Regelungen zu treffen.

§ 80 Abs. 5 SGB X

Die Erhebung, Verarbeitung oder Nutzung von Sozialdaten im Auftrag durch nicht-öffentliche Stellen ist nur zulässig, wenn
1. *beim Auftraggeber sonst Störungen im Betriebsablauf eintreten können oder*
2. *die übertragenen Arbeiten beim Auftragnehmer erheblich kostengünstiger besorgt werden können und der Auftrag nicht die Speicherung des gesamten Datenbestandes des Auftraggebers umfasst. Der überwiegende Teil der Speicherung des gesamten Datenbestandes muss beim Auftraggeber oder beim Auftragnehmer, der eine öffentliche Stelle ist, und die Daten zur weiteren Datenverarbeitung im Auftrag an nicht-öffentliche Auftragnehmer weitergibt, verbleiben.*

Der Server mit den Sozialdaten wird sich bei der IT-GmbH in einem separaten Raum befinden, zu dem nur Bedienstete der Landeshauptstadt Wiesbaden Zutritt haben werden.

Letztlich hat sich die Stadt Wiesbaden entschlossen, die Statistikstelle aus diesem Auftragspaket ganz herauszunehmen und bei der Stadt zu belassen. Das Rechnersystem und die Haltung der Daten der Statistikstelle geschieht in den Räumlichkeiten der Landeshauptstadt Wiesbaden.

Alle Verfahren wurden durch die Verfahrensverantwortlichen einer der Kategorien zugeordnet.

Nachdem die zu erbringenden Leistungen durch die Stadt ausgeschrieben worden sind, wurden mit drei ausgewählten Bietern Detailgespräche geführt, in denen es insbesondere auch um Datenschutz- und Datensicherheitskonzepte ging. An diesen Gesprächen war meine Dienststelle beteiligt.

6.1.2 Bestellung eines externen Datenschutzbeauftragten

Die beauftragte private Firma hat in den weiteren Verhandlungen kundgetan, dass sie eine externe Person, die innerhalb des Gesamtkonzerns mit Datenschutzaufgaben befasst ist, zum Datenschutzbeauftragten für die zu gründende IT-GmbH bestellen möchte. Nach § 4f Abs. 2 Satz 2 BDSG ist die Bestellung eines externen Datenschutzbeauftragten für nicht-öffentliche Stellen zulässig. Das HDSG sieht hingegen die Bestellung eines externen Datenschutzbeauftragten nicht vor. (Der Gesetzgeber hatte sich 1998 bewusst gegen diese Möglichkeit entschieden.) Die IT-GmbH muss sich aber gemäß § 4 Abs. 3 HDSG als Auftragnehmer einer öffentlichen Stelle des Landes Hessen vertraglich verpflichten, die Vorschriften des Hessischen Datenschutzgesetzes zu befolgen.

§ 4 Abs. 3 HDSG

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. …

Damit gilt für die IT-GmbH auch die Regelung des HDSG zur Bestellung des betrieblichen Datenschutzbeauftragten. Die geplante Bestellung eines externen DSB wäre unzulässig. Für einen privaten Dienstleister hätte dies zur Konsequenz, dass er, wenn er verschiedene öffentliche Auftraggeber aus unterschiedlichen Bundesländern hat, u. U. mehrere betriebliche Datenschutzbeauftragte bestellen müsste. Das kann vom Gesetzgeber nicht gewollt gewesen sein. Die Regelung des § 4 Abs. 3 HDSG sollte sicherstellen, dass beim Auftragnehmer die gleichen materiellen datenschutzrechtlichen Bestimmungen gelten wie beim Auftraggeber. Der Ausschluss der Bestellung eines externen Datenschutzbeauftragten ist m. E. nie vor dem Hintergrund der Datenverarbeitung im Auftrag diskutiert worden. Ich habe deshalb gegenüber dem Hessischen Ministerium des Innern und für Sport angeregt, § 4 Abs. 3 HDSG dahingehend zu ergänzen, dass die Bestellung eines externen Datenschutzbeauftragten, wie in § 4f Abs. 2 BDSG vorgesehen, für den privaten Auftraggeber weiterhin möglich bleibt. Das Ministerium hat sich meiner Rechtsauffassung angeschlossen und eine entsprechende Anpassung des HDSG zugesichert.

6.1.3 Datenschutzkonzept der IT-GmbH

Gegenstand der vertraglichen Vereinbarung zwischen der Landeshauptstadt Wiesbaden und der privaten Firma war auch die Festschreibung und Umsetzung eines Datenschutz- und Datensicherheitskonzepts. Allerdings waren sich die Beteiligten darüber einig, dass eine komplette Umsetzung dieses Konzepts nicht mit Beginn der Tätigkeit gegeben sein kann. Vielmehr ist vorgesehen, dass die Umsetzung schrittweise erfolgt. Mit Aufnahme der Tätigkeit der IT-GmbH müssen jedoch mindestens die derzeit bei der Stadt umgesetzten Sicherheitsstandards eingehalten werden.

6.2 Prüfung einer Stadtbibliothek

Einzelregelungen in den Satzungen hessischer Stadtbibliotheken führen manchmal zu rechtlichen Missverständnissen.

Im Rahmen meiner Prüftätigkeit habe ich der Bibliothek einer Stadt in Mittelhessen einen Besuch abgestattet.

Näher untersucht wurde dabei u. a. die Verarbeitung der personenbezogenen Daten der Bibliotheksbenutzer im eingesetzten elektronischen Ausleihsystem. Die Zahl der hier gespeicherten Daten entspricht dem Standard solcher Programme. Vorgesehen sind nur: Name, Vorname, Adresse, Geburtsdatum, Buchtitel, Rückgabedaten, Mahnung. Einen manchmal noch in Bibliotheksprogrammen vorzufindenden Mangel hat das hier vorgefundene System nicht: Nach Rückgabe des Buches wird der Buchtitel gelöscht, sodass ein Leserprofil nicht erstellt werden kann.

Geprüft wurden auch die rechtlichen Grundlagen der Verarbeitung dieser Daten. Dazu wurde mir die Bibliothekssatzung vorgelegt, die üblicherweise auch die rechtlichen Einzelheiten der Datenverarbeitung bei öffentlichen Bibliotheken enthält. Diese vom Gemeindeparlament verabschiedete Satzung ist als Rechtsvorschrift i. S. v. § 7 Abs. 1 HDSG anzusehen, die den allgemeinen Bestimmungen des HDSG insoweit vorgeht und eine sonst notwendige Einwilligung des Betroffenen in die Datenverarbeitung überflüssig macht. Oft enthalten solche Satzungen zwar nicht eine ausdrückliche Ermächtigung zum Verarbeiten der personenbezogenen Daten der Bibliotheksbenutzer. Der Vollzug der Satzung setzt aber i. S. v. § 7 Abs. 1 Nr. 1 diese Datenverarbeitung zwingend voraus. Insoweit ist sie eine Rechtsvorschrift, die die Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten nach dem HDSG bildet.

§ 7 Abs. 1 HDSG

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.

Zahlreiche von mir schon geprüfte Bibliothekssatzungen enthalten gleichwohl immer noch folgende sinngemäß wiedergegebene Regelung:

„Der Nutzer der Bibliothek willigt mit dem Antrag auf Nutzer-Ausweis in die Verarbeitung seiner Daten ein."

Diese Bestimmung ist also nicht nur irreführend, sondern auch rechtlich unzutreffend.

Im Fall der hier geprüften Satzung fand ich folgende Regelung vor:

„Der Benutzer/die Benutzerin gibt sein/ihr Einverständnis für die automatisierte Speicherung seiner/ihrer persönlichen Daten."

Diese Bestimmung war nicht nur unter Berücksichtigung der vorangehenden Ausführungen unzutreffend. Ein zusätzlicher Aspekt ergibt sich, soweit auf die Art der Datenverarbeitung, die Automatisierung, abgehoben wird. Für diese Art der Datenverarbeitung ist eine Einwilligung nicht notwendig. Denn es steht im Belieben der Daten verarbeitenden Stelle, ob sie die Daten manuell oder automatisiert speichert. Für die Art und Weise der Datenverarbeitung ist also eine Befugnisnorm i. S. v. § 7 Abs. 1 HDSG nicht notwendig. Die automatisierte Datenverarbeitung ist heute sogar der Regelfall.

Ich habe die Bibliothek daher gebeten, diesen Passus künftig entfallen zu lassen

6.3 Datenübermittlung des Datums „Lebenspartnerschaft führend" an öffentlich-rechtliche Religionsgesellschaften

Die Übermittlung des Melderegisterdatums „Lebenspartnerschaft führend" an eine öffentlich-rechtliche Religionsgemeinschaft kann schutzwürdige Belange des Betroffenen verletzen. Da derzeit die Angabe zur Aufgabenerfüllung der öffentlich-rechtlichen Religionsgemeinschaften nicht erforderlich ist, greift eine Übermittlung des Datums unverhältnismäßig in das Recht des Betroffenen auf informationelle Selbstbestimmung ein.

Ein Meldepflichtiger beantragte bei seiner Meldebehörde die Übermittlung des Datums „Lebenspartnerschaft führend" an seine Religionsgemeinschaft, die katholische Kirche, zu unterlassen. Da der ständige Rat der Deutschen Bischofskonferenz erklärt hat, dass die Eingehung einer Lebenspartnerschaft mit den Loyalitätsobliegenheiten nach der Grundordnung des kirchlichen Dienstes unvereinbar sei, befürchtet der Petent als Beschäftigter der katholischen Kirche berufliche Nachteile. Das Melderecht sieht für diesen Fall keine Auskunftssperre vor. Die Kommune fragte deshalb an, wie zu verfahren sei.

Im Zuge der Novellierung des Melderechtsrahmengesetzes (MRRG) 2002 wurden §§ 19 Abs. 1 Ziff. 11; 23 Abs. 2 Satz 2 MRRG dahingehend ergänzt, dass die Meldebehörde das Datum „Lebenspartnerschaft führend" an öffentlich-rechtliche Religionsgesellschaften übermitteln darf.

§ 19 Abs. 1 MRRG

Die Meldebehörde darf einer öffentlich-rechtlichen Religionsgesellschaft unter den in § 18 Abs. 1 Satz 1 genannten Voraussetzungen zur Erfüllung ihrer Aufgaben folgende Daten ihrer Mitglieder übermitteln:
1. Familiennamen,
…
11. Familienstand, beschränkt auf die Angabe, ob verheiratet oder eine Lebenspartnerschaft führend oder nicht; zusätzlich bei Verheirateten oder Lebenspartnern: Tag der Eheschließung oder der Begründung der Lebenspartnerschaft,
…

Die Datenübermittlung ist – wie bei dem Familienstand der Ehe – auf die Mitglieder der Religionsgemeinschaft beschränkt und erfolgt zur Erfüllung ihrer zuständigen Aufgaben. Hintergrund der Ergänzung war die ursprüngliche Absicht des Gesetzgebers, eingetragene Lebenspartnerschaften auch (kirchen-) steuerlich der Ehe gleichzustellen. Bis zur Umsetzung der Rahmenvorschrift in das Hessische Landesrecht gilt die Regelung für hessische Gemeinden unmittelbar.

§ 23 Abs. 2 MRRG

§ 2 Abs. 2 Nr. 1 Buchstabe b, Nr. 4 und 6, § 10, soweit er die Speicherung der Tatsache nach § 2 Abs. 2 Nr. 4 betrifft, § 17 Abs. 1 Satz 5 und Abs. 2 soweit dort auf die Fortschreibung der Tatsache nach § 2 Abs. 2 Nr. 6 abgestellt wird, gelten bis zur Anpassung des Melderechts der Länder unmittelbar. Entsprechendes gilt für § 2 Abs. 1 Nr. 14 und 15, soweit sie die Speicherung von Daten des Lebenspartners oder einer Lebenspartnerschaft betreffen, und § 12 Abs. 2 Satz 2, § 16 Abs. 1 Satz 2, § 19 Abs. 1 Nr. 11 und § 21 Abs. 2 Nr. 7 und 8 und Abs. 3 Satz 2 Nr. 6, soweit dort auf den Lebenspartner oder eine Lebenspartnerschaft abgestellt wird.

Die Übermittlung des Melderegisterdatums „Lebenspartnerschaft führend" greift in das Recht auf informationelle Selbstbestimmung aus Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 GG ein. Solche Eingriffe sind – da eine Einwilligung des Betroffenen zur Datenübermittlung nicht vorliegt – nur auf Grund eines Gesetzes zulässig, das u. a. auch dem Verhältnismäßigkeitsprinzip entsprechen muss (BVerfGE 65, 1,44 ff.).

Dies ist bei § 19 Abs. 1 Ziff. 11 i. V. m. § 23 MRRG nicht der Fall. Die ursprüngliche Absicht einer (kirchen-) steuerlichen Gleichstellung hat der Gesetzgeber noch nicht umgesetzt. Es würde daher eine Datenübermittlung erfolgen, für die keine Erforderlichkeit besteht. Andererseits ist nicht auszuschließen, dass die Kenntnis des Datums beim Empfänger dazu genutzt wird, die vom Arbeitgeber geforderten Loyalitätsobliegenheiten im Hinblick auf die private Lebensgestaltung des

Arbeitnehmers durchzusetzen. Das könnte dazu führen, dass entweder die Lebenspartnerschaft oder das Arbeitsverhältnis beendet werden muss.

Damit werden schutzwürdige Belange des Betroffenen verletzt. Die Bestimmung greift unverhältnismäßig in das Recht auf informationelle Selbstbestimmung ein.

In Übereinstimmung mit dem Bundesministerium des Innern als Gesetzgeber des MRRG und dem Hessischen Ministerium des Innern wurde das Datum im vorliegenden Fall von der anfragenden Kommune nicht weitergegeben, und die anderen Meldebehörden über die verfassungskonforme Auslegung der Norm zur Anwendung bei entsprechenden Fällen informiert.

6.4 Datenbankprotokolle im Einwohnerwesen

Im DV-Verfahren „Einwohnerwesen“ ist nicht alles, was praktikabel und technisch möglich ist, auch rechtlich zulässig. Die zweckwidrige Nutzung eines an sich rechtmäßigen Zugriffs auf Meldedaten anderer Kommunen ist unzulässig und kann durch Auswertung von Datenbankprotokollen nachgewiesen werden.

Ein Bürger machte mich darauf aufmerksam, dass bei der Anmeldung seines Gewerbes der zuständige Sachbearbeiter zur Klärung einer Zweifelsfrage auf das Einwohnermelderegister seiner Wohnsitzgemeinde zugegriffen hatte, obwohl diese nicht mit der Standortgemeinde seines Gewerbes identisch ist.

Das Hessische Melderecht geht davon aus, dass jede Gemeinde für die Bearbeitung der Meldedaten ihrer im Zuständigkeitsbereich wohnhaften Einwohner und Einwohnerinnen zuständig ist (§ 1 HMG).

Meine Nachfrage beim zuständigen Rechenzentrum ergab, dass auch der technische Zugriff entsprechend der Vorgaben des Hessischen Melderechts geregelt ist und grundsätzlich jeder Meldesachbearbeiter nur auf die Einwohnermeldedaten seiner eigenen Gemeinde zugreifen kann. Eine Ausnahme besteht jedoch nach § 37a Abs. 3 HMG: Wenn Bürger aus einer anderen Kommunen zuziehen, darf das zur automatisierten Registerführung beauftragte Rechenzentrum den automatisierten Abruf bestimmter Daten durch die Zuzugsgemeinde zulassen. Dabei werden Namen, Geburtsdaten, Geschlecht, Staatsangehörigkeiten, Familienstand und Anschriften sowie das Ordnungsmerkmal zur Aufnahme des Neubürgers in das Einwohnermelderegister in eine Bildschirmmaske der Zuzugsgemeinde übermittelt, um mögliche Fehlerquellen zu vermeiden. Diese Daten werden um die aktuellen Daten vom Meldeamt der Zuzugsgemeinde ergänzt und der Datensatz in das Einwohnermelderegister aufgenommen. Gleichzeitig erfolgt die Abmeldung beim ursprünglichen Wohnort. Die Wegzugsgemeinde wird hiervon unterrichtet. Die beteiligten Meldebehörden können die vorgenommenen Änderungen auf dem Bildschirm sehen und ggf. überprüfen.

Technisch ist es jedoch auch möglich den Zugriff bis zur Anzeige der Daten eines Einwohners durchzuführen und danach den Vorgang ohne eine Änderung im Datensatz abzubrechen. Wollte ein Meldesachbearbeiter oder eine Meldesachbearbeiterin also nur Informationen über bestimmte Einwohner anderer Kommunen haben, kann die Zuzugstransaktion aufgerufen und nach Erhalt der gewünschten Informationen beendet werden. Hierbei wird keines der Einwohnermelderegister verändert. Die vermeintliche Wegzugsgemeinde bemerkt den Zugriff auf ihre Daten nicht.

Durch diese Vorgehensweise werden sowohl die Zweckbindung nach § 13 HDSG als auch die Vorschrift des § 31 HMG zur Datenübermittlung an andere Behörden verletzt. Einwohnermeldebehörden dürfen anderen Behörden nur Daten übermitteln, wenn dies zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben erforderlich ist. Die entsprechende Prüfung der Erforderlichkeit kann eine Kommune, deren Daten wie oben beschrieben unbemerkt abgefragt werden, nicht durchführen. Zudem ist der Zugriff nach § 37a Abs. 3 HMG strikt zweckgebunden, nämlich auf den Anlass der Anmeldung. Die Nutzung eines Abrufes zu Informationszwecken darf das Rechenzentrum nicht zulassen.

Die Selbstverständlichkeit mit der die Abfrage im vorliegenden Fall erfolgt ist, ließ den Verdacht aufkommen, dass es sich möglicherweise um eine verbreitete Vorgehensweise handelt, und Meldesachbearbeiter und Meldesachbearbeiterinnen die Online-Abfrage nach § 37a HMG häufig zweckwidrig nutzen.

Ich ermittelte deshalb gemäß § 29 HDSG den Umfang der abgebrochenen Abrufe aus Anlass einer Anmeldung sowie die betroffenen Kommunen durch Auswertung der entsprechenden Datenbankprotokolle des zuständigen Rechenzentrums. Diese Auswertungen ergaben in den meisten Fällen einen Durchschnittswert von Abbrüchen, der so unbedeutend war, dass die Anzahl mit programmtechnischen Gegebenheiten erklärt werden konnte.

Bei 16 Kommunen lag die Anzahl der protokollierten Abbrüche jedoch so deutlich über dem Durchschnittswert, dass eine Erklärung erforderlich war. Die betroffenen Gemeinden wurden von mir zur Stellungnahme aufgefordert. Erste Ergebnisse der Überprüfung ergaben, dass der unzulässige Abruf als „Tipp und Trick“ für eine schnelle, unbürokratische Melderegisterauskunft die Runde machte und häufig von besonders hilfsbereiten Meldesachbearbeitern und Meldesachbearbeiterinnen genutzt wurde, die deshalb ihrerseits immer wieder um solche Auskünfte gebeten wurden.

Den Mitarbeiterinnen und Mitarbeitern der Kommunen war die Unzulässigkeit der Vorgehensweise nicht ausreichend bewusst. Auch der Umstand, dass Datenbankprotokolle erstellt werden und überprüft werden können, überraschte die Betroffenen. Gemeinden, die bis Redaktionsschluss Stellung genommen hatten, haben erklärt, die Vorgesetzten hätten diese Vorgehensweise inzwischen unterbunden. Ich werde die Angelegenheit weiter verfolgen, auch im Hinblick auf eventuelle andere DV-Verfahren, die eine ähnliche zweckwidrige Nutzung zulassen können.

Die Kundenbetreuung des Fachbereichs Einwohnerwesen der hessischen Kommunalen Gebietsrechenzentren hat mit Schreiben vom 1. Dezember 2004 alle am Verfahren Einwohnerwesen teilnehmenden Kommunen informiert, dass der Abruf von Daten eines Bürgers einer anderen angeschlossenen Kommune nur im Rahmen einer tatsächlichen Anmeldung zulässig ist. Darüber hinaus wurden die Kommunen aufgefordert, rechtlich nicht zulässige Abfragen sofort einzustellen und künftig zu unterlassen.

6.5 Unzulässige Datenübermittlungen eines Ordnungsamtes an das Taxigewerbe im Zusammenhang mit der Rückkehrpflicht von Mietwagen

Bei den Kontrollen zur Rückkehrpflicht von Mietwagenfahrern darf ein Ordnungsamt private Dritte nicht beteiligen. Feststellungen von Rechtsverstößen durch ein Ordnungsamt dürfen zudem nicht routinemäßig an Dritte übermittelt werden.

Im Sommer des Berichtsjahres wurde ich von der anwaltlichen Vertretung mehrerer Mietwagenunternehmer im Großraum einer hessischen Großstadt von einem Sachverhalt unterrichtet, der in der regionalen Presse bereits unter dem Stichwort „Taxi-Krieg“ publik gemacht wurde. Gegenstand des bereits lange andauernden Streites zwischen Taxi- und Mietwagengewerbe waren vermutete oder tatsächliche Verstöße der Rückkehrpflicht von Fahrzeugen des Mietwagengewerbes gemäß § 49 Abs. 4 Personenbeförderungsgesetz (PBefG).

§ 49 Abs. 4 PBefG

Verkehr mit Mietwagen ist die Beförderung von Personen mit Personenkraftwagen, die nur im Ganzen zur Beförderung gemietet werden und mit denen der Unternehmer Fahrten ausführt, deren Zweck, Ziel und Ablauf der Mieter bestimmt und die nicht Verkehr mit Taxen nach § 47 sind. Mit Mietwagen dürfen nur Beförderungsaufträge ausgeführt werden, die am Betriebssitz oder in der Wohnung des Unternehmers eingegangen sind. Nach Ausführung des Beförderungsauftrags hat der Mietwagen unverzüglich zum Betriebssitz zurückzukehren, es sei denn, er hat vor der Fahrt von seinem Betriebssitz oder der Wohnung oder während der Fahrt durch Funk einen neuen Beförderungsauftrag erhalten. Den Eingang des Beförderungsauftrages am Betriebssitz oder in der Wohnung hat der Mietwagenunternehmer buchmäßig zu erfassen und die Aufzeichnung ein Jahr aufzubewahren. Annahme, Vermittlung und Ausführung von Beförderungsaufträgen, das Bereithalten des Mietwagens sowie Werbung für Mietwagenverkehr dürfen weder allein noch in ihrer Verbindung geeignet sein, zur Verwechslung mit dem Taxenverkehr zu führen. Den Taxen vorbehaltene Zeichen und Merkmale dürfen für Mietwagen nicht verwendet werden. Die §§ 21 und 22 sind nicht anzuwenden.

Der Magistrat – Ordnungsamt – der Stadt hatte auf Grund vermuteter und auch tatsächlicher Verstöße gegen die gesetzlich vorgeschriebene Rückkehrpflicht der Mietwagen eine besondere Verfahrensweise eingeführt, um gesetzliche Verhältnisse durchzusetzen. So wurden Kontrollen, das heißt Streifenfahrten des Ordnungsamtes, zum Teil gemeinsam mit Personen des Taxigewerbes durchgeführt. Zudem wurden von kontrollierenden Hilfspolizisten routinemäßig „Eidesstattliche Versicherungen“ über möglicherweise begangene Ordnungswidrigkeiten im Zusammenhang mit der Rückkehrpflicht von Mietwagen gefertigt und Dritten zur Verfügung gestellt. Die Kommune stützte ihr Vorgehen auf das HSOG. Gegen diese Verfahren und die damit verbundene Datenverarbeitung richtete sich die Eingabe des Mietwagengewerbes.

Die Datenverarbeitung des Ordnungsamtes der Stadt wurde von mir unter datenschutzrechtlichen Gesichtspunkten überprüft. Hierbei bin ich zu dem Ergebnis gelangt, dass die Handlungsweise des Ordnungsamtes nicht rechtmäßig ist, weil hierfür keine gesetzliche Grundlage besteht.

6.5.1 Kontrollen gemeinsam mit Personen des Taxi-Gewerbes

Die Kontrollen der Mietwagen im Rahmen der gesetzlich vorgeschriebenen Rückkehrpflicht an sich sowie die dabei erhobenen Daten durch Mitarbeiter des Ordnungsamtes werden nicht in Frage gestellt. Die anfallenden Informationen sind für das Ordnungsamt erforderlich, um seine Aufgabe als Gefahrenabwehrbehörde nach dem Personenbeförderungsgesetz zu erfüllen. Bei der Erhebung der Daten dürfen aber nicht (private) Dritte in der Form beteiligt sein, dass sie quasi mit auf Streife gehen. Jeder Bürger hat ein Recht darauf, dass alle über ihn erhobenen Daten von einer öffentlichen Stelle im Sinne des HDSG vertraulich behandelt und nur im Rahmen der jeweiligen gesetzlichen Verwendungszwecke verarbeitet werden. Dies gilt selbstverständlich auch dann, wenn diese Daten durch die Polizei oder eine Ordnungsbehörde im Rahmen von Verfahren nach dem HSOG oder dem OWiG erhoben werden. Um ein solches Vorgehen handelt es sich bei den beschriebenen Kontrollen.

Natürlich lässt es sich nicht immer verhindern, dass Dritte wahrnehmen können, wenn die genannten Behörden entsprechende Daten aufnehmen, etwa bei der Kontrolle parkender Fahrzeuge. Damit ist die Situation von gemeinsamen Streifen aber nicht vergleichbar, da hier gezielt Dritte bei der Datenerhebung beteiligt werden. Die gemeinsame Streifenfahrt geht auch weit über die Fälle hinaus, in denen ein Privater einen Verstoß anzeigt. Dieses Verfahren lässt sich des Weiteren nicht als (unter bestimmten Voraussetzungen zulässige) Datenerhebung bei Dritten einstufen. Die Ermittlungen zu möglichen Verstößen gegen die Rückkehrpflicht von Mietwagen stellen eine hoheitliche Tätigkeit dar. Diese kann nicht ohne ausdrückliche gesetzliche Grundlage – auch nicht teilweise – auf Private übertragen werden.

6.5.2 Übermittlung von Daten an die Taxi-Unternehmer

Für die Verwendung der bei diesen Streifen als Grundlage der einzuleitenden Ordnungswidrigkeitenverfahren erhobenen Daten sind zunächst auf Grund der Verweisung des § 46 Abs. 1 OWiG die Regelungen der StPO anzuwenden.

§ 46 Abs. 1 OWiG

Für das Bußgeldverfahren gelten, soweit dieses Gesetz nichts anderes bestimmt, sinngemäß die Vorschriften der allgemeinen Gesetze über das Strafverfahren, namentlich der Strafprozessordnung, des Gerichtsverfassungsgesetzes und des Jugendgerichtsgesetzes.

Hieraus folgt, dass die sich die Übermittlung an andere im laufenden Verfahren nach § 475 StPO richtet.

§ 475 StPO

(1) Für eine Privatperson und für sonstige Stellen kann, unbeschadet der Vorschrift des § 406e, ein Rechtsanwalt Auskünfte aus Akten erhalten, die dem Gericht vorliegen oder diesem im Falle der Erhebung der öffentlichen Klage vorzulegen wären, soweit er hierfür ein berechtigtes Interesse darlegt. Auskünfte sind zu versagen, wenn der hiervon Betroffene ein schutzwürdiges Interesse an der Versagung hat.

(2) Unter den Voraussetzungen des Absatzes 1 kann Akteneinsicht gewährt werden, wenn die Erteilung von Auskünften einen unverhältnismäßigen Aufwand erfordern oder nach Darlegung dessen, der Akteneinsicht begehrt, zur Wahrnehmung des berechtigten Interesses nicht ausreichen würde.

(3) Unter den Voraussetzungen des Absatzes 2 können amtlich verwahrte Beweisstücke besichtigt werden. Auf Antrag können dem Rechtsanwalt, soweit Akteneinsicht gewährt wird und nicht wichtige Gründe entgegenstehen, die Akten mit Ausnahme der Beweisstücke in seine Geschäftsräume oder seine Wohnung mitgegeben werden. Die Entscheidung ist nicht anfechtbar.

(4) Unter den Voraussetzungen des Absatzes 1 können auch Privatpersonen und sonstigen Stellen Auskünfte aus den Akten erteilt werden.

Diese Regelung statuiert ein Auskunftsrecht bei berechtigtem Interesse. Unabhängig davon, ob ein solches hier in jedem Einzelfall vorliegt, ergibt sich daraus keine Befugnis einer Übermittlung auf Veranlassung der Behörde; Ausgangspunkt muss jeweils die Anfrage desjenigen sein, der in diesem Einzelfall ein berechtigtes Interesse geltend macht. Für die Verwendung der Daten durch die Gefahrenabwehrbehörde im Übrigen gilt das allgemeine Datenschutzrecht; das bedeutet für diese Fälle gilt dann § 23 HSOG.

§ 23 Abs. 1 HSOG gestattet grundsätzlich eine Übermittlung von Daten auch an andere nichtöffentliche Stellen. Dabei ist aber zu berücksichtigen, dass dies immer eine Einzelfallentscheidung ist. Für jeden festgestellten Fall muss die Entscheidung getroffen werden, warum gerade diese Daten an diesen Empfänger übermittelt werden. Die einzelnen Übermittlungsvoraussetzungen sind zudem jeweils auch unter dem Gesichtspunkt der Verhältnismäßigkeit zu prüfen. Eine pauschale Übermittlung eines Verdachtes auf eigene Veranlassung hin durch die Ordnungswidrigkeitenbehörde an private Dritte in den hier vorliegenden Konstellationen auch ohne zusätzliche Ermittlungen, ob die Beobachtungen bzw. die sich daraus ergebenden Wertungen der Behörde auch zutreffend sind, ist von § 23 HSOG nicht gedeckt.

Die Versorgung von privaten Dritten mit Daten über begangene Ordnungswidrigkeiten, damit diese zivilrechtlich im Rahmen des Wettbewerbsrechts gegen den Betroffenen vorgehen, ist aus meiner Sicht kein Mittel, um die Aufgabenerfüllung der Ordnungsbehörde im Sinne der Gefahrenabwehr zu erfüllen. Für die Verfolgung der Ordnungswidrigkeit gibt es ein vorgesehenes rechtsstaatliches Verfahren. Das Gleiche gilt auch für die Konsequenzen für die Konzession. Zwar kann im Einzelfall ein berechtigtes Interesse an der Vermeidung oder Beseitigung schwerwiegender Beeinträchtigungen der Rechte einer anderen Person gegeben sein. Dies wäre zu belegen und zu prüfen. Eine routinemäßige Unterrichtung einer Taxizentrale über getroffene Feststellungen rechtfertigt dieses Interesse aber keinesfalls.

Meine datenschutzrechtliche Beurteilung habe ich dem Ordnungsamt der betroffenen Stadt übermittelt. Das Ordnungsamt der Stadt hat umgehend reagiert und zusammengefasst folgende Änderungen vorgenommen:

a) An den Kontrollen der Rückkehrpflicht von Mietwagen werden private Dritte nicht mehr beteiligt.

b) Feststellungen der Behörde werden nicht mehr regel- und formularmäßig an das Taxigewerbe weitergegeben.

Das Taxigewerbe wurde vom Ordnungsamt ebenfalls entsprechend unterrichtet.

6.6 Erhebung der Steuernummer durch ein Versorgungsunternehmen

Mit der schriftlichen Aufforderung, die Steuernummer mitzuteilen, irritierte ein Versorgungsunternehmen seine Kunden. Grund hiefür war die Tatsache, dass aus dem Anschreiben nicht ersichtlich war, für welchen Zweck die Steuernummer verwendet werden soll und dass ihre Angabe freiwillig ist.

Ein Bürger hatte kein Verständnis dafür, dass sein Versorgungsunternehmen ihn aufforderte, seine Steuernummer bis zu einem festgesetzten Termin mitzuteilen. Ein Zusammenhang zwischen dem Bezug von Strom bzw. Wasser und seiner Steuernummer war ihm nicht ersichtlich.

Meine Nachfrage bei dem Versorgungsunternehmen ergab, dass das Versorgungsunternehmen nur Fotovoltaikanlagen-Betreiber um die Bekanntgabe der Steuernummer gebeten hatte. Dieser Personenkreis kann u. U. unternehmerisch – und damit ggfs. umsatzsteuerpflichtig (§§ 18, 19 UStG) – tätig werden, wenn z. B. mit der Fotovoltaikanlage dauernd größere Mengen Strom produziert und entgeltlich in das Stromnetz des Versorgungsunternehmens eingespeist werden. In einem solchen Fall kann der private Stromeinspeiser dem Versorgungsunternehmen eine Rechnung über die Lieferung des Stroms erstellen oder mit dem Versorgungsunternehmen vereinbaren, dass dieses über die Lieferung eine Gutschrift erteilt. Diese Gutschrift hat die Wirkung einer Rechnung und muss die Formalien enthalten, die ansonsten vom Fotovoltaikanlagen-Betreiber zu erledigen wären. Dazu gehörten u. a. die Angabe der Steuernummer des Stromeinspeisers, der anzuwendende Steuersatz und der anfallende Steuerbetrag. Diese Arbeitserleichterung wollte das Versorgungsunternehmen dem genannten Personenkreis mit der Abfrage der Steuernummer anbieten. Leider war das Anschreiben aber so formuliert, dass die Betroffenen nicht erkennen konnten, dass es sich nur um ein Leistungsangebot handelt und die Bekanntgabe der Steuernummer freiwillig ist.

Das Versorgungsunternehmen hat nach meiner Aufforderung alle Fotovoltaikanlagen-Betreiber erneut angeschrieben und auf die Freiwilligkeit der Bekanntgabe der Steuernummer ausdrücklich hingewiesen. Darüber hinaus wurde die Löschung von bereits mitgeteilten Steuernummern angeboten, wenn die Betroffenen dies wünschten bzw. gar nicht unter den Personenkreis fallen, der am Umsatzbesteuerungsverfahren teilnimmt.

6.7 Datenspeicherung im Zusammenhang mit dem Kauf einer Karte für ein Thermalbad

Auch wer einen besonderen Service bieten will, muss Bürgerinnen und Bürger aufklären, für welchen Zweck ihre Daten benötigt werden. Besonders wichtig ist in diesem Zusammenhang der Hinweis auf die Freiwilligkeit der Auskunft.

Ein Bürger beschwerte sich darüber, dass er für die Nutzung eines Thermalbades nicht nur Eintrittsgeld und Pfandgebühr für ein Chip-Armband bezahlen musste, sondern auch Namen und Anschrift bekannt geben sollte.

Recherchen bei dem Thermalbadbetreiber ergaben, dass beim Erwerb einer Dauerkarte die Badegäste um Namen und Adresse gebeten werden, um diese im Hinblick auf die nicht unerheblichen Kosten einer solchen Karte beim evtl. Verlust des Chip-Armbandes abzusichern. Geht ein solches Chip-Armband verloren, kann dieses eindeutig identifiziert und gesperrt werden, der betroffene Badegast erhält ein Ersatzarmband und kann das noch vorhandene Guthaben für weitere Schwimmbadbesuche nutzen. Möchte ein Badegast auf dieses Angebot verzichten, kann er auch ohne Namensnennung eine Dauerkarte erwerben. Allerdings wurde auf diese Möglichkeit nicht ausdrücklich hingewiesen, sondern der Eindruck erweckt, dass die Bekanntgabe der Adressdaten zum Erwerb der Dauerkarte unumgänglich ist. Ein im Kassenbereich befindliches Hinweisschild war offensichtlich leicht zu übersehen.

Die Daten der Besucher werden in einer Datenbank gespeichert, auf die ausschließlich die zuständigen Mitarbeiter des Schwimmbadbetreibers Zugriff haben. Auf Wunsch jedes Badegastes werden die Daten gelöscht, wenn das Chip-Armband kein Guthaben mehr enthält. Hierauf werden die Betroffenen bei der Rückgabe des pfandpflichtigen Chip-Armbandes hingewiesen.

Das Chip-Armband selbst enthält keine personenbezogenen Daten, es stellt lediglich die Verbindung zum Server des Betreibers her. Für die Dauer des Thermalbadbesuches werden auf dem Server auch der dem Chip-Armband zugeordnete Spind

sowie ggf. zusätzlich genutzte kostenpflichtige Angebote wie z. B. Massagen oder gastronomische Leistungen gespeichert. Diese Informationen werden sofort nach der korrekten Abrechnung an der Thermalbadkasse gelöscht. Jeder Besucher hat die Möglichkeit, die Daten, die zu seinem Chip-Armband gehören, an zwei Terminals abzulesen.

Aus datenschutzrechtlicher Sicht ist das Zahlungssystem des Thermalbades nicht zu beanstanden, da die Speicherung personenbezogener Daten nur mit Einwilligung der Betroffenen erfolgt. Ich habe jedoch angeregt, die Kassenmitarbeiter und -mitarbeiterinnen nochmals ausdrücklich auf die Freiwilligkeit der Namensnennung hinzuweisen, da dies in der Praxis offensichtlich nicht allen Bediensteten bekannt war.

7. Sonstige Selbstverwaltungskörperschaften und Kammern

7.1 Unzulässigkeit der Weitergabe von Daten aus Auskünften von Postdiensteanbietern durch die Industrie- und Handelskammern

Holt eine Industrie- und Handelskammer aufgrund des § 13 Abs. 1 des Gesetzes über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen bei Anbietern von Postdiensten Auskünfte über Namen und zustellungsfähige Anschriften von am Postverkehr Beteiligten ein, darf sie die erhaltenen Daten nicht an Dritte weitergeben.

Mehrere Rechtsanwälte, die im Auftrag ihrer Mandanten Geldpreise einklagen sollten, baten eine Industrie- und Handelskammer (IHK) um Hilfe bei der Beschaffung zustellungsfähiger Anschriften. Ihre Mandanten hatten von Firmen Briefe erhalten, in denen ihnen mitgeteilt wurde, dass sie Gewinner eines Geldpreises seien. Eigentliches Ziel der Anschreiben war allerdings, die Empfänger zur Teilnahme an Lotteriespielen zu bewegen. Da nach deutschem Recht die Auslobung von Geldpreisen bindend ist, d. h. den Adressaten damit ein Anspruch auf Auszahlung des Preises erwächst, wollten die Empfänger die nicht unerheblichen Geldbeträge einklagen. Schwierigkeiten bereitete jedoch die Beschaffung der dazu notwendigen zustellungsfähigen Anschriften. An ihrem Sitz im Ausland verfügten die Firmen nur über Postfachadressen. Der Versuch der Anwälte, über die Postfachadressen, die die Firmen bei der Deutschen Post AG unterhielten, an die Anschriften zu gelangen, scheiterte an der Weigerung der Deutschen Post AG, die Daten herauszugeben. Ihre Hoffnung setzten die Anwälte daraufhin auf die IHK, die gestützt auf das Unterlassungsklagengesetz die Anschriften bei der Deutschen Post AG erfragen und an sie weiterleiten sollte. Die IHK bat mich um datenschutzrechtliche Beurteilung der Auskunftswünsche.

Die von den Anwälten gewünschten Datenübermittlungen sind unzulässig. Anbieter von Postdiensten haben Namen und Anschriften der am Postverkehr beteiligten Personen grundsätzlich geheim zu halten, denn nicht nur der Inhalt der Postsendungen, sondern auch die näheren Umstände des Postverkehrs unterliegen dem Postgeheimnis, das natürliche wie juristische Personen schützt (§ 39 Abs. 1 PostG). Nur wenn sie durch Gesetz oder Einwilligung der Betroffenen dazu befugt sind, dürfen Postdiensteanbieter dem Postgeheimnis unterliegende Daten an Dritte weitergeben. Eine solche Offenbarungsbefugnis enthält das Gesetz über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen (Unterlassungsklagengesetz – UKlaG). § 13 Abs. 1 UKlaG verpflichtet die Postdiensteanbieter, den IHK zur Durchsetzung von Unterlassungs- und Widerrufsansprüchen bei Allgemeinen Geschäftsbedingungen und zur Durchsetzung von Unterlassungsansprüchen bei verbraucherschutzgesetzwidrigen Praktiken Name und zustellungsfähige Anschrift eines am Postverkehr Beteiligten mitzuteilen.

Das Unterlassungsklagengesetz definiert nicht nur den zulässigen Übermittlungszweck, sondern legt in § 13 Abs. 1 auch den Kreis der Auskunftsberechtigten abschließend fest. Postdiensteabieter dürfen die Daten nur den dort genannten Stellen übermitteln. Wie wichtig dem Gesetzgeber eine Beschränkung des Kreises der Auskunftsberechtigten ist, zeigt auch § 3 Abs. 1 Satz 2 UKlaG, wonach die IHK Ansprüche auf Unterlassung und Widerruf nur an qualifizierte Einrichtungen im Sinne des § 3 Abs. 1 Satz 1 UKlaG abtreten kann.

§ 13 Abs. 1 UKlaG

Wer geschäftsmäßig Post-, Telekommunikations-, Tele- oder Mediendienste erbringt oder an der Erbringung mitwirkt, hat den nach § 3 Abs. 1 Nr. 1 und 3 anspruchsberechtigten Stellen und Wettbewerbsverbänden auf deren Verlangen den Namen und die zustellungsfähige Anschrift eines am Post-, Telekommunikations-, Tele- oder Mediendiensteverkehr Beteiligten mitzuteilen, wenn die Stelle oder der Wettbewerbsverband schriftlich versichert, dass diese Angaben
1. zur Durchsetzung eines Anspruchs nach § 1 oder § 2 benötigt werden …

§ 3 Abs. 1 Nr. 3 UKlaG

Die … Ansprüche auf Unterlassung und auf Widerruf stehen zu: …
3. den Industrie- und Handelskammern und den Handwerkskammern, …

Die Daten, welche die IHK von den Postdiensteanbietern erhalten haben, unterliegen zwar nicht mehr dem Postgeheimnis, denn dieses bindet nur die Diensteanbieter und nicht die IHK (§ 39 Abs. 2 PostG). Das macht die Daten für die IHK aller-

dings nicht frei verfügbar. Würden sie für Dritte bei den Postdiensteanbietern Auskünfte einholen, würden die Bedingungen, die das Unterlassungsklagengesetz für die zulässige Durchbrechung des Postgeheimnisses aufstellt, unterlaufen. Der Gesetzgeber hat bewusst keinen allgemeinen Auskunftsanspruch gegen Postdiensteanbieter geschaffen. Anders als etwa Adressauskünfte aus dem Einwohnermelderegister oder dem Handelsregister, die jeder verlangen kann, ist der Auskunftsanspruch nach dem Unterlassungsklagengesetz auf bestimmte Stellen beschränkt.

Der Datenübermittlung durch die IHK steht außerdem der Zweckbindungsgrundsatz des HDSG entgegen. Danach dürfen personenbezogene Daten grundsätzlich nur für den Zweck weiterverarbeitet werden, für den sie erhoben worden sind (§ 13 Abs. 1 HDSG). Geben die Kammern die erhaltenen Auskünfte der Postdiensteanbieter an Dritte weiter, damit diese zivilrechtliche Leistungsansprüche gegen die Betroffenen geltend machen können, ist dies eine den ursprünglichen Zweck ändernde Weiterverarbeitung der Daten. Das HDSG sieht zwar Ausnahmen von der Zweckbindung vor (§ 12 Abs. 2 i. V. m. § 12 Abs. 2 und 3), die hier jedoch allesamt nicht einschlägig sind.

Ich konnte der IHK auch keine rechtlichen Alternativen, wie die Auskunftswünsche erfüllt werden könnten, aufzeigen. Einzelne Verbraucher haben nach dem Unterlassungsklagengesetz nur einen Auskunftsanspruch gegenüber Postdiensteanbietern, wenn sie die in § 13a UKlaG erwähnten Unterlassungsansprüche geltend machen können, nicht jedoch zur Verfolgung von Leistungsansprüchen.

8. Entwicklungen und Empfehlungen im Bereich der Technik und Organisation

8.1 Probleme des E-Government-Konzepts des Landes

Im Rahmen des Hessischen E-Government-Konzepts sind zahlreiche zentralisierte IT-Strukturen und Datenbestände geplant. Dieses Konzept stellt hohe Anforderungen an Verfügbarkeit, Vertraulichkeit und Integrität, wenn umfangreiche Datenbestände vorgesehen sind, die besonders schützenswerte Daten umfassen, auf die jederzeit zugegriffen werden muss. Bei der vorgesehenen Terminal-Server-Architektur sind mir für einige Probleme keine Lösungen bei Einhaltung des strikt zentralen Ansatzes bekannt. Solange noch Papierdokumente bei den Dienststellen eingehen, ist der vollständige Übergang auf eine elektronische Verarbeitung rechtlich nicht möglich.

8.1.1 Anforderungen an zentrale IT-Verfahren und Strukturen

Die verstärkte Tendenz, DV-Verfahren zu zentralisieren, resultiert u. a. aus dem Wunsch, die gestiegenen Personal- und Sachkosten zu reduzieren, die sich bei dezentralen IT-Strukturen in den letzten Jahren ergeben haben. Ob die jeweils geplante technische Ausgestaltung geeignet ist das Ziel zu erreichen, muss sich zeigen. Es gibt allerdings Anforderungen aus Sicht des Datenschutzes und der Datensicherheit, die in den Planungen oft nicht oder nicht ausreichend berücksichtigt werden:

- Falls Daten mit hoher und sehr hoher Vertraulichkeit zentral verarbeitet werden, muss es technische Möglichkeiten in der Anwendung geben, die eine Kenntnisnahme durch Dritte aber auch durch Personal der zentralen Stelle sicher ausschließen.

- Maßnahmen gegen unbefugte Änderungen von Daten müssen auch gegen Personal der zentralen Stelle wirken. Insbesondere müssen aber die rechtlich geforderten Formvorschriften (z. B. qualifizierte elektronische Signatur) zur Gewährleistung der Verbindlichkeit und damit auch der Integrität durch die gewählte IT-Architektur korrekt umgesetzt sein.

- Die Verfügbarkeit der Anwendungen muss sichergestellt sein. Das betrifft die Übertragungskapazitäten des Kommunikationsnetzes und die Ausfallsicherheit des Netzes und der Server.

- Soweit der Übergang auf ausschließlich elektronische Dokumente bei Vernichtung der Papierdokumente vorgesehen ist, muss es Ausnahmen hierfür nach den rechtlichen Erfordernissen geben.

8.1.1.1 Immanente Probleme der zentralen E-Government-Anwendungen

Zentrale Datenbestände bieten einen Angriffspunkt für unbefugte Zugriffe oder unrechtmäßige Auswertungen. Bei dezentralen Datenbeständen bestehen demgegenüber eine Vielzahl von Angriffspunkten, die aber weniger kritisch sind, da jeweils nur eine Teilmenge der Daten betroffen ist.

Durch die Zentralisierung der Daten werden auch Daten und Informationen mit hohem oder sehr hohem Schutzbedarf betroffen. Das gilt besonders, wenn das Konzept vorsieht alle Daten und Dokumente zentral zu speichern. In dem Fall betrifft es auch Dokumente, die sensitive Daten, besondere Berufs- und Amtsgeheimnisse, Betriebsgeheimnisse oder politisch brisante Informationen betreffen.

Aus dem Kumulationsprinzip (durch Kumulation mehrerer kleinerer Schäden auf einem IT-System entsteht ein insgesamt höherer Gesamtschaden) ergibt sich in vielen Fällen ein hoher oder sehr hoher Schutzbedarf der Datenbestände und für die Datenübertragung. Da die zentralen Datenbestände die Gesamtheit der dezentralen Bestände ausmachen, kann jede Schwachstelle Auswirkungen auf den Datenbestand gesamten Landesverwaltung haben und damit den Super-GAU verursachen.

8.1.1.2 Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit bei zentralen Strukturen

a) *Vertraulichkeit:*
Administratoren, oft auch das Wartungspersonal, haben technisch die Möglichkeit, auf alle Daten zuzugreifen. Falls unberechtigte Dritte Zugriff auf Daten erhalten wollen, können sie ihre Anstrengungen auf nur ein Rechenzentrum konzentrieren und haben als zusätzliche Angriffspunkte die Übertragungswege. Zwar ist es von Vorteil, dass kostspielige, qualitativ hochwertige Sicherheitsvorkehrungen für ein zentrales Rechenzentrum nur einmal anfallen und deshalb leichter finanziert und umgesetzt werden können. Bei der zentralen Lösung fallen aber mehr Übertragungen an, die ebenfalls geschützt werden müssen. Eine gängige Maßnahme ist die verschlüsselte Übertragung und verschlüsselte Speicherung der Daten.

b) *Integrität:*
Analog der Vertraulichkeit können Binnentäter und Externe versuchen, Manipulationen vorzunehmen. Als Sicherheitsmaßnahme kommt zum Beispiel die elektronische Signatur in Betracht (s. auch Verbindlichkeit).

c) *Verfügbarkeit:*
Der Ausfall zentraler Komponenten oder ungenügende Übertragungs- bzw. Verarbeitungskapazitäten haben Einfluss auf alle angeschlossenen Dienststellen. So können sich beispielsweise wenn viele Dienststellen mit einer geringen Bandbreite angebunden sind, Antwortzeitprobleme ergeben.

d) *Verbindlichkeit:*
Mit der elektronischen Signatur kann die Verbindlichkeit erreicht werden. Abhängig von Formvorschriften muss ggf. die qualifizierte elektronische Signatur möglich sein.

8.1.1.3 Beispiele

Als Beispiel für die Hessische Landesverwaltung können DOMEA (Dokumentenverwaltung), eKIS (Kabinettinformationssystem) und eBeihilfe (elektronische Beihilfebearbeitung) genannt werden, für die eine identische technische Lösung für die Datenhaltung und Anbindung der Dienststellen eingesetzt werden soll. Es handelt sich um eine Terminalserver-Lösung, bei der die Dokumente auf zentralen Servern vorliegen und am Arbeitsplatz nur eine Bildschirmanzeige des Dokuments erfolgt. Für die zentrale E-Mail Lösung, die beginnend im Jahr 2004 eingeführt wird, ist eine ähnliche Architektur vorgesehen.

In allen Anwendungen sollen zum Teil Dokumente verarbeitet werden, die einen hohen oder sehr hohen Schutzbedarf haben.

a) *Vertraulichkeit:*

Bei eKIS und eBeihilfe werden die Dokumente verschlüsselt übertragen, bei DOMEA war Ende des Jahres noch keine Entscheidung gefallen, aber es gibt technisch die Möglichkeit dazu.

Auf den zentralen Rechnern sind die Dokumente nach den jetzigen Planungen unverschlüsselt gespeichert. Dies ist problematisch, weil es Dokumente gibt, die wegen besonderer Berufs- und Amtsgeheimnisse, sensitiver oder politisch brisanter Informationen auch Mitarbeiter der HZD oder Wartungstechniker nicht zur Kenntnis nehmen dürfen. Bei der Terminal-Server-Lösung werden Dokumente immer zumindest temporär in der zentralen Stelle unverschlüsselt gespeichert sein. Es gibt keine Möglichkeit, eine Kenntnisnahme durch Mitarbeiter der HZD sicher auszuschließen. Sie ist deshalb für die Behandlung von Dokumenten mit hohem Schutzbedarf nicht geeignet.

Mit einer Client-Server-Lösung (die Dokumente werden zentral gespeichert aber dezentral bearbeitet und können dort ver- und entschlüsselt werden) ließe sich das Problem bewältigen.

Die Vertraulichkeit von E-Mails kann beim angestrebten zentralen Ansatz durch Verschlüsselung erreicht werden. Wenn das Projekt PKI (Public Key Infrastructure) erfolgreich ist, gibt es landesintern die Möglichkeit verschlüsselte E-Mails zu versenden. Auch hier muss jedoch bei einer Terminal-Server-Lösung geprüft werden, ob die Anforderungen an die Vertraulichkeit und insbesondere an die Geheimhaltung privater Schlüssel tatsächlich erfüllt sind. Für behördeninterne Mails ist eine unverschlüsselte Übertragung oft unproblematisch, weil sensible Informationen das behördeninterne Netz nicht verlassen. Im Fall einer zentralen Struktur, d. h. alle E-Mails gehen über die zentrale Stelle, müssten interne E-Mails wie externe

behandelt werden. Dann gelten auch für eigentlich „interne“ E-Mails Einschränkungen, wie sie z. B. in der gemeinsamen Geschäftsordnung der Hessischen Ministerien (GGO) genannt sind, die eine Verschlüsselung erfordern.

b) *Verbindlichkeit und Integrität*
:
Prinzipiell kann durch elektronische Signaturen die Verbindlichkeit hergestellt werden. Es ist mir aber keine Lösung bekannt, mit der in einem Terminal-Server-Umfeld eine fortgeschrittene oder qualifizierte elektronische Signatur vorgenommen werden kann. Gerade im elektronischen Rechtsverkehr ist dies aber erforderlich.
Für Client-Server-Systeme gibt es technische Lösungen.
Wenn die Verbindlichkeit von Dokumenten gewährleistet ist, ist eine unbefugte Änderung nicht möglich. Somit ist die Integrität gegeben. Es können daher die gleichen Maßnahmen zum Tragen kommen, die auch zur Wahrung der Verbindlichkeit dienen.

Bei der zentralen E-Mail kann hinsichtlich Integrität und Verbindlichkeit ebenfalls die elektronische Signatur eine Lösung sein. Das Projekt PKI bietet hier eine Lösung, wobei nach dem jetzigen Stand mit der PKI-Lösung aber noch keine qualifizierte elektronische Signatur möglich ist.

c) *Verfügbarkeit:*

Zwar ist die Verfügbarkeit der Datenbestände auf der HZD-Seite durch deren Back-up-Konzept gesichert. Ein Ausfall der zentralen Server oder der Übertragungstechnik würde aber zu einem Stillstand in den Dienststellen führen. Das Problem lässt sich entweder mit einer Dopplung der Server und Übertragungstechnik (Leitungen) oder mit der Haltung von Kopien auf dezentralen Rechnern lösen.

Infolge des hohen Übertragungsvolumens bei der zentralen E-Mail kann es bei externen, aber eben auch internen Mails, Verzögerungen geben. Bei internen Mails dürften sich die Antwortzeiten bei den Dienststellen verschlechtern, die mit Leitungen angebunden sind, die eine niedrige Übertragungskapazität haben.

8.1.2 Rechtliche Probleme beim vollständigen Übergang auf elektronische Dokumente

Ein vollständiger Übergang auf elektronische Dokumente setzt voraus, dass alle Papierdokumente ohne Auswirkungen auf die Beweisfunktion in elektronische Dokumente umgewandelt werden können und dass Einsendern von Dokumenten kein Rückgaberecht für ihre Originale zusteht. Anderenfalls ist eine Vernichtung nicht zulässig. Die Frage ist weitgehend von allgemein rechtlicher Natur, eine unzulässige Löschung ist aber auch ein Datenschutzverstoß.

Bei der Mehrzahl der Posteingänge wird die Arbeit nur mit dem elektronischen Dokument ohne Papieroriginal unproblematisch sein. Das gilt weitgehend für verwaltungsinterne Schreiben, für Schreiben von Dritten außerhalb der Verwaltung, denen kein Beweiswert zukommt und die nicht Eingang in ein Verwaltungsverfahren finden.

8.1.2.1 Papierdokument mit Beweiswert

Der Beweiswert von Papierdokumenten geht bei der Übertragung in elektronische Form nicht auf das elektronische Dokument über. Auch eine Beglaubigung oder/und elektronische Signatur bei der Überführung in die elektronische Form nach § 33 Abs. 4 Nr. 4a, Abs. 5 Nr. 2 VwVfG (bzw. der gleich lautenden geplanten hessischen Bestimmung) kann dies nicht leisten. Die Beglaubigungserklärung eines in elektronische Form umgesetzten Papierdokuments verbunden mit der Signatur der beglaubigenden Behörde bestätigt nur die inhaltliche Übereinstimmung mit dem Original. Einem bei der Umsetzung in die elektronische Form beglaubigten Dokument kommt kein Beweiswert nach § 292a ZPO zu. Diese Vorschrift regelt nur den Beweiswert von Dokumenten, die die eine Willenserklärung enthalten und bereits elektronisch erstellt und qualifiziert signiert sind; sie hilft hier also nicht weiter. Beim Beweisantritt steht zwar das beglaubigte Dokument, wenn es sich um eine öffentliche Urkunde handelt, dem Original gleich (§ 435 ZPO), gleichwohl kann die Vorlage des Originals verlangt werden. Bei einer Privaturkunde ist dazu nichts geregelt. Eine solche Urkunde ist deshalb zum Beweisantritt immer im Original vorzulegen.

Deshalb müssen Papierdokumente, wie z. B. ein Vertragsangebot, das bereits von der anderen Vertragspartei unterzeichnet ist oder ein von beiden Parteien unterzeichneter Vertrag, ein Antrag, eine Eingabe oder eine rechtsverbindliche Erklärung im Verwaltungsverfahren, weiterhin in Papierform behandelt werden.

8.1.2.2 Papierdokumente mit Rückgabepflicht

Bei Bewerbungen bestehen datenschutzrechtliche Bedenken gegen eine Vernichtung, weil diese zum einen solange nicht zulässig ist, wie die Bewerbung im Hinblick auf eine mögliche Überprüfung der Rechtmäßigkeit des Auswahlverfahrens

noch zu Beweiszwecken erforderlich sind. Nach § 19 Abs. 2 Nr. 2 HDSG dürfen Daten in solchen Fällen nicht gelöscht, sondern nur gesperrt werden. Abgesehen davon besteht die Notwendigkeit, Bewerbern, die nicht zum Zuge gekommen sind, ihre Unterlagen (Lebenslauf, Zeugnisse etc.) wieder zurückzusenden. Darauf besteht ein Anspruch.

Auch im Vergabeverfahren können Ansprüche auf Rücksendung von Unterlagen (z. B. Modellzeichnungen, Pläne) entstehen, die einer Vernichtung entgegenstehen.

8.1.3 Zusammenfassung

Abhängig von der eingesetzten Technik bringen zentrale IT-Strukturen Probleme mit sich, die im Vorfeld gelöst werden müssen. Dabei müssen sich technische und organisatorische Maßnahmen ergänzen. Es gibt dabei Ausprägungen, bei denen neue Sicherheitslösungen gefunden werden müssen. Ist das geschehen, so können die Verfahren datenschutzgerecht betrieben werden.

Das Ziel des vollständigen Übergangs auf elektronische Dokumente lässt sich solange nicht realisieren, wie Post bei den Dienststellen nicht ausschließlich in elektronischer Form eingeht. Abläufe müssen bis dahin weiterhin die Bearbeitung von Papierdokumenten vorsehen.

8.2 Arbeitskreis „Zentrale IT-Security“

Im E-Government Masterplan hat die Hessische Landesregierung unter anderem das Ziel formuliert, eine angemessene IT-Sicherheit zu organisieren. Hierzu wurde der Arbeitskreis „Zentrale IT-Security“ gegründet, den ich beratend unterstütze. Neben anderen Aktivitäten wurde eine Sicherheitsleitlinie erstellt und veröffentlicht sowie ein Entwurf zur Vorgehensweise bei einer Schutzbedarfsfeststellung erarbeitet.

Die Hessische Landesregierung hat mit ihrem E-Government-Masterplan einen Rahmen vorgegeben, in dem die Aktivitäten für eine umfassende Neustrukturierung der Informationstechnik beschrieben sind. Als ein Punkt ist die IT-Sicherheit genannt.

IT-Sicherheit organisieren

Die Durchdringung aller Prozesse mit Informationstechnik, die Vernetzung öffentlicher Verwaltung mit dem Internet und die ressortübergreifende Integration von Verfahren stellen neue Herausforderungen an die IT-Sicherheit dar, denen mit angemessenen Maßnahmen auf Grundlage des IT-Grundschutzhandbuchs des BSI (Bundesamt für Sicherheit in der Informationstechnik) begegnet werden muss.
Im Rahmen der zu erarbeitenden IT-Architektur ist eine angemessene IT-Sicherheit zu organisieren.

Maßnahmen

Schaffung von organisatorischen Rahmenbedingungen zur nachhaltigen Gewährleistung von IT-Sicherheit

Einrichtung eines IT-Sicherheitsmanagements (AK IT-Sicherheit etablieren)

Erarbeitung eines abgestimmten IT-Sicherheitsstandards, einschl. der Definition von Verantwortlichkeiten und Befugnissen

Zentralisierung und Standardisierung von Komponenten, zur Steigerung der IT-Sicherheit

Hinreichende Dokumentation aller Sicherheitsvorkehrungen und -maßnahmen

8.2.1 Sicherheitsleitlinie

Um die Arbeit in den Dienststellen auf eine verlässliche Grundlage zu stellen, wurde eine Sicherheitsleitlinie erarbeitet, die im Staatsanzeiger veröffentlicht wurde (StAnz. 2004, S. 3827) Diese Leitlinie ist den Beschäftigten bekannt zu geben und dient als Grundlage für die IT-Sicherheitsleitlinien der Ressorts. Sie behandelt die folgenden Punkte.

- Grundsätze
  Es ist beschrieben, auf welcher Basis ein angemessenes Sicherheitsniveau erreicht werden soll.

- Ziele
  Es werden Zielvorgaben zum Verhalten der Mitarbeiter entwickelt und die Stellung der IT-Sicherheit im Verhältnis zu anderen Kriterien des IT-Einsatzes festgelegt.

- Maßnahmen
  Die umzusetzenden organisatorischen Maßnahmen werden genannt. Dabei wird – natürlich – nicht auf technische Maßnahmen oder organisatorische Einzelmaßnahmen eingegangen.

- Verantwortlichkeiten
  Hierbei werden die Kompetenzen der Beteiligten gegeneinander abgegrenzt. Es handelt sich um den wohl wichtigsten Punkt.

- Verstöße und deren Folgen
  Diese Aufzählung richtet sich in besonderem Maße an den Mitarbeiter.

Der komplette Text der Sicherheitsrichtlinie ist im Kapitel „Materialien“ zu finden.

8.2.2 Entwurf eines Leitfadens zur Vorgehensweise zur Schutzbedarfsfeststellung im Rahmen der Erstellung eines Sicherheitskonzeptes

8.2.2.1 Motivation

Damit den IT-Anwendungen im E-Government-Umfeld die angemessenen Schutzmaßnahmen zugeordnet werden können, muss zunächst der Schutzbedarf der IT-Anwendungen festgestellt werden. Für die Grundwerte

- Vertraulichkeit
- Integrität
- Verfügbarkeit

muss für jede Anwendung gesondert eine Einstufung in die Schutzbedarfskategorie vorgenommen werden.

Wie bereits einleitend beschrieben, sieht der Masterplan des Landes Hessen ein Vorgehen nach dem IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI) vor. Der Leitfaden folgt daher den Vorgaben in diesem Handbuch und definiert ein Raster in drei Stufen:

- niedriger bis mittlerer Schutzbedarf
- hoher Schutzbedarf
- sehr hoher Schutzbedarf

Im Folgenden werden der Aufbau des Entwurfs des Leitfadens zur Feststellung des Schutzbedarfs und die Einstufung in das dreistufige Raster beschrieben und erläutert.

Die Motivation (Kapitel 1) wurde hier bereits erläutert.

Zur Sensibilisierung werden in Kapitel 2 an die Verantwortlichen der IT-Anwendungen Fragen vom Typ „Was wäre wenn“ gestellt, um ein Bild der möglichen Bedrohungen und Schäden zu erzeugen.

Darauf aufbauend wird im Kapitel 3 die Einordnung in die Schutzbedarfskategorien nach IT-Grundschutzhandbuch anhand der möglichen Konsequenzen beschrieben.

Im Abschnitt 4 wird die Schutzbedarfsfeststellung von IT-Anwendungen und IT-Systemen über eine Bewertungsmatrix unterstützt.

Für die ressortweite Betrachtung der IT-Systeme und Kommunikationsverbindungen wird in Kapitel 5 eine Diskussionsgrundlage vorgelegt. Allerdings ist eine hessenweite Vorgehensweise noch festzulegen.

8.2.2.2 Schutzbedarfsanalyse anhand von Schäden und ihren Folgen – Schadensszenarien

Ausgehend von der Vorstellung, dass Vertraulichkeit, Integrität oder Verfügbarkeit einer IT-Anwendung oder der zugehörigen Daten und Informationen verloren gehen, werden die maximalen Schäden und Folgeschäden betrachtet, die aus einer solchen Situation entstehen können.

Die Vertraulichkeit von Daten und Informationen, d. h. dass diese ausschließlich Befugten in der zulässigen Weise zugänglich sind, bedingt Anforderungen, die auch für die IT-Anwendung oder das IT-System gelten.

Die Integrität fordert die Unversehrtheit der Daten und Informationen und führt ebenfalls zu Konsequenzen für die IT-Anwendung und IT-Systeme.

Die Verfügbarkeit, also die Gewährleistung, dass Informationen und Dienste, wenn diese von den Benutzern gebraucht werden, jederzeit und in der vorgesehenen Geschwindigkeit abgerufen und genutzt werden können, muss gleichfalls durch die IT-Systeme und IT-Anwendungen umgesetzt werden.

Unter der Fragestellung „Was wäre, wenn“ werden aus Sicht der Anwender in den Leitfaden realistische Schadenszenarien entwickelt und die zu erwartenden materiellen oder ideellen Schäden beschrieben.

Um die möglichen Schäden besser einschätzen zu können, werden dort einige typische Schadenskategorien erläutert. Sie werden ergänzt um spezifische Fragestellungen, die bei der Bewertung der möglichen Schäden bzw. Folgeschäden berücksichtigt werden können. Dieser Fragenkatalog ist nicht abschließend.

Die folgenden sieben Schadensszenarien müssen genau beleuchtet werden.

1. Verstoß gegen Gesetze/Vorschriften/Verträge

Der Verlust der Vertraulichkeit, der Integrität und der Verfügbarkeit kann zu einem Verstoß gegen Gesetze, Vorschriften oder Verträge führen. Die Schwere des Schadens ist dabei oftmals abhängig davon, welche rechtlichen Konsequenzen daraus für die Behörde/das Ressort/die Landesverwaltung entstehen können.

2. Beeinträchtigung des informationellen Selbstbestimmungsrechts

Bei der Implementierung und dem Betrieb von IT-Systemen und IT-Anwendungen besteht die Gefahr einer Verletzung des informationellen Selbstbestimmungsrechts bis hin zu einem Missbrauch personenbezogener Daten.

3. Beeinträchtigung der persönlichen Unversehrtheit

Die Fehlfunktion eines IT-Systems oder einer IT-Anwendung kann unmittelbar die Verletzung, die Invalidität oder den Tod von Personen nach sich ziehen. Die Höhe des Schadens ist am direkten persönlichen Schaden zu messen.

4. Beeinträchtigung der Aufgabenerfüllung

Gerade der Verlust der Verfügbarkeit eines IT-Systems oder der Integrität der Daten kann die Aufgabenerfüllung der Behörde/des Ressorts/der Landesverwaltung erheblich beeinträchtigen. Die Schwere des Schadens richtet sich hierbei nach der zeitlichen Dauer der Beeinträchtigung und nach dem Umfang der Einschränkungen der angebotenen Dienstleistungen.

5. Negative Außenwirkung

Durch den Verlust einer der Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit in einer IT-Anwendung können verschiedenartige negative Außenwirkungen entstehen, zum Beispiel Ansehensverlust der Behörde/ des Ressorts /der Landesverwaltung, Vertrauensverlust der Ressorts untereinander oder auch verlorenes Vertrauen in die Arbeitsqualität der Behörde/des Ressorts/der Landesverwaltung.

6. Finanzielle Auswirkungen

Unmittelbare oder mittelbare finanzielle Schäden können durch den Verlust der Vertraulichkeit schutzbedürftiger Daten, die Veränderung von Daten oder den Ausfall eines IT-Systems entstehen.

7. Fachanwendungsspezifische Schadensszenarien

An dieser Stelle wird die Möglichkeit geboten, bisher nicht einzuordnende Schadensszenarien, die auf die individuelle Fachanwendung einwirken können, zu beschreiben. Auch hier muss darauf eingegangen werden, inwieweit die Vertraulichkeit, Integrität und Verfügbarkeit der Daten unter diesem Schadensszenario leiden können.

8.2.2.3 Einordnung in die Schutzbedarfskategorien nach IT-Grundschutzhandbuch

Anhand der aufgeführten Schadensszenarien und der Was-wäre-wenn-Fragen entsteht ein Bild der **möglichen Bedrohungen und Schäden** für Daten, Informationen und IT-Anwendung. Die Fachanwendungen sind nun bezüglich der **möglichen Konsequenzen** in die Schutzbedarfskategorien nach IT-Grundschutzhandbuch einzuordnen.

Um die Schutzbedarfskategorien "niedrig bis mittel", "hoch" und "sehr hoch" voneinander abgrenzen zu können, bietet das IT-Grundschutzhandbuch (Kapitel 2.2; Stand Anfang 2004) zur Orientierung eine Bewertungshilfe, die die Aspekte Vertraulichkeit, Integrität und Verfügbarkeit einzeln betrachtet.

8.2.2.4 Schutzbedarfsfeststellung über eine Bewertungsmatrix

Die nachfolgende Bewertungsmatrix soll die Schutzbedarfsfeststellung für die IT-Anwendung unterstützen (Tabelle 1).

Tabelle 1

Schutzbedarfskategorie / Schadensszenarien		niedrig bis mittel	hoch	sehr hoch
Verstoß gegen – Gesetze – Vorschriften – Verträge	Vertraulichkeit			
	Integrität			
	Verfügbarkeit			
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Vertraulichkeit			
	Integrität			
	Verfügbarkeit			
Beeinträchtigung der persönlichen Unversehrtheit	Vertraulichkeit			
	Integrität			
	Verfügbarkeit			
Beeinträchtigung der Aufgabenerfüllung	Vertraulichkeit			
	Integrität			
	Verfügbarkeit			
Negative Außenwirkung	Vertraulichkeit			
	Integrität			
	Verfügbarkeit			
Finanzielle Auswirkungen	Vertraulichkeit			
	Integrität			
	Verfügbarkeit			
Fachanwendungsspezifische Schadenszenarien	Vertraulichkeit			
	Integrität			
	Verfügbarkeit			

_____

Datum und Unterschrift

Der Verantwortliche für die IT-Anwendung hat zu entscheiden, bei welchen möglichen Bedrohungen und Schäden hinsichtlich der Schutzgüter Vertraulichkeit, Integrität und Verfügbarkeit (Was-wäre-wenn-Fragenkatalog aus Kapitel 2) mit welchen möglichen Konsequenzen (Schutzbedarfskategorie gemäß Bewertungshilfe aus Kapitel 3) zu rechnen ist.

8.2.2.5 Begründungen

Die Entscheidungen sind zu begründen.

8.2.2.6 Schutzbedarfsfeststellung

Hinsichtlich der Schutzgüter Vertraulichkeit, Integrität und Verfügbarkeit ist jeweils der Schutzbedarf nach dem Maximumprinzip festzustellen.

Des Weiteren hat die Schutzbedarfsfeststellung der IT-Anwendung ebenfalls nach dem Maximumprinzip (nach dem maximalen Wert aus der Einstufung von Vertraulichkeit, Integrität und Verfügbarkeit) zu erfolgen.

Abschließend ist der sich für das IT-System aus den untersuchten IT-Anwendungen abgeleitete maximale Schutzbedarf festzulegen (Tabelle 2).

Tabelle 2

Schutzbedarf von	Schutzbedarfskategorie
Vertraulichkeit	
Integrität	
Verfügbarkeit	
IT-Anwendung	
IT-System	

_____
Datum und Unterschrift

8.2.2.7 Abhängigkeiten zwischen IT-Anwendungen

Des Weiteren sind Abhängigkeiten zwischen IT-Anwendungen, beispielsweise zur Bürokommunikation oder E-Mail aufzuführen.

8.2.2.8 Bewertung und weitere Vorgehensweise

Um den Schutzbedarf eines IT-Systems und der Kommunikationsverbindungen festzustellen, müssen zunächst diejenigen IT-Anwendungen, die in direktem Zusammenhang mit diesen stehen, nach den vorangegangenen Aspekten einer Schutzbedarfsanalyse unterzogen werden.

Für die Ermittlung des Schutzbedarfs von IT-Systemen und Kommunikationsverbindungen müssen nun die möglichen Schäden der relevanten IT-Anwendungen in ihrer Gesamtheit sowie unter Berücksichtigung von Abhängigkeiten betrachtet werden.

Für diese Bewertung werden herangezogen:

- Maximum-Prinzip
  Im Wesentlichen bestimmt der Schaden bzw. die Summe der Schäden mit den schwerwiegendsten Auswirkungen den Schutzbedarf des IT-Systems.

- Kumulationseffekte
  Durch Häufung von mehreren Schäden auf einem IT-System kann ein insgesamt höherer Gesamtschaden entstehen.

- Verteilungseffekte
  Ein hoher Schutzbedarf einer IT-Anwendung überträgt sich nicht auf ein IT-System, wenn nur unwesentliche Teile der IT-Anwendung auf dem IT-System laufen.

Die abschließende Schutzbedarfsfeststellung der IT-Systeme obliegt der Zuständigkeit der Ressorts.

8.3 Problemfall Organisations-Administrator

In meinem 31. Tätigkeitsbericht, Ziff. 12.2 habe ich von der Einführung des Active Directory im Netz der hessischen Landesverwaltung berichtet. Besondere Aufmerksamkeit erhielten die mit der Funktion des Organisations-Administrators verbundenen Zugriffsmöglichkeiten in dem Windows-2000-Netz. Im laufenden Betrieb und bei der Erweiterung des Netzes haben sich Probleme mit dem Konzept zur Kontrolle des Organisations-Administrators ergeben.

8.3.1 Organisatorischer Rahmen

Im Jahr 2001 wurde durch den Landesautomationsausschuss beschlossen, eine Netzwerk-Infrastruktur auf Basis des Active Directory der Fa. Microsoft in der Landesverwaltung einzuführen. (s. 31. Tätigkeitsbericht, Ziff. 12.2)

Seit Anfang 2002 werden in einer Fachgruppe „Active Directory“ (FAD) Konzepte zur Planung und zum Betrieb der hessenweiten Active Directory Struktur erarbeitet. Diese werden dem Entscheidungsgremium Active Directory (EGAD) zur Beschlussfassung vorgelegt. Die Geschäftsstelle Active Directory (GAD) bereitet die Konzepte vor und setzt sie um. Änderungen und Ergänzungen zu bestehenden Konzepten und Dokumenten müssen als Änderungsanträge über die GAD eingebracht werden. Sie werden in der FAD diskutiert, ggf. geändert und müssen dann vom EGAD beschlossen werden.

Einer der ersten und wesentlichsten Beschlüsse betraf die Netz- und Domänenstruktur. In Hessen hat man sich entschieden, die „Forest-Root-Domäne“ nur als Klammer für die darunter liegenden Domänen zu nutzen. Sie wird nur soweit genutzt, wie es für die Funktionsfähigkeit des Netzes erforderlich ist. Als Konsequenz können gerade die sicherheitsrelevanten Aktionen der Organisations-Administratoren und Schema-Administratoren auf ein Minimum reduziert werden. In meinem 31. Tätigkeitsbericht, Ziff. 12.2 hatte ich mit der Funktion Organisations-Administrator verbundene Risiken skizziert.

…
Domänen sind das grundlegende Strukturelement für das AD. Die Domäne bildet grundsätzlich eine Grenze bezüglich der Sicherheit und der Administration. Innerhalb einer Domäne haben die Domänenadministratoren weitgehende Zugriffsrechte beziehungsweise können sich die Rechte verschaffen. Rechte in einer anderen, auch hierarchisch untergeordneten Domäne, sind damit nicht verbunden. Sie müssen explizit vergeben werden.

Eine Ausnahme von dieser Regel bilden die Organisations-Administratoren. Das sind die Domänenadministratoren der so genannten Forest-Root-Domäne, der ersten Domäne, die in einem Windows-2000-Netzwerk angelegt wird. Diese Administratoren haben umfassenden Zugriff im gesamten Netzwerk oder können sich den Zugriff verschaffen.
…

In dem Dokument „Sicherheitsaspekte zur Kontrolle der Gesamtstruktur und der Einsatzkontrolle von Organisations- und Schema-Administratoren“ (Version 0.9 – Stand 15.07.2002) wurde die Vorgehensweise festgelegt, mit der dieser Problematik begegnet wird. In dem Dokument sind die Maßnahmen beschrieben, mit denen der Gebrauch der zugehörigen Kennungen kontrolliert wird. Eine Maßnahme sah vor, dass mindestens drei befugte Personen anwesend sein müssen, um mit den Kennungen arbeiten zu können.

Sicherheitsaspekte zur Kontrolle der Gesamtstruktur und der Einsatzkontrolle von Organisations- und Schema-Administratoren

…..
Sicherung der Organisations- und Schema-Administratoren-Accounts
Die Arbeitsgruppe hat für den Einsatz des Organisations- und des Schema-Administrators eine Reihe von Regeln aufgestellt, mit denen eine effektive Handhabung und zum anderen auch ein optimaler Schutz gewährleistet werden kann.
…
Kein einzelner Anwender kennt das Kennwort dieser beiden Administratoren. Stattdessen wird ein Mehraugenpasswort eingesetzt, von dem drei Anwender jeweils nur einen Teil des Kennworts kennen. ….
…

8.3.2 Erfahrungen im laufenden Betrieb

Bis Mitte 2003 stellte sich heraus, dass die im Konzept festgelegte Vorgehensweise im täglichen Betrieb aufwändig war und oft nicht umgesetzt wurde. Entgegen den ursprünglichen Vorstellungen wurde die Funktion des Organisations-Administrators häufig benötigt, um z. B. neue Standorte anzulegen, die Replikation zu überwachen, DHCP-Server zu autorisieren oder die domänenübergreifenden Fehleranalyse durchzuführen. Gerade in der laufenden Aufbauphase waren diese Aktivitäten unvermeidlich und mussten zeitnah durchgeführt werden.

Es ergab sich dann, dass die Inhaber der Teilpasswörter die Durchführung der Tätigkeiten nicht immer überwachen konnten. Die GAD war teilweise mehrere Tage im Besitz des vollständigen Passworts, bis dieses von den Passwortinhabern wieder gemeinsam geändert wurde. In dieser Zeit konnten einzelne Mitarbeiter der GAD mit der Kennung arbeiten und anhand der Protokolle war nicht feststellbar, wer als Organisations-Administrator tätig war.
Die GAD sah keine Möglichkeit anders vorzugehen, da sie die Konsistenz der Gesamtstruktur gewährleisten muss und dafür die entsprechenden Berechtigungen, also die eines Organisations-Administrator, benötigt.

8.3.3 Änderung der Vorgehensweise

Um diese Abweichung vom Konzept zu dokumentieren, eine neue Vorgehensweise zu beschreiben und entsprechend den organisatorischen Vorgaben zur Abstimmung zu stellen, nahm die GAD im Herbst 2003 mit mir Kontakt auf. In der Diskussion wie vorzugehen ist, wurde als Alternative ein Delegationskonzept betrachtet. Danach sollten die einzelnen Aufgaben betrachtet werden, die von der GAD durchzuführen sind. Ziel war es, Administrationsaufgaben und den laufenden Betrieb zu trennen. Für den täglichen Betrieb sollten Kennungen mit reduzierten Berechtigungen benutzt werden.

Als Ergebnis wurde ein Änderungsantrag formuliert und zur Abstimmung gestellt, der folgende Punkte umfasste:

- Es gibt zwei personifizierte Kennungen für die Geschäftsstelle.

- Es werden sämtliche An- und Abmeldungen und Objektzugriffe der beiden Kennungen überwacht.

- Die Protokolle werden im täglichen Betrieb durch die Administratoren der betroffenen Domänen und insgesamt durch den Hessischen Datenschutzbeauftragten kontrolliert.

- Mittelfristig, d h. bis Ende April 2004 wird ein Delegationskonzept durch die GAD erstellt: Ziel ist die Aufgaben- und damit Rollentrennung für die Administration und den laufenden Betrieb.

- Die GAD dokumentiert schriftlich die durchgeführten Tätigkeiten mit den personalisierten Organisations-Administratoren-Kennungen.

- Die Vorgehensweise wird auf das ursprüngliche Konzept zurückgeführt sobald das Delegationskonzept umgesetzt ist, spätestens jedoch nach sechs Monaten. Sofern die GAD Notwendigkeiten sieht, die Personalisierung länger aufrechtzuerhalten, wird ein neuer Antrag an die FAD/EGAD zur Verlängerung gestellt.

Dem Änderungsantrag wurde zugestimmt.

8.3.4 Umsetzung des Änderungsantrags

Mitte 2004 habe ich die Umsetzung des Änderungsantrags geprüft. Dabei musste ich Defizite feststellen. Eine Auswertung der vorhandenen Protokolle war praktisch nicht möglich. Die Aktivitäten der Organisations-Administratoren waren daher nur unvollständig nachzuvollziehen. Die vorgesehene Herauslösung der Windows-2000-Netzwerk-Überwachung aus dem Kontext der Organisations-Administratoren war noch nicht durchgeführt. Die hierbei angedachte Einbindung der Active-Directory-Gesamtstruktur in die bestehende Netzwerk-Überwachung befand sich noch im Stadium der Software-Auswahl.

Die Art und Weise wie die Organisations-Administrator-Kennungen benutzt wurden, war nicht von den Beschlüssen abgedeckt. Um den laufenden Betrieb nicht zu belasten, habe ich eine Übergangszeit für die Verfahrensweise akzeptiert. In diesem Zeitraum musste entweder das Delegationskonzept umgesetzt, auf das ursprüngliche Konzept zurückgegangen oder durch die Geschäftsstelle ein neuer Änderungsantrag gestellt worden sein.

Im Herbst 2004 stellte ich bei einer Prüfung fest, dass noch immer keine Fortschritte zu verzeichnen waren und nicht entsprechend den Beschlüssen verfahren wurde. Ich habe daher gefordert, auf die Vorgehensweise nach dem ursprünglichen Konzept zurückzukehren. Die Forderung wurde am Folgetag umgesetzt.

Ich werde weiterhin den Umgang mit den Organisations-Administrator-Kennungen und das Einhalten der Vorgaben prüfen. Vom Ergebnis her halte ich weiterhin ein Delegationsprinzip, bei dem die für den laufenden Betrieb nötigen Tätigkeiten durch Software unterstützt werden, für die sinnvollere und bessere Alternative.

8.4 Radio Frequency Identification (RFID)

RFID ist eine Technik, die bereits heute das tägliche Leben durchdringt und in Zukunft immer mehr Raum einnehmen wird. Abhängig vom Einsatzgebiet treten unterschiedliche Datenschutzfragen auf, die im Vorfeld berücksichtigt werden müssen. Die Datenschutzbeauftragten haben eine Entschließung veröffentlicht, in der die wesentlichen Aspekte beleuchtet werden.

8.4.1 Die RFID-Technik

Radio Frequency Identifikation (RFID) ist eine Technik, die durch Funkwellen eine kontaktlose automatische Identifikation von Gegenständen ermöglicht, die mit einem RFID-tag versehen sind. RFID-tags, die nach dem Prinzip des so genannten Transponders (Transmitter + Responder) arbeiten, bestehen mindestens aus einem Chip je nach Bauart ein Speicher- oder ein Prozessorchip und einer Antenne. Hauptanwendungsgebiete sind zurzeit die Bereiche Industrieautomation, Zutrittssysteme, Tieridentifikation, Warenmanagement und Diebstahlsicherung (z. B. elektronische Wegfahrsperren). Das Spektrum wird sich aber erweitern. Beispielsweise um Ausweisdokumente, Chipkarten als Fahrscheinersatz im öffentlichen Personennahverkehr, Kleidung oder Medikamentenpackungen.

Um einzelne Gegenstände mit Hilfe von RFID-tags zu identifizieren, müssen die tags in RFID-Systeme eingebunden werden. Die zurzeit verfügbaren Systeme bestehen in der Regel aus folgenden Komponenten:

- der RFID-tag selbst,
- das Schreibgerät zum Schreiben von Daten über den Transponder auf dem Chip,
- das Lesegerät, welches über den Transponder die auf dem Chip enthaltenen Informationen ausliest.

Schreib- und Lesegerät können in einer Einheit zusammengefasst werden. Diese Einheit wird in der Regel mit einer zusätzlichen Schnittstelle ausgestattet, um die vom RFID-tag empfangenen Daten an ein Hintergrundsystem (Datenbank, Automatensteuerung, …) weiterzuleiten. Datenschutzrechtlich muss besonders auf das Gesamtsystem, also RFID und Hintergrundsysteme, geachtet werden.

Datenschutzrelevant ist auch die Tatsache, dass sowohl die Datenübertragung zwischen Schreib-/Lesegerät und RFID-tag als auch in den meisten Fällen die Energieversorgung des RFID-tags drahtlos erfolgen. In diesem Fall spricht man von passiven tags. Aktive tags werden durch eine Batterie mit Strom versorgt und sind deshalb leistungsfähiger.

Die besonderen Datenschutzprobleme ergeben sich daraus, dass

- es ohne Wissen und Wollen des Eigentümers möglich ist mit dem RFID-tag zu kommunizieren,
- kein optischer Kontakt zwischen RFID-tag und Schreib-/Lesegerät erforderlich ist – der RFID-tag kann versteckt angebracht sein –,
- die Kommunikation aus einiger Entfernung von Dritten mitgelesen werden kann.

Passive RFIDs können wegen ihrer hohen Lebensdauer, die mit bis zu zehn Jahren angegeben wird, vielfältig eingesetzt werden. Man unterscheidet RFID-Systeme, die dem Lesegerät immer nur mit einer eindeutigen Nummer antworten und Systeme, die wie herkömmliche Chipkarten eine Verarbeitung von Daten auf dem RFID-Chip erlauben und derzeit bis zu 100 KByte Daten speichern können. Die Entfernung zum Auslesen oder Verarbeiten der Daten im RFID-Chip, der kleiner als 1 Quadratmillimeter sein kann, variiert je nach verwendeter Technologie zwischen einigen Zentimetern und einigen Metern.

8.4.2 Einsatz-Szenarien von RFID

Im letzten Jahr hat die Nutzung der RFID-Technik zu heftigen Diskussionen geführt. Auslöser war die testweise Einführung von RFID in einigen wenigen Warenhäusern. Obwohl die Wirtschaft gegenüber dem öffentlichen Bereich eine Vorreiterrolle einnimmt, wird diese Technologie künftig in vielen Lebensbereichen, auch dem öffentlichen Sektor, eine große Rolle spielen. Die folgenden Beispiele zeigen auf, dass der Bürger bereits jetzt in vielfältiger Art und Weise mit dieser Technologie konfrontiert ist.

8.4.2.1 Einkauf

Wenn Waren mit RFID-tags gekennzeichnet sind, ergeben sich für Käufer möglicherweise gravierende Konsequenzen. Beispielsweise müsste der Eigentümer einer Ware nicht einmal über die Existenz eines tags wissen und trotzdem könnten die Daten gelesen werden. RFID-tags können dann zur Gefährdung der Privatsphäre führen, wenn Daten zu den Waren ausgelesen werden und, z. B. über die Nutzung einer Kundenkarte, mit Daten zur Person des Käufers verknüpft werden. Dies resultiert aus folgenden Aspekten:

- RFID-Systeme arbeiten drahtlos. Das Auslesen der auf dem RFID-tag gespeicherten Daten kann daher prinzipiell ohne Wissen des Besitzers der Ware erfolgen. Der weitere Umgang mit den so erhobenen (personenbezogenen) Daten ist weitgehend intransparent.

- RFID-tags werden in solchen Bauformen angeboten, die ein verstecktes Anbringen an Waren ermöglichen. Wenn der Käufer eines Produktes nichts über die Existenz des RFID-tags weiß, wird er auch keine Schutzmaßnahmen ergreifen, um ein unbemerktes Auslesen zu verhindern.

- RFID-tags ermöglichen eine weltweit eindeutige Kennzeichnung von einzelnen Gegenständen. Somit ist es prinzipiell möglich, weltweit und dauerhaft einzelnen Personen die von ihnen erworbenen Produkte zuzuordnen. Auf diese Weise könnte ein globales Registrierungssystem aufgebaut werden.

- Werden die Daten aus RFID-tags mit personenbezogenen Daten der Besitzer zusammengeführt (beispielsweise beim Bezahlen mit einer entsprechend ausgestalteten Kundenkarte), lässt sich das Kaufverhalten einzelner Kunden detailliert analysieren. Darüber hinaus könnten diese Datensammlungen mit Identifikationssystemen gekoppelt werden, mit deren Hilfe dann weltweite Bewegungsprofile Einzelner erstellt werden können.

8.4.2.2 Diebstahlsicherung

Auch in Bibliotheken werden zunehmend Bücher mit RFID-Etiketten versehen, um Diebstähle zu unterbinden und die Katalogisierung und Ausleihe zu vereinfachen. Mit der Ausleihe von Büchern entsteht über das Ausleihsystem der Bibliothek ein Interessenprofil des Lesers.

Bei Kraftfahrzeugen hat sich mittlerweile zur Realisierung eines wirkungsvollen Diebstahlschutzes die Wegfahrsperre auf Basis von RFID-Systemen durchgesetzt. Der Transponder befindet sich dabei im Autoschlüssel, das Lesegerät ist in der Nähe des Zündschlosses platziert. Das Fälschen eines Schlüssels wird durch kryptographische Verfahren zur Authentifizierung zwischen Schlüssel und Fahrzeug verhindert.

Weit verbreitet ist die Verwendung von RFID-tags als Diebstahlsicherung in Geschäften und Kaufhäusern. Sie sind entweder in Etiketten oder vor allem bei Bekleidung in ca. 3 bis 5 cm große Hartplastikscheiben oder -riegel integriert und enthalten einen 1-bit-Transponder, der lediglich eine ja/nein-Information i. S. v. bezahlt/nicht bezahlt speichern kann. Beim Bezahlen wird die Diebstahlsicherung entfernt oder durch Anlegen eines starken Magnetfeldes deaktiviert. Sollte ein Kunde mit einem noch nicht deaktivierten Transponder das Geschäft verlassen wollen, geben Lesegeräte im Ausgangsbereich akustischen oder optischen Alarm.

8.4.2.3 Zutrittskontrollsysteme

Ein weiteres bewährtes Einsatzgebiet der RFID-Technologie sind Zutrittskontrollsysteme. Bei ausreichender Reichweite der Transponder ist das Passieren einer mit einem Lesegerät gesicherten Tür möglich, ohne dass der Transponder aus der Tasche geholt werden muss. Oft wird dieser gleichzeitig auch zur Zeiterfassung benutzt, die dadurch weitgehend automatisiert werden kann.

8.4.2.4 Tieridentifikation

RFID-Systeme haben sich als sehr hilfreich bei der Identifizierung von Tieren erwiesen. Bei Rindern können sich die Transponder mit einer Seriennummer beispielsweise im Halsband oder in der Ohrmarke befinden. Es werden aber auch injizierbare Transponder verwendet, die sich in einem Glasgehäuse befinden und im Körper des Tieres verbleiben. Damit ist es möglich, die Tiere individuell zu erfassen und so z. B. die Fütterung zu automatisieren. Auch der Herkunftsnachweis und Transport der Tiere wird durch die kontaktlose automatische Identifikation erleichtert. Dieselbe Technik wird zur Identifikation von Hunden benutzt, deren RFID-tag eine eindeutige Nummer speichert, die in einer bundesweiten Datenbank auf die Daten des Halters verweist.

8.4.2.5 Öffentlicher Personennahverkehr

Im Personennahverkehr gibt es Projekte, in denen eine Chipkarte als Fahrscheinersatz getestet wird. Auf der Chipkarte befindet sich neben den Fahrdaten auch eine eindeutige Kennung, die bei persönlichen Karten den Kunden identifiziert. Diese Kennung wird von den Kartenlesern im Bus oder in der Bahn kontaktlos ausgelesen. In den Hintergrundsystemen entstehen dann Bewegungsprofile.

8.4.3 Kontrollfragen zum Datenschutz

Bei der Beurteilung, ob ein bestimmter Einsatz von RFID-Technik datenschutzgerecht ist, sind einige Fragen in jedem Fall zu beantworten. Neben den allgemeinen datenschutzrechtlichen Fragestellungen sind vor dem Einsatz dieser Technik die folgenden Kontrollfragen zu beantworten, die speziell die wesentlichen datenschutzrechtlichen Gesichtspunkte betreffen, die durch die RFID-Komponenten (Chipkarte, tag, Token, …) veranlasst sind.

- Wann und wie kommt es zum Personenbezug?
  Der Personenbezug kann bei der Herausgabe der Komponente oder später erfolgen. Er kann durch die Komponente selbst oder durch Hintergrundsysteme entstehen.

- Welche Rechtsgrundlagen gibt es für die Verarbeitung der Daten?

- Ist der Datenvermeidungs-/Erforderlichkeitsgrundsatz erfüllt?
  Wenn die personenbezogenen Daten nicht mehr benötigt werden, müssen sie gelöscht werden. Die Entscheidung sollte der Betroffene zumindest dann treffen können, wenn er Eigentümer der mit dem tag versehenen Sache ist.

- Wer kann wie auf welche Daten zugreifen?

- Wie wird ein unbefugter Zugriff auf Daten verhindert?

- Sind die Sicherheitsmaßnahmen angemessen, um unbefugte Zugriffe zu verhindern?

- Ist die Anwendung für den Betroffenen transparent?

- Wie kann der Betroffene seine Auskunftsrechte geltend machen?
  Dies muss durch technische Maßnahmen unterstützt werden.

- Sind Kommunikationsvorgänge, die auf einem personenbezogenen RFID-tag eine Datenverarbeitung auslösen, für den Betroffenen eindeutig erkennbar? (vgl. § 6c BDSG, § 8 Abs. 2 HDSG)

§ 6c BDSG

(1) Die Stelle, die ein mobiles personenbezogenes Speicher- und Verarbeitungsmedium ausgibt oder ein Verfahren zur automatisierten Verarbeitung personenbezogener Daten, das ganz oder teilweise auf einem solchen Medium abläuft, auf das Medium aufbringt, ändert oder hierzu bereithält, muss den Betroffenen

1. *über ihre Identität und Anschrift,*
2. *in allgemein verständlicher Form über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten,*
3. *darüber, wie er seine Rechte nach den §§ 19, 20, 34 und 35 ausüben kann, und*
4. *über die bei Verlust oder Zerstörung des Mediums zu treffenden Maßnahmen unterrichten, soweit der Betroffene nicht bereits Kenntnis erlangt hat.*

(2) Die nach Absatz 1 verpflichtete Stelle hat dafür Sorge zu tragen, dass die zur Wahrnehmung des Auskunftsrechts erforderlichen Geräte oder Einrichtungen in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen.

(3) Kommunikationsvorgänge, die auf dem Medium eine Datenverarbeitung auslösen, müssen für den Betroffenen eindeutig erkennbar sein.

§ 8 Abs. 2 HDSG

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 verarbeitet werden, etwa in Form einer Chipkarte, 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 der 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.

8.4.4 Datenschutzprobleme und daraus resultierende Anforderungen

Mit den datenschutzrechtlichen Fragestellungen beim Einsatz der RFID-Technologie haben sich die Datenschutzbeauftragten des Bundes und der Länder befasst. Sie haben in einer Entschließung auf die wesentlichen Probleme aufmerksam gemacht (Ziff. 10.5).

Wenn mit dem Einsatz von RFID-Technologie personenbezogene Daten erhoben werden, ohne dass Betroffene davon Kenntnis erlangen oder den Erhebungsvorgang beeinflussen können, können mit diesen Daten detaillierte Verhaltens-, Nutzungs- und Bewegungsprofile einzelner Personen – die entsprechend gekennzeichnete Gegenstände mit sich führen – ohne deren Wissen erstellt werden.

Diese Technologie hat Vorteile etwa zur Kontrolle der Logistik oder beim Diebstahlschutz. Anders als mit Bar-Codes ist es sogar möglich, jeden einzelnen Gegenstand mit einer eigenen Nummer zu kennzeichnen. Man könnte also zum Beispiel zwei Packungen des gleichen Produkts unterscheiden. Mit der breiten Einführung von derart gekennzeichneten Waren besteht die Gefahr, dass Verbindungen zwischen den RFID-Kennungen und dem Käufer/Nutzer der Ware hergestellt und dauerhaft gespeichert werden. Auch könnte in Zukunft ein Personenbezug unbemerkt durch Identitätspapiere mit RFID-Chip hergestellt werden, wenn wie derzeit diskutiert, Ausweisdokumente ohne Schutz gegen unbefugtes Ansehen eingeführt werden.

Aus Sicht des Datenschutzes ist es deshalb als unzulässig zu betrachten, wenn

- RFID-tags versteckt angebracht und verdeckt ausgelesen werden,
- Daten der RFID-tags aus verschiedenen Produkten ohne Rechtsgrundlage mit personenbezogenen Daten zusammengeführt werden,
- Verhaltens-, Nutzungs- und Bewegungsprofile ohne Rechtsgrundlage erzeugt und gespeichert werden.

Aus Datenschutzsicht sollten Hersteller und Betreiber von RFID-Systemen, die Produzenten von RFID-gekennzeichneten Waren und der Handel deshalb,

- die Betroffenen umfassend über Einsatz, Verwendungszweck und Inhalt von RFID-tags informieren,
- RFID-Daten nur solange zu speichern, wie es zur Erreichung des Zwecks erforderlich ist,
- Betroffenen Gelegenheit geben, sich Kenntnis über die auf einem RFID-tag gespeicherten Informationen zu verschaffen,
- Möglichkeiten zur Deaktivierung/Löschung von RFID-Chips schaffen, insbesondere dann, wenn Daten für die spezifischen Zwecke nicht mehr erforderlich sind,
- bei RFID-tags wirksame Blockierungsmechanismen, mit denen ein Auslesen der gespeicherten Daten fallweise unterbunden werden kann, entwickeln und über diese informieren, so dass kein Nutzungszwang gegeben und anonymes Kaufen weiterhin möglich ist,
- die Vertraulichkeit der gespeicherten und der übertragenen Daten durch wirksame Authentisierung der beteiligten Geräte und Verschlüsselung sicherstellen,
- bei RFID-Technologie mit Verarbeitungsfunktion Systeme anbieten, die keine Seriennummer tragen.

Soweit personenbezogene RFID-tags, zum Beispiel RFID-Chipkarten, eingesetzt werden, sind entsprechend den Anforderungen der Datenschutzgesetze (z. B. §§ 3 Abs. 10, 6c BDSG; § 8 Abs. 2 HDSG) Kommunikationsvorgänge, die auf dem RFID-tag eine Datenverarbeitung auslösen, für die Betroffenen eindeutig erkennbar zu machen. Anderenfalls sind den Nutzerinnen und Nutzern Mechanismen an die Hand zu geben, die eine Kommunikation unterbinden.

Nur durch einen transparenten Umgang mit dieser Technologie können auch zukünftig die in den Datenschutzgesetzen geforderte Zweckbindung, Datensparsamkeit und Vertraulichkeit, bei der Verarbeitung personenbezogenen Daten sichergestellt werden. Das Recht auf informationelle Selbstbestimmung muss auch bei der Nutzung von RFID-Systemen gewährleistet werden.

8.5 Anforderungen an die Ausgestaltung eines Meta-Directory

In der Hessischen Landesverwaltung wird ein Meta-Directory, eine Art Mitarbeiterverzeichnis mit Informationen zu allen Mitarbeitern, eingeführt. Ausnahmsweise muss es möglich sein, Daten von bestimmten Bediensteten nicht zur Auskunft zur Verfügung zu stellen.

Verschiedene Überlegungen haben dazu geführt, dass die Hessische Landesverwaltung die Einführung eines Meta-Directory plant, das Informationen zu allen Bediensteten enthält. Bisher werden an vielen Stellen Informationen gespeichert, die wie ein Telefonbuch dazu dienen, Beschäftigte innerhalb der Verwaltung erreichbar zu machen. Es handelt sich dabei im Allgemeinen um dienstliche Daten wie Name, Dienststelle, Telefonnummer, E-Mail-Adresse (dienstlich) usw. Die Daten in den Verzeichnissen sind jedoch oft nicht vollständig, nicht aktuell oder sogar falsch und können nicht landesweit abgefragt werden. In verschiedenen Ministerien und deren nachgeordnetem Bereich gibt es eigene Lösungen, die aber keine übergreifende Suche zulassen. Um diesen Missstand zu beheben, soll das neue Meta-Directory als zentrales Verzeichnis eingerichtet werden, das sich aus möglichst aktuellen Daten speist.

Auch bei der Konzeption des HCN2004, der Fortentwicklung des jetzigen Landesnetzes HCN2000, spielt ein gemeinsames Verzeichnis für alle Bereiche eine wesentliche Rolle. Das übergeordnete Verzeichnis soll bestimmte Daten der in den Ressorts existierenden verschiedenen Verzeichnisse bündeln und weitere mitarbeiterbezogene Daten umfassen, die zur Infrastruktur des Landesnetzes gehören. Auch diese Funktion soll das Meta-Directory erfüllen.

In einem ersten Schritt wurde ein Produkt ausgewählt, mit dem das angegebne Ziel erreicht werden soll. Es wird von den – untergeordneten – Verzeichnissen und SAP HR, dem einheitlich für die Landesverwaltung vorgesehenen Verfahren für die Personalverwaltung, beliefert. In einem zukünftigen Schritt soll von SAP/HR aus das Meta-Directory mit aktuellen Mitarbeiterdaten versorgt werden. Vom Meta-Directory aus werden dann die untergeordneten Verzeichnisse aktualisiert. Diese übermitteln ihrerseits ressortspezifische Daten zurück an das Meta-Directory.

Neben der Funktion des landesweiten Mitarbeiterverzeichnisses soll das Meta-Directory im Landesnetz weitere Infrastruktur-Aufgaben übernehmen. Dazu gehört beispielsweise die Speicherung von Zertifikaten zur Signaturprüfung und solchen zur Verschlüsselung. Wenn ein Single-Sign-On, d. h. die einmalige Anmeldung an allen IT-Systemen, landesweit zur Verfügung gestellt wird, werden in diesem Verzeichnis auch Logon-Daten gespeichert.

Damit das Meta-Directory seine Funktion erfüllen kann, müssen alle Beschäftigten der Landesverwaltung auf die Daten zugreifen können, die zur Kontaktaufnahme nötig sind. Für bestimmte Beschäftigtengruppen kann das aber – nicht so sehr aus Gründen des Datenschutzes, sondern aus der Fürsorgepflicht des Arbeitgebers heraus – unzulässig sein. Wenn ein Polizist oder ein Staatsanwalt beispielsweise im Bereich der Organisierten Kriminalität arbeitet, so kann es nötig sein, die Daten nicht im Verzeichnis zu speichern. Dies trifft auch für Beamtinnen und Beamte der Sondereinsatzkommandos, Bedienstete des LfV, des LKA und andere sicherheitsrelevanter Bereiche zu.

Um die Datenbestände im Meta-Directory möglichst aktuell zur Verfügung zu stellen, beabsichtigt die Landesregierung eine Schnittstelle zu schaffen, um die notwendigen Mitarbeiterdaten aus SAP/HR zu übertragen.

Aus den vorgenannten Gründen halte ich es für unbedingt notwendig, dass konzeptionell konkret geregelt wird, wie sichergestellt werden soll, dass nur Datensätze aus SAP/HR an das Meta-Directory übertragen werden, die auch abrufbar sein dürfen. Hierzu ist es notwendig, dass jede personalführende Dienststelle entscheidet, welche Datensätze übermittelt werden sollen. Ich habe mit der Landesregierung vereinbart, dass ein entsprechendes Konzept erstellt und mit mir abgestimmt wird, in dem geregelt wird, wer für die „Freigabe“ der Daten verantwortlich ist und wie ein entsprechendes Merkmal im System hinterlegt werden kann.

8.6 Hinterlegen von Passwörtern

Eine Dienststellenleitung darf ihre Beschäftigten nicht dazu verpflichten, dass sie ihre Passwörter sowohl bei der Dienststellenleitung als auch beim Systemadministrator hinterlegen.

Mitte des Jahres erhielt ich einen Hinweis, dass eine hessische Dienststelle ihre Beschäftigten angewiesen habe, alle Passwörter bei der Dienststellenleitung zu hinterlegen. Dies betreffe die Passwörter zum Novell-Netzwerk, zu Lotus Notes und für private Telefongespräche. Ihre Forderung habe die Dienststellenleitung damit begründet, dass sie die Passwörter für die Systemadministration benötige; daher seien die Beschäftigten zur Mitteilung ihres Passwortes verpflichtet. In der auf Grund dieses Hinweises eingeholten Stellungnahme der betroffenen Dienststelle wurde diese Behauptung abgestritten.

Daraufhin haben drei meiner Bediensteten die genannte Dienststelle unangemeldet überprüft. Sie konnten feststellen, dass der Hinweis den Tatsachen entsprach. Im Safe der Dienststelle waren sämtliche Passwörter aller Beschäftigten hinterlegt. Zugang zu diesem Safe hatten neben der Dienststellenleitung immerhin sieben weitere Beschäftigte.

Die Dienststellenleitung wurde darauf hingewiesen, dass eine Verpflichtung der Beschäftigten zur Passworthinterlegung rechtlich unzulässig sei. Diesen Grundsatz habe ich bereits in meinem 19. Tätigkeitsbericht unter Ziff. 15.5.5 dargelegt.

Im Zusammenhang mit der Dokumentation von Passworten gilt folgender Grundsatz:

Ein Benutzer muss sein Passwort gegenüber anderen Personen geheim halten. Es darf folglich nicht so dokumentiert werden, dass andere Personen einen Zugriff darauf haben.

Obwohl diese Forderung für alle Benutzer Gültigkeit hat, ist eine Ausnahme denkbar: Wenn beispielsweise alle Personen in einem Rechenzentrums-Betrieb ausfallen, die die Datenschutzsoftware administrieren, ist eine ordnungsgemäße Datenverarbeitung nicht mehr möglich. Es können dann keine Benutzerkennungen angelegt oder gesperrt werden und es ist beispielsweise auch nicht möglich, Berechtigungen zu vergeben. Man kann sich sogar Fälle vorstellen, in denen der Betrieb für lange Zeit eingestellt werden muss, da auf Fehler nicht mehr reagiert werden kann. Um diese Gefahr möglichst gering zu halten, wäre es denkbar, die Funktion der Administration vielen Benutzern zu geben. Dieser Ansatz ist jedoch verfehlt, da der Kreis der Benutzer mit dieser Funktion so klein wie möglich zu halten ist. Eine Möglichkeit wäre aber z. B. eine Benutzerkennung mit Passwort zu dokumentieren, die die Berechtigung zur Administration der Schutzsoftware besitzt.

Diese Lösung, zu bestimmten Funktionen für Notfälle eine Benutzerkennung mit Passwort zu dokumentieren, ist in jedem Fall restriktiv zu handhaben. Sie ist nur zu verantworten, wenn auf dem DV-System kein weiterer Benutzer (in einer anderen Funktion) vorhanden ist, der die nötigen Berechtigungen für die ausgefallene Funktion vergeben kann. Beispiele für solche Funktionen sind die ACF2-Administration (Access Control Facility) oder der Superuser auf UNIX-Systemen.

Wenn ein derartiger „Notuser" angelegt wird, müssen die Art der Aufbewahrung und die Nutzung sorgfältig geregelt werden. Dabei kann man sich an dem Umgang mit Betriebsgeheimnissen oder den Vorschriften für den Umgang mit VS-Sachen der Stufe VS-Vertraulich und höher orientieren. Wenn mit diesem „Notuser" gearbeitet wurde, ist umgehend eine dafür vorgesehene Instanz zu informieren. Ferner ist die benutzte „Notuser"-ID zu löschen und eine neue anzulegen.

Auch im Grundschutzhandbuch des BSI (Bundesamt für Sicherheit in der Informationstechnik) wird eine Hinterlegung von Passwörtern nur in wenigen Fällen für nötig erachtet. Dies kann erforderlich sein, wenn das System ein Zurücksetzen von Passwörtern durch die Administratoren nicht vorsieht. Diese Möglichkeit ist bei neuen Betriebssystemen und Anwendungen jedoch regelmäßig vorhanden.

Ich habe deshalb eine Vernichtung der im Safe gelagerten Unterlagen und ein Vernichtungsprotokoll gefordert. Dieser Aufforderung ist die Dienststelle umgehend nachgekommen. Des Weiteren wurde das Sicherheitskonzept der Dienststelle nach dem Besuch meiner Bediensteten neu strukturiert. So wurde beispielsweise bestimmt, dass, wenn eine Mitarbeiterin oder ein Mitarbeiter das Passwort des Lotus Notes Accounts nicht mehr wissen sollte, die gesamte ID gelöscht und die erstmalig vergebene ID mit dem Lotus Notes Standardpasswort neu in das System kopiert wird. Dieses Passwort ist von der Mitarbeiterin oder dem Mitarbeiter umgehend zu ändern. Es erfolgt keine Abfrage der Passwörter und auch keine zentrale Archivierung mehr.

Da die geprüfte Dienststelle die festgestellten Mängel umgehend behoben hat, habe ich von einer förmlichen Beanstandung abgesehen.

9. Bilanz

9.1 Auftragsdatenverarbeitung durch die HZD im Bereich der Justiz (31. Tätigkeitsbericht, Ziff. 5.1)

Im 31. Tätigkeitsbericht hatte mein Amtsvorgänger ausführlich über die Rahmenbedingungen des IT-Einsatzes im Justizbereich berichtet und das Konzept der Landesregierung zur Ausgestaltung der Datenverarbeitung bei den Gerichten und Staatsanwaltschaften dargestellt und bewertet. In diesem Zusammenhang wurde – auch von der Richterschaft – u. a. sehr intensiv die Frage diskutiert, inwieweit durch das vorgesehene Konzept, insbesondere durch die Beteiligung der HZD, die richterliche Unabhängigkeit tangiert sei. Eine Arbeitsgruppe aus Mitarbeitern des Justizministeriums und aus dem Hause des Datenschutzbeauftragten hat daraufhin ausführlich diese Fragen erörtert und Rahmenbedingungen, gerade auch für das Auftragsverhältnis zwischen der Justiz und der HZD niedergelegt.

Die damals von der Arbeitsgruppe auch unter Beteiligung von Mitarbeitern aus dem Hause des Datenschutzbeauftragten formulierten allgemeinen Aussagen zur Gewaltenteilung und richterlichen Unabhängigkeit sind selbstverständlich zutreffend.

Die konkrete Schlussfolgerung, die mein Amtsvorgänger daraus gezogen hat, – eine von der HZD betriebene Systembetreuung greife in den Kernbereich richterlicher Unabhängigkeit ein – halte ich nicht für zwingend und darüber hinausgehend für unrichtig. Solange Aufsichtsrechte der Justiz über die HZD gewährleistet sind, ist die organisatorische Zuordnung der HZD zur Exekutive verfassungsrechtlich unproblematisch.

Inzwischen hat es Änderungen der eingesetzten Technik gegeben. Als Server-Betriebssystem wird Windows 2003 genutzt und auf den Arbeitsplätzen wird Windows XP professional eingesetzt. Das bedingte einige technische Änderungen im Vergleich zur früheren Netzbeschreibung. Außerdem wurde den Wünschen der Anwender in einigen Fällen gefolgt. Die wesentlichen Unterschiede zum bisherigen Konzept sind:

- Es gibt die Möglichkeit auf der lokalen Festplatte Daten zu speichern.
  Die Datensicherung (Backup) muss durch den Anwender selbst vorgenommen werden. Über die Möglichkeiten und Konsequenzen muss jeder Anwender informiert werden.

- Es sind Softwareinstallationen im Rahmen der eingeräumten Zugriffsrechte zugelassen.
  Da bei Eröffnung dieser Möglichkeit die technischen Sicherheitsvorkehrungen nicht ausreichen, wurden organisatorische Maßnahmen ergriffen. Eine Dienstanweisung regelt, unter welchen Bedingungen Software installiert werden darf.

§ 19 IT-Dienstanweisung

1. *Unter dem Betriebssystem XP/WE 2003 dürfen die Anwender dienstlich veranlasste Software auf dem Arbeitsplatzrechner in eigener Verantwortung installieren.*

2. *Nicht zulässig ist insbesondere die Installation von Software, die einer Ermittlung von Zugangsdaten (z. B. Passwörter) oder einem unbefugten Zugriff auf Datenbestände dient. Programme, die zu einer Veränderung der vorgegebenen Sicherheitseinstellungen genutzt werden können, dürfen ebenfalls nicht installiert werden.*

- USB-Schnittstellen sind verfügbar.
  Diese Möglichkeit ist kritisch zu bewerten (siehe auch 32. Tätigkeitsbericht, Ziff. 18.4). Bis eine praktikable Lösung vorhanden ist, bleibt die Möglichkeit auf BIOS-Ebene blockiert. Die HZD hat mittlerweile Software getestet, mit deren Hilfe USB- und andere Schnittstellen kontrolliert werden können. Die Software erfüllt die gestellten Anforderungen. Die Entscheidung des Ministeriums über den Einsatz steht noch aus.

- Der Remote-Zugriff wird mit den Windows XP-eigenen Funktionen vorgenommen.
  Das stellt keine funktionelle Änderung zum bisherigen Stand dar.

- Administratoren können eine Besitzübernahme rückgängig machen.
  Damit kann sich der Administrator Zugriffsrechte zu einer Datei verschaffen und anschließend den alten Zustand wieder herstellen. Es entfällt eine wichtige Schutzfunktion bei den persönlichen Dateien und anderen sensiblen Daten im Vergleich zum bisherigen Zustand. Um dieser Verschlechterung entgegenzuwirken, wurden mehrere Maßnahmen ergriffen, die in der Netzbeschreibung genau dargelegt sind:

  Zum Schutz persönlicher Dateien können diese mit den Windows-eigenen Verschlüsselungsfunktionen (MS-EFS) verschlüsselt werden. Es wird erläutert auf welche Punkte zu achten ist, um eine Kenntnisnahme durch Administratoren zu verhindern.

In der Beschreibung für den Systemrevisor wird im Detail erläutert, wie Besitzübernahmen zu erkennen sind.

Die Mitarbeiter erhalten eine Anleitung, um die Berechtigungen ihres persönlichen Ordners zu prüfen.

Mit den vorgesehenen Sicherheitsmaßnahmen ist eine angemessene Datensicherheit erreichbar. Ich habe daher keine Bedenken gegen die geplante Umstellung.

9.2 Vermeidung von Doppelanfragen polizeilicher Datenbestände bei Einbürgerungen und bei ausländerrechtlichen Entscheidungen (31. Tätigkeitsbericht, Ziff. 9.1)

Im 31. Tätigkeitsbericht Ziff. 9.1 hatte ich kritisiert, dass es im Zusammenhang mit Einbürgerungen Fallkonstellationen gibt, in denen polizeiliche Datenbestände zum selben Zweck mehrere Male von unterschiedlichen Polizeibehörden abgefragt und ausgewertet werden. Dabei hatte ich nicht die Datenverwendung als solche in Frage gestellt, lediglich die Redundanz war – abgesehen vom überflüssigen Verwaltungsaufwand – auch aus datenschutzrechtlicher Sicht „nicht erforderlich“ und damit problematisch. Eine ähnliche Thematik ergab sich bei der Einholung von Auskünften der Ausländerbehörden, einmal bei den örtlichen Polizeibehörden, und ein weiteres Mal beim Hessischen Landeskriminalamt vor der Erteilung von Aufenthaltstiteln in bestimmten Fällen.

Ich hatte das Hessische Ministerium des Innern und für Sport gebeten, eine Koordination der beteiligten Stellen herbeizuführen, um eine Lösung zu finden, die den datenschutzrechtlichen Belangen der Betroffenen besser Rechnung trägt.

Das Hessische Ministerium des Innern und für Sport – Landespolizeipräsidium – hat nun mit einem Erlass die Ausländerbehörden gebeten, ihre Ersuchen um Personenüberprüfungen künftig entgegen der bisherigen Regelung nicht mehr an die Polizeipräsidien, sondern für den polizeilichen Bereich nur noch an das Hessische Landeskriminalamt (HLKA) zu richten. Bei den Polizeipräsidien unmittelbar eingehende Ersuchen der Ausländerbehörden von Personenüberprüfungen sind an das HLKA weiterzuleiten. Dieses Verfahren ist nunmehr auch bei Anspruchs- und Ermessungseinbürgerungen anzuwenden; die Verwaltungsvorschrift über das Verfahren wird in Kürze angepasst. Damit ist dem datenschutzrechtlichen Aspekt Rechnung getragen.

9.3 Rasterfahndung (32. Tätigkeitsbericht, Ziff. 5.1)

Ich hatte im letzten Jahr ausführlich über die Durchführung der Rasterfahndungsmaßnahmen im Anschluss an die Ereignisse des 11. Septembers 2001 berichtet. Auch in diesem Jahr habe ich die Abarbeitung der so genannten Verdachtsfälle weiter begleitet.

Sobald die Einzelfallbearbeitung durch das zuständige Polizeipräsidium zu einer Negativbewertung des Trefferfalles geführt hat, wurde die jeweilige Akte manuell vernichtet, der zugehörige Datensatz wurde aus der angelegten Crime-Datenbank gelöscht und die Betroffenen gemäß § 26 Abs. 5 HSOG benachrichtigt.

§ 26 HSOG

(3) Ist der Zweck der Maßnahme erreicht oder zeigt sich, dass er nicht erreicht werden kann, sind die übermittelten und im Zusammenhang mit der Maßnahme zusätzlich angefallenen Daten auf dem Datenträger zu löschen und die Unterlagen, soweit sie nicht für ein mit dem Sachverhalt zusammenhängendes Verfahren erforderlich sind, unverzüglich zu vernichten. Über die getroffenen Maßnahmen ist eine Niederschrift anzufertigen. Diese Niederschrift ist gesondert aufzubewahren, durch technische und organisatorische Maßnahmen zu sichern und am Ende des Kalenderjahres, das dem Jahr der Vernichtung der Unterlagen nach Satz 1 folgt, zu vernichten.

(5) Personen, gegen die nach Abschluss einer Maßnahme nach Abs. 1 weitere Maßnahmen durchgeführt werden, sind hierüber durch die Polizei zu unterrichten, sobald dies ohne Gefährdung des Zweckes der weiteren Datennutzung erfolgen kann. § 15 Abs. 7 HSOG gilt entsprechend.

In keinem Fall ist mir eine Reaktion eines Betroffenen auf diese Benachrichtigung bekannt geworden. Etwa zwei Drittel der Fälle waren laut einer Mitteilung des HLKA schon zu Jahresbeginn in dieser Weise erledigt. Anfang Oktober dieses Jahres waren noch einige wenige Fälle nicht abgeschlossen.

Alle Vorgänge, die in einer Polizeidienststelle bearbeitet werden, werden im Vorgangsbearbeitungssystem ComVor erfasst. Dieses ist durch ein – im Prinzip landesweit für alle Dienststellen der Polizei zugängliches – Index-System erschlossen. Damit kann jeder berechtigte Nutzer sehen, ob eine bestimmte Person schon in der Rolle „Angeschuldigter“ dem System bekannt ist. Dann kann er die Personalien übernehmen ohne sie neu zu erfassen, ggf. auch mit der für den schon vorhandenen Vorgang befassten Dienststelle/Sachbearbeiter bzw. Kollegen Kontakt aufnehmen, um notwendige Informationen auszutauschen, Zusammenarbeit zu organisieren usw. Ausgeschlossen vom landesweiten Zugriff sind nur die Datensätze, die mit einem entsprechenden Schutz gekennzeichnet sind. Dann bekommen nur bestimmte Organisationseinheiten diese angezeigt.

In der Datei enthalten sind die Personalien, die zuständige Dienststelle mit Ansprechpartner sowie der Grund/das Delikt, das dem Verfahren zugrunde liegt. Ist das Verfahren abgeschlossen erfolgt eine Kennzeichnung: „intern abgeschlossen“ (aus welchem Grund auch immer) oder „abverfügt“ (an die Staatsanwaltschaft oder an eine andere zuständige Behörde etwa die Ordnungswidrigkeitenbehörde oder eine außerhessische Polizeidienststelle oder Staatsanwaltschaft). Diese Speicherung erfolgt, damit für einen bestimmten Zeitraum noch nachvollzogen werden kann, dass es ein Verwaltungsverfahren gab und was daraus geworden ist. Deshalb führt die Einstellung/Beendigung des Verfahrens auch nicht zwangsläufig zur Löschung aller Daten, da weitere Nachfragen nicht ausgeschlossen und eine Dokumentation des „rechtmäßigen Vorgehens“ für eine bestimmte Zeit notwendig und sinnvoll ist. Die Prüffrist für die Vorgangsbearbeitung zur Entscheidung über die Löschung beträgt drei Jahre.

Somit waren zunächst auch die Personen, die darüber benachrichtigt wurden, dass alle Unterlagen vernichtet sind, trotzdem noch bei der Polizei gespeichert und als Betroffene der Rasterfahndung erkennbar. Damit haftete ihnen ein Makel an, der mit den Vorgaben des § 26 HSOG nicht zu vereinbaren war. Insoweit spielt es auch keine Rolle, dass diese Datei nicht zu

Auskunftszwecken Verwendung finden darf. Auch der Polizei bzw. allen Beamten selbst dürfen diese Informationen nicht mehr vorliegen.

Grundsätzlich ist eine Einzellöschung im ComVor-Index auch möglich, etwa wenn der zuständige Sachbearbeiter eine ursprüngliche Eingabe als offensichtliche Fehlerfassung erkennt. Deshalb hatte ich das LKA gebeten in diesen Fällen von dem Grundsatz der weiteren Speicherung aller Fälle ausnahmsweise Abstand zu nehmen und diese Datensätze zu löschen, um somit den Anforderungen des § 26 HSOG – Löschung aller Unterlagen – nachzukommen.

Im Lauf des Jahres ist das LKA diesem Begehren gefolgt und hat – ausnahmsweise – wegen der besonderen Brisanz der Rasterfahndung auch die Daten im ComVor-Index gelöscht.

9.4 Datensicherheitsmaßnahmen beim Landratsamt Marburg-Biedenkopf (32. Tätigkeitsbericht, Ziff. 6.2)

Über Mängel im Hinblick auf die Datensicherheit beim Landratsamt Marburg-Biedenkopf hatte ich in meinem letzten Bericht (Tätigkeitsbericht Nr. 32 Ziff. 6.2) informiert. Im Jahr 2003 hatte ich offene Schränke mit Bewerbungsunterlagen und für jedermann frei zugängliche Wohngeldakten auf den Fluren des Landratsamtes im Zuge einer Prüfung in anderer Angelegenheit feststellen und beanstanden müssen.

Das Landratsamt hatte zugesagt, Abhilfe zu schaffen. Bei einem unangemeldeten Kontrollbesuch konnte ich feststellen, dass die Schränke mit den Personalunterlagen nicht mehr auf den Fluren abgestellt sind. Sämtliche Stahlschränke, die sich noch auf den Fluren befanden, waren abgeschlossen. Damit sind die Mängel behoben.

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

10.1 Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 13. Februar 2004: Übermittlung von Flugpassagierdaten an die US-Behörden

Die Datenschutzbeauftragten des Bundes und der Länder bestärken die Bundesregierung darin, sich für Verbesserungen des Datenschutzes bei der Übermittlung von Flugpassagierdaten an die Zoll- und Sicherheitsbehörden der USA einzusetzen.

Durch einseitigen Rechtsakt haben die USA die Fluggesellschaften, die ihr Land anfliegen, unter Androhung teilweise empfindlicher Strafen verpflichtet, den US-Zoll- und Sicherheitsbehörden den Zugang zu ihren Reservierungsdatenbanken zu eröffnen, um anhand der darin enthaltenen Informationen über die Fluggäste mögliche terroristische oder kriminelle Aktivitäten frühzeitig zu erkennen. In den Reservierungsdatenbanken halten die an der Reisedurchführung beteiligten Stellen alle Informationen fest, die sie benötigen, um die Flugreise abzuwickeln. Es werden z. B. Name, Reiseverlauf, Buchungsstelle, Art der Bezahlung, bei Zahlung mit Kreditkarte deren Nummer, Sitzplatz, Essenswünsche, notwendige Reisevorkehrung wegen einer Erkrankung eines Fluggastes, Hotel- und Mietwagenreservierungen im Buchungssystem gespeichert. Teilweise sind die gespeicherten Daten sensitiv, weil sie Rückschlüsse auf die Gesundheit einzelner Fluggäste oder religiöse oder politische Anschauungen ermöglichen.

Die US-Zollbehörden wollen alle Reservierungsdaten mindestens 3 1/2 Jahre speichern ungeachtet der Tatsache, ob gegen eine Person ein Verdachtsmoment vorlag oder nicht. Passagierdaten, die im Einzelfall überprüft wurden, sollen zudem weitere 8 Jahre gespeichert werden.

Die Datenschutzbeauftragten verkennen nicht, dass nach den Ereignissen des 11. Septembers 2001 ein erhöhtes Bedürfnis nach Sicherheit im Flugverkehr offensichtlich ist. Sie verschließen sich deshalb keineswegs Forderungen, die auf eine sichere Identifikation der Fluggäste zielen. Dennoch muss festgestellt werden, dass die Forderungen der USA weit über das hinausgehen, was erforderlich ist. Da die Reservierungsdatenbanken nicht für Sicherheitszwecke sondern zur Durchführung der Flugreisen angelegt werden, enthalten sie auch eine Vielzahl von Daten der Reisenden, die für eine Sicherheitsüberprüfung der Passagiere irrelevant sind.

Mit dem Zugriff ist wegen der teilweise hohen Sensibilität der Daten ein tiefer Eingriff in die Persönlichkeitsrechte der Betroffenen verbunden. Besonders hervorzuheben ist in diesem Zusammenhang, dass die US-Behörden hier aufgrund US-amerikanischen Rechts auf Datenbanken außerhalb ihres Hoheitsbereichs zugreifen. Die betroffenen Personen werden gegenüber dem Zugriff auf ihre Daten durch eine ausländische Stelle in ihren Datenschutzrechten weitgehend schutzlos gelassen. Ein vergleichbares Ansinnen deutscher Sicherheitsbehörden wäre schwerlich mit unserer Verfassung vereinbar.

Die Problematik kann sich weiter verschärfen, wenn die USA die Passagierdaten zukünftig auch im CAPPS II-System einsetzen wollen. Dieses System ermöglicht sowohl einen automatisierten Abgleich mit Fahndungslisten als auch mit Informa-

tionen aus dem privaten Sektor. Insbesondere sollen Kreditkarten- und Adressdaten mit Informationen aus der Kreditwirtschaft abgeglichen werden.

Die Europäische Kommission bemüht sich seit über einem Jahr in Verhandlungen darum, den Datenzugang der US-Behörden auf ein angemessenes Maß zu beschränken. Leider führten die Verhandlungen nur in Teilbereichen zum Erfolg. Die erzielten Ergebnisse in ihrer Gesamtheit gewähren den Reisenden keinen angemessenen Schutz ihrer Persönlichkeitsrechte. Dies hat die Gruppe nach Art. 29 der europäischen Datenschutzrichtlinie (EG-DSRL) in ihrer Stellungnahme vom 29. Januar 2004 deutlich herausgearbeitet:
http://www.europa.eu.int/comm/internal_market/privacy/workingroup/wp2004/wpdocs04_de.htm.

Die darin vertretenen Positionen werden von den Datenschutzbeauftragten ausdrücklich unterstützt. Dennoch beabsichtigt die Europäische Kommission das Ergebnis ihrer Verhandlungen als einen angemessenen Datenschutzstandard förmlich anzuerkennen. Die Datenschutzbeauftragten appellieren an die Bundesregierung, sich gegen diese Entscheidung der Kommission zu wenden. Wenn die Kommission diesen unbefriedigenden Verhandlungsergebnissen ein angemessenes Datenschutzniveau attestiert, setzt sie damit Maßstäbe sowohl für die Auslegung der EU-Datenschutzrichtlinie als auch für Verhandlungen mit anderen Staaten über die Anerkennung des dortigen Datenschutzniveaus. Die Bundesregierung sollte sich demgegenüber für eine Lösung einsetzen, die Sicherheitsaspekte und den Schutz der Persönlichkeitsrechte in ein angemessenes Verhältnis setzt. Insbesondere sind die Informationen ausdrücklich zu benennen, die für die Passagieridentifikation benötigt werden. Diese Daten können zu einem angemessenen Zeitpunkt vor dem Abflug bereitgestellt werden. Ein unmittelbarer pauschaler Zugriff auf europäische Datenbanken, wie er zurzeit praktiziert wird, muss ausgeschlossen werden.

10.2 Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 2004: Personennummern

Das Bundesverfassungsgericht hat schon in seinem „Volkszählungsurteil“ aus dem Jahre 1983 besonders betont, dass ein Personenkennzeichen nicht verfassungsgemäß ist. Deshalb gibt die Einführung von einheitlichen Personennummern z. B. im Steuerbereich oder auch im Arbeits-, Gesundheits- und Sozialbereich Anlass zu grundsätzlicher Kritik. Der Staat darf seine Bürgerinnen und Bürger nicht zur Nummer abstempeln. Durch die technische Entwicklung sind vorhandene Dateien leicht miteinander zu verknüpfen und könnten zu einer vom Bundesverfassungsgericht strikt abgelehnten allgemeinen Personennummer führen.

Die Konferenz appelliert an die Gesetzgeber, solche Personennummern zu vermeiden. Soweit jedoch im Einzelfall derartige Nummern unerlässlich sind, muss der Gesetzgeber strenge Zweckbindungen und Verwendungsverbote vorsehen.

10.3 Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 2004: Entscheidungen des Bundesverfassungsgerichts vom 3. März 2004 zum Großen Lauschangriff und zur präventiven Telekommunikationsüberwachung

Das Urteil des Bundesverfassungsgerichts vom 3. März 2004 zum Großen Lauschangriff ist ein wichtiger Orientierungspunkt in der rechts- und sicherheitspolitischen Diskussion um den sachgerechten Ausgleich zwischen dem staatlichen Auftrag zur Verfolgung und Verhütung von Straftaten einerseits und dem Schutz der grundgesetzlich garantierten Bürgerrechte andererseits. Das Urteil bekräftigt den hohen Rang des Grundrechts auf Unverletzlichkeit der Wohnung und des Rechts auf informationelle Selbstbestimmung. Das Gericht betont, dass der absolut geschützte Kernbereich privater Lebensgestaltung nicht zugunsten der Strafverfolgung eingeschränkt werden darf. Damit darf es keine Strafverfolgung um jeden grundrechtlichen Preis geben.

Die Ausführungen des Bundesverfassungsgerichts sind nicht nur für die Vorschriften über die akustische Wohnraumüberwachung in der Strafprozessordnung von Bedeutung. Auf den Prüfstand müssen jetzt auch andere Eingriffsbefugnisse, wie etwa die Telekommunikationsüberwachung und andere Formen der verdeckten Datenerhebung mit zwangsläufigen Berührungen zum Bereich privater Lebensgestaltung gestellt werden, wie etwa die längerfristige Observation, der verdeckte Einsatz technischer Mittel, der Einsatz von Vertrauenspersonen oder von verdeckten Ermittlern. Hiervon betroffen sind nicht nur Bundesgesetze, sondern beispielsweise auch die Polizei- und Verfassungsschutzgesetze der Länder.

Insbesondere angesichts zunehmender Bestrebungen, auch die Telefonüberwachung für präventive Zwecke in Polizeigesetzen zuzulassen, ist darauf hinzuweisen, dass das Bundesverfassungsgericht in einem Beschluss zum Außenwirtschaftsgesetz ebenfalls am 3. März 2004 der präventiven Überwachung des Postverkehrs und der Telekommunikation klare Grenzen gesetzt hat.

Die Datenschutzbeauftragten fordern die Gesetzgeber des Bundes und der Länder deshalb auf, zügig die einschlägigen Vorschriften nach den Maßstäben der verfassungsgerichtlichen Entscheidungen vom 3. März 2004 zu korrigieren. Die mit der praktischen Durchführung der gesetzlichen Eingriffsbefugnisse befassten Gerichte, Staatsanwaltschaften und die Polizeien sind aufgerufen, die Vorgaben des Gerichts schon jetzt zu beachten.

10.4 Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 2004: Automatische Kfz-Kennzeichenerfassung durch die Polizei

Die Datenschutzbeauftragten des Bundes und der Länder betrachten einen anlassfreien und lageunabhängigen Einsatz von automatischen Kfz-Kennzeichen-Lesesystemen im Straßenverkehr mit Sorge, weil sich diese Maßnahmen zu einem weiteren Schritt zur Überwachung aller Bürgerinnen und Bürger entwickeln können.

Es ist zu befürchten, dass mit dem Einsatz der automatischen Kfz-Kennzeichenerfassung eine neue Infrastruktur geschaffen wird, die künftig noch weit tiefergehende Eingriffe in das Persönlichkeitsrecht ermöglicht.

Die Nutzung dieser neuen Technik hätte zur Folge, dass die Kfz-Kennzeichen aller an den Erfassungsgeräten vorbeifahrenden Verkehrsteilnehmerinnen und -teilnehmer erfasst und mit polizeilichen Fahndungsdateien abgeglichen würden. Schon der mit der Feststellung gesuchter Fahrzeuge verbundene Abgleich würde zu einem neuen Eingriff in das Recht auf informationelle Selbstbestimmung von Personen führen, die weit überwiegend keinen Anlass für eine polizeiliche Verarbeitung ihrer personenbezogenen Daten gegeben haben.

Auf jeden Fall muss ausgeschlossen werden, dass Daten über unverdächtige Personen gespeichert werden und dass ein allgemeiner Datenabgleich mit polizeilichen Informationssystemen durchgeführt wird.

Die Datenschutzbeauftragten weisen darauf hin, dass schon mehrere Länder eine Kfz-Kennzeichen-Erfassung ablehnen.

10.5 Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 2004: Radio Frequency Identification (RFID)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder schließt sich voll inhaltlich der folgenden Entschließung der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre an:

Entschließung zu Radio Frequency Identification vom 20. November 2003 (Übersetzung)

Radio Frequency Identification (RFID) Technologie wird zunehmend für eine Reihe unterschiedlicher Zwecke eingesetzt. Während es Situationen gibt, in denen diese Technologie positive und günstige Auswirkungen hat, sind auch negative Folgen für die Privatsphäre möglich. RFID-Etiketten werden bisher vorwiegend zur Identifikation und Organisation von Gegenständen (Produkten), zur Kontrolle der Logistik oder zum Schutz der Authentizität einer Produktmarke (Warenzeichen) verwendet; sie können aber auch mit personenbezogenen Informationen wie Kreditkarten-Daten verknüpft werden und auch zur Erhebung solcher Informationen oder zur Lokalisierung oder Profilbildung über Personen benutzt werden, die Gegenstände mit RFID-Etiketten besitzen. Diese Technologie würde die unbemerkte Verfolgung und das Aufspüren von Individuen ebenso wie die Verknüpfung erhobener Daten mit bestehenden Datenbanken ermöglichen.

Die Konferenz hebt die Notwendigkeit hervor, Datenschutzprinzipien zu berücksichtigen, wenn RFID-Etiketten verknüpft mit personenbezogenen Daten eingeführt werden sollen. Alle Grundsätze des Datenschutzrechts müssen beim Design, der Einführung und der Verwendung von RFID-Technologie berücksichtigt werden. Insbesondere

a) sollte jeder Datenverarbeiter vor der Einführung von RFID-Etiketten, die mit personenbezogenen Daten verknüpfbar sind oder die zur Bildung von Konsumprofilen führen zunächst Alternativen in Betracht ziehen, die das gleiche Ziel ohne die Erhebung von personenbezogenen Informationen oder die Bildung von Kundenprofilen erreichen;

b) wenn der Datenverarbeiter darlegen kann, dass personenbezogene Daten unverzichtbar sind, müssen diese offen und transparent erhoben werden;

c) dürfen personenbezogene Daten nur für den speziellen Zweck verwendet werden, für den sie ursprünglich erhoben wurden und sie dürfen nur solange aufbewahrt werden, wie es zu Erreichung dieses Zwecks erforderlich ist und

d) soweit RFID-Etiketten im Besitz von Personen sind, sollten diese die Möglichkeit zur Löschung der gespeicherten Daten oder zur Deaktivierung oder Zerstörung der Etiketten haben.

Diese Grundsätze sollten bei der Gestaltung und bei der Verwendung von Produkten mit RFID berücksichtigt werden.

Das Auslesen und die Aktivierung von RFID-Etiketten aus der Ferne ohne vernünftige Gelegenheit für den Besitzer des etikettierten Gegenstandes, diesen Vorgang zu beeinflussen, würde zusätzliche Datenschutzrisiken auslösen.

Die Konferenz und die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation wird die technischen Entwicklungen in diesem Bereich genau und detaillierter verfolgen, um die Achtung des Datenschutzes und der Privatsphäre in einer Umgebung allgegenwärtiger Datenverarbeitung sicherzustellen.

10.6 Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 2004: Einführung eines Forschungsgeheimnisses für medizinische Daten

In vielen Bereichen der Forschung werden sensible medizinische Daten der Bürgerinnen und Bürger verarbeitet. Dabei ist häufig eine Verarbeitung auch personenbezogener Daten erforderlich. Diese Daten können mit Einwilligung der Betroffenen insbesondere von Ärztinnen und Ärzten, aber auch von Angehörigen anderer Heilberufe an Forscher und Forscherinnen übermittelt werden. Dies ist im Interesse der Forschung zwar grundsätzlich zu begrüßen. Mit der Übermittlung verlieren die Daten aber regelmäßig den strafrechtlichen Schutz vor Offenbarung und den Beschlagnahmeschutz im Strafverfahren. Auch ein Zeugnisverweigerungsrecht bezüglich dieser Daten steht den Forschenden – anders als insbesondere den behandelnden Ärztinnen und Ärzten – nicht zu. Zum Schutze der Forschung, vor allem aber zum Schutz der durch die Datenübermittlung und -verarbeitung Betroffenen, sollte vom Gesetzgeber deshalb sichergestellt werden, dass die bei den übermittelnden Stellen geschützten personenbezogenen medizinischen Daten auch nach ihrer Übermittlung zu Forschungszwecken den gleichen Schutz genießen.

Die Datenschutzbeauftragten fordern daher den Bundesgesetzgeber auf,

- in § 203 StGB die unbefugte Offenbarung von personenbezogenen medizinischen Forschungsdaten unter Strafe zu stellen,

- in §§ 53, 53a StPO für personenbezogene medizinische Daten ein Zeugnisverweigerungsrecht für Forscher und ihre Berufshelfer zu schaffen,

- in § 97 StPO ein Verbot der Beschlagnahme personenbezogener medizinischer Forschungsdaten zu schaffen.

Die Datenschutzbeauftragten sehen in diesen Vorschlägen einen ersten Schritt zu einer generellen Regelung des besonderen Schutzes personenbezogener Daten in der Forschung.

10.7 Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 28./29. Oktober 2004: Gesetzentwurf der Bundesregierung zur Neuregelung der akustischen Wohnraumüberwachung

Die Bundesregierung hat einen Gesetzentwurf zur Neuregelung der akustischen Wohnraumüberwachung vorgelegt. Sie setzt damit in großen Teilen das Urteil des Bundesverfassungsgerichts vom 3. März 2004 um, wonach die Vorschriften der Strafprozessordnung zum „Großen Lauschangriff“ in wesentlichen Teilen verfassungswidrig sind. Allerdings sind zentrale Punkte, wie die Begriffsbestimmung des „unantastbaren Kernbereichs der privaten Lebensgestaltung“ und die Bestimmung des Kreises der Menschen „des persönlichen Vertrauens“ offen geblieben.

Ungeachtet dessen drohen im weiteren Verlauf des Gesetzgebungsverfahrens schwerwiegende Verschlechterungen: So wird diskutiert, die Vorgaben des Bundesverfassungsgerichts dadurch zu unterlaufen, dass auch bei erkannten Eingriffen in den absolut geschützten Kernbereich die technische Aufzeichnung fortgesetzt wird. Dies steht in eklatantem Widerspruch zur eindeutigen Vorgabe des Bundesverfassungsgerichts, die Aufzeichnung in derartigen Fällen sofort zu beenden. Darüber hinaus wird versucht, den Anwendungsbereich der akustischen Wohnraumüberwachung dadurch auszuweiten, dass auch nicht strafbare Vorbereitungshandlungen einbezogen werden. Auch dies widerspricht den verfassungsgerichtlichen Vorgaben und verwischt die Grenzen zwischen Strafverfolgung und Gefahrenabwehr.

Die Datenschutzbeauftragten bekräftigen im Übrigen ihre Forderung, dass es im Hinblick auf die Heimlichkeit der Überwachung und ihrer zwangsläufigen Berührung mit dem Kernbereich privater Lebensgestaltung erforderlich ist, alle Formen der verdeckten Datenerhebung an den Maßstäben der verfassungsgerichtlichen Entscheidung vom 3. März 2004 zu messen und auszurichten sowie die einschlägigen gesetzlichen Befugnisregelungen des Bundes und der Länder auf den Prüfstand zu stellen und gegebenenfalls neu zu fassen. Dies gilt etwa für die präventive Telekommunikationsüberwachung, die längerfristige Observation, den verdeckten Einsatz technischer Mittel, den Einsatz nachrichtendienstlicher Mittel und von verdeckten Ermittlern. Dabei sind insbesondere Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung und zum Schutz vertraulicher Kommunikation mit engsten Familienangehörigen und anderen engsten Vertrauten sowie mit Personen, die einem Berufsgeheimnis unterliegen, zur Einhaltung der Zweckbindung bei Weiterverwendung der durch die Eingriffsmaßnahmen erlangten Daten, zu der dazu erforderlichen Kennzeichnungspflicht und zur Benachrichtigung aller von der Eingriffsmaßnahme Betroffenen sowie zur detaillierten Ausgestaltung von Berichtspflichten gegenüber den Parlamenten vorzusehen.

10.8 Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 28./29. Oktober 2004: Datensparsamkeit bei der Verwaltungsmodernisierung

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen die Bemühungen, Dienstleistungen der öffentlichen Verwaltung bürgernäher und effizienter zu erbringen. Sie fordern, dass im Zug von Maßnahmen der Verwaltungsreform die sich dadurch bietenden Möglichkeiten genutzt werden, um das Datenschutzniveau zu verbessern. Verwaltungsvereinfachung muss auch dazu genutzt werden, weniger personenbezogene Daten zu verarbeiten. Künftig müssen Verfahren und Datenflüsse wesentlich besser überschaubar und nachvollziehbar sein. Besonders sollen die Möglichkeiten der Technik genutzt werden, Risiken zu minimieren, die mit der Zentralisierung von Datenbeständen verbunden sind.

Werden Rechtsvorschriften, etwa im Steuerrecht oder im Arbeits- und Sozialrecht und hier insbesondere bei Änderungen in den Systemen der sozialen Sicherung, mit dem Ziel der Verwaltungsvereinfachung erlassen, sind die Auswirkungen auf den Datenschutz frühzeitig zu prüfen. Im Ergebnis müssen die Normen den gesetzlich verankerten Grundsatz der Datenvermeidung umsetzen und somit das Recht auf informationelle Selbstbestimmung gewährleisten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deswegen, bei Vorschlägen zur Verwaltungsvereinfachung und darüber hinaus bei allen Regelungsvorhaben darauf zu achten, dass das damit verbundene Potential an Datensparsamkeit und Transparenz ausgeschöpft wird.

Hierzu ist eine Folgenabschätzung auf mögliche Beeinträchtigungen der informationellen Selbstbestimmung vorzunehmen. Die Ergebnisse sind in geeigneter Form zu dokumentieren.

10.9 Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 28./29. Oktober 2004: Gravierende Datenschutzmängel bei Hartz IV

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass es bei der praktischen Umsetzung der Zusammenlegung von Arbeitslosen- und Sozialhilfe zu erheblichen datenschutzrechtlichen Mängeln gekommen ist. Diese bestehen sowohl bei den Verfahren der Datenerhebung durch die verwendeten Antragsformulare als auch bei der Leistungsberechnungs-Software (A2LL). Die Datenschutzdefizite wären vermeidbar gewesen, wenn datenschutzrechtliche Belange von Anfang an angemessen berücksichtigt und umgesetzt worden wären.

Zwar stellt die Bundesagentur für Arbeit (BA) seit dem 20. September 2004 sog. "Ausfüllhinweise zum Antragsvordruck Arbeitslosengeld II" zur Verfügung, in denen viele Bedenken der Datenschutzbeauftragten aufgegriffen werden. Allerdings ist hierbei zu berücksichtigen, dass durch die Ausfüllhinweise nicht mehr alle antragstellenden Personen erreicht werden können. Umso wichtiger ist es, dass die örtlich zuständigen Leistungsträger die verbindlichen Ausfüllhinweise beachten und die antragstellenden Personen, die ihren Antrag noch nicht eingereicht haben, vor der Abgabe auf diese hingewiesen werden. Personen, die ihren Antrag früher gestellt haben, dürfen nicht benachteiligt werden. Überschussinformationen, die vorhanden sind und weiterhin erhoben werden, sind zu löschen.

Darüber hinaus will die BA die in den Antragsformularen nachgewiesenen Datenschutzmängel in vielen Bereichen in der nächsten Druckauflage korrigieren und für das laufende Erhebungsverfahren zur Verfügung stellen. Gleichwohl ist zu befürchten, dass die Formulare nicht das erforderliche Datenschutzniveau erreichen.

Hinsichtlich der Software A2LL bestehen immer noch wesentliche Datenschutzmängel, die zu erheblichen Sicherheitsrisiken führen. Insbesondere besteht für die Sachbearbeitung ein uneingeschränkter bundesweiter Zugriff auf alle Daten, die im Rahmen von A2LL erfasst wurden, auch soweit diese Daten für die Sachbearbeitung nicht erforderlich sind. Dieser Mangel wird dadurch verschärft, dass noch nicht einmal eine Protokollierung der lesenden Zugriffe erfolgt und damit missbräuchliche Zugriffe nicht verfolgt werden können. Das Verfahren muss über ein klar definiertes Zugriffsberechtigungskonzept verfügen. Die Beschäftigten der zuständigen Leistungsträger dürfen nur den zur Aufgabenerfüllung erforderlichen Zugriff auf die Sozialdaten haben.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die BA auf, die notwendigen Schritte unverzüglich einzuleiten und nähere Auskunft über den Stand des Verfahrens zu erteilen.

10.10 Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 26. November 2004: Staatliche Kontenkontrolle muss auf den Prüfstand

Das „Gesetz zur Förderung der Steuerehrlichkeit“ vom 23. Dezember 2003 (BGBl. I 2003, S. 2928) enthält mit den §§ 93 Abs. 7, 8 und 93b der Abgabenordnung Regelungen, die das Grundrecht auf informationelle Selbstbestimmung aller Bürgerinnen und Bürger im Bereich ihrer finanziellen und wirtschaftlichen Betätigung in erheblichem Maße beschränken. Die neuen Regelungen treten am 1. April 2005 in Kraft. Sie sehen vor, dass nicht nur Finanzbehörden, sondern auch eine unbestimmte Vielzahl weiterer Behörden Zugriff auf Bankdaten erhalten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, diese Regelungen mit dem Ziel zu überarbeiten, das Recht auf informationelle Selbstbestimmung zu gewährleisten. Insbesondere das verfassungsrechtliche Gebot der Normenklarheit und die Transparenz des Verfahrens müssen beachtet werden.

Die Neuregelung erlaubt einen Zugriff auf Bankdaten, die von den Kreditinstituten bereits seit April 2003 zur Aufdeckung illegaler Finanztransaktionen vor allem zur Terrorismusbekämpfung nach § 24c des Kreditwesengesetzes vorgehalten werden müssen. Dabei handelt es sich um die Kontenstammdaten der Bankkundinnen und Bankkunden und sonstigen Verfügungsberechtigten, wie z. B. Name, Geburtsdatum, Kontonummern. Mit der neuen Regelung einher geht bereits eine von den Datenschutzbeauftragten des Bundes und der Länder im Gesetzgebungsverfahren Ende 2003 kritisierte Zweckänderung der Verwendung der von den Kreditinstituten vorzuhaltenden Daten.
Nunmehr sollen neben Finanzbehörden auch andere Behörden, z. B. die zahlreichen Stellen der Sozialleistungsträger, Auskunft erhalten, wenn die anfragende Behörde ein Gesetz anwendet, das „an Begriffe des Einkommensteuergesetzes“ anknüpft und eigene Ermittlungen dieser Behörde ihrer Versicherung nach nicht zum Ziel geführt haben oder keinen Erfolg versprechen. Welche Behörden dies sein sollen, geht aus dem Gesetz nicht eindeutig hervor. Da das Einkommensteuerrecht eine Vielzahl von „Begriffen“ verwendet (neben den Begriffen „Einkommen“ und „Einkünfte“ etwa auch „Wohnung“, „Kindergeld“, „Arbeitnehmer“), ist wegen fehlender Begriffsbestimmungen nicht abschließend bestimmbar, welche Behörden die Auskunftsersuchen stellen dürfen. Dies jedoch ist nach dem verfassungsrechtlichen Bestimmtheitsgebot unverzichtbar. Zudem wird nicht deutlich, welche Zwecke ein Auskunftsersuchen rechtfertigen und nach welchen Regeln sie erfolgen sollen.

Von der Tatsache des Datenabrufs erfahren Kreditinstitute und Betroffene zunächst nichts. Die Betroffenen erhalten hiervon allenfalls bei einer Diskrepanz zwischen ihren Angaben (z. B. anlässlich Steuererklärung, BAföG-Antrag) und den Ergebnissen der Kontenabfragen Kenntnis, nicht jedoch bei einer Bestätigung ihrer Angaben durch die Kontenabfragen.
Die Auskunft erstreckt sich zwar nicht auf die Kontostände; auf Grund der durch den Abruf erlangten Erkenntnisse können jedoch in einem zweiten Schritt weitere Überprüfungen, dann auch im Hinblick auf die Guthaben direkt beim Kreditinstitut erfolgen.

Dass Betroffene von Abfragen, die zu keiner weiteren Überprüfung führen, nichts erfahren, widerspricht dem verfassungsrechtlichen Transparenzgebot. Danach sind sie von der Speicherung und über die Identität der verantwortlichen Stelle sowie über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung zu unterrichten. Geschieht dies nicht, hat das zur Konsequenz, dass die Rechtsschutzgarantie des Art. 19 Abs. 4 GG verletzt wird. Die Bürgerinnen und Bürger haben einen substantiellen Anspruch auf eine tatsächlich wirksame gerichtliche Kontrolle (s. Volkszählungsurteil, BVerfGE 65, 1, 70).

11. Materialien

IT-Sicherheitsleitlinie für die Hessische Landesverwaltung

1. Vorbemerkung

Die Prozesse zur Aufgabenerfüllung in der Hessischen Landesverwaltung werden zunehmend von Informations- und Kommunikationstechniken (IT) in miteinander vernetzten Systemen unterstützt. Vor diesem Hintergrund ist eine angemessene IT-Sicherheit zu organisieren. Danach sind

- organisatorische Rahmenbedingungen zur nachhaltigen Gewährleistung von IT-Sicherheit zu schaffen,
- ein IT-Sicherheitsmanagement einzurichten,
- abgestimmte Sicherheitsstandards einschließlich der Definition von Verantwortlichkeiten und Befugnissen zu erarbeiten,
- Komponenten zur Steigerung der IT-Sicherheit zu zentralisieren und standardisieren und alle Sicherheitsvorkehrungen und -maßnahmen hinreichend zu dokumentieren.

Die Regelungen dieser IT-Sicherheitsleitlinie sind vom zentralen IT-Sicherheitsmanagement der Hessischen Landesverwaltung auf Grundlage des IT-Grundschutzhandbuchs des Bundesamts für Sicherheit in der Informationstechnik (BSI) erstellt worden. Sie wurden von der Landesregierung gebilligt und sind mit ihrer Veröffentlichung für den Einsatz in der IT der Landesverwaltung verbindlich.

2. Grundsätze

In Abwägung der Werte der zu schützenden Informationen, der Risiken sowie des Aufwands an Personal und Finanzmitteln für IT-Sicherheit soll für eingesetzte und geplante IT-Systeme in der Hessischen Landesverwaltung ein angemessenes IT-Sicherheitsniveau angestrebt und erreicht werden. Für IT-Systeme mit niedrigem bis mittlerem Schutzbedarf sind Sicherheitsmaßnahmen auf der Grundlage des IT-Grundschutzhandbuchs des BSI als Standard vorzusehen und umzusetzen. Für Bereiche, in denen ein höherer Schutzbedarf festgestellt wird, müssen ergänzende Sicherheitsmaßnahmen eingeführt werden.

3. Ziele

3.1 Alle Beschäftigten gewährleisten die IT-Sicherheit durch ihr verantwortliches Handeln und halten die für die IT-Sicherheit relevanten Gesetze, Vorschriften, Richtlinien, Anweisungen und vertraglichen Verpflichtungen ein.

3.2 Für den IT-Einsatz sind die Sicherheitsziele Verfügbarkeit, Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit im jeweils erforderlichen Maße zu erreichen. Die daraus abgeleiteten Sicherheitsmaßnahmen sind auch dann anzuwenden, wenn sich daraus Beeinträchtigungen für die IT-Nutzung ergeben.

3.3 Die Sicherheit der IT-Verfahren ist neben der Leistungsfähigkeit und Funktionalität zu gewährleisten. Bleiben im Einzelfall trotz der Sicherheitsvorkehrungen Risiken untragbar, ist an dieser Stelle auf den IT-Einsatz zu verzichten.

4. Maßnahmen

4.1 Für bereits betriebene und für geplante Informationstechnik sind IT-Sicherheitskonzepte zu erstellen. Im Rahmen dieses Verfahrens sind die personalvertretungsrechtlichen Beteiligungsrechte zu wahren.

4.2 Um den möglichen Risiken und Schäden vorzubeugen, sind organisatorische und technische Maßnahmen zur IT-Sicherheit umzusetzen.

4.3 Die Verantwortlichen haben bei Verstößen und Beeinträchtigungen die zur Aufrechterhaltung des IT-Betriebes und der IT-Sicherheit geeigneten und angemessenen Maßnahmen zu ergreifen.

4.4 Der Zugriff auf IT-Systeme, -Anwendungen und Daten und Informationen ist auf den unbedingt erforderlichen Personenkreis zu beschränken. Jeder Bedienstete erhält nur auf diejenigen Daten und Informationen die Zugriffsberechtigungen, die er zur Erfüllung seiner dienstlichen Aufgaben benötigt.

4.5 Die Sicherheit soll besonders durch Anwendung von Verfahren und Tools nach dem jeweiligen Stand der Technik erreicht werden.

4.6 Die für die Umsetzung der IT-Sicherheitsmaßnahmen erforderlichen Ressourcen und Investitionsmittel sind bereitzustellen.

4.7 Die Wirksamkeit der Sicherheitsmaßnahmen ist regelmäßig zu kontrollieren.

5. Verantwortlichkeiten

5.1 Die Dienststellenleitung trägt in dem Bereich, den sie beeinflussen kann, die Verantwortung für eine angemessene IT-Sicherheit.

5.2 Ein Sicherheitsmanagement besteht aus dem bzw. der IT-Sicherheitsbeauftragten, den Zuständigen für die Fachanwendungen, für den IT-Service und für den IT-Betrieb. Es ist damit zu betrauen, gemäß den Sicherheitsvorgaben die Sicherheit im Umgang mit der IT und den Schutz der Daten und Informationen zu gewährleisten. Ebenso gehört es zu seinen Aufgaben, das IT-Sicherheitskonzept fortzuschreiben und Maßnahmen umzusetzen, die ein angemessenes und dem Stand der Technik entsprechendes IT-Sicherheitsniveau sicherstellen. Der behördliche Datenschutzbeauftragte unterstützt den Dienststellenleiter bei der Umsetzung der IT-Sicherheit. Ihm ist deshalb die Teilnahme an den Beratungen des IT-Sicherheitsmanagements zu ermöglichen, soweit er dies wünscht.

5.3 Die Mitarbeiter sind dafür verantwortlich, dass die Sicherheitsmaßnahmen in ihrem Bereich umgesetzt werden. Unterstützt durch sensibilisierende Schulung und Benutzerbetreuung am Arbeitsplatz soll jeder im Rahmen seiner Möglichkeiten Sicherheitsvorfälle von innen und außen vermeiden. Sicherheitsrelevante Ereignisse sind den Zuständigen umgehend zu melden, damit schnellstmöglich Abhilfemaßnahmen eingeleitet werden können.

5.4 Die jeweils Zuständigen für Daten, Informationen und Verfahren sowie für unterstützende Systeme, Netze und Infrastruktur entscheiden, wer in welchem Umfang Zugriff auf das jeweilige System hat. Wenn sie Vorgaben zur Sicherheit formulieren, haben sie auch die angemessene Sicherheitsstufe, Finanzierbarkeit bzw. Wirtschaftlichkeit abzuwägen.

5.5 Ein Auftragnehmer (vgl. § 4 HDSG), der für die Verwaltung Leistungen erbringt, hat Vorgaben des Auftraggebers zur Einhaltung der IT-Sicherheitsziele (Wahrung der Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Verbindlichkeit) gemäß dieser IT-Sicherheitsleitlinie einzuhalten. Der Auftraggeber hat Sicherheitsanforderungen vertraglich festzulegen und deren Einhaltung zu kontrollieren. Der Auftraggeber hat den Auftragnehmer zu verpflichten, bei erkennbaren Mängeln oder Risiken eingesetzter Sicherheitsmaßnahmen den Auftraggeber zu informieren.

5.6 Die Einhaltung der IT-Sicherheit bei der Verarbeitung, Nutzung und Kontrolle von Daten und Informationen ist zu überprüfen. Art und Umfang der Kontrolle sind von der Dienststellenleitung auf der Grundlage des jeweiligen Sicherheitskonzeptes festzulegen. Eine Kontrolle kann durch unabhängige Dritte erfolgen. In diesem Fall ist zu gewährleisten, dass keine unzulässige Kenntnisnahme von Daten und Informationen damit verbunden ist.

6. Verstöße und Folgen

Verhalten, das die Sicherheit von Daten, Informationen, IT-Systemen oder des Netzes gefährdet, kann disziplinar- oder arbeitsrechtlich geahndet werden. Unter Umständen kann das Verhalten als Ordnungswidrigkeit oder als Straftat verfolgt werden. Als Straftat kommen insbesondere in Betracht:

- das unbefugte Verschaffen von Daten anderer, die gegen unberechtigten Zugang besonders gesichert sind (§§ 202a, 274 Abs. 1 Nr. 2 StGB)

- der Computerbetrug durch unrichtige Gestaltung eines Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder durch unbefugte Einwirkung auf den Ablauf (§ 263a StGB)

- die fälschliche Beeinflussung einer Datenverarbeitung (§§ 270, 269 StGB), das rechtswidrige Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern von Daten (§ 303a StGB)

- das Zerstören, Beschädigen, Unbrauchbarmachen, Beseitigen oder Verändern einer Datenverarbeitungsanlage oder eines Datenträgers (§ 303b StGB)

- die Verwendung personenbezogener Daten entgegen den Vorschriften des HDSG (§ 40 HDSG).

Beschäftigte, die die Sicherheit von Daten, Informationen, IT-Systemen oder des Netzes gefährden und einen Schaden für das Land oder einen Dritten verursachen, können darüber hinaus zum Schadenersatz (§ 91 HBG, § 14 BAT, § 823 BGB) herangezogen werden oder einem Rückgriffanspruch (Art. 34 GG i. V. m. § 839 BGB) ausgesetzt sein.

7. Umsetzung

Diese IT-Sicherheitsleitlinie wird im Staatsanzeiger veröffentlicht; sie ist allen Beschäftigten in geeigneter Weise bekannt zu geben. Auf der Grundlage dieser IT-Sicherheitsleitlinie haben die Ressorts ihre IT-Sicherheitsleitlinien auszugestalten.

8. Bekanntgabe

Diese IT-Sicherheitsleitlinie tritt am 1. Dezember 2004 in Kraft.