16. Wahlperiode

Drucksache **16/2131**

HESSISCHER LANDTAG

05. 04. 2004

Zweiunddreißigster Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

vorgelegt zum 31. Dezember 2003
vom Hessischen Datenschutzbeauftragten
Prof. Dr. Michael Ronellenfitsch
nach § 30 des Hessischen Datenschutzgesetzes vom 7. Januar 1999

Eingegangen am 5. April 2004 · Ausgegeben am 29. April 2004
Druck: Druckerei Chmielorz GmbH, 65205 Wiesbaden · Auslieferung: Kanzlei des Hessischen Landtags, Postfach 3240, 65022 Wiesbaden

INHALTSVERZEICHNIS

Vorwort

Der vorliegende Tätigkeitsbericht beschränkt sich wiederum auf die Präsentation von Schwerpunkten, Fragestellungen mit Wirkung über den Einzelfall hinaus, eklatante Einzelfälle sowie Entwicklungstendenzen.

Der jährliche Tätigkeitsbericht kann nämlich naturgemäß nur einen Teil der Arbeiten zur Erfüllung meiner gesetzlichen Aufgaben wiedergeben. Die tägliche "Kleinarbeit" eignet sich demgegenüber grundsätzlich nicht zur Darstellung im Tätigkeitsbericht. Das gilt namentlich für drei große Bereiche, die viel Zeit und Kapazität in Anspruch nehmen, aber andererseits auch die Grundlage auf dem Weg der Sicherstellung des Datenschutzes in der Gegenwart und im Hinblick auf künftige Entwicklungen sind.

- Der erste Bereich betrifft die oft mühevolle Arbeit der Problemerkennung, -aufarbeitung und Positionsfindung in datenschutzrelevanten Fragestellungen. So ist die - nicht selten kontroverse - Diskussion in zahlreichen Gremien mit dem Ziel, eine einheitliche Linie zu finden und die Arbeit zu koordinieren (z. B. in Arbeitskreisen zusammen mit den Datenschutzbeauftragten des Bundes und der Länder, der Kommunen und anderer Daten verarbeitender Stellen), ebenso notwendige Basis für die Arbeitsergebnisse wie die Mitarbeit in Gremien, die in erster Linie der Informationssammlung und Aufbereitung von Themen und dem Gedankenaustausch mit Interessenverbänden (insbesondere im Informatikbereich) und mit anderen interessierten Berufsgruppen (wie z. B. im Forschungs- und Gesundheitsbereich) dient. Ergebnisse dieser notwendigen Vorarbeiten fließen in den Tätigkeitsbericht oft nur insoweit ein, wie sie in Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, in Orientierungshilfen und Arbeitspapieren Eingang gefunden haben.

- Als zweiter Bereich, der im Tätigkeitsbericht keinen Niederschlag findet, sind die zahlreichen Anfragen von Bürgern und Behörden zu nennen, soweit sie keine über den Einzelfall hinausgehenden Wirkungen entfalten und nicht in anderer Weise exemplarisch sind oder nur im Tätigkeitsbericht bereits mehrfach dargestellte wiederkehrende Themen betreffen. Hierzu gehört auch ein großes Pensum an Beratungen, da meine Dienststelle zunehmend im Vorfeld eingeschaltet wird, um Datenschutzprobleme gar nicht erst entstehen zu lassen. Einen besonders breiten Raum hat im vergangenen Jahr dabei die Beratung bei der Einführung von SAP R/3 in der Landesverwaltung eingenommen; insbesondere haben die datenschutzrechtlichen Fragestellungen im Zusammenhang mit dem für die Personalverwaltung vorgesehenen Modul HR erhebliche Kapazitäten in Anspruch genommen.

- Der dritte Bereich ohne Resonanz im Tätigkeitsbericht betrifft die Aktivitäten zur Information und Schulung zum Thema Datenschutz. Wegen des grundlegend neuen Konzeptes ist im Tätigkeitsbericht aus diesem Spektrum nur der Online-Kurs erwähnt. Darüber hinaus sind Bedienstete meines Hauses auch in konventionellen Schulungs- und Informationsveranstaltungen bei der Hessischen Zentrale für Datenverarbeitung, dem Verwaltungsschulverband, der IT-Akademie des Hessischen Kultusministeriums, in der Polizeischule und fallweise auch unmittelbar in Daten verarbeitenden Stellen und bei sonstigen Veranstaltungen als Referenten zu Datenschutz- und Datensicherheitsthemen tätig. Auch mein Internetangebot und die Mitarbeit im "virtuellen Datenschutzbüro", einer von vielen Datenschutzinstitutionen unter Geschäftsführung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein getragenen Informationsplattform, ist ein arbeitsintensives Tätigkeitsfeld, das zum unverzichtbaren, aber selbstverständlichen Aufgabenspektrum zählt.

Im vergangenen Jahr haben zusätzlich die Vorbereitungsarbeiten zur Einführung von SAP R/3 im eigenen Haus, die - wie auch in anderen Dienststellen des Landes - neben der "normalen" Last bewältigt werden mussten, trotz aller Anstrengungen auch Kapazitäten aus den originären Aufgaben reduziert. Schon wegen der Besonderheit der Aufgaben und der infolge der Funktion als Kontrollstelle auch besonderen rechtlichen Ausgestaltung passen die auf klassische Verwaltung ausgerichteten Prozesse und Verfahren nicht so recht. Gerade für eine kleine Dienststelle ist die Verwaltungslast durch ein solches Großverfahren erheblich und wirkt sich angesichts des geringen Optimierungs- und Einsparpotentials unverhältnismäßig hoch aus. So haben schon allein die notwendigen Fortbildungsmaßnahmen mehr als 100 Personentage in Anspruch genommen - ein Vielfaches der üblicherweise durch Fortbildung jährlich "ausfallenden" Tage.

Dies vorausgeschickt, verdeutlicht auch der vorliegende Tätigkeitsbericht die besondere Funktion, die dem Datenschutz im Land Hessen zukommt.

1. Kernpunkte des 32. Tätigkeitsberichts

1. Die Hessische Landesregierung fördert Telearbeit als Chance für eine bessere Vereinbarkeit von Familie und Beruf. Gerade weil Telearbeit im häuslichen Umfeld stattfindet, ist auf Datenschutzaspekte sowohl bei der Auswahl der für Telearbeit geeigneten Aufgaben als auch bei der Ausgestaltung der technischen und organisatorischen Rahmenbedingungen besonders zu achten. Die "Sicherheitskriterien Telearbeit" bieten eine wertvolle Hilfestellung (Ziff. 2.1).

2. Die diskutierte Ausweitung des Anwendungsbereichs der DNA-Analyse im Bereich der Strafverfolgung ist mit der durch den Grundsatz der Verhältnismäßigkeit gebotenen Zurückhaltung zu betreiben und darf die rasanten Weiterentwicklungen der Wissenschaft bei der Genforschung und -analyse im Hinblick auf die sich daraus ergebenden Auswirkungen auf das Recht auf informationelle Selbstbestimmung nicht aus den Augen verlieren (Ziff. 5.2; 20.10).

3. Bei der Aufklärung schwerer Straftaten setzt die Polizei immer häufiger das Instrument der Massenuntersuchungen auf freiwilliger Basis ein. Eine Rechtsgrundlage hierfür gibt es nicht. Wesentliche Säule unseres Rechtsstaats ist die Unschuldsvermutung im Strafrecht, die nicht zu einem "freiwilligen" Unschuldsnachweis mutieren darf. Deshalb ist es notwendig, Rechtsgrundlagen für solche Massenscreenings zu schaffen, die den Einsatzbereich klar begrenzen und enge Zweckbindung sowie Löschfristen regeln (Ziff. 5.3).

4. Die Einwohnermeldeämter bekommen vor Wahlen immer wieder Anforderungen der Parteien zur Übermittlung von Einwohnerdaten. Die Gesetzeslage lässt die Übermittlung von Adressdaten nach Altersgruppen zu, die Übermittlung der Daten aller Wahlberechtigten ist unzulässig. In Übereinstimmung mit dem Innenministerium interpretiere ich die Vorschrift so, dass nur Daten von Einwohnergruppen übermittelt werden sollen, die nicht über 50 v.H. der Wahlberechtigten umfassen (Ziff. 8.3).

5. Das Baugesetzbuch ermöglicht die Beteiligung privater Dritter als Verwaltungshelfer an der Bauleitplanung, auch für die Auswertung von Einwendungen der Bürger. Die Weiterleitung von personenbezogenen Daten an einen solchen Verwaltungshelfer ist deshalb datenschutzrechtlich nicht zu beanstanden. Die Gemeinde sollte aber aus Gründen der Transparenz die Bürger auf die Einbeziehung von Dritten in das Verfahren hinweisen (Ziff. 9.2).

6. Die Einsicht in Abiturprüfungsunterlagen darf nicht abgelehnt werden, nur weil die Prüfung schon mehrere Jahre zurückliegt. Die gesetzliche Regelung in Hessen enthält nämlich keine zeitliche Einschränkung des Einsichtsrechts (Ziff. 12.2).

7. Die Reform der gesetzlichen Krankenversicherung hat vor allem durch die vorgesehene Einführung der elektronischen Gesundheitskarte und den Aufbau eines zentralen Datenpools erhebliche Auswirkungen auf die Verarbeitung medizinischer Daten der ca. 60 Millionen Versicherten. Hier konnten weitgehend datenschutzfreundliche Lösungen erreicht werden, deren tatsächliche Umsetzung in der Zukunft sichergestellt werden muss (Ziff. 14.1; 20.12).

8. Die Praxis des in Hessen durchgeführten Neugeborenen-Screenings muss auf eine neue Basis gestellt werden. Im neuen Screening-Zentrum Hessen sollen die Daten und Blutproben aller Neugeborenen Hessens flächendeckend zentral erfasst werden. Aufgrund meiner Forderungen sollen die Proben und medizinischen Daten der Neugeborenen pseudonymisiert und die Zwecke, zu denen über einen Treuhänder depseudonymisiert werden darf, abschließend festgelegt werden (Ziff. 14.2).

9. Der Landeswohlfahrtsverband hat einer ehemaligen Bediensteten Einsicht in Unterlagen verweigert. Er hat darüber hinaus - nachdem ich die Einsicht in die Unterlagen angekündigt hatte, diese vernichtet und damit nicht nur das Einsichtsrecht einer ehemaligen Bediensteten sondern auch meine Informationsrechte missachtet. Dies führte zu einer förmlichen Beanstandung (Ziff. 16.2).

10. Die in der Diskussion um die Neuordnung der Rundfunkfinanzierung von den Rundfunkanstalten geäußerten Informationswünsche würden – sollten die Landesgesetzgeber sie erfüllen – zu einer erheblichen Verschlechterung des Datenschutzes führen (Ziff. 17.1).

11. Der Ankauf der Anschriften, mit denen die Gebühreneinzugszentrale im Auftrag des Hessischen Rundfunks Briefaktionen durchführt, um Schwarzhörer und -seher aufzuspüren, verstößt gegen das Datenschutzrecht (Ziff. 17.2).

2. Querschnittsthemen

2.1
Telearbeit

Die Hessische Landesregierung fördert die Telearbeit als Mittel, die Flexibilität im Berufsleben für die Beschäftigten zu erhöhen. Es wurden die nötigen Vereinbarungen getroffen, um das Pilotprojekt in den normalen Betrieb zu überführen. Eine wesentliche Komponente bilden dabei die "Sicherheitskriterien Telearbeit", die unter meiner Beteiligung erarbeitet wurden.

2.1.1
Telearbeit in Hessen

Im Jahr 2000 hat die Hessische Landesregierung einen „Modellversuch Alternierende Telearbeit“ begonnen. Ziel war es, die Vereinbarkeit von Beruf und Familie für Frauen und Männer zu verbessern. Im Jahr 2002 wurde der Versuch abgeschlossen und ein Erfahrungsbericht erstellt. Auf Basis der Erfahrungen wurde 2003 die alternierende Telearbeit ein Angebot, das nach den Vorstellungen der Landesregierung bis auf wenige Ausnahmen allen Beschäftigten eingeräumt werden soll. Die getroffenen Vereinbarungen und der unten genannte Kriterienkatalog sind im Staatsanzeiger für das Land Hessen (2003, S. 2748) veröffentlicht.

Die Einrichtung eines Telearbeitsplatzes kann aber nur erfolgen, wenn auch datenschutzrechtliche Vorgaben zur Sicherung der zu verarbeitenden Daten eingehalten werden.

2.1.2
Datenschutzrechtliche Aspekte

In der Anschlussvereinbarung zur "Einführung von alternierender Telearbeit im Bereich der hessischen Landesverwaltung" vom 20. Juni 2003 werden verschiedene datenschutzrechtliche Forderungen gestellt.

Unter Ziff. 2 der Vereinbarung werden Kriterien für Tätigkeiten genannt, die für Telearbeit geeignet sind. Dabei ist auch auf den Datenschutz verwiesen.

Ziff. 2

… und insbesondere unter Beachtung des Datenschutzes im häuslichen Bereich der Beschäftigten erledigt werden können.

Bei der Telearbeit gibt es im Vergleich zum Büroarbeitsplatz zusätzliche datenschutzrelevante potentielle Schwachstellen:

a) Die Organisation der Telearbeit ist komplizierter, da die räumliche Entfernung größer ist und der Arbeitgeber nur indirekte Möglichkeiten der Einflussnahme hat.

b) Die Kommunikationsverbindung zwischen Arbeitsplatzrechner und Institution geht in der Regel über öffentliche Leitungen.

c) Es gibt einen zusätzlichen Zugang zum Netz der Verwaltung.

d) Die Möglichkeiten des Zugriffs und der Kontrolle durch den behördlichen Datenschutzbeauftragten und den Administrator sind eingeschränkt.

e) Der Arbeitsplatzrechner ist unberechtigten Zugriffen eher ausgesetzt.

f) Der Arbeitsplatzrechner kann zu nicht vorgesehenen Zwecken verwandt werden.

g) Daten und Akten können leichter in unbefugte Hände gelangen.

Der Arbeitgeber kann einige der Probleme durch eigene Vorkehrungen lösen (a – c). Die anderen Schwachstellen müssen zusammen mit den Beschäftigten kontrolliert werden. Eine in der Vereinbarung nicht explizit genannte Voraussetzung der Teilnahme an der Telearbeit ist die Zuverlässigkeit des Beschäftigten. Wenn der Arbeitgeber nicht sicher ist, dass der Beschäftigte die Vereinbarungen umsetzt und insbesondere unbefugten Personen die Einsicht in Unterlagen verwehrt, muss er eine Teilnahme ablehnen.

Ziff. 8.1

Vertrauliche Daten und Informationen gegenüber Dritten sind in der häuslichen Arbeitsstätte so zu schützen, dass ein unbefugter Zugang zu und ein unberechtigter Zugriff auf die Daten wirksam verhindert wird.

Brisant ist auch die Verarbeitung äußerst sensibler Daten. In der Vereinbarung heißt es:

Ziff. 8.1

…. Tätigkeiten, bei denen überwiegend personenbezogene und äußerst sensible Daten verarbeitet werden (z. B. Personal-, Disziplinar-, Steuer- und Beihilfeangelegenheiten), ist datenschutzrechtlich besondere Aufmerksamkeit zu widmen.

Bezüglich dieser Aufgabenfelder muss sich jede Dienststelle sehr genau überlegen, ob diese Tätigkeiten aufgrund ihrer besonderen Sensibilität überhaupt einer Telearbeit zugänglich sein sollten. Entscheidet die Dienststelle gleichwohl, dass derartige Daten in Telearbeit verarbeitet werden können, dann sind besonders hohe Anforderungen an die zu treffenden Sicherheitsmaßnahmen zu stellen. Das heißt, der unten genannte Kriterienkatalog muss komplett umgesetzt sein. Die Frage der Zuverlässigkeit der Beschäftigten gewinnt hier noch an Bedeutung. Der Arbeitgeber muss aufgrund der Beobachtung der bisherigen Arbeitsweise den Eindruck einer absolut zuverlässigen Einhaltung der Vorgaben nach Ziff. 8.1 der Vereinbarung haben, so dass er dem Beschäftigten uneingeschränkt vertrauen kann. Anderenfalls ist die Telearbeit datenschutzrechtlich nicht möglich. Gleiches gilt, wenn die Räumlichkeiten nicht adäquat sind.

Vor der Aufnahme der Telearbeit muss geprüft werden, ob die räumlichen Verhältnisse den Erfordernissen entsprechen und es müssen Zutrittsrechte zu Kontrollzwecken eingeräumt werden. (Ziff. 6, 8.3 und 8.4 der Vereinbarung). So muss auch der Hessische Datenschutzbeauftragte eine Datenschutzkontrolle des Telearbeitsplatzes durchführen können.

Ich habe die Absicht, im kommenden Jahr an einigen Arbeitsplätzen die korrekte Umsetzung der Vereinbarung zu prüfen.

2.1.3
Technische und organisatorische Standards

Neben den rechtlichen Rahmenbedingungen müssen auch technische und organisatorische Standards eingehalten werden.

Der "Kriterienkatalog zu technischen und organisatorischen Standards bei der Einrichtung und für den Betrieb von Telearbeitsplätzen in der hessischen Landesverwaltung" wurde leider erst mit einiger Verspätung am 15. Dezember 2003 (StAnz. 2003, S. 4963 ff.) veröffentlicht. Der Katalog wurde durch eine ressortübergreifende Arbeitsgruppe erarbeitet, in der Mitarbeiter meiner Dienststelle beratend mitgewirkt haben. Den Text ist unter Ziff. 21 in diesem Tätigkeitsbericht abgedruckt.

In meinem 31. Tätigkeitsbericht (Ziff. 25.4) hatte ich eine Orientierungshilfe veröffentlicht, in der die wesentlichen Punkte und Fragestellungen genannt wurden, die bei der Einführung von Telearbeit eine Rolle spielen können. Dazu gehören insbesondere technische Sicherheitsvorkehrungen. Die dort genannten Kriterien waren Basis der von mir in der Arbeitsgruppe vorgeschlagenen Maßnahmen.

2.2
Neues Online-Seminar „Datenschutz und Datensicherheit“

Beschäftigte meines Hauses haben zusammen mit der Hessischen Zentrale für Datenverarbeitung das Thema Datenschutz und Datensicherheit als Online-Seminar entwickelt und eingesetzt.

E-Mail, E-Commerce, E-Government, die Liste neuer Worte mit diesem plakativen Buchstaben wird jedes Jahr länger. Immer häufiger begegnet man auch dem Begriff "E-Learning". Während sich in virtuellen Hochschulen und Online-Akademien diese Lehr- und Lernform schon etabliert hat, betritt die hessische Verwaltung hier Neuland. Traditionelle Weiterbildungsangebote bekannter Fortbildungseinrichtungen in Hessen wie z. B. Hessische Zentrale für Datenverarbeitung (HZD) beschränkten sich bis vor zwei Jahren auf so genannte Präsenzseminare. Neuerdings werden einige Kurse auch als Online-Seminare angeboten. Vorteile dieser Lernform sind flexible Zeiteinteilung, individuelles Arbeiten, multimediale Unterstützung und als wesentlicher Faktor, der die Effizienz des Online-Seminars wesentlich mitbestimmt, die persönliche Betreuung der Kursteilnehmer durch einen Tutor.

Auf der Basis dieser Erkenntnisse erarbeiteten Beschäftigte meines Hauses in Zusammenarbeit mit der HZD das landesweit erste Online-Seminar zum Thema „Datenschutz und Datensicherheit“. Die Erfahrungen, die die HZD schon mit Onlineseminaren gemacht hatte, kamen diesem Projekt zugute. Der Weiterbildungsbedarf ist groß, wie meine Erfahrungen aus Prüfbesuchen bei Behörden zeigen. Die meisten datenschutzrechtlichen Defizite waren darauf zurückführen, dass sowohl bei Behördenleitungen, behördlichen Datenschutzbeauftragten und Bediensteten das notwendige Basisfachwissen oft nicht vorhanden ist.

Das seit dem Jahr 2003 angebotene Online-Seminar erstreckt sich über fünf Wochen. In der ersten Woche wird der Umgang mit dem neuen Medium am dienstlichen PC erprobt, in den vier weiteren Wochen erhalten die Teilnehmer per E-Mail die vorbereiteten Lerninhalte in Form von Studienbriefen. Die empfohlene wöchentliche Lernzeit liegt bei ca. drei Stunden. Die tutorielle Betreuung erfolgt in dieser Zeit durch Mitarbeiter meines Hauses. Die Lösungen der Übungsaufgaben, die wöchentlich verteilt werden, erhalten die Teilnehmer als E-Mail auf ihren dienstlichen PC und können sie individuell kommentieren. Gelegenheit zur Vertiefung besteht durch zahlreiche Internet-Links in den Studienbriefen. Gleichzeitig können die Teilnehmer untereinander und mit den Tutoren in einem Diskussionsforum weitergehende Fragen diskutieren.

So lebendig die Interaktionsmöglichkeiten bei einem solchen Online-Seminar auch ausfallen, es bleibt doch manchmal das Gefühl der technisch bedingten Distanz zur Lerngruppe. Deshalb schließt das Seminar am Ende mit einem eintägigen Workshop in der HZD. Die praktische Erfahrung bestätigte das damit gewünschte Ziel: Die gute fachliche Vorbereitung ermöglicht den Teilnehmern, mit dem nun vorhandenen Basiswissen vertieft zu diskutieren und sich gerade auch aktuellen rechtlichen und DV-technischen Themen zu widmen.

Aus technischen Gründen stand das Online-Seminar bisher nur den Nutzern des Landesintranets zur Verfügung. Für 2004 ist auch der Zugang über das Internet geplant.

Nähere Informationen sind über meine Homepage verfügbar (www.datenschutz.hessen.de).

3. Europa

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
Allgemeines

Die Zusammenlegung der Geschäftsstellen für Schengen, EUROPOL und das Zollinformationssystem in einer gemeinsamen Geschäftsstelle hat sich bewährt. Die Vorbereitung der Sitzungen der Gemeinsamen Kontrollinstanz und die Qualität der Entwürfe von Stellungnahmen und anderen Meinungsäußerungen haben sich deutlich verbessert.

Im Juni 2003 fand die erste Sitzung der Gemeinsamen Kontrollinstanz statt, an der Vertreter der zehn neuen Beitrittsländer als Beobachter teilnahmen.

Der zuständige Ausschuss des Europäischen Parlaments organisierte zusammen mit der Gemeinsamen Kontrollinstanz im Oktober 2003 ein Seminar über neue Entwicklungen des Schengener Informationssystems, an dem Vertreter des Europarats, Mitglieder der Kommission und Pressevertreter teilnahmen. Der Diskussionsstand ist unter Ziff. 3.2 dargestellt.

3.2
Entwicklungen des Schengener Informationssystems

Im 31. Tätigkeitsbericht (Ziff. 4.2) habe ich über Pläne für eine Erweiterung des Schengener Informationssystem (SIS), das so genannte SIS II und die zu diesem Thema erfolgten Stellungnahmen der Gemeinsamen Kontrollinstanz berichtet.

Die Schaffung einer neuen Generation des Schengener Informationssystems mit einer neuen Technik ist notwendig, weil das jetzige SIS nur für 18 Staaten ausgelegt ist, nach Beitritt der neuen EU-Länder aber ein System erforderlich ist, das mindestens 25 Teilnehmer zulässt. Das SIS II soll im Jahr 2006 einsatzbereit sein.

An der Entwicklung des SIS II sind mehrere Arbeitsgruppen des Rates und der Kommission beteiligt und es ist für die Gemeinsame Kontrollinstanz teilweise schwierig, jeweils den aktuellen Stand der Pläne zu erfahren: Ein gerade von der Gemeinsamen Kontrollinstanz diskutierter Vorschlag zur Änderung des SIS kann schon morgen nicht mehr aktuell oder gänzlich abgeändert sein. Die deutsche Delegation hält die Entwicklung des Schengener Informationssystems für das derzeit wichtigste Thema und beteiligt sich aktiv in der hierzu eingesetzten Arbeitsgruppe.

Das Zusammenspiel der diskutierten Änderungen lässt jedenfalls eines erkennen: Das SIS wurde konzipiert als ein System mit dessen Hilfe z. B. der Polizeibeamte vor Ort schnell feststellen konnte, ob eine Ausschreibung für die betroffene Person besteht und welche unmittelbaren Maßnahmen zu treffen sind (Treffer/Kein-Treffer-System). Damit sollte es als Kompensation für den Wegfall der Kontrollen an den Binnengrenzen des Schengenraumes dienen. Durch die Aufnahme einer Reihe neuer Datenkategorien und die Bereitstellung für neue Nutzer zu unterschiedlichen Zwecken entwickelt sich das SIS immer mehr von einem Treffer/Kein-Treffer-System zu einem Analysesystem für die Polizeibehörden und andere Stellen. Es geht damit weit über die ursprüngliche Zielsetzung hinaus. Zudem ist zu fragen, inwieweit redundante Funktionen im Hinblick auf schon bestehende Informationssysteme auf europäischer Ebene geschaffen werden.

3.2.1
Kurzfristig zu realisierende Änderungen

Eine Reihe von Änderungen des SIS sollen bald vom Rat verabschiedet werden. Sie gehen auf eine Initiative der spanischen Ratspräsidentschaft zurück, die eine kurzfristige Effizienzsteigerung des bestehenden Informationssystems durch eine Änderung rechtlicher Regelungen zum Ziel hatte. Enthalten sind sie in Entwürfen für eine Verordnung und einen Beschluss des Rates über die Einführung neuer Funktionen für das Schengener Informationssystem. Die Wahl der unterschiedlichen Rechtsformen hängt damit zusammen, dass aufgrund des Amsterdamer Vertrags die Vorschriften im Schengener Durchführungsübereinkommen (SDÜ) zum Teil dem Europäischen Gemeinschaftsvertrag (EGV) und zum Teil dem Vertrag über die Europäische Union (EUV) zugeordnet wurden. Eine Novellierung der verschiedenen Vorschriften des SDÜ bedarf deshalb unterschiedlicher Rechtsakte.

- **Rechtsgrundlage für SIRENE**

  Erstmals gibt es eine rechtliche Regelung der Tätigkeit der SIRENE-Büros und der Verarbeitung der dort anfallenden Unterlagen. Bei SIRENE (**S**upplementary **I**nformation **Re**quest at the **N**ational **E**ntry) handelt es sich um die jeweilige nach Art. 108 SDÜ von den Nationalstaaten zu bestimmende Stelle (in Deutschland das Bundeskriminalamt), die das nationale Schengener Informationssystem (NSIS) betreibt, die aber auch andere damit zusammenhängende Aufgaben – wie die Verarbeitung entsprechender Informationen in Papierform – wahrnimmt. Die Gemeinsame Kontrollinstanz hat die

Schaffung der Rechtsgrundlagen begrüßt. Zu kritisieren ist aber, dass eine Regelung nachgeschoben wurde, die zwar bestimmte Löschungsfristen für die konventionellen Unterlagen bei der SIRENE vorsieht, es aber zulässt, dass personenbezogene Angaben aus den SIRENE-Unterlagen in nationale Dateien überführt werden können und diese den Löschungsfristen des nationalen Rechts unterliegen.

- **Neue Zugriffsrechte für EUROPOL, EUROJUST und Staatsanwaltschaften**
  Neu ist weiter, dass die nationalen Justizbehörden - also in Deutschland die Staatsanwaltschaften und Gerichte - Zugriff auf alle im SIS enthaltenen Daten erhalten. Das Europäische Polizeiamt (EUROPOL) und die Europäische Stelle zur justiziellen Zusammenarbeit (EUROJUST) dürfen in eingeschränktem Rahmen auf SIS-Daten zugreifen. Ausgenommen vom Zugriff sind die Ausschreibungen nach Art. 96 SDÜ also die zur Einreiseverweigerung ausgeschriebenen Drittausländer. Des Weiteren dürfen Europol und Eurojust keine Verbindung zwischen den eigenen Informationssystemen und SIS herstellen.

- **Protokollierung**
  Die Gemeinsame Kontrollinstanz hat es positiv bewertet, dass nunmehr jeder Zugriff auf das SIS protokolliert werden soll und nicht mehr nur jede zehnte Übermittlung wie früher vorgesehen. Die Aufbewahrungszeiten für die Protokolldaten wurden verlängert von sechs Monaten auf mindestens ein Jahr und längstens zwei Jahre.

- **Zugriff der Geheimdienste**
  Bei dem nach Art. 99 Abs. 3 SDÜ zulässigem Zugriff von Geheimdiensten auf das SIS hat sich die Bundesrepublik bisher nicht beteiligt. Die Vorschrift wurde dahingehend geändert, dass vor einer Ausschreibung die Vertragspartei nunmehr nicht mehr verpflichtet ist, die anderen Vertragsparteien zu konsultieren, sondern nur noch zu informieren.

3.2.2
Änderungsvorschläge für ein Informationssystem der nächsten Generation (SIS II)

Folgende Vorschläge sind u. a. in der Diskussion:

- **Übernahme der Daten aus dem Europäischen Haftbefehl**
  Im Rahmenbeschluss des Rates vom 13. Juni 2002 über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedsstaaten (ABl. 2002 L 190/1 der Europäischen Gemeinschaft) ist vorgesehen, dass die für den Europäischen Haftbefehl obligatorischen Daten auch im SIS enthalten sein sollen. Dabei geht es beispielsweise um die Beschreibung der Umstände unter denen die Straftat begangen wurde, um die Art und rechtliche Würdigung der Straftat oder um die verhängte Strafe und andere Folgen der Straftat. Die Gemeinsame Kontrollinstanz vertritt die Auffassung, dass diese Daten in konventioneller Form bei den SIRENE-Büros bleiben und nicht im SIS gespeichert werden sollen.

- **Aufnahme von Lichtbildern, Finderabdrücken und anderen biometrischen Daten**
  Gegen die Aufnahme von Lichtbildern zur Feststellung der Identität einer Person hat die Gemeinsame Kontrollinstanz keine Einwände. Bei den Fingerabdrücken stellt sich schon die Frage nach der Praktikabilität, ob nämlich dem Beamten vor Ort damit geholfen ist, wenn ihm der digitalisierte Fingerabdruck einer Person zur Verfügung steht. Unklar ist noch, ob und welche weiteren biometrischen Daten eingestellt werden und welchen Nutzern, zu welchen Zwecken diese zur Verfügung stehen sollen.

- Zugriff der Kraftfahrzeugregisterstellen auf bestimmte im in Art. 100 SDÜ gespeicherte Sachdaten, um beispielsweise vor Zulassung eines Kfz feststellen zu können, ob es als gestohlen gemeldet wurde.

- Die Forderungen, dass private Kreditinstitute oder auch bestimmte Stellen von Nicht-EU-Staaten im Rahmen der Terrorismusbekämpfung Zugriff erhalten, tauchen immer wieder auf.

Einige dieser Vorschläge werden in einer von der Kommission in Auftrag gegebenen Machbarkeitsstudie für das SIS II diskutiert, die derzeit von der Gemeinsamen Kontrollinstanz geprüft wird.

3.3
Gemeinsame Überprüfung der Ausschreibungen zu Drittausländern

Fast 90 v.H. aller Ausschreibungen sind solche von Drittausländern zur Einreiseverweigerung nach Art. 96 SDÜ. Angesichts dieses Zahlenverhältnisses und verschiedenen Hinweisen, dass es auch Ausschreibungen zu solchen Personen geben soll, die die Voraussetzungen von Art. 96 SDÜ nicht erfüllen (z. B. Globalisierungsgegner), hat die Gemeinsame Kontrollinstanz eine gemeinsame Überprüfung der Ausschreibungen zu Art. 96 SDÜ beschlossen. Zu diesem Zweck wurde ein Fragebogen erarbeitet, mit dem das nationale Verfahren und entsprechende Rechtsgrundlagen erfragt werden sollen. Die abgestimmte Überprüfung soll Anfang 2004 durch die nationalen Datenschutzkontrollinstanzen erfolgen. In Deutschland bedeutet dies, dass neben dem Bundesbeauftragten für den Datenschutz auch die Landesdatenschutzbeauftragten zur Kontrolle aufgerufen sind, da die Ausländerbehörden der Länder die Ausschreibungen vornehmen.

3.4
Überprüfung Europäischer Informationssysteme

Unter der griechischen Ratspräsidentschaft gab es erneut Überlegungen unter anderem die Informationssysteme EUROPOL, SIS, Zollinformationssystem und EURODAC (Europäisches Fingerabdrucksystem) auf Gemeinsamkeiten zu überprüfen. Ziel solcher Pläne ist es, gemeinsame Regelungen für die Informationssysteme zu schaffen - insbesondere auch gemeinsame

Datenschutzvorschriften -, um der jetzigen Zersplitterung der Rechtsgrundlagen und der damit zusammenhängenden Intransparenz entgegenzuwirken. Die Gemeinsame Kontrollinstanz beteiligt sich aktiv an dieser Arbeit und achtet darauf, dass die Datenschutzstandards keinesfalls nach unten verschoben werden.

3.5
Kontrolle des zentralen Teils des Schengener Informationssystems (CSIS)

Die Gemeinsame Kontrollinstanz hat auch im Jahr 2003 eine Prüfung des zentralen Teils des Schengener Informationssystems (CSIS) unternommen. Der hierzu erfolgte Prüfbericht ist als vertraulich eingestuft.

4. Justiz

4.1
Postzensur in Justizvollzugsanstalten

Der Briefwechsel zwischen Insassen von Justizvollzugsanstalten und meiner Dienststelle unterliegt nicht der Postzensur in Justizvollzugsanstalten.

Der Insasse einer hessischen Justizvollzugsanstalt hatte einige Fragen an mich gerichtet, die ich beantwortet hatte. Danach machte er mich darauf aufmerksam, dass ihm die von mir an ihn gerichteten Schreiben geöffnet überreicht worden sind.
Das Strafvollzugsgesetz (StVollzG) regelt dazu in § 29:

§ 29 StVollzG

(1) Der Schriftwechsel des Gefangenen mit seinem Verteidiger wird nicht überwacht. …

(2) Nicht überwacht werden ferner Schreiben des Gefangenen an Volksvertretungen des Bundes und der Länder sowie an deren Mitglieder, soweit die Schreiben an die Anschriften dieser Volksvertretungen gerichtet sind und den Absender zutreffend angeben. Entsprechendes gilt für Schreiben an das Europäische Parlament und dessen Mitglieder, den Europäischen Gerichtshof für Menschenrechte, die Europäische Kommission für Menschenrechte, den Europäischen Ausschuss zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe und die Datenschutzbeauftragten des Bundes und der Länder. Schreiben der in den Sätzen 1 und 2 genannten Stellen, die an den Gefangenen gerichtet sind, werden nicht überwacht, sofern die Identität des Absenders zweifelsfrei feststeht.

(3) Der übrige Schriftwechsel darf überwacht werden, soweit es aus Gründen der Behandlung oder der Sicherheit oder Ordnung der Anstalt erforderlich ist.

Durch die ausdrückliche Aufführung in § 29 Abs. 2 StVollzG ist der Schriftwechsel zwischen Gefangenen und dem Datenschutzbeauftragten von der Postzensur in Justizvollzugsanstalten ausgenommen. Dem entsprach die in dem von dem Gefangenen berichteten Sachverhalt geschilderte Vorgehensweise nicht. Der Strafgefangene hatte deshalb einen Antrag auf gerichtliche Entscheidung gestellt und teilte mir die dem Gericht erteilte Stellungnahme der Anstaltsleitung mit. Danach meinte die Anstaltsleitung, ein Freistempelaufdruck auf einem behördlichen Briefumschlag alleine, genüge nicht, um einen eingehenden Brief dem Absender zuzuordnen. Der Aufdruck könne auch gefälscht sein. Deshalb sei es rechtmäßig gewesen, den Brief zu öffnen.

Ich bat die Anstaltsleitung um Mitteilung wie die Ausnahme von der Postkontrolle bei mir und bei den anderen in § 29 Abs. 2 StVollzG genannten Stellen sichergestellt wird. Die bloße Annahme einer Fälschung des Freistempelaufdruckes reiche meiner Ansicht nach nicht, die gesetzliche Regelung einfach zu ignorieren. Des Weiteren bat ich um Prüfung, ob noch nachvollziehbar ist, dass meine an den Gefangenen gerichteten Briefe, wie ansonsten alle Briefe meiner Behörde, nicht auch im Sichtfenster des Briefumschlages die üblichen Absenderkurzangaben enthielt. In Ihrer Stellungnahme bestätigte die Anstaltsleitung, dass die Briefumschläge deutlich gekennzeichnet waren aber trotzdem geöffnet worden sind. Sie schrieb, dass sie die gegenüber der Strafvollstreckungskammer geäußerte Rechtsauffassung nicht mehr weiter vertrete. Sie entschuldigte sich und sicherte zu, durch organisatorische Maßnahmen sichergestellt zu haben, dass künftig Post meiner Behörde unzensiert weitergeleitet wird. Sollte die Identität einmal unklar sein, werde Kontakt mit mir aufgenommen. Den Gefangenen habe ich entsprechend informiert. Angesichts des Ergebnisses habe ich von einer förmlichen Beanstandung nach § 27 HDSG abgesehen.

5. Polizei und Strafverfolgungsbehörden

5.1
Fortsetzung der Rasterfahndung als Reaktion auf den 11. September 2001

Bei der Durchführung der Rasterfahndung war das Augenmerk verstärkt auf die genaue Abwicklung der einzelnen Ermittlungsschritte zu richten, damit vor allem die Interessen der Vielzahl unbescholtener Studierenden gewahrt wurden.

5.1.1
Richterliche Entscheidung zur Zulässigkeit der Rasterfahndungsmaßnahmen

Die im letzten Jahr beschriebenen Diskussionen (vgl. 31. Tätigkeitsbericht, Ziff. 2.1; 2.3) über die Auslegung des novellierten § 26 des Hessischen Gesetzes über die Sicherheit und Ordnung (HSOG) zu den Voraussetzungen einer rechtmäßigen

Anordnung einer Rasterfahndungsmaßnahme wurden durch eine Entscheidung des Hessischen Verwaltungsgerichtshofes (VGH) vom 30. Januar 2003 (Az.: 10 TG 3113/02) beendet.

§ 26 HSOG

(1) Die Polizeibehörden können von öffentlichen Stellen oder Stellen außerhalb des öffentlichen Bereichs zur Verhütung von Straftaten erheblicher Bedeutung

1. gegen den Bestand oder die Sicherheit des Bundes oder eines Landes oder
2. bei denen Schäden für Leben, Gesundheit oder Freiheit oder gleichgewichtige Schäden für die Umwelt zu erwarten sind,

die Übermittlung von personenbezogenen Daten bestimmter Personengruppen zum Zwecke des automatisierten Abgleichs mit anderen Datenbeständen verlangen, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dies zur Verhütung dieser Straftaten erforderlich und dies auf andere Weise nicht möglich ist. Rechtsvorschriften über ein Berufs- oder besonderes Amtsgeheimnis bleiben unberührt.

(2) Das Übermittlungsersuchen ist auf Namen, Anschriften, Tag und Ort der Geburt sowie auf im einzelnen Falle festzulegende Merkmale zu beschränken. Werden wegen technischer Schwierigkeiten, die mit angemessenem Zeit- oder Kostenaufwand nicht beseitigt werden können, weitere Daten übermittelt, dürfen diese nicht verwertet werden.

(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.

(4) Die Maßnahme nach Abs. 1 bedarf der schriftlich begründeten Anordnung durch die Behördenleitung und der Zustimmung des Landespolizeipräsidiums. Von der Maßnahme ist die oder der Hessische Datenschutzbeauftragte unverzüglich zu unterrichten.

(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.

Der VGH hatte angeführt, dass die Universitäten im Rahmen der Amtshilfe lediglich zu überprüfen hätten, ob das Landeskriminalamt (LKA) zuständig und ob das Vorbringen schlüssig war. Nach der Beurteilung des VGH sei dieses erfolgt, das LKA habe dargelegt, dass die Voraussetzungen des § 26 Abs. 1 HSOG vorlägen, nämlich dass zur Bekämpfung von Straftaten die angeforderten Daten über den beschriebenen Personenkreis benötigt würden.

Daraufhin haben die Universitäten dann auch die Daten geliefert und das LKA hat die Arbeiten wieder aufgenommen.

5.1.2
Reichweite der Auskunftsersuchen betroffener Studenten gegenüber den Hochschulen auf Grundlage des Hessischen Datenschutzgesetzes

§ 18 Abs. 3 HDSG gibt den Betroffenen ein Auskunftsrecht auch über die Empfänger übermittelter Daten.

§ 18 Abs. 3 HDSG

Datenverarbeitende Stellen, die personenbezogene Daten automatisiert speichern, haben dem Betroffenen auf Antrag gebührenfrei Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten,
2. den Zweck und die Rechtsgrundlage der Verarbeitung sowie
3. die Herkunft der Daten und die Empfänger übermittelter Daten, soweit dies gespeichert ist.

In dem Antrag soll die Art der Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden.

Von diesem Recht wollten einige Studierende bei verschiedenen Hochschulen Gebrauch machen. Bei den Hochschulen war allerdings keine Kopie der übermittelten Daten vorhanden, denn dies wäre unzulässig gewesen. Im Rahmen einer ordnungsgemäßen Datenverarbeitung war die nachvollziehbare Dokumentation ausreichend, mit welchem Verfahren aus welchem Datenbestand die zu übermittelnden Daten selektiert worden waren. Für eigene Zwecke benötigten die Hochschulen das Ergebnis dieser Verarbeitung nicht. Deshalb mussten mögliche Sicherheitskopien spätestens nach Abklärung mit dem LKA, dass die gelieferten Datensätze technisch verarbeitbar waren, gelöscht werden.

§ 18 Abs. 3 HDSG stellt die Auskunft ausdrücklich unter den Vorbehalt, dass die entsprechenden Angaben überhaupt gespeichert sind. Hier kommt der Erforderlichkeitsgrundsatz zum Tragen. Eine Speicherung solcher Daten kann nicht damit begründet werden, dass ggf. Auskunftsansprüchen von Betroffenen nachzukommen ist. Die Interessen der Betroffenen

werden auch dadurch gewahrt, dass für die Datenschutzkontrolle nachvollziehbar bleibt, dass die Verarbeitung entsprechend den gesetzlichen Vorgaben erfolgte.

5.1.3
Durchführung des automatisierten Datenabgleichs

Abgeglichen wurden die Daten von Personen, die dem schon im Jahre 2001 festgelegten Profil entsprachen. Betroffen waren daher vor allem Studenten technischer Fachrichtungen aus vorwiegend arabischen Herkunftsländern mit Wohnsitz in Hessen. Dazu wurden die von den Hochschulen angelieferten Datensätze mit Daten aus den Melderegistern und dem Ausländerzentralregister abgeglichen. Ein weiterer Abgleich erfolgte dann beim Bundeskriminalamt (BKA) mit dort erhobenen Daten anderer Stellen, etwa der Besucher von sicherheitsrelevanten Einrichtungen wie Atomkraftwerken.

Dazu wurde beim LKA eine Crime-Datenbank eingerichtet. Entsprechende Datenbanken werden auch in anderen Fällen von der Polizei eingesetzt, um komplexe Vorgänge zu analysieren. Nach Auswertung in der Datenbank wurden die Daten, die dem Raster nicht entsprachen, gelöscht. Gleichzeitig hatte das LKA veranlasst, alle Daten einschließlich der Datenträger, die an das BKA übermittelt worden waren, zu löschen.

Weiterhin aufbewahrt wurden zunächst allerdings sowohl die Datenträger, auf denen die Sätze von den Hochschulen angeliefert worden waren, als auch die jeweils erstellten Sicherheitskopien. Diese lagerten unter Verschluss beim behördlichen Datenschutzbeauftragten des LKA. Nachdem ich dieses kritisiert hatte, sind auch diese Datenbestände gelöscht worden.

5.1.4
Weitere Ermittlungen im Anschluss an den automatisierten Abgleich

Für die übrig gebliebenen Prüffälle wurde jeweils eine Papierakte angelegt. Die weitere Bearbeitung erfolgte dann durch das jeweils örtlich zuständige Polizeipräsidium. Dabei wurden auch weitere Daten bei Dritten erhoben. Grundlage dafür ist § 13 Abs. 1 Nr. 3 HSOG.

§ 13 HSOG

(1) Die Gefahrenabwehr- und die Polizeibehörden können personenbezogene Daten zur Erfüllung ihrer Aufgaben erheben, wenn

…

3. es zur Abwehr einer Gefahr, zur Erfüllung der ihnen durch andere Rechtsvorschriften zugewiesenen weiteren Aufgaben (§ 1 Abs. 2) oder zum Schutz privater Rechte (§ 1 Abs. 3) erforderlich ist, auch über andere als die in den §§ 6 und 7 genannten Personen, oder

…

(6) Personenbezogene Daten sind mit Ausnahme der Fälle des Abs. 1 Nr. 1 und 2 grundsätzlich bei der betroffenen Person zu erheben. Ohne ihre Mitwirkung können sie von anderen Behörden oder öffentlichen Stellen oder von Dritten beschafft werden, wenn sonst die Erfüllung gefahrenabwehrbehördlicher oder polizeilicher Aufgaben gefährdet oder erheblich erschwert würde; besondere gesetzliche Übermittlungsregelungen bleiben unberührt.

Diese Daten durften auch ohne Kenntnis der Betroffenen erhoben werden, da in aller Regel davon auszugehen war, dass aufgrund der besonderen Struktur des zu ermittelnden Personenkreises die Daten nicht unbedingt beim Betroffenen selbst erhoben werden konnten (§ 13 Abs. 6 S. 2 HSOG).

Bei diesen Ermittlungen sollte laufend geprüft werden, ob auf Grund der vorhandenen Erkenntnisse die entsprechende Person aus dem Kreis der Trefferfälle auszuscheiden war und weitere Maßnahmen überflüssig wurden.

In der Praxis stützten sich die ermittelnden Polizeibehörden bei ihren Anfragen zum Teil jedoch statt auf § 13 auf § 26 HSOG. Da dieser Teil der Ermittlungen aber nicht mehr zur Durchführung des automatisierten Abgleichs erfolgte, war dafür kein Raum. Diese Rechtsauffassung wurde auch vom Hessischen Innenministerium bestätigt und die Praxis entsprechend informiert.

Ende Oktober waren etwas über die Hälfte der Trefferfälle durch die zuständigen Präsidien abgearbeitet. Anschließend wurden jeweils die Ergebnisse im LKA geprüft und bewertet. Soweit diese Bewertung ergab, dass die "Person als Schläfer eher auszuschließen ist" wurden die Akten manuell vernichtet und die Einzeldatensätze in der Crime-Datenbank gelöscht. Im Anschluss erfolgte dann die schriftliche Benachrichtigung der Betroffenen gemäß § 26 Abs. 5 HDSG. In diesem Schreiben wurden die Betroffenen jeweils ausdrücklich informiert, dass gegen sie keine Verdachtsmomente vorliegen und dass alle im Zusammenhang mit der Rasterfahndung erhobenen Daten und Akten gelöscht wurden.

Ich gehe davon aus, dass in Kürze diese Aktion insgesamt beendet ist.

5.2
Neue Herausforderungen an die Verwendung der DNA-Analyse im Strafverfahren

Bei der im Grundsatz zu billigenden Ausweitung des Anwendungsbereiches der DNA-Analyse für Zwecke der Strafverfolgung ist gleichwohl Augenmaß zu wahren. Dies gilt vor allem mit Rücksicht auf die rasanten wissenschaftlichen Weiterentwicklungen auf dem Gebiet der Genforschung und Genanalyse.

5.2.1
Ausweitung der gesetzlichen Grundlagen

Im Laufe dieses Jahres wurde wieder verstärkt darüber diskutiert, die gesetzlichen Grundlagen für die Anwendung der DNA-Analyse im Bereich der Strafverfolgung zu überarbeiten. Dabei hatte die Diskussion zwei Schwerpunkte: Zum einen die Überarbeitung der vorhandenen Verfahrensregelungen und zum zweiten die Ausweitungen des Anwendungsbereiches.

5.2.1.1
Verfahren zur Anordnung der DNA-Analyse

Im Bereich der Verfahrensregelungen dreht sich die Diskussion im Wesentlichen um die Notwendigkeit der richterlichen Anordnung der DNA-Analysen. So gewinnen Initiativen an Gewicht, die Notwendigkeit entfallen zu lassen. Begründet werden diese Initiativen, die vor allem aus dem Kreis der Länder bzw. dem Bundesrat gestartet wurden, mit der Gleichsetzung der Identitätsfeststellung mit Hilfe der DNA-Analyse und den üblichen erkennungsdienstlichen Methoden, insbesondere dem klassischen Fingerabdruck. Diese Gleichsetzung überzeugt mich nicht vollständig. Sie würde voraussetzen, dass durch die DNA-Analyse bzw. die Ergebnisse, die in der entsprechenden Datei beim Bundeskriminalamt gespeichert werden, auf keinen Fall andere Informationen als die Feststellung der Identität möglich sind. Durch die weitere wissenschaftliche Entwicklung ist dies aber nicht (mehr) unbedingt gewährleistet. Näheres dazu siehe nachfolgend (Ziff. 5.2.2).

Dabei macht es aus meiner Sicht auch wenig Unterschied, ob zum Zeitpunkt der Untersuchungsanordnung das Untersuchungsmaterial von einem konkreten Beschuldigten stammt oder es um die Auswertung von zurzeit noch nicht einer bestimmten Person zugeordneten Spuren geht. Immer ist Ziel dieser Analysen, eine bestimmte Person zu ermitteln. In der Regel ist auch beabsichtigt, sobald der Täter identifiziert ist, diese Ergebnisse für künftige Ermittlungsverfahren in der entsprechenden Datenbank beim Bundeskriminalamt vorzuhalten. In allen Fällen werden personenbeziehbare Daten verarbeitet, auch wenn der konkrete Bezug zu einer bestimmten Person erst zu einem anderen Zeitpunkt hergestellt werden kann. Das Ziel der Untersuchung ist jedoch gerade die Herstellung dieses Bezuges. Ein Unterschied in der Eingriffsintensität für den Spurenverursacher ist mir daher nicht plausibel.

Der Richtervorbehalt sollte daher aus datenschutzrechtlichen Gründen grundsätzlich weiterhin gewahrt bleiben. Dies schließt Modifikationen nicht aus. In diesem Sinne ist der Gesetzentwurf der Fraktionen der SPD und Bündnis 90/DIE GRÜNEN zur Änderung der Vorschriften über die Straftaten gegen die sexuelle Selbstbestimmung und zur Änderung anderer Vorschriften (BTDrucks. 15/350) zu sehen. Dort ist durch eine entsprechende Ergänzung des § 81g Abs. 3 der Strafprozessordnung (StPO) vorgesehen, dass das Gericht in seiner schriftlichen Begründung einzelfallbezogen darzulegen hat, worauf es seine Entscheidung stützt.

§ 81g Abs. 3 Satz 2 StPO-Entwurf

In der schriftlichen Begründung des Gerichts sind einzelfallbezogen darzulegen

1. im Fall des Absatzes 1 Nr. 1 die für die Beurteilung der Erheblichkeit der Straftat bestimmenden Tatsachen,
2. die Erkenntnisse, auf Grund derer Grund zu der Annahme besteht, dass gegen den Beschuldigten künftig Strafverfahren wegen Straftaten von erheblicher Bedeutung zu führen sein werden, sowie
3. die Abwägung der jeweils maßgeblichen Umstände.

Diese Klarstellung im Gesetz macht den Stellenwert der richterlichen Anordnung deutlich. Sie ist keine Förmelei, sondern dient bei schwerwiegenden Eingriffen in Grundrechte der Wahrung der Interessen der Betroffenen.

Diese Regelung wird nunmehr zum 1. April 2004 in Kraft treten (BGBl. 2003, S. 3007 ff.).

5.2.1.2
Erweiterter Anwendungsbereich der Analysen

Ein Schwerpunkt dieser Diskussionen ist die Erweiterung des Katalogs der Anlasstaten auf Straftaten mit sexuellem Hintergrund. Hauptpunkt der streitigen Diskussion ist dabei der Rahmen, der gezogen werden soll, insbesondere wie weit der sexuelle Bezug einer Straftat reichen soll. Während der erwähnte Entwurf der Koalitionsfraktionen an die Sexualstraftaten im rechtstechnischen Sinne, wie sie im Strafgesetzbuch eingeordnet sind, anknüpft, gehen andere Vorschläge darüber hinaus und fordern in unterschiedlicher Ausprägung die Aufnahme zusätzlicher Delikte in den Katalog bis hin zu allen Vergehen, wenn die Tat einen sexuellen Hintergrund aufweist. Eine präzise Definition bleibt dabei offen.

Einigkeit besteht insoweit, dass zukünftig bei der Analyse der Proben nicht nur das definierte Identifizierungsmuster durch die Labors ermittelt, sondern auch das Geschlecht festgestellt werden darf. Dies fand in der Praxis häufig schon bisher statt, da die Standardverfahren, die den Labors zur Verfügung standen, dies so vorsahen. Andere waren offensichtlich auf dem

Markt nicht zu erhalten. In der Regel erfolgt damit auch keine Feststellung, die nicht schon aus anderen Gründen bekannt war.

Die Diskussion aller Vorschläge wurde im laufenden Jahr nicht abgeschlossen. Die Justizministerkonferenz hat im Mai eine Arbeitsgruppe eingesetzt, die unter anderem eine Expertenanhörung durchführen soll. Ein Ergebnis wird nicht vor Juni 2004 erwartet.

Nunmehr gibt es auch Überlegungen, die DNA-Analyse präventiv bei der Polizei auch dann einzusetzen, wenn die Regelungen der StPO nicht greifen - etwa bei strafunmündigen Kindern. Einen solchen Vorschlag enthält z. B. ein zum Ende des Berichtsjahres vorgelegter Entwurf zur Novelle des Hessischen Gesetzes für die öffentliche Sicherheit und Ordnung.

5.2.2
Neue Erkenntnisse der Forschung

Erstmals im Jahre 1997 hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung die aus Sicht des Datenschutzes notwendigen Anforderungen an den Einsatz dieser Methode bzw. den Aufbau einer entsprechenden Datenbank formuliert (vgl. 26. Tätigkeitsbericht, Ziff. 25.2). Schon damals hatte die Konferenz Vorkehrungen gefordert, falls durch weitere wissenschaftliche Erkenntnisse auch aus dem Vorhandensein bzw. der Struktur der so genannten nicht-codierenden Abschnitte Rückschlüsse auf die genetische Disposition der Untersuchten möglich erscheinen.

5.2.2.1
Struktur der durch DNA-Analyse gewonnenen Daten

Die DNA-Analyse zur Identitätsfeststellung macht sich zu Nutze, dass auf den Genen so genannten Short-Tandem-Repeats (STR) vorhanden sind, bei denen eine bestimmte Basenabfolge mehrmals wiederholt wird (z. B. TCA – TCA – TCA). Aufgrund von Forschungen an anderen Lebewesen ist man sich relativ sicher, dass diese STR selbst keine Funktion für die Produktion von Aminosäuren und damit als Erbanlage haben.

Es gibt eine Vielzahl dieser STR. Die Anzahl der Wiederholungen ist individuell verschiedenen. Sie unterliegt der Vererbung. Wenn beispielsweise STR 1 bei einem Elternteil 15- und beim anderen Elternteil 14-mal wiederholt wird, ist eine entsprechende Kombination auch beim Kind feststellbar (also z. B. A 15, 14; B 14; C 13, 15; D 12, 14). Darauf beruht letztlich im Sinne eines mathematischen Wahrscheinlichkeitsverfahrens auch die Identitätsfeststellung. Wenn für mehrere STR die entsprechenden Werte festgestellt werden, ergibt sich aus der Kombination eine eindeutige Zuordnung zu einer Person.

Diese Ergebnisse, d. h. die jeweiligen Zahlenkombinationen sind im Übrigen auch das, was als DNA-Muster in der Datei beim Bundeskriminalamt (BKA) gespeichert wird. Die Vergleichbarkeit mit den Ergebnissen der Untersuchung anderer Proben (auch durch andere Labors zu anderen Zeitpunkten) wird dadurch sichergestellt, dass immer genau definierte STR ausgewertet werden; für diese gibt es eine weltweit eindeutige Nomenklatur.

Die Verteilung der einzelnen Wiederholungen pro Merkmal ist unterschiedlich, u. a. bei verschiedener ethnischer Herkunft. Deshalb muss zur Ableitung der Wahrscheinlichkeiten auch die Verteilung der Merkmalsgruppen in bestimmten Bevölkerungsgruppen erforscht sein. Dazu werden Übersichten der Häufigkeitsverteilungen angelegt. Daraus ließe sich z. B. grundsätzlich auch ablesen, ob es sich bei einer Probe wahrscheinlich um die eines Weißen oder eines Farbigen handelt. Für die Anwendung in der Praxis ist zu berücksichtigen, dass eine solche Wahrscheinlichkeitsfeststellung der Merkmalsverteilung bzw. die Rückschlüsse daraus im Rahmen der deutschen Untersuchungen (Auswertung von acht festgelegten STR) noch zu vage sind. Eine Auswertung der Analyseergebnisse über die gesetzlich erlaubte Identitätsfeststellung hinaus würde derzeit daher wohl nicht zu einem sinnvoll verwertbaren Ergebnis führen.

5.2.2.2
Indirekte Aussagen der STR über genetische Merkmale

Eine weitere schon häufiger geäußerte These lautet: diese STR sind zwar selber nicht codierend, aber bestimmte dieser STR treten immer in Nachbarschaft bestimmter Gene auf.

Es liegt zwischenzeitlich das Ergebnis einer Forschergruppe vor, die versucht hat, dies am Beispiel der Schizophrenie zu belegen. Dazu wurde die Verteilung eines bestimmten STR untersucht. Die Gene, die die Anlage zur Schizophrenie begründen, sind bekannt. Das Team hat als Ergebnis seiner Untersuchung festgestellt, dass bei dem untersuchten Personenkreis das ausgewählte STR in einer bestimmten Häufigkeit auftaucht, die nicht mit der durchschnittlichen Häufigkeit der Bevölkerungsgruppe, der die Erkrankten angehören, übereinstimmt. Daraus hat es geschlossen, dass das Auftreten des STR in dieser Häufigkeit ein Indiz für die Anlage zur Schizophrenie sein kann. Dies ist zwar noch kein absoluter wissenschaftlicher Beweis, diese Ergebnisse konnten aber auch noch nicht widerlegt werden.

Ein weiteres Beispiel für indirekte Erkenntnisse und damit zusätzliche Informationen aus den Angaben zum Auftreten bestimmter STR hat der parlamentarische Staatssekretär im Bundesjustizministerium auf eine schriftliche Anfrage der Abgeordneten Piltz angeführt (BTDrucks. 15/1513 S. 25). Bei Personen mit Down-Syndrom tritt das Chromosom 21 in den Körperzellen nicht 2fach, sondern 3fach auf. Falls es auf diesen Chromosomen drei unterschiedliche Ausprägungen des untersuchten Merkmalssystems gibt, wird dies im Identifizierungsmuster erkannt. Dies stellt nach Aussage der Fachleute zwar wohl keine sichere Diagnose, aber doch ein Indiz für das Vorliegen des Trisomie 21 dar.

Durch die in der Praxis eingesetzten Untersuchungsverfahren sind grundsätzlich im Rahmen der DNA-Analyse auch andere Erkrankungen erkennbar, die auf Unregelmäßigkeiten der Chromosomen beruhen. Eine solche Chromosomenanomalie bezogen auf die Zahl der X-Chromosomen tritt beim Klinefelter-Syndrom auf, das etwa 2 v.H. der männlichen Bevölkerung betrifft.

Die Beobachtung solcher Erkenntnisse ist vor allem auch deshalb wichtig, da zwar in der Datenbank beim BKA nicht genetisches Material enthalten ist, aber die Zahlenkombinationen gespeichert werden, aus denen sich ablesen lässt, welches Merkmal wie häufig vertreten ist. Und genau aus diesen Angaben lassen sich ja möglicherweise die entsprechenden Rückschlüsse ziehen.

Diese Punkte waren letztlich auch Grundlage für die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. Juli 2003 "Bei der Erweiterung der DNA-Analyse Augenmaß bewahren" (vgl. Ziff. 20.10 dieses Tätigkeitsberichts). Dies bedeutet aus meiner Sicht, dass die Erweiterung datenschutzrechtlich grundsätzlich nicht ausgeschlossen ist, dass es aber gilt, einen Dammbruch zu verhindern.

5.3
Fehlende Rechtsgrundlagen für Massenscreenings

Für die immer häufiger zum Einsatz kommenden Massenuntersuchungen auf freiwilliger Basis gibt es derzeit keine ausreichende Rechtsgrundlage.

Bei der Aufklärung von schweren Straftaten greift die Polizei – auch auf Grund der verbesserten technischen Möglichkeiten bzw. Erfolgssaussichten – immer häufiger auch zum Einsatz der DNA-Analyse im Rahmen so genannten Massenscreenings. Eine nach bestimmten Kriterien zusammengesetzte Gruppe der Bevölkerung mit einem bestimmten Bezug zum Tatort oder Opfer wird gebeten, auf freiwilliger Basis Daten zur Verfügung zu stellen. Die Besonderheit in diesen Fällen ist, dass zusätzlich zu dem Auswahlmerkmal über den Personenkreis keine weiteren Erkenntnisse mit einem Zusammenhang zu der aufzuklärenden Straftat vorliegen. Deshalb kommt eine richterliche Anordnung der Teilnahme am Test im Rahmen des § 81f StPO nicht in Betracht, denn ein hinreichender Tatverdacht zur Begründung der Eigenschaft als Beschuldigter liegt ja gerade nicht vor.

Inzwischen bin ich von Seiten der Staatsanwaltschaft in mehreren Fällen, in denen nicht eine DNA-Analyse Untersuchungsgegenstand sein sollte, gebeten worden, aus datenschutzrechtlicher Sicht zum Einsatz von Massenscreenring-Verfahren auf Grund freiwilliger Beteiligung Stellung zu nehmen.

In diesen Fällen sollte ein größerer Personenkreis - in einem Fall ca. 500, in einem anderen 15.000 Personen - auf "freiwilliger" Basis Fingerabdrücke abgeben. Diese sollten mit Tatortspuren abgeglichen werden. Der Personenkreis wurde jeweils nach einem Profiling durch die Polizei abgegrenzt, nachdem andere Ermittlungsmaßnahmen nicht zum Erfolg führten.

In den mir bekannten Fällen habe ich auf Grund der Tatumstände durchaus Verständnis für das Ansinnen der Strafverfolgungsorgane und der Polizei, alles Denkbare zu versuchen, die Taten aufzuklären. Andererseits darf man in diesem Zusammenhang nicht außer Acht lassen, dass dieser Ermittlungsansatz sich nicht unwesentlich von den sonstigen Mitteln, die unser Rechtsstaat zu Verfügung stellt, unterscheidet. Diesen Ermittlungsmaßnahmen ist immanent, dass in großem Umfang Daten Nichtbeschuldigter erhoben werden. Im Grunde müssen diese mit der Teilnahme an den Massentests ihre Unschuld nachweisen. Die Verfahren zielen darauf ab, dass durch den sozialen Druck im Umfeld der Kreis der Personen, die sich nicht beteiligen, so gering wie möglich gehalten wird.

Auf Grund dieser Sachlage ist die Freiwilligkeit fragwürdig. Dies gilt in den Fällen der DNA-Analyse erst Recht dann, wenn in den Aufforderungen zur Teilnahme darauf hingewiesen wird, dass andernfalls ggf. ein Richter die Entnahme des Materials anordnen könnte. Die Nicht-Teilnahme an einem solchen "freiwilligen" Screening kann aber in aller Regel nicht ausreichend sein, den vorher nicht vorhandenen Tatverdacht zu begründen und diese Personen nunmehr als Beschuldigte anzusehen.

Ein solch schwerwiegender Eingriff in das Recht auf informationelle Selbstbestimmung bedarf einer ausreichenden Rechtsgrundlage. Eine solche ist derzeit weder in der Strafprozessordnung noch für präventivpolizeiliche Zwecke im Hessischen Gesetz über die Öffentliche Sicherheit und Ordnung enthalten.

Festzulegen wäre zum einen der Bereich der Straftaten, für deren Aufklärung ein solches Instrumentarium eingesetzt werden darf, bzw. für den präventiven Bereich eine genaue Definition der vorliegenden Gefahrensituation. Darüber hinaus müssten eine strikte Zweckbindung der so erhobenen Daten sowie kurze Löschungsfristen festgelegt werden.

Ich habe die Hessischen Minister der Justiz und des Inneren aufgefordert, entsprechend tätig zu werden.

Unabhängig von diesen grundsätzlichen Bedenken, habe ich in den Fällen, in denen die Staatsanwaltschaften darum gebeten hatten, mich bemüht, die jeweiligen Verfahrensabläufe so auszugestalten, dass die Rechte der Betroffenen gewahrt wurden. Dazu gehörte eine ausreichende Information, die sorgfältige Formulierung der Einwilligungserklärung, Festlegung der Aufbewahrungsdauer der Untersuchungsmaterialien und -ergebnisse sowie Festlegungen zur Wahrung einer strikten Zweckbindung.

5.4
Diskrete Ladung zur Vorsprache bei der Polizei

Bei der Organisation von Arbeitsabläufen innerhalb der Verwaltung sollten auch datenschutzrechtliche Auswirkungen vorab bedacht werden.

Ein Petent hatte sich bei mir beschwert über die Art, wie ihm eine Vorladung der Polizei zugestellt wurde. Er war aufgefordert worden, bei der Polizei zur Abgabe einer Speichelprobe vorzusprechen. Im Anschreiben war darauf hingewiesen worden, dass man das Verfahren möglichst diskret abwickeln wolle.

Der Brief war zusätzlich zum Freistempler auf der Rückseite mit einem roten Stempelaufdruck versehen:

Polizeipräsidium, Kriminaldirektion
K40/SG 42 – Erkennungsdienst –

Handschriftlich war hinzugefügt:

AG-DNA sowie ein Namenskürzel.

Mit einer solchen Kennzeichnung wird m. E. in das Recht auf informationelle Selbstbestimmung des Empfängers des Briefes eingegriffen. Ein solcher Aufdruck gibt Informationen zur Kenntnis aller der Personen, die zwangsläufig mit dem Umschlag in Kontakt kommen, die deutlich mehr aussagen – und damit auch zu Spekulationen bzw. Eindrücken über den Empfänger Anlass geben – als der Aufdruck des Freistemplers des Polizeipräsidiums. Dies gilt natürlich erst recht in einem Fall wie diesem, wo neben dem Hinweis auf den Erkennungsdienst auch noch der sprechende Verweis auf eine AG-DNA enthalten ist.

Eine solche Kennzeichnung ist m. E. auch für einen geordneten Ablauf innerhalb der Verwaltung nicht notwendig. Für Antworten auf ein solches Schreiben wird sich der Empfänger in der Regel auf die im Schreiben befindlichen Angaben wie Aktenzeichen etc. beziehen.

Soweit es darum geht, unzustellbare Rückläufer ohne großen Aufwand zuzuordnen - und dies ggf. auch ohne die Notwendigkeit, dass ein größerer Personenkreis in der Behörde den Inhalt des Schreibens zur Kenntnis nehmen muss - kann dies auch auf anderem Wege erfolgen. Dazu würde z. B. auch ausreichen, wenn ein Schreiben als zusätzliche Kennzeichen lediglich die entsprechende Kurzbezeichnung - hier etwa SG 42 - enthielte. Diese wäre nach außen nur sehr viel eingeschränkter sprechend.

Das betroffene Polizeipräsidium hat meine Einschätzung geteilt, sich bei dem Petenten entschuldigt und versichert, dass zukünftig eine solche Kennzeichnung nicht mehr erfolgen würde.

5.5
Anfertigung von Fotografien bei Demonstrationen

In mehreren Fällen habe ich die Rechtmäßigkeit der Datenerhebung durch die Polizei bei Demonstrationsteilnehmern überprüft. Außerdem wurde geprüft, ob die Datenerhebungen zu Datenspeicherungen führten. Die Datenschutzbestimmungen waren eingehalten.

Im Berichtszeitraum wandten sich mehrere Personen an mich, die berichteten, sie seien - manche gezielt, manche unbeabsichtigt - in eine Demonstration geraten. Sie schilderten z. B., Polizeikräfte hätten die Straße abgeriegelt und von allen Anwesenden Lichtbilder angefertigt und ihre Personalien aufgenommen. Es wendeten sich auch Eltern minderjähriger Kinder an mich, die ähnliche Schilderungen ihrer Kinder wiedergaben. Zum Teil wurde auch geschildert, dass Videoaufnahmen angefertigt wurden. Die Beschwerdeführer fragten jeweils, ob die Erhebung der personenbezogenen Daten rechtmäßig war, was mit den Lichtbildern und Videoaufnahmen geschieht und ob die Daten nun in einer Datei über Demonstranten oder Ähnlichem gespeichert sind. Sie verlangten die Löschung ihrer Daten bzw. der Daten ihrer Kinder.

Ich habe die Anfrager jeweils auf die Regelung in § 14 Abs. 2 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) aufmerksam gemacht.

§ 14 Abs. 2 HSOG

Die Polizeibehörden können personenbezogene Daten auch über andere als die in den §§ 6 und 7 genannten Personen bei oder im Zusammenhang mit öffentlichen Versammlungen oder Aufzügen erheben, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass bei oder im Zusammenhang mit der Versammlung oder dem Aufzug Straftaten drohen. Die Unterlagen sind unverzüglich nach Beendigung der Versammlung oder des Aufzuges oder zeitlich und sachlich damit unmittelbar in Zusammenhang stehender Geschehnisse zu vernichten, soweit sie nicht zur Abwehr einer Gefahr, zur Verfolgung einer Straftat oder Ordnungswidrigkeit oder zur Strafvollstreckung benötigt werden. Eine Verarbeitung für andere Zwecke ist unzulässig. § 20 Abs. 7 bleibt unberührt.

Mit der gesetzlichen Beschreibung "*wenn … Anhaltspunkte die Annahme rechtfertigen, dass … Straftaten drohen*" ist die Schwelle, ab wann die Polizei Daten bei öffentlichen Versammlungen oder Aufzügen erheben darf, sehr niedrig. Andererseits muss, wenn die Daten nicht in ein Strafverfahren (etc. s. Zitat) überführt werden, unverzüglich nach Beendigung der Versammlung, gelöscht werden.

Schwierig ist es, die Befugnis nach § 14 Abs. 2 HSOG gegenüber der Befugnis nach den Vorschriften des Versammlungsgesetzes (VersammlG) abzugrenzen. Einschlägig ist hier § 12a.

§ 12a VersammlG

(1) Die Polizei darf Bild- und Tonaufnahmen von Teilnehmern bei oder im Zusammenhang mit öffentlichen Versammlungen nur anfertigen, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass von ihnen erhebliche Gefahren für die öffentliche Sicherheit oder Ordnung ausgehen. Die Maßnahmen dürfen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

(2) Die Unterlagen sind nach Beendigung der öffentlichen Versammlung oder zeitlich und sachlich damit unmittelbar im Zusammenhang stehender Ereignisse unverzüglich zu vernichten, soweit sie nicht benötigt werden

1. für die Verfolgung von Straftaten von Teilnehmern oder
2. im Einzelfall zur Gefahrenabwehr, weil die betroffene Person verdächtig ist, Straftaten bei oder im Zusammenhang mit der öffentlichen Versammlung vorbereitet oder begangen zu haben, und deshalb zu besorgen ist, dass von ihr erhebliche Gefahren für künftige öffentliche Versammlungen oder Aufzüge ausgehen.

Unterlagen, die aus den in Satz 1 Nr. 2 aufgeführten Gründen nicht vernichtet wurden, sind in jedem Fall spätestens nach Ablauf von drei Jahren seit ihrer Entstehung zu vernichten, es sei denn, sie würden inzwischen zu dem in Satz 1 Nr. 1 aufgeführten Zweck benötigt.

(3) Die Befugnisse zur Erhebung personenbezogener Informationen nach Maßgabe der Strafprozessordnung und des Gesetzes über Ordnungswidrigkeiten bleibt unberührt.

Diese Vorschrift gilt sowohl für öffentliche Veranstaltungen in geschlossenen Räumen als auch gemäß § 19a VersammlG für Versammlungen unter freiem Himmel und Aufzüge. Soweit die Vorschriften des Versammlungsgesetzes einschlägig sind, also wenn es sich um eine Versammlung im Sinne des Versammlungsgesetzes handelt und soweit es um Bild- und Tonaufzeichnungen geht, verdrängen sie als bundesgesetzliche Regelung die Anwendung des ähnlich gefassten aber allgemein auf "Datenerhebungen" abgestellten § 14 Abs. 2 HSOG. Die landesgesetzliche Regelung im HSOG gilt darüber hinaus auch für so genannte Spontanversammlungen, für die es in der Regel keinen Veranstalter oder Leiter gibt und deshalb das Versammlungsgesetz nicht zur Anwendung kommt.

Bei allen Demonstrationen, bei denen mich Betroffene eingeschaltet hatten, habe ich nachvollziehen können, dass tatsächlich konkrete Anhaltspunkte vorlagen, dass Straftaten drohen. In jedem Einzelfall war auch die Voraussetzung des § 12a VersammlG erfüllt. Tatsächliche Anhaltspunkte rechtfertigten die Annahme, dass von der Versammlung erhebliche Gefahren für die öffentliche Sicherheit und Ordnung ausgehen. Meist handelte es sich um unangemeldete Gegendemonstrationen zu Demonstrationen von Rechtsextremisten wobei u. a. in öffentlichen Aufrufen davon die Rede war "um jeden Preis" oder "auch mit Gewalt" den Aufzug der Rechtsextremisten zu verhindern. Insofern war die Polizei zur Datenerhebung, auch zur Anfertigung von Bild- und Tonaufnahmen, befugt. Ich konnte aber auch feststellen, dass in keinem der von mir überprüften Fälle Datenspeicherungen zu den Anfragern vorlagen. Die Registrierung am Demonstrationsort führte also nicht zu einer Datenspeicherung in einem polizeilichen Informationssystem. Die Lichtbilder und Videodokumentationen - so versicherte mir jeweils die Polizei - sind vernichtet bzw. überspielt worden. Vermerke, in denen die Vernichtung dokumentiert wurde, habe ich zum Teil eingesehen.

5.6
Gefährderansprache durch die Polizei

Durch eine Gefährderansprache erlangte ein Betroffener den Eindruck, die Polizei speichere Daten über ihn. Da ein Auskunftsersuchen bei der Polizei keine Datenspeicherung ergab, wandte er sich an mich. Ich stellte fest, dass der Gefährderansprache eine zulässige Datensammlung und Datenübermittlung des Landesamtes für Verfassungsschutz zugrunde lag.

Im Vorfeld einer Großdemonstration zum 1. Mai wurde der Betroffene von der Polizei gefragt, ob er beabsichtige an der Demonstration teilzunehmen. Ausdrücklich wurde darauf hingewiesen, dass Störungen der öffentlichen Sicherheit und Ordnung im Zusammenhang mit der Veranstaltung nicht geduldet würden. Auf Nachfrage, weshalb er dazu befragt werde, erklärte der Polizeibeamte, er sei doch schon im Vorjahr im Kreise der Gegendemonstranten gewesen und doch schon einmal bei einer Durchsuchung in einem dem linken Spektrum zugeordneten Café verhaftet worden. Verwundert über diese Ansprache und die Kenntnis dieser Details, fragte der Betroffene über einen Rechtsanwalt schriftlich bei der Polizei nach, welche Daten dort zu seiner Person gespeichert sind. Die Antwort - es seien keine gespeichert - glaubte er nicht. In einem zweiten Schreiben fragte er deshalb nach, ob die Aussage wirklich alle Dateien auch schutzpolizeiliche, kriminalpolizeiliche, staatsschutzpolizeiliche und verwaltungspolizeiliche Dateien betreffe. Die Polizei erläuterte, die Aussage, es seien keine Daten zu der Person gespeichert, sei umfassend, alle nachgefragten Bereiche seien damit gemeint. Sie fügte ihm sogar einen Auszug aus einem Computerausdruck bei. Daraus war ersichtlich, dass im polizeilichen Auskunftssystem POLAS unter Angabe der Personalien des Betroffenen die Antwort des Systems "0 Treffer" lautete. Ein gleiches Ergebnis - so das Polizeipräsidium - werde bei der Abfrage im nationalen und im internationalen Informationssystem erreicht. In zwei Schreiben wandte der Betroffene sich an das Landeskriminalamt; mit demselben Ergebnis: keine Datenspeicherungen. Nun schrieb er noch einmal das Polizeipräsidium an, schilderte das Gespräch mit dem Polizeibeamten und fragte, wieso er auf die eventuelle Teilnahme an der anstehenden Demonstration angesprochen worden war. Daraufhin erläuterte die Polizei, dass er Adressat einer so genannten Gefährderansprache gewesen sei. Diese Maßnahme sei grundsätzlich ein geeignetes

präventives Instrument, um mögliches Störerpotenzial bereits im Vorfeld von Veranstaltungen, bei denen mit einem gewalttätigen Verlauf gerechnet werden müsse, darauf hinzuweisen, dass Störungen der öffentlichen Sicherheit nicht geduldet würden. Die Maßnahme werde - insbesondere vor dem Hintergrund der polizeilichen Erfahrung aus vorherigen Einsatzlagen - als der Gefahrenabwehr dienlich angesehen und sei von § 11 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) gedeckt. Sie sei bei Personen eingesetzt worden, bei denen aus der Vergangenheit Erkenntnisse im Zusammenhang mit gewalttätigen Auseinandersetzungen anlässlich von Demonstrationen vorlägen. Also - so die Schlussfolgerung des Betroffenen - müssten doch Daten zu seiner Person gespeichert sein und die früheren Auskünfte seien falsch. Er wandte sich an mich. Ich griff den Widerspruch auf und bat das Polizeipräsidium um Stellungnahme zu der anscheinend falschen Auskunft.

Das Polizeipräsidium versicherte mir, es gebe tatsächlich weder in automatisierten noch in nichtautomatisierten Dateien der Behörde eine Information über den Betroffenen. Die Details, mit denen der Beamte ihn konfrontierte, stammten aus dem Erinnerungsvermögen. Der Beamte arbeite schon lange in der Staatsschutzabteilung des Präsidiums. Er sei ein "ausgesprochener Kenner der Szene" und sei bei der von ihm erwähnten Verhaftung zugegen gewesen. Ebenso sei er bei der Demonstration am Vorjahrestag im Einsatz gewesen. Er könne die betroffene Person sogar näher beschreiben, obwohl eine Speicherung in Dateien nicht existiere. Die Gefährderansprachen seien auch durch die Polizei lediglich ausgeführt worden. Die Festlegung des Personenkreises sei nicht durch die Polizei erfolgt, sondern das Hessische Landesamt für Verfassungsschutz habe aus seinen Erkenntnissen eine Liste von Personen zusammengestellt, die mit der Gefährderansprache dazu bewegt werden sollten, sich bei einer Teilnahme an der Demonstration friedlich zu verhalten. In dieser Liste war auch der Betroffene aufgeführt. Damit war der Widerspruch, der sich zunächst offenbart hatte, ausgeräumt. Die Erklärung über die Sachkenntnis des Beamten war schlüssig und die Löschungsgebote der Datenschutzbestimmungen finden Grenzen im Erinnerungsvermögen der Bediensteten. Dass die Daten in einer Liste aufgeführt sind, widerspricht nicht der Aussage, dass sie nicht in Dateien gespeichert sind. Sie tauchen zwar auf einer Liste mit Namen für vorgeschlagene Gefährderansprachen auf, doch diese Information lies sich nur mit unverhältnismäßig hohem Aufwand anhand der Personalien des Anfragers erschließen. Listen können Bestandteile von Akten (§ 2 Abs. 7 HDSG) sein. Sie sind aber keine Dateien im Sinne des Datenschutzrechts (§ 2 Abs. 8 HDSG). Folgerichtig bezieht sich das Einsichtsrecht auf Akten nach § 18 Abs. 5 HDSG zunächst auf Akten, die zur Person des Betroffenen geführt werden. Werden die Akten aber nicht zur Person des Betroffenen geführt, so müssen Angaben gemacht werden, die das Auffinden der personenbezogenen Daten möglich machen. Im vorliegenden Falle war dies erst gegeben, als in der Anfrage der Bezug zu der Gefährderansprache gemacht wurde. Die entsprechende Regelung im Polizeirecht, die nicht Akteneinsicht aber Auskunft vorsieht ist § 29 Abs. 1 HSOG.

§ 2 Abs. 7 und Abs. 8 HDSG

(7) Eine Akte ist jede der Aufgabenerfüllung dienende Unterlage, die nicht Teil der automatisierten Datenverarbeitung ist.

(8) Soweit andere landesrechtliche Vorschriften den Dateibegriff verwenden, ist Datei

1. eine Sammlung von Daten, die durch automatisierte Verfahren ausgewertet werden kann (automatisierte Datei), oder
2. eine gleichartig aufgebaute Sammlung von Daten, die nach bestimmten Merkmalen geordnet und ausgewertet werden kann (nicht automatisierte Datei).

§ 18 Abs. 5 HDSG

Sind personenbezogene Daten in Akten gespeichert, die zur Person des Betroffenen geführt werden, dann kann er bei der speichernden Stelle Einsicht in die von ihm bezeichneten Akten verlangen. Werden die Akten nicht zur Person des Betroffenen geführt, hat er Angaben zu machen, die das Auffinden der zu seiner Person gespeicherten Daten mit angemessenem Aufwand ermöglichen.

Ich habe mir vor Ort die Liste angesehen und konnte die Ausführungen der Polizei bestätigen: Die Liste wurde vom Hessischen Landesamt für Verfassungsschutz erstellt. In ihr sind Personen aufgelistet, gegliedert in die Bereiche Rechts-, Links- und Ausländerextremismus, die nach Einschätzung dieser Behörde für präventiv-polizeiliche Maßnahmen in Frage kommen. Als präventiv-polizeiliche Maßnahmen waren Gefährderansprachen, begründet auf § 11 HSOG sowie Unterbindungsgewahrsam nach § 32 HSOG erwogen.

Zusammenfassend konnte ich aus datenschutzrechtlicher Sicht den Vorwurf nicht bestätigen, dass das Polizeipräsidium falsche oder unvollständige Auskünfte über Datenspeicherungen erteilt hat.

Da die Liste vom Hessischen Landesamt für Verfassungsschutz (LfV) stammt, drängte sich die Frage auf, ob die mit der Übersendung der Liste verbundene Datenübermittlung sowie die dieser Datenübermittlung zugrunde liegende Datensammlung rechtmäßig sind. Ich bin dem nachgegangen und habe beim LfV die infrage kommenden Unterlagen eingesehen. Dabei habe ich festgestellt, dass das Sammeln von Daten über den Betroffenen der Aufgabenstellung dieser Behörde nach § 2 Abs. 1 und 2 LfV-Gesetz entspricht.

§ 2 LfV-Gesetz

(1) Aufgabe des Landesamtes für Verfassungsschutz ist es, den zuständigen Stellen zu ermöglichen, rechtzeitig die erforderlichen Maßnahmen zur Abwehr von Gefahren für die Länder zu treffen. Das Landesamt für Verfassungsschutz dient auch dem Schutz vor organisierter Kriminalität.

(2) Zur Erfüllung dieser Aufgaben beobachtet das Landesamt für Verfassungsschutz

1. Bestrebungen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind oder eine ungesetzliche Beeinträchtigung der Amtsführung der Verfassungsorgane des Bundes oder eines Landes oder ihrer Mitglieder zum Ziele haben,

Es sammelt zu diesem Zweck Informationen, insbesondere sach- und personenbezogene Auskünfte, Nachrichten und Unterlagen, über solche Bestrebungen oder Tätigkeiten und wertet sie aus.

Auch die Übermittlung der Daten an die Polizei entspricht der rechtmäßigen Aufgabenwahrnehmung der Verfassungsschutzbehörde. Sie war gemäß § 11 Abs. 1 Nr. 3 LfV-Gesetz rechtmäßig und konnte von mir nicht beanstandet werden.

§ 11 Abs. 1 Nr. 3 LfV-Gesetz

Die Übermittlung ist über die §§ 9 und 10 hinaus zulässig an

3. Polizei- und Ordnungsbehörden, wenn dies zu ihrer Aufgabenerfüllung erforderlich ist und die Übermittlung der Abwehr einer im Einzelfall bestehenden erheblichen Gefahr oder zur Verhütung der in Nr. 2 genannten Straftaten sowie von Verbrechen, für deren Vorbereitung konkrete Hinweise vorliegen, dient.

Am Vorliegen dieser Voraussetzung gab es nach den Erkenntnissen der Sicherheitsbehörden keinen Zweifel.

Den Betroffenen habe ich informiert.

5.7
Gelöscht und doch nicht gelöscht

Gibt die Polizei einem Antrag des Betroffenen auf Löschung seiner Daten statt, muss sie sicherstellen, dass die Daten in allen polizeilichen Dateien gelöscht werden.

Ein Fernsehmoderator wurde beschuldigt, einen Mord geplant zu haben. Er beabsichtige - so eine ausländische Polizeibehörde in einem Fax an die deutsche Polizei - vor laufender Kamera einen politisch motivierten Mord zu begehen. Unter weiteren Angaben wurden, neben der unmittelbar bevorstehenden angeblichen Tatzeit, der Fernsehmoderator, ein Mittäter und das Opfer namentlich benannt. Es liegt auf der Hand, dass die Polizei sofort handeln musste. Der Fernsehmoderator wurde verhaftet; doch er bestritt den Plan. Sein Büro, seine Wohnung und sein Auto wurden durchsucht. Es wurden Fingerabdrücke genommen, er wurde fotografiert und es fanden umfangreiche Ermittlungen statt. Es wurde nichts gefunden. Alle Ermittlungen verliefen "im Sande". Das Verfahren wurde eingestellt. Danach beantragte der Fernsehmoderator die Löschung seiner Daten bei der Polizei. Die Polizei gab dem Antrag statt und bestätigte ihm die Löschung.

In der Folgezeit machte der Fernsehmoderator Wahrnehmungen, die ihn an der Löschung zweifeln ließen. Er wandte sich an mich. Nach Auskunft durch das Landeskriminalamt habe ich ihm mitgeteilt, dass im hessischen polizeilichen Auskunftssystem POLAS keine Daten zu seiner Person gespeichert seien und dass auch keine Datenspeicherung im bundesweiten Datenbestand der Polizei (INPOL) durch hessische Polizeibehörden veranlasst sei. Ebenso werde keine Akte zu seiner Person geführt. Nach einiger Zeit meldete der Fernsehmoderator sich erneut und konkretisierte seine Zweifel an der Löschung der Daten. Er nannte eine Bundesbehörde, die ihm "aus Sicherheitsgründen" eine Genehmigung versagt hatte. Außerdem sei er im Rahmen seiner journalistischen Tätigkeit von Beamten einer Bundespolizeibehörde vorläufig in Gewahrsam genommen und später unter Hinweis auf ein Versehen wieder entlassen worden. Daraufhin wurde der Bundesbeauftragte für den Datenschutz eingeschaltet. Auf dessen Veranlassung stellte das Bundeskriminalamt nun doch eine Datenspeicherung fest, für die eine hessische Polizeibehörde verantwortlich war. Es handelte sich um die Polizeibehörde, die wegen des angeblichen Mordkomplotts ermittelt hatte. Das Bundeskriminalamt informierte das Landeskriminalamt. Der Bundesdatenschutzbeauftragte informierte mich. Nun stellte sich heraus, dass trotz der Löschung in POLAS noch eine Datenspeicherung in der Datei APIS existierte. Die Datei APIS ist eine für Zwecke der inneren Sicherheit geführte Arbeitsdatei, die gemeinsam von den Staatsschutzabteilungen des Bundeskriminalamtes und den Staatsschutzabteilungen der Landeskriminalämter geführt wird. Die hessischen Staatsschutzabteilungen der Polizeipräsidien haben zwar keinen eigenen technischen Zugriff auf diese Datei, sie liefern aber Daten über ihr Landeskriminalamt an. Der politisch motivierte Mordplan war ein typischer "Fall" für diese Datei. Daher veranlasste damals die Staatsschutzabteilung der ermittelnden Polizeibehörde die Datenspeicherung in APIS; sie lautete u. a. "Verdacht des versuchten Mordes". Ursache für die vom Betroffenen geschilderten Schwierigkeiten war Folgendes: Das Polizeipräsidium hatte auf Antrag des Betroffenen die Löschung der Daten verfügt. Diese Verfügung führte zur Löschung in den polizeilichen Informationssystemen POLAS und ggf. auch INPOL. Ebenso zur Vernichtung der Fingerabdrücke und der angefertigten Lichtbilder. Auch die Aussonderung des dem Bundeskriminalamt zur Verfügung zu stellenden Doppels der erkennungsdienstlichen Unterlagen wurde veranlasst. Ebenso die Vernichtung der Kriminalakte. Auch eine polizeiinterne Abstimmung mit dem zuständigen Staatsschutzkommissariat hat stattgefunden. Allerdings wurde die Löschung des Datensatzes in APIS versäumt.

Das Polizeipräsidium räumte in der von mir erbetenen Stellungnahme das Versäumnis ein. Infolge der polizeiinternen Abstimmung mit dem Staatsschutzkommissariat über die Löschungsreife des Datensatzes, hätte die Löschung auch in APIS veranlasst werden müssen. Alle Mitarbeiter des Kommissariats seien auf den einzuhaltenden Gang des Verfahrens hingewiesen worden. Der Vorgang wurde zum Gegenstand einer Dienstbesprechung gemacht. Damit sei, so wurde mir versichert, durch organisatorische Maßnahmen sichergestellt, dass Wiederholungsfälle ausgeschlossen werden können.

Den Betroffenen habe ich informiert.

5.8
Prüfung der Luftverkehrsbehörde beim Polizeipräsidium Frankfurt

Bei der Luftverkehrsbehörde des Polizeipräsidiums Frankfurt habe ich den Umgang mit personenbezogenen Daten von Betroffenen kontrolliert, deren Zuverlässigkeit nach dem Luftverkehrsgesetz überprüft wurde. Die Prüfung ergab keine Beanstandungen.

5.8.1
Anlass der Prüfung

Im Berichtszeitraum erreichten mich eine Reihe von Eingaben von Personen, die einer Prüfung nach der Luftverkehrszuverlässigkeitsüberprüfungsverordnung unterzogen worden waren. Sie gaben an, wegen geringfügigen Rechtsverstößen sei ihre Zuverlässigkeit im Sinne des Luftverkehrsrechtes angezweifelt worden. Die Rechtsverstöße würden schon lange zurückliegen, seien geringfügig gewesen bzw. nie strafrechtlich geahndet worden, trotzdem müssten sie jetzt deswegen um ihren Arbeitsplatz bangen. Ich bin den Vorwürfen nachgegangen und habe bei der Hessischen Luftverkehrsbehörde eine Datenschutzprüfung vorgenommen.

5.8.2
Rechtslage

5.8.2.1
Luftverkehrsgesetz

Als Reaktion auf die Terroranschläge in den USA am 11. September 2001 wurde mit dem Terrorismusbekämpfungsgesetz vom 9. Januar 2002 § 29d des Luftverkehrsgesetzes (LuftVG) geändert.

§ 29d LuftVG

(1) Zum Schutz vor Angriffen auf die Sicherheit des Luftverkehrs (§ 29c Abs. 1 Satz 1) hat die Luftfahrtbehörde die Zuverlässigkeit folgender Personen zu überprüfen:

1. Personen, denen zur Ausübung einer beruflichen Tätigkeit nicht nur gelegentlich Zugang zu nicht allgemein zugänglichen Bereichen (§ 19b Abs. 1 Satz 1 Nr. 3, § 20a Abs. 1 Satz 1 Nr. 2) gewährt werden soll,
2. Personal der Flugplatz- und Luftfahrtunternehmen sowie des Flugsicherungsunternehmens, das aufgrund seiner Tätigkeit Einfluss auf die Sicherheit des Luftverkehrs hat; sofern sich Flugplatz-, Luftfahrt- oder Flugsicherungsunternehmen zur Wahrnehmung ihrer Aufgaben des Personals anderer Unternehmen bedienen, steht dieses eigenem Personal gleich,
3. Personen, die nach § 29c Abs. 1 Satz 3 als Hilfsorgane eingesetzt oder nach § 31b Abs. 1 Satz 2 mit Aufgaben nach § 27c Abs. 2 beauftragt werden.

Die Überprüfung bedarf der Zustimmung des Betroffenen. Sie entfällt, wenn der Betroffene im Inland innerhalb der letzten zwölf Monate einer zumindest gleichwertigen Überprüfung unterzogen worden ist und keine Anhaltspunkte für eine Unzuverlässigkeit des Betroffenen vorliegen oder der Betroffene der erweiterten Sicherheitsüberprüfung nach § 9 des Sicherheitsüberprüfungsgesetzes oder der erweiterten Sicherheitsüberprüfung mit Sicherheitsermittlungen nach § 10 des Sicherheitsüberprüfungsgesetzes unterliegt.

(2) Zur Überprüfung der Zuverlässigkeit darf die Luftfahrtbehörde folgende Maßnahmen treffen:

1. Prüfung der Identität des Betroffenen,
2. Anfragen bei den Polizei- und Verfassungsschutzbehörden der Länder sowie, soweit im Einzelfall erforderlich, dem Bundeskriminalamt, dem Bundesamt für Verfassungsschutz, dem Bundesnachrichtendienst, dem Militärischen Abschirmdienst und dem Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik nach vorhandenen, für die Beurteilung der Zuverlässigkeit bedeutsamen Informationen,
3. Einholung einer unbeschränkten Auskunft aus dem Bundeszentralregister,
4. soweit im Einzelfall erforderlich, Anfragen bei den Flugplatz-, Luftfahrt- und Flugsicherungsunternehmen sowie dem gegenwärtigen Arbeitgeber des Betroffenen nach dort vorhandenen, für die Beurteilung der Zuverlässigkeit bedeutsamen Informationen.

(3) Bei Zweifeln an der Zuverlässigkeit des Betroffenen darf die Luftfahrtbehörde außerdem zur Behebung dieser Zweifel erforderliche Auskünfte von Strafverfolgungsbehörden einholen.

(4) Die Luftfahrtbehörde gibt dem Betroffenen vor ihrer Entscheidung Gelegenheit, sich zu den eingeholten Auskünften zu äußern, soweit diese Zweifel an seiner Zuverlässigkeit begründen und Geheimhaltungspflichten nicht entgegenstehen. Stammen die Erkenntnisse von einer der in Abs. 2 Nr. 2 genannten Stellen, ist diese vorher zu hören. Der Betroffene ist verpflichtet, wahrheitsgemäße Angaben zu machen und ihm nachträglich bekannt werdende, für die Überprüfung bedeutsame Tatsachen unverzüglich anzuzeigen. Er kann Angaben verweigern, die für ihn, eine der in § 52 Abs. 1 der Strafprozessordnung genannten Personen oder den Lebensgefährten die Gefahr strafrechtlicher Verfolgung oder von disziplinar- oder arbeitsrechtlichen Maßnahmen begründen könnten. Über das Verweigerungsrecht ist der Betroffene vorher zu belehren.

(5) Die Luftfahrtbehörde darf die nach Abs. 2 erhobenen Daten nur zum Zwecke der Überprüfung der Zuverlässigkeit verarbeiten und nutzen. Sie unterrichtet den Betroffenen, dessen gegenwärtigen Arbeitgeber und das Flugplatz-, Luftfahrt- oder Flugsicherungsunternehmen über das Ergebnis der Überprüfung; dem Flugplatz-, Luftfahrt- oder Flugsicherungsunternehmen und dem gegenwärtigen Arbeitgeber dürfen die dem Ergebnis zugrunde liegenden Erkenntnisse nicht mitgeteilt werden. Weitere Informationen dürfen dem Flugplatz-, Luftfahrt- oder Flugsicherungsunternehmen und dem gegenwärtigen Arbeitgeber mitgeteilt werden, soweit sie für die Durchführung eines gerichtlichen Verfahrens im Zusammenhang mit der Zuverlässigkeitsüberprüfung erforderlich sind. § 161 der Strafprozessordnung bleibt unberührt.

Die Änderungen sind:

- an Stelle der bisherigen Befugnis, die Zuverlässigkeit der betroffenen Personen zu prüfen, tritt die Pflicht zur Überprüfung,
- die Prüfung muss jetzt jedes Jahr stattfinden (zuvor konnte sie alle fünf Jahre erfolgen),
- Abs. 2 konkretisiert, bei welchen Behörden Informationen eingeholt werden dürfen. Neu ist die Berechtigung zur Einholung unbeschränkter Auskünfte aus dem Bundeszentralregister, außerdem die ausdrückliche Befugnis, bei Zweifeln an der Zuverlässigkeit, Auskünfte von den Staatsanwaltschaften einzuholen.

5.8.2.2
Luftverkehrszuverlässigkeitsüberprüfungsverordnung

Schon vor Änderung des LuftVG hat die Bundesregierung die „Verordnung zur Regelung des Verfahrens der Zuverlässigkeitsüberprüfung auf dem Gebiet des Luftverkehrs“ (LuftVZÜV) erlassen, die mit Wirkung vom 8. Oktober 2001 in Kraft trat. Diese Verordnung wurde mit dem Terrorismusbekämpfungsgesetz in § 4 Abs. 1 und 4 noch einmal geändert. Sie enthält u. a. Regelungen über die Datenerhebung (§ 3), das Einholen von Informationen bei anderen Stellen (§ 4) und über die Bewertung dieser Informationen (§ 5).

§ 3 LuftVZÜV

(1) Personen gemäß § 29d Abs. 2 Satz 1 Nr. 1 des Luftverkehrsgesetzes beantragen die Durchführung der Zuverlässigkeitsüberprüfung über ihren Arbeitgeber und das Flugplatz- oder Luftfahrtunternehmen, zu dessen in § 29d Abs. 1 des Luftverkehrsgesetzes genannten Bereichen und Anlagen ihnen der Zugang gewährt werden soll.

(2) Die Flugplatz- oder Luftfahrtunternehmen sollen der nach § 2 Abs. 1 oder 2 zuständigen Luftfahrtbehörde zur Durchführung der Zuverlässigkeitsüberprüfung die nach Abs. 3 erforderlichen Daten und Sachverhalte der zu überprüfenden Person vier Wochen vor der geplanten Aufnahme ihrer Tätigkeit übermitteln. Die Luftfahrtbehörde soll die Zuverlässigkeitsüberprüfung innerhalb dieser Frist durchführen.

(3) In dem Antrag sind vom Betroffenen anzugeben:

1. Name, einschließlich frühere Namen,
2. Geburtsname,
3. sämtliche Vornamen,
4. Geburtsdatum,
5. Geburtsort und -land
6. Wohnsitze der letzten zehn Jahre vor der Überprüfung, hilfsweise der gewöhnliche Aufenthaltsort,
7. Staatsangehörigkeit,
8. Personalausweis- oder Passnummer,
9. Arbeitgeber,
10. vorgesehene Tätigkeit,
11. für die Tätigkeit zu betretende Flugplätze,
12. sonstige für die Beurteilung der Zuverlässigkeit bedeutsame Sachverhalte im Sinne des § 5.

§ 4 LuftVZÜV

(1) Die Luftfahrtbehörde ersucht zum Zwecke der Zuverlässigkeitsüberprüfung die Polizei- und die Verfassungsschutzbehörden der Länder, vorhandene bedeutsame Informationen im Sinne des § 5 zu übermitteln. Das Ersuchen ist an die nach Landesrecht zuständige Polizeibehörde zu richten. Hat der Betroffene seinen Hauptwohnsitz und seinen gewöhnlichen Aufenthalt außerhalb des Zuständigkeitsbereiches der nach Satz 2 zuständigen Polizeibehörde, ist die insoweit zuständige Polizeibehörde zu beteiligen. Die Abfrage erstreckt sich auf

1. die Personenfahndungsdateien,
2. die Kriminalaktennachweise,
3. die polizeilichen Staatsschutzdateien.

Die Polizeibehörden teilen sämtliche vorhandene Erkenntnisse mit. Bei der für den Sitz der Luftfahrtverkehrsbehörde zuständigen Landesbehörde für Verfassungsschutz erfolgt die Abfrage des nachrichtendienstlichen Informationssystems. Die Luftfahrtbehörde holt eine unbeschränkte Auskunft aus dem Bundeszentralregister ein und ersucht, soweit im Einzelfall erforderlich, die sonstigen in § 29d Abs. 2 Nr. 2 und 4 des Luftverkehrsgesetzes genannten Stellen um Auskunft über vorhandene, für die Beurteilung der Zuverlässigkeit bedeutsame Informationen.

(2) Hatte der Betroffene in den letzten zehn Jahren vor der Überprüfung weitere Wohnsitze auch in anderen Bundesländern, so sind auch die für diese Wohnsitze zuständigen Polizeibehörden um Übermittlung dort vorhandener bedeutsamer Informationen im Sinne des § 5 zu ersuchen.

(3) Hat der Betroffene im Geltungsbereich des Luftverkehrsgesetzes weder Wohnsitz noch gewöhnlichen Aufenthaltsort, so ist die für den Unternehmenssitz seines Arbeitgebers zuständige Polizeibehörde um Übermittlung der Informationen nach Abs. 1 zu ersuchen. Hat auch der Arbeitgeber keinen Unternehmenssitz im Geltungsbereich des Luftverkehrsgesetzes, so ist die für den Sitz der Luftverkehrsbehörde zuständige Polizeibehörde um Übermittlung der Informationen nach Abs. 1 zu ersuchen.

(4) Bestehen auf Grund der nach Abs. 1 übermittelten Informationen Anhaltspunkte für Zweifel an der Zuverlässigkeit des Betroffenen, kann die zuständige Behörde mit Zustimmung des Betroffenen zusätzlich zur Behebung dieser Zweifel bei den Strafverfolgungsbehörden Auskünfte einholen. Sie kann vom Betroffenen selbst weitere Informationen einholen oder gegebenenfalls deren Vorlage verlangen. In den Fällen des Abs. 3 kann die Luftfahrtbehörde vom Betroffenen zusätzlich Zeugnisse seines Aufenthaltsstaates verlangen, aus denen sich seine Zuverlässigkeit ergibt.

(5) Die bei der Luftfahrtbehörde vorhandenen Informationen über die Zuverlässigkeitsüberprüfung sind nach Ablauf von zehn Jahren nach Bekanntgabe des letzten Überprüfungsergebnisses zu löschen, soweit nicht eine neue Überprüfung gemäß § 9 Abs. 3 beantragt wird.

§ 5 LuftVZÜV

(1) Die Luftfahrtbehörde bewertet die Zuverlässigkeit des Betroffenen auf Grund einer Gesamtwürdigkeit des Einzelfalles.

(2) In der Regel fehlt es an der erforderlichen Zuverlässigkeit,

1. wenn der Betroffene innerhalb der letzten zehn Jahre vor der Überprüfung wegen versuchter oder vollendeter Straftaten rechtskräftig verurteilt wurde, oder
2. tatsächliche Anhaltspunkte dafür bestehen, dass der Betroffene Bestrebungen nach § 3 Abs. 1 Nr. 1 oder 3 des Bundesverfassungsschutzgesetzes verfolgt oder unterstützt oder innerhalb der letzten zehn Jahre verfolgt oder unterstützt hat.

(3) Bei Verurteilungen und Bestrebungen nach Abs. 2, die länger als zehn Jahre zurückliegen, oder bei Vorliegen sonstiger Erkenntnisse ist im konkreten Einzelfall zu prüfen, ob sich daraus im Hinblick auf die Sicherheit des Luftverkehrs Zweifel an der Zuverlässigkeit der zu überprüfenden Person ergeben. Als sonstige Erkenntnisse kommen insbesondere in Betracht:

1. laufende oder eingestellte Ermittlungs- und Strafverfahren,
2. der Verdacht der Tätigkeit für fremde Nachrichtendienste,
3. tatsächliche Anhaltspunkte für das Unterhalten von Kontakten zu Organisationen im Sinne des § 3 Abs. 1 Nr. 1 oder 3 des Bundesverfassungsschutzgesetzes,
4. Sachverhalte, aus denen sich eine Erpressbarkeit für Dritte ergibt,
5. Betäubungsmittel- und gegebenenfalls Alkoholabhängigkeit.

(4) § 51 Abs. 1 des Bundeszentralregistergesetzes ist zu beachten.

5.8.2.3
Verordnung zur Bestimmung von luftverkehrsrechtlichen Zuständigkeiten

Mit Verordnung vom 30. Oktober 2001 übertrug die Hessische Landesregierung mit Wirkung vom 1. Januar 2002 die Zuständigkeit der Luftfahrtbehörde i.S.d. § 29d LuftVG dem Polizeipräsidium Frankfurt und der obersten Luftfahrtbehörde für diesen Bereich dem Innenministerium.

§ 2 der Verordnung zur Bestimmung von luftverkehrsrechtlichen Zuständigkeiten

(1) Das für Polizeiangelegenheiten zuständige Ministerium als Landespolizeipräsidium ist oberste Luftfahrtbehörde, soweit das Polizeipräsidium Frankfurt am Main Aufgaben als Luftfahrtbehörde nach § 29d in Verbindung mit § 31 Abs. 2 Nr. 19 Satz 1 des Luftverkehrsgesetzes wahrnimmt.

(2) Luftfahrtbehörde im Sinne des § 29d des Luftverkehrsgesetzes ist das Polizeipräsidium Frankfurt am Main.

Zuvor war das Verkehrsministerium für solche Prüfungen zuständig gewesen.

5.8.3
Die Prüfung

Entsprechend der Zuständigkeitsverordnung existiert beim Polizeipräsidium Frankfurt die Organisationseinheit "Luftverkehrsbehörde". Sie ist personell besetzt mit 14 Angestellten und Beamten der Frankfurter Polizei. Im Jahre 2002 gingen dort ca. 41.000 Anträge ein. Die durchschnittliche Bearbeitungsdauer beträgt 6 bis 7 Tage. Die Ablehnungsquote beträgt einschließlich zurückgenommener Anträge ca. 1,8 v.H.

Die Anträge werden von dem Träger des Flughafens Frankfurt, der Frankfurt Airport Services Worldwide AG (Fraport AG), in elektronischer Form übermittelt. Die Inhalte entsprechen dem in § 3 Abs. 3 der Verordnung beschriebenen Datenumfang. Die Verarbeitung des Datensatzes erfolgt zunächst ebenfalls elektronisch. So wird mit den Identifizierungsdaten ein Abfragedatensatz für das polizeiliche Auskunftssystem POLAS erstellt. Ebenfalls elektronisch erfolgt der Informations-

austausch mit der Staatsschutzdatei APIS (s. Ziff. 5.7.) beim Hessischen Landeskriminalamt und dem Bundeszentralregister beim Generalbundesanwalt. Teilautomatisiert erfolgt der Informationsaustausch mit dem Hessischen Landesamt für Verfassungsschutz. Je nach Vollständigkeit der jeweils eingegangenen Negativauskünfte erhält der Datensatz eine bestimmte Kennung. Ist z. B. gerade der vollständige Eingang des Datensatzes bei der Luftverkehrsbehörde registriert, erhält er die Kennung "00". Hat das Datenverarbeitungssystem POLAS die Information übermittelt, dass die Person dem polizeilichen Informationssystem unbekannt ist, erhält der Datensatz die Kennung "10". Hat das Bundeszentralregister mitgeteilt, dass über die Person keine Verurteilungen existieren, erhält er die Kennung "20" usw. Wird ein bestimmter Wert erreicht, wird automatisch die Bescheinigung über die Anerkenntnis der luftverkehrsrechtlichen Zuverlässigkeit erstellt und an die Fraport AG übermittelt. Insoweit findet ein sehr rationeller und auch datensparsamer Umgang mit den personenbezogenen Daten der Betroffenen statt. Solange keinerlei Negativinformation über den Antragsteller bekannt wird, nimmt bis einschließlich der Ausstellung der Lizenz, kein Bearbeiter bewusst die Daten des Antragstellers zur Kenntnis. Es wird nicht einmal eine Papierakte angelegt. Es existiert lediglich der elektronische Datensatz. Eine datenschutzrechtlich interessante Relevanz entsteht erst, wenn eine der befragten Stellen Erkenntnisse übermittelt. In diesem Falle wird der automatische Ablauf gestoppt und es erfolgt eine manuelle Bearbeitung des Antrages. An dieser Stelle bin ich dem Vorhalt von Betroffenen "wegen jeder Kleinigkeit" würde die Zuverlässigkeit in Frage gestellt, nachgegangen. Meine Prüfung hat dies nicht bestätigt. Ich habe dagegen zahlreiche Einzelfälle festgestellt, in denen die Luftverkehrsbehörde trotz Vorliegen eines Grundes nach § 5 Abs. 2 Nr. 1 LuftVZÜV oder auch mehrerer Informationen nach § 5 Abs. 3 Nr. 1 LuftVZÜV in sachgerechter Gewichtung der Informationen die Zuverlässigkeit der Antragsteller nicht in Frage gestellt, sondern die Zuverlässigkeitsbescheinigung erteilt hat. In Zweifelsfällen wurde der Betroffene - wie in § 29 Abs. 4 vorgesehen – angehört. Auch innerhalb dieser Fallgruppe habe ich zahlreiche Einzelfälle festgestellt, in denen nach Anhörung der betroffenen Person, trotz Vorliegen eines förmlichen Versagungsgrundes nach Abwägung der Information mit der Einlassung der Betroffenen, die luftverkehrsrechtliche Zuverlässigkeit bescheinigt wurde.

Wenig Nachsicht hat die Luftverkehrsbehörde bei Hinweisen auf eine Drogenabhängigkeit. Liegen solche Hinweise vor, ist nach § 5 Abs. 3 LuftVZÜV im konkreten Einzelfall zu prüfen, ob sich daraus im Hinblick auf die Sicherheit des Luftverkehrs Zweifel an der Zuverlässigkeit der zu überprüfenden Person ergeben. Um solche Zweifel auszuräumen, wird von den Betroffenen verlangt, ein Drogenscreening vorzulegen. Bei 90 der ca. 41.000 Probanden war dies im Jahr 2002 der Fall. 46 Personen legten daraufhin einen negativen Drogentest vor. Bei 20 Personen verlief der Test positiv, 24 verweigerten den Test. Bei den beiden letztgenannten Gruppen wurde die Zuverlässigkeit nicht bescheinigt.

Alle von mir geprüften Fälle, in denen die Zuverlässigkeit nicht bescheinigt wurde, waren überzeugend begründet und aus meiner Sicht nicht zu beanstanden.

6. Ausländerbehörden

Prüfung der Ausländerbehörde des Landkreises Marburg

Bei der Prüfung stellte ich - mit Ausnahme gravierender Mängel bei der Datensicherheit im Gebäude des Landratsamts - keine datenschutzrechtlichen Probleme fest.

6.1
Einholung von Auskünften beim Landesamt für Verfassungsschutz und Landeskriminalamt im Rahmen von Aufenthaltsgenehmigungen

Auf Grund verschiedener Eingaben von Bürgern und Ausländerorganisationen interessierte mich die Frage, wie die durch das Terrorismusbekämpfungsgesetz vom 11. Dezember 2001 mit § 64a in das Ausländergesetz (AuslG) eingefügte Vorschrift in der Praxis umgesetzt wird. Diese Vorschrift eröffnet im Zusammenhang mit der Feststellung von besonderen Versagungsgründen für Aufenthaltsgenehmigungen die Datenübermittlung u. a. an das Landesamt für Verfassungsschutz (LfV) und das Landeskriminalamt (LKA).

§ 64a Abs. 2 AuslG

Die Ausländerbehörden können zur Feststellung von Versagungsgründen nach § 8 Abs. 1 Nr. 5 vor der Erteilung oder Verlängerung einer sonstigen Aufenthaltsgenehmigung die bei ihr gespeicherten personenbezogenen Daten der betroffenen Person an das Landesamt für Verfassungsschutz und das Landeskriminalamt übermitteln.

Besondere Versagungsgründe liegen nach § 8 Abs. 1 Nr. 5 AuslG u. a. vor bei der Unterstützung verfassungsfeindlicher Ziele, politisch motivierten Gewalttätigkeiten oder Mitgliedschaft oder Unterstützung terroristischer Vereinigungen.

§ 8 Abs. 1 Nr. 5 AuslG

Die Aufenthaltsgenehmigung wird auch bei Vorliegen der Voraussetzungen eines Anspruchs nach diesem Gesetz versagt, wenn

5. er die freiheitliche demokratische Grundordnung oder die Sicherheit der Bundesrepublik Deutschland gefährdet oder sich bei der Verfolgung politischer Ziele an Gewalttätigkeiten beteiligt oder öffentlich zur Gewaltanwendung aufruft oder mit Gewaltanwendung droht oder wenn Tatsachen belegen, dass er einer Vereinigung angehört, die den internationalen Terrorismus unterstützt, oder er eine derartige Vereinigung unterstützt.

Das Hessische Ministerium des Innern hat durch Erlass vom 9. Juli 2003 die Vorschrift dergestalt konkretisiert, dass bei bestimmten Staatsangehörigen vor der Ersterteilung oder Verlängerung befristeter Aufenthaltsgenehmigungen Anfragen an das LfV und das LKA zu erfolgen haben. Vor der Erteilung unbefristeter Aufenthaltserlaubnisse und Aufenthaltsberechtigungen sind bei allen Staatsangehörigen derartige Anfragen zu stellen.

Nach unseren Feststellungen verfährt die Ausländerbehörde zwar entsprechend den Vorgaben des Erlasses, in keinem der Fälle wurden jedoch Erkenntnisse an die Ausländerbehörde übermittelt. Deshalb konnten wir uns kein Bild von den tatsächlichen Sachverhalten machen, die unter § 8 Abs. 1 Nr. 5 AuslG subsumiert werden.

Da die Polizeibehörden auf Grund anderer Vorschriften (§ 76 Abs. 4 AuslG, § 42 Abs. 1 Anordnung über die Mitteilung in Strafsachen [MiStra]) schon zur Übermittlung bestimmter Erkenntnisse verpflichtet sind, stellt sich die Frage, ob eine erneute Anfrage an das LKA überhaupt ein Mehr an Informationen bringen kann. Hierzu hat sich das Hessische Ministerium des Innern noch nicht abschließend geäußert.

6.2
Datensicherheit im Gebäude des Landratsamtes

Gravierende datenschutzrechtliche Mängel wurden bei der Datensicherheit im Gebäude des Landratsamts festgestellt:

Im ersten Stock des Gebäudes angrenzend an den Treppenumgang neben dem Wartebereich des Publikums befanden sich frei zugängliche Wohngeldakten.

Im zweiten Stock wurden festgestellt:

- ein offener Stahlschrank mit Unterlagen des Schulamts
- vor den Türen des Rechtsamts des Kreisausschusses eine ganze Reihe offen stehender Stahlschränke mit Unterlagen über Gerichtsverfahren und Schriftwechsel des Kreises
- vor einem weiteren Zimmer offene Holzschränke mit Personalunterlagen, u. a. mehrere Ordner mit Bewerbungen und entsprechende Anlagen, Ausbildungsunterlagen von Praktikanten und Inspektorenanwärtern und Schwerbehindertenangelegenheiten.

Im dritten Stock befanden sich:

- offene Stahlschränke mit Akten über naturschutzrechtliche Prüfungen
- unverschlossene Schränke mit Akten über Bauvorhaben.

Es wurde uns zugesagt, dass diese Mängel sofort behoben werden.

7. Finanzen

7.1
Aufrechnungen von Forderungen eines Steuerpflichtigen gegenüber Behörden mit Ansprüchen aus dem Steuerschuldverhältnis

Die Rechtsgrundlage für eine regelmäßige Anfrage von öffentlich-rechtlichen Zahlungsschuldnern bei Finanzbehörden vor der Auszahlung von Forderungen ist vor einigen Jahren weggefallen. Das Aufrechnen von öffentlich-rechtlichen Forderungen ist nur zulässig, wenn bereits Anhaltspunkte vorliegen, die auf Steuerrückstände des Zahlungsempfängers schließen lassen.

Immer wieder erreichen mich Anfragen von Bürgern, deren Geldforderungen an das Land Hessen für erbrachte Leistungen mit Ansprüchen der Finanzbehörden aus dem Steuerschuldverhältnis aufgerechnet werden. Da diese Geldforderungen der Bürger im Allgemeinen nicht gegenüber Finanzbehörden entstanden sind, muss der Aufrechnung eine Datenübermittlung vorausgegangen sein. Voraussetzung für die Rechtmäßigkeit einer Datenübermittlung ist eine Rechtsgrundlage.

Auf meine Nachfragen bei den betroffenen Behörden wurde mir wiederholt als Rechtsgrundlage ein Erlass des Hessischen Ministeriums der Finanzen vom 18. Februar 1981 genannt, der aber bereits im Rahmen der Erlassbereinigung außer Kraft getreten ist. Auf eine Neubekanntmachung wurde verzichtet. Es gibt daher derzeit keine Rechtsgrundlage für regelmäßige Datenübermittlungen von öffentlichen Stellen an Finanzbehörden vor Auszahlung eines Forderungsbetrags. Entsprechende Datenübermittlungen verstoßen somit gegen das Hessische Datenschutzgesetz. Dementsprechend ist die Beantwortung solcher Anfragen durch die Finanzbehörden nicht rechtmäßig.

Eine Aufrechnung von Forderungen ist dann zulässig, wenn bereits Anhaltspunkte vorliegen, die auf Steuerrückstände des Zahlungsempfängers schließen lassen. Deshalb können Anfragen derzeit auch nur erfolgen, wenn die betroffene Behörde im Einzelfall Anhaltspunkte für Steuerrückstände hat.

Ich habe die betroffenen Behörden auf die Rechtslage hingewiesen und die zuständigen Fachministerien aufgefordert, auf eine rechtmäßige Verfahrensabwicklung ihrer Dienststellen hinzuwirken.

7.2
Elektronische Signatur im Finanzbereich

Die Datenschutzbeauftragten des Bundes und der Länder haben die Zulassung einer fortgeschrittenen Signatur im Finanzbereich kritisiert wegen der teilweise fehlenden Kontrollkompetenz der deutschen Datenschutzbehörden und wegen der im Vergleich zur qualifizierten Signatur geringeren Sicherheit und Überprüfbarkeit.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat auf Vorschlag des Arbeitskreises Finanzen eine Entschließung zur elektronischen Signatur im Finanzbereich gefasst (s. Ziff. 20.6).

Aus Sicht der Datenschutzbeauftragten ist die Zulassung von Zertifizierungsdiensten im außereuropäischen Ausland, für die weder eine Kontrolle durch deutsche Datenschutzbehörden noch eine freiwillige Akkreditierung gemäß Signaturgesetz möglich ist, besonders problematisch.

Für den Bürger wird das ohnehin komplizierte Thema Signatur durch die Schaffung einer neuen so genannten "qualifizierten elektronischen Signatur mit Einschränkung", die in Wirklichkeit eine fortgeschrittene Signatur ist, immer undurchschaubarer. Er hat auch keinen Vorteil vom Einsatz einer solchen Signatur für die elektronische Steuererklärung ELSTER, weil er nach wie vor dem Finanzamt die erforderlichen Belege zur Steuererklärung auf dem Postweg zuschicken muss. Bei seiner Entscheidung, ob sich für ihn der finanzielle Aufwand für die erforderliche Infrastruktur (Karte und Lesegerät) lohnt, muss er berücksichtigen, dass er nur einmal pro Jahr eine Einkommenssteuererklärung abgibt und dass er mit diesem Verfahren auch andere Dokumente nicht rechtsverbindlich signieren kann.

Umgekehrt könnte die elektronische Steuererklärung ELSTER mit einer qualifizierten Signatur und beispielsweise einer finanziellen Förderung der Bürger für die Erstausstattung mit der benötigten Infrastruktur eine gute Möglichkeit sein, um rechtsverbindlichen und langfristig überprüfbaren Signaturen zum Durchbruch zu verhelfen.

Die Finanzverwaltung selbst muss nach der derzeitigen Rechtslage bis Ende 2005 ihre elektronischen Dokumente ebenfalls nicht rechtsverbindlich signieren. Dabei bräuchte sie hierfür über die technische Infrastruktur für die "qualifizierte elektronische Signatur mit Einschränkungen" hinaus lediglich ein qualifiziertes Zertifikat. Es ist nicht nachvollziehbar, warum die Finanzbehörden nicht von vornherein alle elektronischen Dokumente qualifiziert signiert versenden. Weder im Verwaltungsverfahrensänderungsgesetz noch in der Steuerdatenübermittlungsverordnung wurde hierfür eine Begründung angegeben.

8. Kommunen

8.1
Internetportal Gewerbemeldungen

Das Hessische Statistische Landesamt bietet ein Internetportal an, über das Kommunen Mitteilungen über Gewerbeanmeldungen oder -änderungen an andere Institutionen leiten können. Die Daten werden als Datei an das Hessische Statistische Landesamt übertragen und in einer Datenbank gespeichert. Anschließend räumt das Hessische Statistische Landesamt nach den Vorgaben der Kommune den anderen Institutionen Zugriffsrechte ein. Es findet eine Datenverarbeitung im Auftrag gemäß § 4 Hessisches Datenschutzgesetz statt.

Im Zuge von E-Government Aktivitäten stellt das Hessische Statistische Landesamt (HSL) hessischen Kommunen als Dienstleistung die Möglichkeit zur Verfügung, Gewerbeanmeldungen oder -änderungen über das HSL an die Institutionen zu übermitteln, die auf Grund des § 14 Abs. 5 Gewerbeordnung (GewO) regelmäßig die Daten aus der Gewerbeanmeldung erhalten.

8.1.1
Technische Abläufe

Die Daten werden per Filetransfer übertragen. Es handelt sich um Dateien im EDIFACT-Format. Die Übertragung erfolgt gesichert durch Secure Socket Layer (SSL), sowohl beim Heraufladen auf den Server durch die Kommune als auch beim Herunterladen durch den jeweiligen Empfänger.

Zu jeder übertragenen Datei wird auf dem Server des HSL ein Metadatensatz gespeichert. In diesem Datensatz wird u. a. gespeichert, ob alle Abrufe bereits erfolgt sind. Haben alle potenziellen Empfänger die Daten empfangen, läuft die Frist zur Löschung.

Alle beteiligten Kommunen und Institutionen sind durch ein eindeutiges Kennzeichen identifiziert. Diese Zahl ist bei Kommunen die Gemeindekennziffer. Weitere Informationen zu Kommunen sind u. a. im Gemeindedatensatz gespeichert.

Im Gemeindedatensatz sind die möglichen Empfänger-Institutionen mit ihrem Kennzeichen vermerkt. Wenn die Gemeinde eine Datei zum Server schickt, wird dort zu der Datei der Metadatensatz erzeugt. Gleichzeitig wird zu allen in diesem Zeitpunkt bei der Gemeinde gespeicherten Empfängern eine Datenbankverknüpfung erzeugt. D. h. nur diesen Empfängern ist bekannt, wo sich die Datei befindet. Es wird für jeden Empfänger eine E-Mail generiert, dass eine Datei vorhanden ist.

Um auf die Datei zuzugreifen, meldet sich die Institution mit einer Kennung und dem zugehörigen Passwort an. Über die Datenbankverknüpfung wird der Zugriff auf die Datei ermöglicht. Bei der Darstellung am Bildschirm und später auch beim

Herunterladen wird für jedes Feld geprüft, ob zu diesem Empfänger-Typ für das Feld eine Darstellung bei der Anmeldung/Ummeldung/Abmeldung erfolgen darf oder nicht. Darf das Feld nicht angezeigt werden, so werden "xxxx" angezeigt bzw. gedruckt oder übertragen. Anschließend wird nach einer Bestätigung der erfolgreichen Übertragung die Datenbankverknüpfung gelöscht, d. h. der Empfänger "sieht" die Datei nicht mehr. Ferner wird der Abrufzähler hochgesetzt. Sind der Abrufzähler und die Anzahl der Empfänger identisch, beginnt die Löschfrist zu laufen.

8.1.2
Datenschutzrechtliche Bewertung

8.1.2.1
Datenverarbeitung im Auftrag

Die Serviceleistung, die das HSL mit seinem E-Government Portal Gewerbemeldungen erbringen will, ist rechtlich als Datenverarbeitung im Auftrag i.S.d. § 4 HDSG zu werten. Das HSL verteilt die Gewerbeanzeigen im Auftrag der angeschlossenen Kommunen und muss insoweit mit allen teilnehmenden Gemeinden einen Vertrag i.S.d. § 4 Abs. 2 HDSG abschließen, der die Rechte und Pflichten von Auftraggeber und Auftragnehmer im Einzelnen festlegt.

8.1.2.2
Erforderliche Anpassungen

Es gab noch einige Anpassungen, die vorgenommen werden mussten.

- Nach einer Überprüfung wurde festgelegt, auf welche Datenfelder verzichtet werden kann.
- Es wurde durch entsprechende organisatorische Maßnahmen erreicht, dass die Kommune bei der Auftragsbestätigung erfährt, welche Empfänger eingetragen sind. Dies gilt sowohl für den Ersteintrag wie auch für spätere Änderungen.
- Die Teilnehmer wurden darauf hingewiesen, dass nur berechtigten Personen die Benutzerkennung und das Passwort bekannt sein dürfen, mit denen das Herunterladen durchgeführt wird.
- Die Anmeldeprozedur und die Passwortverwaltung wurden so angepasst, dass die Anforderungen des Grundschutzhandbuchs des Bundesamtes für Sicherheit in der Informationstechnik (BSI) erfüllt sind.
- Das HSL stellt sicher, dass die Einträge zu den Institutionen und die anderen sicherheitsrelevanten Daten korrekt sind.

Unter diesen Bedingungen hatte ich keine Einwände gegen das Verfahren.

Zwischenzeitlich sind auch die Verträge mit den teilnehmenden Kommunen mit mir abgestimmt. Ich werde im nächsten Jahr prüfen, ob die Vorgaben umgesetzt wurden.

8.2
Tonbandaufzeichnungen von öffentlichen Sitzungen

Wird einem Bürger während einer öffentlichen Sitzung das Recht eingeräumt, sich mit eigenen Redebeiträgen zu beteiligen, hat er auch einen Anspruch auf Tonbandauszüge bzw. Wortprotokolle.

Zwei Bürger verschiedener Kommunen haben mich um datenschutzrechtliche Prüfung gebeten, ob ihnen Auszüge aus Tonbandaufzeichnungen über eigene Redebeiträge während öffentlicher Sitzungen zustehen. In beiden Fällen wurden Anfragen der Betroffenen von den Kommunen negativ beantwortet.

Nach § 61 Hessische Gemeindeordnung (HGO) sind über Sitzungen der Stadtverordnetenversammlungen Niederschriften zu fertigen. Zur Unterstützung der Protokollführer werden oft Tonbandaufzeichnungen angefertigt. Grundsätzlich sind Niederschriften über Sitzungen von Gemeindevertretungen nicht öffentlich zugänglich. Lediglich Gemeindevertreter haben ein Recht auf Einsicht in die Protokolle. Das Recht des Bürgers auf Information erschöpft sich in der Teilnahme an öffentlichen Sitzungen. Allerdings sieht die Hessische Gemeindeordnung auch nicht vor, dass anwesende Bürger sich an den Gemeindevertretersitzungen beteiligen können.

§ 61 HGO

(1) Über den wesentlichen Inhalt der Verhandlungen der Gemeindevertretung ist eine Niederschrift zu fertigen. Aus der Niederschrift muss ersichtlich sein, wer in der Sitzung anwesend war, welche Gegenstände verhandelt, welche Beschlüsse gefasst und welche Wahlen vollzogen worden sind. Die Abstimmungs- und Wahlergebnisse sind festzuhalten. Jedes Mitglied der Gemeindevertretung kann verlangen, dass seine Abstimmung in der Niederschrift festgehalten wird.

(2) Die Niederschrift ist von dem Vorsitzenden und dem Schriftführer zu unterzeichnen. Zu Schriftführern können Gemeindevertreter oder Gemeindebedienstete - und zwar auch solche, die ihren Wohnsitz nicht in der Gemeinde haben - oder Bürger gewählt werden.

(3) Die Niederschrift ist innerhalb eines in der Geschäftsordnung festzulegenden Zeitraumes offen zu legen. Die Geschäftsordnung kann neben der Offenlegung die Übersendung von Abschriften der Niederschrift an alle Gemeindevertreter vorsehen. Über Einwendungen gegen die Niederschrift entscheidet die Gemeindevertretung.

In diesem Punkt unterscheiden sich die mir vorgetragenen Fälle von den Regelungen der HGO. Aus unterschiedlichen Gründen wurden Bürgern Rederechte während einer öffentlichen Sitzung eingeräumt. Das bedeutet, dass die Tonbandaufzeichnungen der öffentlichen Sitzungen auch Redebeiträge von Bürgern beinhalteten.

Die Einsichtsrechte von Bürgern richten sich nicht nach den Bestimmungen der HGO, sondern nach § 18 Abs. 3 bzw. Abs. 5 HDSG.

§ 18 HDSG

(3) Datenverarbeitende Stellen, die personenbezogene Daten automatisiert speichern, haben dem Betroffenen auf Antrag gebührenfrei Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten,
2. den Zweck und die Rechtsgrundlage der Verarbeitung sowie
3. die Herkunft der Daten und die Empfänger übermittelter Daten, soweit dies gespeichert ist.

In dem Antrag soll die Art der Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden.

(5) Sind personenbezogene Daten in Akten gespeichert, die zur Person des Betroffenen geführt werden, dann kann er bei der aktenführenden Stelle Einsicht in die von ihm bezeichneten Akten verlangen. Werden die Akten nicht zur Person des Betroffenen geführt, hat er Angaben zu machen, die das Auffinden der zu seiner Person gespeicherten Daten mit angemessenem Aufwand ermöglichen. Die Einsichtnahme ist unzulässig, wenn die Daten des Betroffenen mit Daten Dritter oder geheimhaltungsbedürftigen nicht personenbezogenen Daten derart verbunden sind, dass ihre Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist. In diesem Fall ist dem Betroffenen Auskunft nach Abs. 3 zu erteilen. Im Übrigen kann ihm statt Einsicht Auskunft gewährt werden.

Diese Vorschrift gibt jedem Betroffenen das Recht, Auskunft über die zu seiner Person gespeicherten Daten zu erhalten. Dies gilt auch für Redebeiträge in Protokollen oder auf Tonträgern. Das Wortprotokoll oder der Tonbandauszug muss hierbei auf die Beiträge des jeweiligen Bürgers beschränkt werden. Hierzu gehören aber ebenso die Antworten, Kommentare oder sonstigen Redebeiträge von Mandatsträgern zu den vom Bürger angeschnittenen Themen. Die Vorschriften des Hessischen Datenschutzgesetzes stehen dieser Datenübermittlung nicht entgegen, da Mandatsträger während der Sitzungen keine Grundrechtsträger, sondern Amtsträger sind, ihre Antworten und Äußerungen unterliegen damit nicht den Datenschutzbestimmungen.

Ich habe deshalb die Kommunen aufgefordert, den anfragenden Bürgern die jeweiligen Tonbandausschnitte bzw. Wortprotokolle zur Verfügung zu stellen.

8.3
Datenübermittlungen an Parteien aus dem Einwohnermelderegister

Die Übermittlung von Daten der Wahlberechtigten an Parteien ist nach dem Hessischen Meldegesetz im Zusammenhang mit Wahlen zulässig. Allerdings sollte die Anzahl der Personen der gewünschten Altersgruppen fünfzig Prozent der Wahlberechtigten nicht überschreiten. Möchte eine Partei alle Wahlberechtigten erreichen, so ist dies durch Postwurfsendungen oder über die Presse datenschutzfreundlicher möglich.

In den letzten Jahren haben mich Anfragen von Kommunen und Bürgern veranlasst, mich mit der Weitergabe von Meldedaten an Parteien im Zusammenhang mit Wahlen nach § 35 Abs. 1 Hessisches Meldegesetz (HMG) zu befassen. Streitig zwischen Parteien und Meldeämtern war immer wieder die Frage, in welchen Fällen von einer Abfrage von "Gruppen" i. S. d. § 35 Abs. 1 HMG zu sprechen ist. Die Vorschrift ist so unklar gefasst, dass dies immer wieder zu unterschiedlichen Auslegungen führte.

§ 35 Abs. 1 HMG

Die Meldebehörde darf Parteien, anderen Trägern von Wahlvorschlägen und Wählergruppen im Zusammenhang mit Wahlen zum Deutschen Bundestag, zum Europäischen Parlament, mit Landtags- und Kommunalwahlen sowie mit Ausländerbeiratswahlen in den sechs der Wahl vorangehenden Monaten Auskunft aus dem Melderegister über die in § 34 Abs. 1 Satz 1 bezeichneten Daten von Gruppen von Wahlberechtigten erteilen, soweit für deren Zusammensetzung das Lebensalter bestimmend ist. Die Geburtstage der Wahlberechtigten dürfen nicht mitgeteilt werden. Die Empfängerin oder der Empfänger hat die Daten spätestens einen Monat nach der Wahl zu löschen.

§ 34 Abs. 1 Satz 1 HMG

Personen, die nicht Betroffene sind, und anderen als den in § 31 Abs. 1 bezeichneten Stellen darf die Meldebehörde nur Auskunft über

1. Vor- und Familiennamen,
2. Doktorgrad und
3. Anschriften einzelner bestimmter Einwohnerinnen und Einwohner

übermitteln (einfache Melderegisterauskunft).

Der Hessische Verwaltungsgerichtshof hat mit seinem Beschluss vom 26. Oktober 2001 zumindest klargestellt, dass nicht alle Altersgruppen gemeint sind und daher die Adressdaten aller Wahlberechtigten nicht übermittelt werden dürfen. Unklar blieb jedoch weiterhin, welche Lückenbildung in der Altersgruppenregelung dem Sinn des § 35 Abs. 1 HMG entspricht. Ich habe daher das Hessische Innenministerium gebeten, im Rahmen der Novellierung des Hessischen Meldegesetzes die Vorschriften des § 35 Abs. 1 HMG genauer zu fassen.

Das Innenministerium hat sich nach einer Umfrage in den anderen Bundesländern entschlossen, im Erlasswege die hessischen Meldebehörden darauf hinzuweisen, dass sich Gruppenauskünfte an Parteien immer nur auf einen Teil der Wahl- oder Stimmberechtigten beziehen können und dass "eine Gruppenbildung, die über 50 v.H. der Wahlberechtigten erfasst, möglichst nicht zugelassen werden sollte".

Aus Gründen der Rechtssicherheit und Rechtsklarheit halte ich meine Empfehlung, § 35 Abs. 1 HMG im Rahmen der anstehenden Novellierung des Hessischen Meldegesetzes genauer zu fassen, trotzdem aufrecht.

8.4
Datenübermittlungen zwischen Ordnungsamt und Steueramt wegen Haltens gefährlicher Hunde

Auch bei zwischenbehördlicher Datenübermittlung ist strikt darauf zu achten, dass nicht mehr Daten übermittelt werden als die zugrunde liegende Rechtsvorschrift es erlaubt.

Eine Bürgerin bat mich, die Rechtmäßigkeit einer Datenübermittlung vom Ordnungsamt an das Steueramt zu überprüfen. Nachdem das Ordnungsamt festgestellt hatte, dass der von dieser Bürgerin gehaltene Hund als gefährlich eingestuft werden muss, bekam sie vom Kassen- und Steueramt einen neuen Steuerbescheid und die Aufforderung zum Austausch der Hundemarke.

Gemäß § 15 Abs. 6 der Gefahrenabwehrverordnung über das Halten und Führen von Hunden (HundeVO) hat die Behörde, die für die Erteilung der Erlaubnis zur Haltung eines gefährlichen Hundes zuständig ist, der für die Erhebung der Hundesteuer zuständigen Stelle innerhalb der Kommune Namen und Anschriften von Haltern gefährlicher Hunde mitzuteilen.

§ 15 Abs. 6 HundeVO

Die zuständige Behörde teilt der für die Erhebung der Hundesteuer zuständigen Stelle innerhalb der Gemeinde Namen und Anschriften von Halterinnen und Haltern gefährlicher Hunde mit.

In dem mir vorgelegten Fall erfolgte die Information des Steueramts der Einfachheit halber durch die Übersendung einer Kopie der Erlaubnis, die der Betroffene zum Halten seines Hundes erhält. Diese Erlaubnis enthielt aber neben dem Namen und der Adresse auch das Geburtsdatum und den Geburtsort der Betroffenen. Die Weitergabe dieser beiden Daten an das Steueramt ist in der HundeVO nicht vorgesehen und daher datenschutzrechtlich unzulässig.

Ich habe die Kommune aufgefordert, nur noch die erforderlichen Daten an das Steueramt zu übermitteln. Das Verfahren wurde von der Kommune entsprechend geändert: die Kopie für das Steueramt enthält nur noch den Namen und die Adresse der betroffenen Hundehalter.

9. Baurecht

9.1
Planfeststellungsverfahren zum Bau der A380-Wartungshalle – Behandlung der Einwenderdaten

Das Regierungspräsidium Darmstadt hat im Rahmen des Planfeststellungsverfahrens zum Bau der Wartungshalle für den Airbus A380 die Auswertung der Einwendungen gegen den geplanten Bau einer Privatfirma übertragen. Die zu schließenden Verträge sowie die ordnungsgemäße Datenverarbeitung bei dieser Firma habe ich datenschutzrechtlich überprüft. Die Frage, ob die Einwenderdaten personenbezogen an die Betreiberin weitergeben werden dürfen war in diesem Fall zu verneinen, da sie selbst vorgetragen hat, dass sie diese Daten lediglich in anonymisierter Form benötigt.

9.1.1
Auftragsdatenverarbeitung

Wie im vergangenen Jahr beim Raumordnungsverfahren zum Ausbau des Frankfurter Flughafens hatte das Regierungspräsidium (RP) Darmstadt die Auswertung der Einwendungen als Auftragsdatenverarbeitung gemäß § 4 HDSG einer Privatfirma übertragen. Hinsichtlich der Überprüfung der Verträge zwischen dem RP als Auftraggeber und der privaten Firma als Auftragnehmerin sowie der Datenverarbeitung bei der Auftragnehmerin beziehe ich mich auf meine Darstellung im 31. Tätigkeitsbericht, Ziff. 3.2. Die Ausgestaltung der Verträge und die Ablauforganisation im Planfeststellungsverfahren waren im Wesentlichen identisch, sodass meine Ausführungen auch für die diesjährige Prüfung gelten.

9.1.2
Behandlung der Einwenderdaten

In der Vergangenheit wurden in Hessen bei der Durchführung von Planfeststellungsverfahren grundsätzlich alle Daten der Einwender personenbezogen an die Vorhabenträgerin weitergegeben. Diese Vorgehensweise war auch in anderen Bundesländern gebräuchlich, ist aber im Zusammenhang mit dem Ausbau des Flughafens Berlin-Schönefeld vom Bundesverwal-

tungsgericht (Beschluss vom 14. August 2000, Az.: BVerwG 11 VR 10.00) gerügt worden. Das Gericht hatte zwar grundsätzlich die personenbezogene Weitergabe der Daten nicht beanstandet, jedoch ausgeführt, dass eine anonymisierte Weitergabe der Daten zu erfolgen habe, "*wenn der Einwender im Einzelfall darlegen kann, dass ihm durch die Weitergabe seiner nicht anonymisierten Einwendung besondere und unzumutbare und mithin von der Funktion des Anhörungsverfahrens nicht mehr gedeckte Nachteile entstehen, die es gebieten, das Verfahrens- und Rechtsverfolgungsinteresse der Vorhabenträger ausnahmsweise hinter dem Recht auf informationelle Selbstbestimmung zurücktreten zu lassen*".

Gegenüber dem RP hatte ich deshalb darauf gedrungen, dass dies in den Text über die ortsübliche Bekanntmachung der Planauslegung Eingang finden müsse.

In dem vom RP entworfenen Muster für eine ortsübliche Bekanntmachung über die Auslegung der Pläne befand sich dann folgende Passage:

> *"Es wird darauf hingewiesen, dass die Einwendungen grundsätzlich personenbezogen an die Vorhabenträgerin weitergeleitet werden, damit diese zur geltend gemachten Betroffenheit Stellung nehmen kann.*
> *Nur in besonders begründeten Einzelfällen können die personenbezogenen Daten der Einwenderinnen und Einwender vor der Weitergabe an die Vorhabenträgerin anonymisiert werden. Diese Ausnahme kommt grundsätzlich nur in Betracht, wenn der Einwenderin bzw. dem Einwender durch die Weitergabe der Daten an die Vorhabenträgerin unzumutbare Nachteile entstehen würden. …*
> *Die Einwenderinnen und Einwender werden daher gebeten, Gründe, aus denen sich ggf. ein besonderes Schutzbedürfnis ableiten lässt, das gegen eine personenbezogene Weitergabe der Einwendung an die Frankfurt Airport Services Worldwide AG (Fraport AG) spricht, im Einwendungsschreiben detailliert darzulegen."*

Dieses Muster hat der RP den vom Bau der Wartungshalle betroffenen Kommunen für die Planauslegung zur Verfügung gestellt. Daneben wies der RP auch auf seiner Homepage darauf hin, dass die Möglichkeit existiert, Einwendungen gegen den Bau der Wartungshalle vorzutragen. Dieser Text enthielt allerdings die oben zitierte Passage nicht, wonach beim RP ein Antrag auf anonymisierte Weitergabe der Daten an die Fraport AG gestellt werden konnte.

Viele Bürger haben nur den Hinweis im Internet wahrgenommen und deshalb keine Kenntnis darüber erlangt, dass die Möglichkeit besteht, eine anonymisierte Weitergabe ihrer Daten an die Vorhabenträgerin zu beantragen. Folglich haben sie von diesem Recht auch keinen Gebrauch gemacht. Dagegen richteten sich diverse Bürgerbeschwerden. Gespräche mit der Fraport AG haben ergeben, dass die Fraport AG in diesem speziellen Verfahren weder den Namen noch die genaue Adresse des Einwenders benötigt. Für die Fraport AG war wegen der örtlichen Zuordnung lediglich die Kenntnis der Postleitzahl der Einwender von Bedeutung. Weitere Daten hätte sie nur dann benötigt, soweit diese zur Erwiderung auf ein Sachargument erforderlich wären.

Da in diesem Planfeststellungsverfahren die Vorhabenträgerin explizit erklärt hat, Einwendungen nur anonymisiert zu benötigen, ist eine personenbezogene Weitergabe der Daten nicht erforderlich. Ich habe daher dem RP in Darmstadt mitgeteilt, dass die Weitergabe der Einwendungen nur anonymisiert, also ohne Name, Straße und Hausnummer erfolgen darf. Das RP hat die Daten daraufhin nur in anonymisierter Form an die Fraport AG übermittelt.

9.2
Beteiligung privater Dritter an der Bauleitplanung

Zur Beschleunigung des Bauleitplanverfahrens können die Gemeinden Teile des Verfahrens auf private Dritte übertragen. Insbesondere gilt dies für die nach dem Baugesetzbuch erforderliche Bürgerbeteiligung an der Bauleitplanung. Dies sieht § 4b Baugesetzbuch ausdrücklich vor. Wenn von dieser Möglichkeit Gebrauch gemacht wird, sollten die Verwaltungen die Bevölkerung darüber informieren.

Ein Betroffener hatte sich darüber beschwert, dass seine Gemeindeverwaltung im Zuge der Aufstellung des Bebauungsplans und der Änderung des Flächennutzungsplans seine Eingaben zu diesen Plänen an ein privates Planungsbüro weitergegeben hatte. Er sah in der Weitergabe seiner Einwendungen einen Verstoß gegen datenschutzrechtliche Bestimmungen. Die Einwendungen gegen den Bebauungsplan und die Änderung des Flächennutzungsplans seien allein für die Gemeinde bestimmt gewesen; in die Weitergabe an eine private Firma habe er nie eingewilligt.

Die Gemeinde rechtfertigte die Hinzuziehung eines privaten Planungsbüros unter Hinweis auf § 4b Baugesetzbuch (BauGB), der die Gemeinde berechtige, zur Beschleunigung des Bauleitplanverfahrens die Vorbereitung und Durchführung von Verfahrensschritten auf einen Dritten zu übertragen.

§ 4b BauGB

Die Gemeinde kann insbesondere zur Beschleunigung des Bauleitplanverfahrens die Vorbereitung und Durchführung von Verfahrensschritten nach den §§ 2a bis 4a einem Dritten übertragen.

Der Gesetzgeber wollte mit dieser Norm Teile des Planungsverfahrens bewusst in private Hände legen. Vorbild der Regelung war insoweit das aus dem Amerikanischen bekannte Mediationsverfahren; das ist die Suche nach einer interessengerechten kooperativen Konfliktlösung zwischen Beteiligten - Planungsbehörde einerseits, Einwender andererseits - vermittels eines neutralen Dritten, der weder Entscheidungsbefugnis noch Zwangsmittel innehat.

Zu den in den §§ 2a bis 4a BauGB angesprochenen Verfahrensschritten gehört insbesondere auch die Bürgerbeteiligung, die in § 3 BauGB geregelt ist. Daraus folgt, dass die Gemeinde, wenn sie einen privaten Dritten als Verwaltungshelfer in das

Verfahren mit einbezieht, diesem auch Einwendungen von Bürgern zur Auswertung übertragen kann. Dies sehen die angesprochenen Normen im Baugesetzbuch gerade vor; denn der Verwaltungshelfer kann die Bürgerbeteiligung nach § 3 BauGB nur dann angemessen durchführen, wenn ihm auch etwaige Einwendungen überlassen werden, die dann in eine Empfehlung gegenüber der Gemeinde einfließen. Der Verwaltungshelfer (Mittler) hat letztlich allerdings keine Entscheidungsbefugnis. Er bereitet die hoheitliche Entscheidung der Gemeinde lediglich vor. Durch die angesprochenen Regelungen des Baugesetzbuchs, die Mitte der 90er Jahre vom Bundesgesetzgeber verabschiedet wurden, ist die Offenbarung der von Privatpersonen vorgetragenen Einwendungen gegenüber einem Verwaltungshelfer datenschutzrechtlich nicht zu beanstanden.

Aus datenschutzrechtlicher Sicht mangelt es dem Verfahren in der im Baugesetzbuch geregelten Form allerdings an der nötigen Transparenz. Auch wenn die Einbeziehung eines Dritten zulässig ist, muss durch entsprechende Mitteilung den Einwendern deutlich gemacht werden, dass u. a. der Verfahrensschritt Bürgerbeteiligung nicht von der Verwaltung selbst durchgeführt wird, sondern von einer Privatfirma. Im Sinne der Nachvollziehbarkeit des Verfahrens für alle Beteiligten habe ich deshalb empfohlen, bei künftigen Planungsverfahren die Bevölkerung auf diesen Umstand hinzuweisen.

9.3
Beteiligung des Denkmalbeirats im Baugenehmigungsverfahren

Personenbezogene Daten aus einem Baugenehmigungsverfahren, in dem auch die Denkmalbehörde zu beteiligen ist, dürfen auch gegenüber den Mitgliedern des Denkmalbeirats offenbart werden. Diese unterliegen der gleichen Verschwiegenheitspflicht wie Stadtverordnete.

Ein Bürger hatte sich bei meiner Dienststelle darüber beschwert, dass seine Bauantragsunterlagen in personenbezogener Form an den Denkmalbeirat seiner Heimatgemeinde weitergegeben worden waren. Er kritisierte in diesem Zusammenhang, dass die Mitglieder des Denkmalbeirats keine gewählten Parlamentsmitglieder seien, sondern "Leute aus der Stadt".

Die Einbeziehung des Denkmalbeirates war datenschutzrechtlich nicht zu beanstanden. Für das anstehende Baugenehmigungsverfahren war die Beteiligung der unteren Denkmalschutzbehörde gesetzlich vorgeschrieben, da es um eine Baumaßnahme innerhalb eines denkmalgeschützten Bereichs ging.

Die Bildung eines Denkmalbeirates, der die Behörde bei der Entscheidung unterstützt, findet ihre rechtliche Grundlage in § 3 Abs. 3 des Hessischen Denkmalschutzgesetzes (HDSchG).

§ 3 Abs. 3 HDSchG

Bei der unteren Denkmalschutzbehörde soll nach Anhörung der Denkmalfachbehörde vom Kreisausschuss oder Magistrat ein sachverständiger, weisungsunabhängiger Beirat berufen werden, der die Denkmalschutzbehörde bei der Durchführung ihrer Aufgaben unterstützt. Der Beirat kann bestimmte Aufgaben auf ehrenamtliche Vertrauensleute übertragen.

Der nach dem HDSchG explizit vorgesehene Denkmalbeirat dient der fachlichen Unterstützung der Unteren Denkmalbehörde. Er ist als sachkundiges Gremium, nicht als politisches Repräsentationsorgan konstruiert. Um der beratenden Tätigkeit nachgehen zu können, benötigt dieses Gremium die entsprechenden Sachinformationen, die bei einem konkreten Baugenehmigungsverfahren zwangsläufig personenbezogen sind. Die Kritik an der Zusammensetzung des Denkmalbeirats geht fehl, da das Denkmalschutzgesetz bewusst die Einbeziehung von Personen in die Beratung vorsieht, die außerhalb der Verwaltung und des Parlaments stehen, aber aufgrund ihrer beruflichen Tätigkeit ihre Sachkunde in die Entscheidungsfindung einbringen können. Im konkreten Fall gehörten dem Beirat z. B. mehrere Architekten an. Die Mitglieder des nach § 3 Abs. 3 HDSchG gebildeten Beirats sind im Übrigen ehrenamtlich Tätige im Sinne der Hessischen Gemeindeordnung (HGO). Damit unterliegen sie der gleichen Verschwiegenheitspflicht wie Stadtverordnete. Ein Verstoß gegen Verschwiegenheitspflichten wäre eine Ordnungswidrigkeit gemäß § 24a Nr. 2 HGO.

10. Forschung

10.1
Aufbau eines Forschungsdatenzentrums der Statistischen Landesämter

Die Statistischen Landesämter streben den Aufbau eines gemeinsamen Forschungsdatenzentrums an. Das Datenschutzkonzept ist derzeit noch Gegenstand der Diskussion zwischen den Statistischen Landesämtern und den Datenschutzbeauftragten des Bundes und der Länder.

Die vom Bundesministerium für Bildung und Forschung eingesetzte Kommission zur Verbesserung der informationellen Infrastruktur zwischen Wissenschaft und Statistik hat 2001 ein Gutachten "Wege zu einer besseren informationellen Infrastruktur" vorgelegt (veröffentlicht von der Nomos Verlagsgesellschaft, 2001). In diesem Gutachten geht die Kommission davon aus, dass die Leistungsfähigkeit der Dateninfrastruktur eine entscheidende Grundlage für die Leistungsfähigkeit der Gesellschaft sowie für eine im internationalen Maßstab innovationsfähige sozial- und wirtschaftswissenschaftliche Forschung ist. Die Empfehlungen der Kommission werden zurzeit vom Gründungsausschuss des Rates für Sozial- und Wirtschaftsdaten umgesetzt. Der Gründungsausschuss hat mehrere Datenproduzenten - darunter auch die Statistischen Ämter - aufgefordert, so genannte Forschungsdatenzentren einzurichten.

10.1.1
Ausgestaltung und Ziel des Forschungsdatenzentrums

Die Einrichtung des Forschungsdatenzentrums des Statistischen Bundesamtes erfolgte im Oktober 2001. 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. Nach dem derzeitigen Konzept wird das Forschungsdatenzentrum in Form einer Arbeitsgemeinschaft der Statistischen Landesämter betrieben, wobei jedes Statistische Landesamt jeweils einen regionalen Standort des Forschungsdatenzentrums bildet. 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 v.H. 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.

10.1.2
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, u. a. hat in dem von mir geleiteten Arbeitskreis "Wissenschaft" und in dem Arbeitskreis "Statistik" der Datenschutzbeauftragten eine gemeinsame Diskussion der datenschutzrechtlichen Fragen stattgefunden. Insbesondere die Fragen der rechtlichen Grundlagen einer Zentralisierung der Statistiken bei einzelnen Landesämtern und des Bereitstellens von Mikrodaten für die Wissenschaft sind Gegenstand von Diskussionen.

10.1.2.1
Aufbau einer fachlich zentralisierten Datenhaltung

Die geplante Zusammenführung und Aufbereitung der Einzeldatensätze bei dem für die betreffende Fachstatistik auf Grund interner Absprache zuständigen Landesamt (dem fachlich federführenden "Serveramt") ist nach Auffassung der Statistischen Landesämter als Datenverarbeitung im Auftrag zu qualifizieren. Die Serverämter sollen insbesondere

- die Daten bei den „Eignerämtern“ anfordern,
- die Daten auf Vollständigkeit und formale Korrektheit prüfen,
- die Daten speichern und
- die Daten vor der Weitergabe oder Veröffentlichung stellvertretend für alle statistischen Landesämter überprüfen.

Diskutiert wurde von den Datenschutzbeauftragten, ob die zentrale Vorhaltung von Statistikdaten der Bundesländer bei jeweils einem Statistischen Landesamt auf der rechtlichen Grundlage einer Datenverarbeitung im Auftrag möglich ist oder ob sie als Funktionsübertragung qualifiziert werden muss - mit der Folge der Notwendigkeit einer gesetzlichen Regelung (z. B. Staatsvertrag). Im Ergebnis gehe ich wie auch die meisten anderen Datenschutzbeauftragten davon aus, dass für die auf drei Jahre begrenzte Pilotphase die zentrale Vorhaltung der Statistikdaten auf der Grundlage einer Datenverarbeitung im Auftrag akzeptiert werden kann, und zwar im Hinblick darauf, dass

- die rechtliche Zuständigkeit bei den Eignerämtern verbleiben soll und
- jede weitere Verarbeitung und Nutzung der Daten, z. B. auch die Weitergabe an Wissenschaftler, nur auf Grund einer schriftlichen Weisung des Eigneramtes erfolgen soll.

Nach Auffassung der Datenschutzbeauftragten sollten aber die zentral vorgehaltenen Daten soweit wie möglich verschlüsselt werden. Einzelheiten hinsichtlich des Umfangs und der Art und Weise der Verschlüsselung der Statistikdaten sind noch offen. Mittelfristig sollte eine gesetzliche Regelung des neuen Verfahrens erfolgen, da die Infrastruktur im Statistikbereich erheblich verändert wird.

10.1.2.2
Bereitstellung von Mikrodaten für die Wissenschaft

Nach den Regelungen der Statistikgesetze (§ 16 Abs. 6 Bundesstatistikgesetz und die entsprechenden Regelungen der Landesstatistikgesetze) können Wissenschaftler auf anonymisierte Mikrodaten zugreifen, wenn

- die anfordernde Stelle eine Hochschule oder sonstige Einrichtung mit der Aufgabe unabhängiger wissenschaftlicher Forschung ist,
- die angeforderten statistischen Einzelangaben für die Durchführung eines wissenschaftlichen Vorhabens vorgesehen sind,
- die Einzelangaben nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft zugeordnet werden können und
- die Empfänger Amtsträger oder ihnen Gleichgestellte sind.

Eine Übermittlung nicht anonymisierter Einzeldatensätze an externe Wissenschaftler ist in den Statistikgesetzen nicht vorgesehen, ist also mit dem Statistikgeheimnis nicht vereinbar.

In dem Konzept der Statistischen Landesämter sind folgende Möglichkeiten der Bereitstellung von Mikrodaten für Wissenschaftler in den Forschungsdatenzentrum vorgesehen:

- **Faktisch anonymisierte Mikrodaten zur Off-site-Nutzung (Scientific use files)**
  Scientific use files werden bereits seit längerer Zeit von den Statistischen Ämtern erstellt. Ebenso wie auch meine Kolleginnen und Kollegen sehe ich insoweit keine datenschutzrechtlichen Probleme.

- **Faktisch anonymisierte Mikrodaten zur On-site-Nutzung**
  Den Wissenschaftlern sollen faktisch anonymisierte Mikrodaten an einem abgeschotteten Arbeitsplatz im Serveramt zur Verfügung gestellt werden.
  Auch insoweit sehe ich - wie auch die anderen Datenschutzbeauftragten - keine datenschutzrechtlichen Probleme. Die rechtlichen Anforderungen an die Anonymisierung bleiben grundsätzlich gleich. Für die Prüfung, ob eine hinreichende Anonymisierung vorliegt, kann es aber von Bedeutung sein, dass der Wissenschaftler an einem Arbeitsplatz in einem Statistischen Landesamt arbeitet und z. B. das Zuspielen von Zusatzwissen durch Abschottung des PC unterbunden wird.

- **Nicht anonymisierte Mikrodaten für die On-site-Nutzung im Rahmen von Projekten, die im Auftrag einer Bundes- oder Landesbehörde als Zusatzaufbereitung oder im eigenen Interesse eines Statistischen Amtes durchgeführt werden**
  Angestrebt wird von den Landesämtern über die vorgenannten Pläne hinaus die Möglichkeit, dass für die Durchführung eines Forschungsvorhabens zwischen dem jeweils beteiligten Amt und dem Wissenschaftler ein Vertrag geschlossen wird, durch den der Wissenschaftler für die Zeit seiner Tätigkeit im statistischen Amt zum Mitarbeiter der amtlichen Statistik wird, d. h., er soll in das Amt inkorporiert werden mit der rechtlichen Folge, dass er nicht als externer Dritter zu qualifizieren ist und die Datenweitergabe an ihn nicht als Datenübermittlung im Sinne der Statistikgesetze. Auf diesem Wege soll dem Wissenschaftler Zugang zu nicht anonymisierten Mikrodaten gewährt werden können. Diese rechtliche Konstruktion ist jedoch problematisch, weil sie im Ergebnis die Regelungen der Statistikgesetze zum Statistikgeheimnis relativiert. Wenn dieser neue Weg des Datenzugangs routinemäßig bei allen Serverämtern eröffnet werden soll, bedarf es einer klaren Regelung des Gesetzgebers in den Statistikgesetzen.

Die konkrete Ausgestaltung des Datenschutzkonzepts für das Forschungsdatenzentrum wird 2004 zwischen den Statistischen Landesämtern und den Datenschutzbeauftragten des Bundes und der Länder abschließend diskutiert werden.

10.2
Datenschutzrechtliche Anforderungen an den Aufbau von medizinischen Forschungsnetzen

10.2.1
Prüfung der Umsetzung des Datenschutzkonzepts für das Kompetenznetz Parkinson

Das Kompetenznetz Parkinson hat das mit den Datenschutzbeauftragten abgestimmte Datenschutzkonzept im Wesentlichen korrekt umgesetzt. Hinsichtlich der von mir festgestellten Defizite wurden inzwischen die notwendigen Maßnahmen getroffen.

Das Kompetenznetz Parkinson ist eines der vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Kompetenznetze, die die Durchführung von interdisziplinären Forschungsprojekten zu speziellen Krankheitsbildern intensivieren sollen (siehe www.kompetenznetz-parkinson.de). Die Kompetenznetze gehören der Telematikplattform für medizinische Forschungsnetze (TMF) an. Der Zusammenschluss im Rahmen der TMF hat u. a. zum Ziel, die Kompetenzen der Forschungsnetze auf dem Gebiet der Telematik zu bündeln und den Transfer von Know-how innerhalb der Forschungsnetze und untereinander zu systematisieren und zu koordinieren (s. www.german-health-research-net.de).

Als federführend zuständiger Datenschutzbeauftragter habe ich das Kompetenznetz hinsichtlich der datenschutzrechtlichen Anforderungen beraten. Am Beispiel des Kompetenznetzes Parkinson wurde parallel dazu auch im Arbeitskreis Wissenschaft der Datenschutzbeauftragten des Bundes und der Länder, teilweise auch gemeinsam mit Vertretern der TMF, grundsätzlich über die datenschutzrechtlichen Rahmenbedingungen des Aufbaus von Forschungsnetzen diskutiert. Das auf Grund der Diskussionen entwickelte Datenschutzkonzept für das Kompetenznetz Parkinson wurde von mir in Abstimmung mit allen Datenschutzbeauftragten akzeptiert (eingehend zum Datenschutzkonzept 29. Tätigkeitsbericht, Ziff. 9.2; 30. Tätigkeitsbericht, Ziff. 26.6; DuD 2002, S. 605 ff.).

In diesem Jahr habe ich die Umsetzung des Datenschutzkonzepts in Marburg überprüft. Die Prüfung führte zu folgenden Ergebnissen:

- **Aktueller Sachstand**
  Am Kompetenznetz nahmen zum Zeitpunkt der Prüfung (16. Juli 2003) 143 Ärzte bundesweit teil. Die Daten von 3.104 Patientinnen und Patienten waren bereits eingegeben.

- **Pseudonymisierungsverfahren**
  Das festgelegte Verfahren der Pseudonymisierung der Patientendaten vor einer Datenübermittlung vom behandelnden Arzt an die zentrale Datenbank des Kompetenznetzes mit Einsatz eines Treuhänders hat in der Praxis funktioniert und zu keinen erwähnenswerten Problemen geführt.

- **Verfahren der Freigabe von Daten aus der zentralen Datenbank**
  Bisher hat kein externer Forscher die Freigabe von pseudonymisierten Patientendaten aus der zentralen Datenbank des Kompetenznetzes beantragt. Soweit Anträge interner Forscher auf Freigabe von pseudonymisierten Patientendaten vom Vorstand genehmigt wurden, wurde zwar im Ergebnis korrekt verfahren, das Verfahren war jedoch nicht ausreichend schriftlich dokumentiert. Ich habe gefordert, dass künftig eine Herausgabe von Daten durch das Netzwerksekretariat nur auf Grund einer schriftlichen Anweisung des Vorstands erfolgt, die zur Dokumentation des Verfahrens aufbewahrt wird, damit die Abläufe bei evtl. später auftretenden Fragen oder Problemen nachvollzogen werden können. Entsprechende Formulare wurden nach der Prüfung umgehend entwickelt und auch bereits verwendet.

- **Kontrolle des Vorliegens der Einwilligung des Patienten**
  Bei einer Demonstration des Eingabeverfahrens durch den behandelnden Arzt haben wir festgestellt, dass die Patientendaten nicht auf dem Server gespeichert werden können, solange nicht die Angabe "Einwilligungserklärung vom Patienten unterschrieben" vom Arzt bestätigt wurde.

- **Löschung von Patientendaten**
  Geprüft wurde von mir das Verfahren der Löschung von Patientendaten. Eine Löschung der Daten erfolgt entweder wenn der Patient die Einwilligung zurückzieht oder wenn der Patient verstirbt. Festgestellt habe ich, dass gelöschte Daten bei bestimmten Auswertungen der Datenbank noch angezeigt wurden. Ich habe daher gefordert, dass die Löschung für alle Auswertungen zum Tragen kommt.

- **Datensicherheitsmaßnahmen**
  Bei den räumlichen Sicherungsmaßnahmen ergaben sich kleinere Defizite. So mussten an den Türen Änderungen vorgenommen werden. Ferner war eine Alarmanlage installiert, zu deren Einsatz allerdings noch organisatorische Regelungen getroffen werden mussten die sicherstellen, dass die Alarmanlage außerhalb der Arbeitszeiten aktiv ist und im Fall eines Alarms Kontrollen erfolgen.

  Die eingesetzte Firewall war eine eigenprogrammierte Lösung auf UNIX-Basis. Die Lösung war zertifiziert. Der Zertifizierungsreport konnte eingesehen werden. Die darin geforderten zusätzlichen Maßnahmen waren soweit ersichtlich umgesetzt. Ergänzend zur Firewall wurden zwei Intrusion Detection Systeme eingesetzt. Es war mit Checklisten sichergestellt, dass alle Protokolle täglich kontrolliert wurden. Die Checkliste und das Serverlogbuch wurden schriftlich geführt. Sie waren vollständig.

  Die Passwörter waren mindestens 8-stellig mit Sonderzeichen und Ziffern. Nach 30 Tagen waren sie zu ändern. Die zur Administration der Komponenten nötigen Passwörter waren schriftlich hinterlegt. Daraus ergab sich kein Problem, da eine Anmeldung nur mit dem SU-Kommando möglich war und jeder Administrator seine eigene Anmeldekennung hat.

  Die Verschlüsselung der Kommunikationsverbindung mit SSL war aktiv (RC4 mit 128 Bit).

10.2.2
Generische Modelle für den Datenschutz in Forschungsnetzen

Die TMF und die Datenschutzbeauftragten des Bundes und der Länder haben gemeinsam ein allgemeines Datenschutzkonzept für die medizinische Forschung erstellt, das auf nahezu beliebig vernetzte medizinische Forschungsvorhaben in Deutschland übertragbar ist und künftig allen Forschungsnetzen zur Verfügung gestellt werden kann.

Vor dem Hintergrund der Diskussion über das Datenschutzkonzept des Kompetenznetzes Parkinson (s. Ziff. 10.2.1) hat die TMF gemeinsam mit dem Arbeitskreis Wissenschaft der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ein allgemeines, generisches Datenschutzkonzept erarbeitet, damit die datenschutzrechtlichen Fragen nicht bei jedem Forschungsnetz erneut, teuer und zeitraubend anhand des jeweiligen Einzelkonzepts umfassend diskutiert werden müssen und den Forschungsnetzen Musterlösungen für die Erstellung ihres Datenschutzkonzepts zur Verfügung stehen. Die medizinischen Forschungsnetze haben je nach Forschungsgegenstand, Kreis der beteiligten Institutionen und Arbeitsweise unterschiedlichen Bedarf an Daten und Strukturen der Datenverarbeitung. Verbindlich festgelegte Standardlösungen für alle Netze kann es daher nicht geben. Erstellt wurden jedoch modifizierbare Musterlösungen für zwei Varianten von medizinischen Forschungsnetzen:

- **Datenschutzkonzept für klinisch fokussierte Forschungsnetze**
  Bei diesem Netztypus erheben und dokumentieren vor allem die Ärzte und ihre Mitarbeiter Daten ihrer Patienten direkt aus dem Behandlungsprozess heraus. Sie können die im Forschungsnetz erfassten Daten - auch die Daten der die Patienten jeweils mitbehandelnden Ärzte - auch für den Behandlungsprozess wieder nutzen. Aus Datensicherheitsgründen ist sichergestellt, dass zu keinem Zeitpunkt an irgendeiner Stelle außer beim behandelnden Arzt die Identifikationsdaten und die medizinischen Daten eines Patienten gemeinsam verfügbar sind, zwei räumlich und organisatorisch getrennte Datenbanken gewährleisten eine strikte Trennung der beiden Datenbestände. Zugriff von Wissenschaftlern ist nur offline und in der Regel nur auf pseudonymisierte Daten möglich.

- **Datenschutzkonzept für wissenschaftlich fokussierte Netze**
  Bei diesem Netztypus werden die Patientendaten in einem vom Behandlungsprozess abgekoppelten Dokumentationsvorgang in einer zentralen Datenbank pseudonymisiert gespeichert. Die Forschungsdatenbank steht auf Antrag für den Online-Zugriff durch Wissenschaftler zur Verfügung.

Bei beiden Konzepten muss die Einwilligung der Patienten in die Verarbeitung ihrer Daten eingeholt werden. In beiden Konzepten sind zum Teil vergleichbare Strukturen und Prozeduren sowie kryptographische und technisch-organisatorische Schutzmaßnahmen enthalten. Musterlösungen für vertragliche Regelungen, Einverständniserklärungen der Patienten im Hinblick auf die Verarbeitung ihrer Daten und die Verwendung ihrer Blut- und Gewebeproben sind in den Konzepten ebenfalls enthalten. Beide Modelle ermöglichen es, dass der Patient über seinen Hausarzt eine Mitteilung erhält, wenn die wissenschaftliche Auswertung seiner Daten bzw. Proben zu wesentlichen neuen Erkenntnissen für den Behandlungsprozess führt.

Die generischen Modelle werden gegen Ende des Jahres veröffentlicht (Kurzfassung s. Reng, Deutsches Ärzteblatt, Heft 33, S. A2134 ff.) und datenschutzrechtlichen Beratungen durch die TMF und durch die Datenschutzbeauftragten ab sofort zugrunde gelegt.

11. Hochschulen

Videoeinsatz an Hochschulen

Die Hochschulen können bei Einhaltung datenschutzrechtlicher Anforderungen Videoüberwachung einsetzen, um den Diebstahl von IT-Geräten in studentischen Rechnerräumen zu verhindern.

Die Bedürfnisse der Verwaltung, die Videoüberwachung zur Vermeidung von möglichen Straftaten einzusetzen, wachsen offensichtlich unaufhaltsam. Die Universität Marburg hat seit längerer Zeit mit dem Problem zu kämpfen, dass IT-Geräte (PC, Bildschirme, Beamer) aus verschiedenen Rechnerräumen der Hochschule gestohlen werden. Diese Räume stehen den Studierenden zur Nutzung offen, werden aber oft aus Kostengründen nicht durch anwesendes Personal überwacht. Selbst technische Sicherungen gegen Diebstahl, etwa durch Metallkästen oder Stahlseilbefestigungen, halten Diebe nicht ab. Daher bat mich die Hochschulleitung, die Frage der Zulässigkeit des Videoeinsatzes zu klären, wie schon in der Vergangenheit in ähnlichen Fällen (s. 30. Tätigkeitsbericht, Ziff. 17.5.2).
Als einschlägige Rechtsvorschrift war hier § 14 Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) zu prüfen.

§ 14 Abs. 4 HSOG

Die Gefahrenabwehrbehörden dürfen offen Bildaufzeichnungen anfertigen:

1. Zur Sicherung öffentlicher Straßen und Plätze, auf denen wiederholt Straftaten begangen worden sind, sofern tatsächlich Anhaltspunkte für weitere Straftaten bestehen,
2. zum Schutz besonders gefährdeter öffentlicher Einrichtungen,
3. zur Steuerung von Anlagen zur Lenkung oder Regelung des Straßenverkehrs soweit Bestimmungen des Straßenverkehrsrechts nicht entgegenstehen.

Gefahrenabwehrbehörde im Sinne der Nr. 2 ist auch der Inhaber des Hausrechts. Abs. 1 Satz 2 und 3 gilt entsprechend.

Im Hinblick auf die nach Ortsbesichtigung eingeschätzte Gefahrenlage, dass die Wahrscheinlichkeit eines Diebstahls fortbesteht – insoweit sind die Voraussetzungen des § 14 Abs. 4 Nr. 2 erfüllt – und alternative kostengünstige Gegenmaßnahmen nicht erkennbar waren, habe ich die Zulässigkeit des Videoeinsatzes in dieser Situation bejaht unter folgenden Bedingungen:

1. Es sind Hinweisschilder zu errichten, die auf die besondere Gefahr des Diebstahls und auf die Video-Erfassungsbereiche verweisen,
2. die Kameras werden so positioniert, dass es unmöglich ist, zu erkennen, welche Texte sich auf dem Monitor befinden,
3. in den betroffenen Räumen erfolgt an verschiedenen Stellen ein deutlich sichtbarer Hinweis auf Videoüberwachung. Es wird auch darauf hingewiesen, dass der Film nur kurzzeitig gespeichert und nur im Falle von Straftaten ausgewertet wird,
4. die Filme werden zentral auf einem besonders gesicherten Rechner gespeichert und spätestens nach sieben Tagen gelöscht, sofern kein Diebstahl erfolgt ist,
5. der Film wird - soweit notwendig - in Anwesenheit des Datenschutzbeauftragten der Hochschule ausgewertet. Sind Mitarbeiter von der Videoanlage erfasst worden, ist dem Vorsitzenden des Personalrats Gelegenheit zu geben, bei der weiteren Auswertung anwesend zu sein,
6. bei tatsächlichen Anhaltspunkten für Straftaten können die Aufzeichnungen der Staatsanwaltschaft zugänglich gemacht werden,
7. spätestens nach einem Jahr ist zusammen mit dem internen Datenschutzbeauftragten eine schriftlich dokumentierte Evaluation des Videoeinsatzes vorzunehmen.

Ich halte diese Bedingungen für angemessen und geeignet zum Schutz der Persönlichkeitsrechte der vom Videoeinsatz betroffenen Studierenden und Mitarbeiter der Hochschule, soweit sie durch den Lehrbetrieb gezwungen sind, die Rechner-

räume zu nutzen. Entscheidend ist dabei der Umstand, dass nur eine Speicherung des von der Kamera aufgenommenen Filmes erfolgt und die nachfolgende baldige Löschung vorgesehen ist, sofern nicht der Film als Beweis im Rahmen eines erfolgten Diebstahls notwendig genutzt werden muss.

Ich gehe davon aus, dass auch andere Hochschulen in Hessen diese Rahmenbedingungen nutzen werden, um gleichgelagerten Gefahrensituationen zu begegnen.

12. Schulverwaltung, Schulen, Bildungseinrichtungen

12.1
Datenerhebung im Rahmen der Einschulung

Auch die Datenerhebung im Rahmen der Einschulung muss sich am Prinzip der Erforderlichkeit orientieren.

Die hessischen Schulen erfüllen im Rahmen der ihnen nach dem Schulgesetz zugewiesenen Pflichten zur Erziehung und Wissensvermittlung eine Fülle von Einzelaufgaben. Die dazu notwendigen Informationen über die Schüler und ihre Eltern entstammen zunächst der ersten Kontaktaufnahme, der Phase der Einschulung. Mit dieser werden verschiedene Einzelangaben über Schüler und ihre Eltern erhoben, ohne die eine ordnungsgemäße Schulverwaltung nicht möglich ist. Rechtsgrundlage für die Erhebung dieser Daten ist das datenschutzrechtliche Prinzip der Erforderlichkeit, das in § 83 Abs. 1 Schulgesetz (SchulG) konkretisiert ist.

§ 83 Abs. 1 SchulG

Schulen dürfen personenbezogene Daten von Schülerinnen und Schülern, deren Eltern und Lehrerinnen und Lehrern verarbeiten, soweit dies zur rechtmäßigen Erfüllung des Bildungs- und Erziehungsauftrags der Schule und für einen jeweils damit verbundenen Zweck oder zur Durchführung schulorganisatorischer Maßnahmen erforderlich ist.

Welche Daten der Schüler und ihrer Eltern für die Einschulung erforderlich sind, ist in Anlage 1 der "Verordnung über die Verarbeitung personenbezogener Daten in Schulen" vom 30. November 1993 (ABl. 1994, S. 114) als Ausschließlichkeitskatalog festgelegt.

Anlage 1

Daten von Schülerinnen und Schülern und Eltern, die von den Schulen verarbeitet werden dürfen

1. Individualdaten der Schülerinnen und Schüler
   - 1.1 Name, ggf. Geburtsname, Vorname
   - 1.2 Adresse
   - 1.3 Telefon
   - 1.4 Geschlecht
   - 1.5 Familienstand
   - 1.6 Geburtsdatum
   - 1.7 Geburtsort
   - 1.8 Staatsangehörigkeit (einschließlich Spätaussiedlereigenschaft, erforderlichenfalls Muttersprache)
   - 1.9 Konfession bzw. Religionszugehörigkeit sofern keine Befreiung vom Religionsunterricht vorliegt

2. Daten der Eltern
   - 2.1 Name, Vornamen
   - 2.2 Adresse
   - 2.3 Telefon
   - 2.4 Vermerk über schulische Funktionen
   - 2.5 Erziehungsberechtigung

Über den in der Verordnung festgelegten Katalog hinausgehende Daten dürfen nur auf freiwilliger Basis erhoben werden. Gleichwohl entspricht die Schulwirklichkeit häufig nicht diesen verbindlichen Vorgaben. Kontakte mit Grundschulen ergeben immer wieder die Feststellung, dass die Formulare für die Einschulung nicht nur die Katalogdaten, sondern zusätzliche Daten erheben, ohne deutlich auf die Unterscheidung zwischen Pflichtangaben und freiwilligen Angaben hinzuweisen. So wird häufig gefragt nach dem Beruf der Eltern sowie der Zahl der Geschwister und dem besuchten Kindergarten. Diese Daten sind nicht im Katalog enthalten, weil sie für die Schulverwaltung nicht erforderlich sind.

Um dieser Entwicklung entgegenzusteuern, hatte das Hessische Kultusministerium in Abstimmung mit mir ein Musterformular entwickelt, dessen Nutzung es den Grundschulen schon mit Runderlass vom 19. Dezember 1995 empfohlen hatte. Die Übernahme dieses Formulars ist aber nicht die Regel.

12.2
Akteneinsicht in Abiturprüfungsunterlagen bei Schulen

Eine langjährige Verwaltungsübung kann das gesetzlich verbriefte Recht auf Akteneinsicht nicht ausschalten.

Im Mai 2003 ging mir eine Beschwerde zu, die Anlass zur Verwunderung geben konnte. Der Beschwerdeführer hatte 1998 das Abitur an einer hessischen Schule abgelegt und bat im Mai 2003 die betroffene Schule, ihm Einsicht in seine Abitur-Prüfungsunterlagen zu geben und ihm die Abiturklausuren auszuhändigen. Die zuständige Schule lehnte die Herausgabe der Unterlagen ab mit dem Argument, die Abiturunterlagen einschließlich der Prüfungsarbeiten stünden im Eigentum des Landes. Das Akteneinsichtsrecht erlösche außerdem ein Jahr nach der Prüfung. Rechtsgrundlagen zur Begründung der Ablehnung wurden nicht genannt. Das zuständige Staatliche Schulamt verwies auf eine entsprechende langjährige Praxis und bestätigte die Auffassung der Schule. Der Beschwerdeführer bestand jedoch weiter auf seinem Akteneinsichtsrecht und wandte sich an mich.

Eine kurze Prüfung der einschlägigen Rechtsvorschrift ergab eine andere Rechtslage, die ich dem Beschwerdeführer auch mitteilte: Ihm steht das Einsichtsrecht in alle ihn betreffenden Abitur-Prüfungsunterlagen zu. Geregelt ist dies in § 72 Abs. 4 Hessisches Schulgesetz (HSchulG), der den allgemeinen Bestimmungen des HDSG als lex spezialis vorgeht:

§ 72 Abs. 4 HSchulG

Jugendliche, die Eltern und volljährige Schülerinnen und Schüler haben das Recht, Akten der Schule, Schulaufsichtsbehörden und des schulärztlichen Dienstes, in denen Daten über sie gespeichert sind, einzusehen. Die Einsichtnahme ist unzulässig, wenn die Daten der Betroffenen mit Daten Dritter derart verbunden sind, dass die Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist. In diesem Fall ist den Betroffenen über die zu ihrer Person gespeicherten Daten Auskunft zu erteilen.

Die von der Schule und dem Schulamt in der Begründung für die Ablehnung angeführte Befristung des Einsichtsrechtes lässt sich hieraus nicht herleiten. Sie wird auch nicht dem Rechtsgedanken des § 18 Abs. 5 HDSG gerecht, dem die zitierte Vorschrift eigentlich entspringt.

§ 18 Abs. 5 HDSG

Sind personenbezogene Daten in Akten gespeichert, die zur Person des Betroffenen geführt werden, dann kann er bei der speichernden Stelle Einsicht in die von ihm bezeichneten Akten verlangen. Werden die Akten nicht zur Person des Betroffenen geführt, hat er Angaben zu machen, die das Auffinden der zu seiner Person gespeicherten Daten mit angemessenem Aufwand ermöglichen. Die Einsichtnahme ist unzulässig, wenn die Daten des Betroffenen mit Daten Dritter oder geheimhaltungsbedürftigen nicht personenbezogenen Daten derart verbunden sind, dass ihre Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist. In diesem Fall ist dem Betroffenen Auskunft nach Abs. 3 zu erteilen. Im Übrigen kann ihm statt Einsicht Auskunft gewährt werden.

Die vollkommene Transparenz der staatlichen Datenverarbeitung dem Betroffenen gegenüber kann nicht davon abhängig gemacht werden, wann die Unterlagen entstanden sind. Es mag bestimmte praktische Gründe des Verwaltungsaufwandes geben, das Einsichtsrecht in Abiturarbeiten zu beschränken auf die Widerspruchs- und Klagefrist, die maximal ein Jahr beträgt. Solange keine gesetzliche Grundlage dieses Einsichtsrecht befristet, besteht der Rechtsanspruch darauf; die Einsicht darf nicht verweigert werden. Allerdings endet das Einsichtsrecht faktisch nach zehn Jahren, da dann die Abiturunterlagen nach der Erlasslage vernichtet werden müssen.

12.3
Datenschutz in Volkshochschulen

Bei der Prüfung einer Volkshochschule habe ich Mängel bei der Einhaltung des Hessischen Datenschutzgesetzes festgestellt.

Bei dem Prüfbesuch einer Kreis-Volkshochschule (VHS) im nordhessischen Bereich fand ich zahlreiche datenschutzrechtliche Mängel vor. Diese erschienen insbesondere deshalb problematisch, weil die VHS neben den Daten über ihre Beschäftigten auch über beachtliche Datenmengen hinsichtlich der Kursteilnehmer verfügt. Erwähnenswert sind folgende Details, die auch auf andere Volkshochschulen zutreffen könnten:

12.3.1
Vorabkontrolle und Verfahrensverzeichnis

Die VHS benutzt seit wenigen Jahren für die Verwaltung der Kursteilnehmer-Daten das Programm BASIS. Da das Programm erst nach In-Kraft-Treten des neuen HDSG eingesetzt wurde, verlangt § 7 Abs. 6 HDSG eine vorhergehende so genannte Vorabkontrolle.

§ 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.

Da eine solche jedoch nicht vorhanden war, wurde mir die nachträgliche Erstellung zugesagt.

Zudem verlangt § 6 Abs. 1 HDSG bei Nutzung von Verwaltungsprogrammen zur Verarbeitung von personenbezogenen Daten die Beschreibung des Verfahrens in dem so genannten Verfahrensverzeichnis.

§ 6 Abs. 1 HDSG

Wer für den Einsatz eines Verfahrens zur automatisierten Verarbeitung personenbezogener Daten zuständig ist, hat in einem für den behördlichen Datenschutzbeauftragten bestimmten Verzeichnis festzulegen:

1. Name und Anschrift der datenverarbeitenden Stelle,
2. die Zweckbestimmung und die Rechtsgrundlage der Datenverarbeitung,
3. die Art der gespeicherten Daten,
4. den Kreis der Betroffenen,
5. die Art regelmäßig übermittelter Daten, deren Empfänger sowie die Art und Herkunft regelmäßig empfangener Daten,
6. die zugriffsberechtigten Personen oder Personengruppen,
7. die technischen und organisatorischen Maßnahmen nach § 10,
8. die Technik des Verfahrens,
9. Fristen für die Löschung nach § 19 Abs. 3,
10. eine beabsichtigte Datenübermittlung nach § 17 Abs. 2,
11. das begründete Ergebnis der Untersuchung nach § 7 Abs. 6 Satz 3.

Auch dieses fehlte und musste nachträglich erstellt werden.

12.3.2
Aufklärung bei der Datenerhebung

Die VHS erhebt in der Phase des Antrages auf Kursteilnahme zahlreiche personenbezogene Daten der Kursteilnehmer. Die entsprechende Aufklärung des Betroffenen hinsichtlich der Anwendung des HDSG bestand jedoch nur in dem schriftlichen Formularhinweis, dass die Bestimmungen des Datenschutzgesetzes beachtet würden. Dies genügt jedoch nicht den Anforderungen des § 12 Abs. 4 HDSG.

§ 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.

Ich bat daher die VHS, diese Hinweise in das Anmeldeformular vollständig aufzunehmen.

12.3.3
Räumliche Sicherung

Der Raum, in dem sich der Server mit allen personenbezogenen Daten der Kursteilnehmer befindet, liegt im Erdgeschoss und ist von der öffentlichen Straße aus vollständig und leicht einsehbar. Sicherheitsfenster waren nicht vorhanden. Wegen der damit erheblich gestiegenen Einbruchsgefahr riet ich dringend zur Installation einer geeigneten Einbruchs-Alarmanlage, denn § 10 Abs. 2 Nr. 1 HDSG verlangt bereits im baulichen Bereich der datenverarbeitenden Stelle eine geeignete Schutzhülle, die den Zutritt Unbefugter effektiv verhindern soll.

§ 10 Abs. 2 Nr. 1 HDSG

… Außerdem sind Maßnahmen anzuordnen, die nach dem jeweiligen Stand der Technik und der Art des eingesetzten Verfahrens erforderlich sind, um zu gewährleisten, dass

1. Unbefugte keinen Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, erhalten (Zutrittskontrolle)

Eine solche Anlage bietet zudem den Vorteil, auch Einbruchsversuchen aus dem Inneren des Gebäudes zu begegnen, da die Tür vom jederzeit öffentlich zugänglichen Flur zum Verwaltungstrakt der VHS keine geeigneten Sicherungen enthielt.

12.3.4
Datensicherung

Die Datensicherung gehört zu den Grundstandards aller technischen Sicherungsmaßnahmen für die automatisierte Datenverarbeitung. Der Verlust der personenbezogenen Daten, insbesondere durch höhere Gewalt wie Blitzschlag, Stromüberspannung oder Feuer wäre auch für die Funktionsfähigkeit des Betriebes fatal. Daher verlangt § 10 Abs. 2 Nr. 4 HDSG entsprechende Maßnahmen.

§ 10 Abs. 2 Nr. 4 HDSG

… Außerdem sind Maßnahmen anzuordnen, die nach dem jeweiligen Stand der Technik und der Art des eingesetzten Verfahrens erforderlich sind, um zu gewährleisten, dass …

4. personenbezogene Daten nicht unbefugt oder nicht zufällig gespeichert, zur Kenntnis genommen, verändert, kopiert, übermittelt, gelöscht, entfernt, vernichtet oder sonst verarbeitet werden (Datenverarbeitungskontrolle)

Die vorgefundenen Sicherungskopien lagen direkt neben dem Server. Abgesehen von der Gefahr des schnellen Zugriffs Unbefugter auf diese Datenträger gab es also keinen wirksamen Schutz gegen Feuer. Es wurde mir daher zugesagt, die Sicherungskopien in einem speziell gesicherten Schrank in einem anderen Zimmer aufzubewahren.

12.3.5
Netzstrukturen

Die VHS verfügt über eine Vernetzung mit der Datenverarbeitung eines zweiten Standortes innerhalb des Kreises. Details der Netzstruktur und der Einbindung in öffentliche Netze waren jedoch nicht durch entsprechende Unterlagen erkennbar, wie dies § 10 Abs. 2 Nr. 7 HDSG verlangt.

§ 10 Abs. 2 Nr. 7 HDSG

… Außerdem sind Maßnahmen anzuordnen, die nach dem jeweiligen Stand der Technik und der Art des eingesetzten Verfahrens erforderlich sind, um zu gewährleisten, dass…

7. durch eine Dokumentation aller wesentlichen Verarbeitungsschritte die Überprüfbarkeit der Datenverarbeitungsanlage und des -verfahrens möglich ist (Dokumentationskontrolle)

Auch zu diesen technischen Details wurde mir eine umfangreiche schriftliche Dokumentation zugesagt.

13. Bibliotheken

Ergebnisse der Prüfung einer öffentlichen Bibliothek

Auch öffentliche Bibliotheken unterliegen den Erfordernissen des Hessischen Datenschutzgesetzes. Bei der Prüfung einer großen öffentlichen Bibliothek habe ich Mängel festgestellt, die auch für andere Bibliotheken exemplarisch sein könnten.

Im Berichtsjahr stattete ich dem Medienzentrum des Kreises Bad Hersfeld in Rotenburg einen Prüfbesuch ab. Es handelt sich um eine öffentliche Bibliothek. Dabei stellte ich verschiedene datenschutzrechtliche Mängel fest. Erwähnenswert sind folgende Details.

13.1
Antragsdaten

Die im Rahmen des Antrages auf einen Nutzerausweis erhobenen Daten waren nicht zu beanstanden bis auf die Information über die Nationalität des Benutzers, die verzichtbar ist. Dem verwendeten Antragsformular fehlte jedoch die Information des Betroffenen gemäß den Vorgaben des § 12 Abs. 4 HDSG.

§ 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.

Es wurde zugesagt, die Angaben künftig zu ergänzen.

13.2
Vorabkontrolle und Verfahrensverzeichnis

Für die Bibliotheksverwaltung war seit wenigen Jahren das Standard-Programm WINBIAP im Einsatz. Meine Frage nach der Existenz eines Verfahrensverzeichnisses und der Durchführung einer so genannten Vorabkontrolle wurde verneint.

Nach § 6 Abs. 1 HDSG hat die datenverarbeitende Stelle ein Verfahrensverzeichnis zu erstellen. Vor dem ersten Einsatz eines Verfahrens zur automatisierten Datenverarbeitung hat sie nach § 7 Abs. 6 HDSG außerdem eine Vorabkontrolle durchzuführen und das Ergebnis zu dokumentieren.

§ 6 Abs. 1 HDSG

Wer für den Einsatz eines Verfahrens zur automatisierten Verarbeitung personenbezogener Daten zuständig ist, hat in einem für den behördlichen Datenschutzbeauftragten bestimmten Verzeichnis festzulegen:

1. Name und Anschrift der datenverarbeitenden Stelle,
2. die Zweckbestimmung und die Rechtsgrundlage der Datenverarbeitung,
3. die Art der gespeicherten Daten,
4. den Kreis der Betroffenen,
5. die Art regelmäßig übermittelter Daten, deren Empfänger sowie die Art und Herkunft regelmäßig empfangener Daten,
6. die zugriffsberechtigten Personen oder Personengruppen,
7. die technischen und organisatorischen Maßnahmen nach § 10,
8. die Technik des Verfahrens,
9. Fristen für die Löschung nach § 19 Abs. 3,
10. eine beabsichtigte Datenübermittlung an Drittstaaten nach § 17 Abs. 2,
11. das begründete Ergebnis der Untersuchung nach § 7 Abs. 6 Satz 3.

§ 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.

Ich bat die Bibliotheksverwaltung, Verfahrensverzeichnis und Vorabkontrolle nachträglich anzufertigen und die Dokumentation des Programms zuzusenden.

13.3
Auftragsdatenverarbeitung

Die automatisierte Weiterbearbeitung der Bestands- und Benutzerdaten nimmt das Medienzentrum nicht selbst vor. Es nimmt lediglich die Daten über vorhandene PCs auf und bedient sich im Weiteren eines externen Fachunternehmens, dem je zum Tagesabschluss die in den Computern gespeicherten Daten per Mail zur weiteren Auswertung übermittelt werden. Die Details der vertraglichen Beziehungen zwischen dem Medienzentrum und dem Unternehmen konnten zunächst nicht geklärt werden. Ich bat daher um Zusendung des schriftlichen Vertrages, der den Anforderungen des § 4 Abs. 2 und 3 HDSG entsprechen muss.

§ 4 Abs. 2 und 3 HDSG

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Zuverlässigkeit und der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen; dabei sind der Gegenstand und der Umfang der Datenverarbeitung, die technischen und organisatorischen Maßnahmen sowie etwaige Unterauftragsverhältnisse festzulegen. Für ergänzende Weisungen gilt Satz 2 entsprechend. Der Auftraggeber hat zu prüfen, ob beim Auftragnehmer die nach § 10 erforderlichen Maßnahmen getroffen und die erhöhten Anforderungen bei der Verarbeitung von Daten, die besonderen Amts- oder Berufsgeheimnissen unterliegen sowie der in § 7 Abs. 4 genannten Daten eingehalten werden. An nicht-öffentliche Stellen darf ein Auftrag nur vergeben werden, wenn weder gesetzliche Regelungen über Berufs- oder besondere Amtsgeheimnisse noch überwiegende schutzwürdige Belange entgegenstehen.

(3) Sofern die Vorschriften dieses Gesetzes auf den Auftragnehmer keine Anwendung finden, ist der Auftraggeber verpflichtet, vertraglich sicherzustellen, dass der Auftragnehmer die Bestimmungen dieses Gesetzes befolgt und sich der Kontrolle des Hessischen Datenschutzbeauftragten unterwirft. Der Auftraggeber hat den Hessischen Datenschutzbeauftragten vorab über die Beauftragung zu unterrichten.

Die spätere Durchsicht des Vertrages ergab, dass die nach § 4 Abs. 2 HDSG notwendigen Festlegungen von technischen Sicherungsmaßnahmen fehlten. Auch die Unterwerfung des Auftragnehmers unter meine Kontrollbefugnis nach § 4 Abs. 3 HDSG fehlt. Ohne die Festlegung der technischen Sicherheitsmaßnahmen hätte bereits die Beauftragung nicht erfolgen dürfen. Ich habe daher die Medienverwaltung aufgefordert, den vorhandenen Vertrag um diese notwendigen Bestandteile zu ergänzen.

14. Gesundheitswesen

14.1
Datenschutzrechtliche Aspekte der Reform der gesetzlichen Krankenversicherung

Die Reform der gesetzlichen Krankenversicherung hat auch erhebliche Auswirkungen auf Umfang, Zweck sowie Art und Weise der Verarbeitung medizinischer Daten der ca. 60 Millionen Versicherten. Bezüglich der vorgesehenen Einführung der elektronischen Gesundheitskarte und des Aufbaus eines zentralen Datenpools konnten datenschutzfreundliche Lösungen erreicht werden. Hingegen bringt die Ausgestaltung des neuen Vergütungssystems eine Verschlechterung des Datenschutzes mit sich.

Die mit dem Gesetz zur Modernisierung der gesetzlichen Krankenversicherung - GKV-Modernisierungsgesetz (GMG) - (BGBl. I 2003, 2190) vom Bundestag beschlossene Reform der gesetzlichen Krankenversicherung umfasst strukturelle Reformen und eine Neuordnung der Finanzierung. Die Ausgestaltung der Reform ist auch von zentraler Bedeutung für die Entwicklung des Patientendatenschutzes, da etwa 90 v.H. der Bevölkerung der gesetzlichen Krankenversicherung angehören. In dem umfangreichen Gesetz sind insbesondere die Einführung der elektronischen Gesundheitskarte, der Aufbau eines zentralen Datenpools und die Ausweitung der Datenübermittlungen an die Krankenkassen bei ambulanter Behandlung von erheblicher datenschutzrechtlicher Relevanz (s. auch die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. September 2003, Ziff. 20.4).

14.1.1
Einführung der elektronischen Gesundheitskarte

Die derzeitige Krankenversichertenkarte wurde als Krankenscheinersatz in Chipkartenform eingeführt. Die Karte muss von jedem Versicherten bei jeder Inanspruchnahme einer Leistung vorgelegt werden. Die bisherigen Regelungen des § 291 SGB V legten zum Schutz des Versicherten fest, dass diese Karte keine medizinischen Daten enthalten darf, sondern lediglich Verwaltungsdaten, und nur für den Nachweis der Berechtigung zur Inanspruchnahme von Leistungen sowie für die Abrechnung mit den Leistungsträgern verwendet werden darf.

In der jetzt verabschiedeten Neuregelung des § 291 SGB V ist vorgesehen, dass die Krankenversichertenkarte die Verwaltungsdaten der Versicherten enthalten muss, ferner ein Lichtbild der Versicherten. Sie ist damit auch weiterhin Berechtigungsausweis für jede Inanspruchnahme von Leistungen, und zwar jetzt auch im Bereich der Europäischen Union.

Darüber hinaus legt der neue § 291a SGB V fest, dass die Krankenversichertenkarte bis spätestens 1. Januar 2006 zu einer elektronischen Gesundheitskarte erweitert wird. Die elektronische Gesundheitskarte wird eine Reihe von Funktionen enthalten, die eine Verarbeitung medizinischer Daten auf der Karte mit sich bringen. Hierbei ist zu unterscheiden zwischen Anwendungen, die zwingend vorgesehen sind, und Anwendungen, die mit Einverständnis des Versicherten genutzt werden können.

Die Anwendung "elektronisches Rezept", die das Papierrezept ersetzen soll, ist zwingend vorgesehen.

§ 291a Abs. 2 SGB V

Die elektronische Gesundheitskarte hat die Angaben nach § 291 Abs. 2 zu enthalten und muss geeignet sein, Angaben aufzunehmen für

1. die Übermittlung ärztlicher Verordnungen in elektronischer und maschinell verwertbarer Form sowie
2. den Berechtigungsnachweis zur Inanspruchnahme von Leistungen im Geltungsbereich der Verordnung (EWG) Nr. 1408/71 und der Verordnung (EWG) Nr. 574/72.

Ferner sind eine Reihe weitere Anwendungen vorgesehen, die ausschließlich mit Einverständnis des Versicherten genutzt werden dürfen:

- Notfalldaten
- Arzneimitteldokumentation
- elektronischer Arztbrief
- elektronische Patientenakte
- eigene Daten des Versicherten sowie
- Daten über in Anspruch genommene Leistungen und deren vorläufige Kosten für den Versicherten.

§ 291a Abs. 3 Nr. 1–6 SGB V

Über den Absatz 2 hinaus muss die Gesundheitskarte geeignet sein, folgende Anwendungen zu unterstützen, insbesondere das Erheben, Verarbeiten und Nutzen von

1. medizinischen Daten, soweit sie für die Notfallversorgung erforderlich sind,
2. Befunden, Diagnosen, Therapieempfehlungen sowie Behandlungsberichten in elektronischer und maschinell verwertbarer Form für eine einrichtungsübergreifende, fallbezogene Kooperation (elektronischer Arztbrief),
3. Daten einer Arzneimitteldokumentation,
4. Daten über Befunde, Diagnosen, Therapiemaßnahmen, Behandlungsberichte sowie Impfungen für eine fall- und einrichtungsübergreifende Dokumentation über den Patienten (elektronische Patientenakte),
5. durch von Versicherten selbst oder für sie zur Verfügung gestellte Daten sowie

6. Daten über in Anspruch genommene Leistungen und deren vorläufige Kosten für die Versicherten (§ 305 Abs. 2).

Die Datenschutzbeauftragten des Bundes und der Länder haben sich in den vergangenen Jahren bereits mehrfach mit den datenschutzrechtlichen Aspekten einer geplanten Erweiterung der Krankenversichertenkarte befasst (24. Tätigkeitsbericht, Ziff. 4.1 und 20.15; 25. Tätigkeitsbericht, Ziff. 5.3; 26. Tätigkeitsbericht, Ziff. 7.2). Zentraler Aspekt war dabei, dass die bisher bestehende Entscheidungsfreiheit der Patienten, welchem Arzt sie für welche Zwecke welche persönlichen Daten anvertrauen, auch bei der Einführung neuer Techniken gewahrt werden muss. Es darf nicht dazu kommen, dass die Patienten rechtlich oder faktisch gezwungen sind, überall im Gesundheitsbereich pauschal ihre medizinischen Daten zu offenbaren. Auf Grund der Forderungen von mir und den anderen Datenschutzbeauftragten enthält die neue Regelung des § 291a Abs. 3 bis 8 SGB V eine Reihe von datenschutzgerechten Festlegungen, die die Rechte der Patienten sicherstellen sollen:

- Die Krankenkassen müssen die Versicherten spätestens bei der Versendung der Karte umfassend über deren Funktionsweise informieren.

- Mit dem Erheben, Verarbeiten und Nutzen von Daten der Versicherten nach Abs. 3 darf erst begonnen werden, wenn die Versicherten jeweils gegenüber dem Arzt, Zahnarzt oder Apotheker ihre Einwilligung erklärt haben. Die Einwilligung ist bei erster Verwendung der Karte vom Leistungserbringer auf der Karte zu dokumentieren; die Einwilligung ist jederzeit widerruflich und kann auf einzelne Anwendungen beschränkt werden.

- Durch technische Vorkehrungen ist zu gewährleisten, dass in den Fällen des Absatzes 3 Satz 1 Nr. 2 bis 6 der Zugriff nur durch Autorisierung des Versicherten möglich ist.

- Der Zugriff auf die auf der Karte gespeicherten Daten darf durch die berechtigten Ärzte, Zahnärzte etc. grundsätzlich nur in Verbindung mit einem elektronischen (Heil-)Berufsausweis erfolgen, der über eine qualifizierte elektronische Signatur verfügt.

- Auf der Karte gespeicherte Daten nach Abs. 2 Satz 1 Nr. 1 (elektronisches Rezept) und Abs. 3 Satz 1 (alle freiwilligen Anwendungen) müssen auf Verlangen der Versicherten gelöscht werden.

- Durch technische Vorkehrungen ist zu gewährleisten, dass mindestens die letzten 50 Zugriffe auf die Daten für Zwecke der Datenschutzkontrolle protokolliert werden.

- Es besteht ein gesetzliches Verbot, vom Karteninhaber den Zugriff auf die Daten zu anderen als den gesetzlich vorgesehenen Zwecken zu verlangen. Dies schließt z. B. aus, dass Arbeitgeber von ihren Arbeitnehmern die Vorlage der Karte verlangen.

- Der Versicherte hat ein uneingeschränktes Einsichtsrecht in alle auf der Karte gespeicherten Daten.

Die technische Umsetzung der Regelungen ist derzeit noch offen. Das Gesetz sieht vor, dass die Spitzenverbände der Krankenkassen, die Kassenärztliche Bundesvereinigung, die Kassenzahnärztliche Bundesvereinigung, die Bundesärztekammer, die Bundeszahnärztekammer, die Deutsche Krankenhausgesellschaft sowie die Spitzenorganisation der Apotheker die erforderliche Informations-, Kommunikations- und Sicherheitsinfrastruktur vereinbaren. 2004 soll mit Pilotprojekten begonnen werden. Zusammen mit den anderen Datenschutzbeauftragten werde ich mich dafür einsetzen, dass die jetzt getroffenen datenschutzfreundlichen Festlegungen auch angemessen umgesetzt werden.

14.1.2
Aufbau eines zentralen Datenpools der Krankenkassen

Das Gesetz enthält Neuregelungen für die Herstellung von Transparenz im GKV-System (§§ 303a ff. SGB V). Durch die bisher übliche getrennte Letzterfassung der Leistungs- und Abrechnungsdaten bei den ca. 400 Krankenkassen einerseits und der ärztlichen bzw. zahnärztlichen Leistungsdaten bei den zahlreichen Kassenärztlichen bzw. Kassenzahnärztlichen Vereinigungen andererseits ist die Verwendung der Mittel, die von der gesetzlichen Krankenversicherung insgesamt für Gesundheitsleistungen ausgegeben werden, nicht transparent. Das Gesetz sieht jetzt eine sektoren- und kassenübergreifende Zusammenführung der Leistungs- und Abrechnungsdaten aller Versicherten in einem zentralen Datenpool vor, damit eine valide Datenbasis geschaffen werden kann für eine zielgerichtete Systemsteuerung durch die Selbstverwaltung und die Politik auf Bundes- und Landesebene. Die Spitzenverbände der Krankenkassen und die Kassenärztliche Bundesvereinigung bilden eine Arbeitsgemeinschaft für Aufgaben der Datentransparenz. Diese Arbeitsgemeinschaft für Aufgaben der Datentransparenz hat die Erfüllung der Aufgaben einer Vertrauensstelle und einer Datenaufbereitungsstelle zu gewährleisten. Durch die Datenaufbereitungsstelle sollen die im Rahmen der Leistungsabrechnung übermittelten Daten kassenarten- und sektorenübergreifend zusammengeführt und anschließend aufbereitet werden.

Bei den in der Datenaufbereitungsstelle gespeicherten Abrechnungs- und Leistungsdaten der Versicherten handelt es sich um medizinische Daten von ca. 60 Millionen Personen. Für den Aufbau dieses umfangreichen sensitiven Datenbestandes haben die Datenschutzbeauftragten eine Reihe von Datenschutzmaßnahmen gefordert, die im Gesetz überwiegend festgelegt wurden:

- Die Vertrauensstelle hat den Versicherten- und Leistungserbringerbezug der ihr von den Krankenkassen und den kassenärztlichen Vereinigungen übermittelten Leistungs- und Abrechnungsdaten zu pseudonymisieren. Es ist auszuschließen, dass Versicherte oder Leistungserbringer durch die Verarbeitung und Nutzung der Daten bei der Vertrauensstelle, der Datenaufbereitungsstelle oder den nutzungsberechtigten Stellen wieder identifiziert werden können.

- Die Vertrauensstelle ist räumlich, organisatorisch und personell von den Trägern der Arbeitsgemeinschaft für Datentransparenz und ihren Mitgliedern sowie von den nutzungsberechtigten Stellen zu trennen. Sie gilt als öffentliche Stelle, unterliegt dem Sozialgeheimnis i.S.v § 35 SGB I und untersteht der Rechtsaufsicht des Bundesministeriums für Gesundheit und Soziale Sicherung (BMGS).

- Auch die Datenaufbereitungsstelle ist räumlich, organisatorisch und personell von den Trägern der Arbeitsgemeinschaft für Datentransparenz und ihren Mitgliedern sowie von den nutzungsberechtigten Stellen zu trennen. Sie gilt ebenfalls als öffentliche Stelle, unterliegt dem Sozialgeheimnis i.S.v. § 35 SGB I und untersteht der Rechtsaufsicht des BMGS.

Die bei der Datenaufbereitungsstelle gespeicherten Daten können von zahlreichen, im Gesetz abschließend festgelegten Stellen verarbeitet und genutzt werden, soweit sie für die Erfüllung ihrer Aufgaben erforderlich sind.

14.1.3
Übermittlung der Abrechnungen von ambulanten Behandlungen an die Krankenkasse künftig mit versichertenbezogener Diagnose

Durch das GKV-Modernisierungsgesetz wird das bisherige Vergütungssystem grundlegend geändert. Die Vergütung der ärztlichen Leistungen nach Kopfpauschalen wird durch das System der morbiditätsorientierten Regelleistungsvolumina abgelöst. Mit der Neuregelung des ärztlichen Honorarsystems wird die Verantwortung für die Abrechnungs- und Plausibilitätsprüfung der ärztlichen Leistungsabrechnungen zwischen den kassenärztlichen Vereinigungen und den Krankenkassen neu ausgestaltet. Im Zusammenhang damit ist festgelegt, dass die Krankenkassen jetzt auch im Sektor der ambulanten ärztlichen Versorgung versichertenbezogene - nicht wie bisher lediglich fallbezogene - Abrechnungs- und Leistungsdaten von den kassenärztlichen Vereinigungen erhalten und auch umfassend prüfen (§§ 106a, 284, 295 SGB V). Infolge dieser neuen versichertenbezogenen Übermittlung der ärztlichen Abrechnungsdaten in der ambulanten Versorgung erhalten die Krankenkassen erheblich mehr personenbezogene medizinische Daten der Versicherten als bisher. Dass dies durch das neue Vergütungssystem zwingend geboten ist, wurde den Datenschutzbeauftragten bisher nicht ausreichend dargelegt. Die Datenschutzbeauftragten sind zu diesen im Schnellverfahren realisierten Änderungen des ursprünglichen Gesetzentwurfs nicht rechtzeitig und nicht ausreichend beteiligt worden. Dadurch war u. a. eine Diskussion über Möglichkeiten der Pseudonymisierung der Versichertendaten nicht möglich. Bei der künftigen Umsetzung der neuen Regelungen muss sichergestellt werden, dass keine umfassenden Versichertenprofile bei den Krankenkassen entstehen und die Daten ausschließlich zweckgebunden verwendet werden.

14.2
Datenschutzkonzept für das Neugeborenen-Screening in Hessen

Im neuen Screening-Zentrum Hessen sollen die Daten und Blutproben aller Neugeborenen Hessens flächendeckend zentral erfasst werden. Auf Grund meiner Forderungen wird vom Hessischen Sozialministerium ein Datenschutzkonzept für den sensitiven Datenbestand erstellt, das insbesondere eine Pseudonymisierung der Proben und medizinischen Daten der Neugeborenen vorsieht und die Zwecke, zu denen depseudonymisiert werden darf, abschließend festlegt.

14.2.1
Ziel des Screenings

Das Neugeborenen-Screening zeichnet sich dadurch aus, dass die gesamte Population der Neugeborenen (unabhängig vom Vorliegen klinischer Symptome oder eines erhöhten Risikos) auf angeborene Stoffwechselkrankheiten und Hormonstörungen untersucht wird, die ohne rechtzeitige Behandlung zu einer schweren geistigen und/oder körperlichen Behinderung des Kindes führen. Nur mit Hilfe einer Blutuntersuchung innerhalb von wenigen Tagen nach der Geburt lassen sich diese Krankheiten bzw. Störungen feststellen. Mit der rechtzeitigen und richtigen Behandlung können dauerhafte Schäden ganz überwiegend verhindert werden.

In Hessen wird das Neugeborenen-Screening - in begrenzterem Umfang - bereits seit 1964 am Untersuchungsamt in Dillenburg durchgeführt. Seit 1. April 2002 hat das Screeningzentrum Hessen an der Universitätskinderklinik Gießen seine Funktion aufgenommen. Das Screening-Zentrum erhält derzeit von ca. 95 v.H. aller Neugeborenen in Hessen Trockenblutproben von ca. 1.100 Einsendern (Krankenhäuser, Belegkliniken, niedergelassene Gynäkologen, Kinderärzte und Hebammen).

Bei dem Screening handelt es sich nicht um Gen-Analysen, sondern um Messungen von phänotypischen Eigenschaften. Die Screening-Ergebnisse erlauben keine direkten eindeutigen Schlüsse auf genetische Mutationen. Es ist davon auszugehen, dass der Umfang des Screenings weiter zunimmt und dass künftig auch DNA-Analysen durchgeführt werden.

14.2.2
Datenschutzrechtliche Aspekte

Die Durchführung des Neugeborenen-Screenings ist aus datenschutzrechtlicher Sicht nie in Frage gestellt worden. Ich habe jedoch eine datenschutzgerechte Ausgestaltung und Regelung des Verfahrens gefordert. Dies ist insbesondere vor dem Hintergrund wichtig, dass

- eine flächendeckende Erfassung der Daten aller Neugeborenen in Hessen angestrebt wird (wie auch in anderen Bundesländern, s. einstimmigen Beschluss der 75. Konferenz der Gesundheitsministerkonferenz am 20./21. Juni 2002 Top 9.1),

- die Daten im Screening-Zentrum jetzt automatisiert verarbeitet werden,

- der Umfang des Screenings kontinuierlich zunimmt. Blutproben können immer schneller, preiswerter und umfassender auf genetisch bedingte Erkrankungen untersucht werden: Zum einen wird zunehmend die neue Screeningtechnologie TMS (Tandemmassenspektronomie) eingesetzt (s. hierzu auch den o.a. Beschluss der Gesundheitsministerkonferenz, in dem die Nutzung dieser Technologie als erforderlich angesehen wird), die es ermöglicht, mit einem einzigen Analyseverfahren sehr viele Erkrankungen unterschiedlicher Inzidenz und Therapierbarkeit gleichzeitig ohne finanziellen Mehraufwand zu erfassen. Es ist absehbar, dass die rapiden inhaltlichen Fortschritte des Humangenomprojekts künftig zu einer erheblichen zusätzlichen Ausweitung der präventiven Medizin führen werden. So wird z. B. in der Richtlinie zur Organisation und Durchführung des Neugeborenen-Screenings auf angeborene Stoffwechselstörungen und Endokrinopathien in Deutschland von 1997 ein Screening auf fünf Defekte empfohlen. Die derzeitige Praxis in den Bundesländern differiert. In Hessen wird bereits auf 27 Defekte untersucht. Diskutiert wird in Deutschland auch bereits die Frage, ob ein Screening auf nicht behandelbare Krankheiten, die evtl. einmal später behandelbar sind, erstreckt werden sollte.

Von diesem Ausgangspunkt aus erhält eine zentrale bevölkerungsbezogene Speicherung der Daten und Aufbewahrung der Restblutproben erhebliche Brisanz. Die rechtlichen Rahmenbedingungen für das Neugeborenen-Screening sind daher bereits mehrfach Gegenstand öffentlicher Diskussion gewesen (s. z. B. die Debatte im Hessischen Landtag am 10. Juli 2003 [Plenarsitzung 16/11 und Tagesordnungspunkt 25 über die Beschlussfassung und Bericht des Innenausschusses zum 30. Tätigkeitsbericht] und die Antwort der Bundesregierung auf die Kleine Anfrage betr. "Rechtsstaatlicher Umgang mit Restblutproben beim Neugeborenen-Screening", BTDrucks. 15/1610). Aus datenschutzrechtlicher Sicht ist es unerlässlich, zu klären und verbindlich festzulegen, in welchem Umfang, zu welchem Zweck und in welchem Verfahren Daten und Blutproben gewonnen und weiterverwendet werden, wer zu welchem Zweck Zugang dazu hat und wann die Daten bzw. Proben gelöscht und vernichtet werden. Das Hessische Sozialministerium erarbeitet derzeit daher ein Datenschutzkonzept für die Durchführung des Neugeborenen-Screenings in Hessen. Die Inhalte des Datenschutzkonzepts sind Gegenstand von Gesprächen zwischen dem Ministerium, dem Screening-Zentrum, weiteren hessischen Experten für Screening-Maßnahmen, der Hessischen Krankenhausgesellschaft und mir.

14.2.3
Rechtsgrundlage der Datenverarbeitung im Screening-Zentrum

Das Screening ist eine medizinische Maßnahme. Die Untersuchungen sind freiwillig. Es gibt ein Merkblatt des Screening-Zentrums des Universitätsklinikums Gießen, in dem Eltern darüber informiert werden, warum eine Untersuchung des Neugeborenen notwendig ist, wie das Verfahren ausgestaltet ist, dass eine Trockenblutkarte an das Screening-Zentrum Hessen versandt wird und wer in welcher Form über das Untersuchungsergebnis unterrichtet wird. Das Merkblatt enthält eine abschließende konkrete Auflistung der untersuchten Hormon- und Stoffwechseldefekte und ist insoweit auch aus datenschutzrechtlicher Sicht zu begrüßen, weil es Transparenz herstellt. Es fehlen in dem Merkblatt jedoch noch Informationen über die Verwendung der Daten und Proben. Vor allem aber wird durch die Auslage des Merkblatts des Screening-Zentrums in einem Krankenhaus bzw. durch die Aushändigung des Merkblatts durch die Hebamme oder den Kinderarzt das Screening noch nicht Bestandteil des Behandlungsvertrags. So lautete z. B. auch die Antwort der Bundesregierung auf die in der Kleinen Anfrage (s. o.) gestellte Frage nach der Rechtsgrundlage des Screenings:

"Eltern müssen vor der Probenentnahme über Ziele, Inhalte und mögliche Folgen des Neugeborenen-Screenings und den Umgang mit der Probe und den erhobenen Daten angemessen informiert werden. Wie andere freiwillige medizinische Maßnahmen auch erfordert das Screening die in der Krankenakte dokumentierte Einwilligung des gesetzlichen Vertreters des Neugeborenen …"

Die Einwilligung der Eltern in das Screening muss sichergestellt werden, und zwar in einer Form, die die rechtzeitige Durchführung des Screenings im Interesse des Kindes nicht in Frage stellt.

14.2.4
Dauer der Speicherung der Daten und Aufbewahrung der Blutproben

In Bayern werden derzeit alle Restblutproben nur drei Monate aufbewahrt, danach werden alle im Screening negativen Filterkarten vernichtet und nur noch die auffälligen Karten sowie eine Stichprobe weiterhin gelagert. Das Hessische Sozialministerium hat ein hiervon abweichendes Verfahren befürwortet, damit im Einzelfall weitere gezielte Untersuchungen des Restblutes vorgenommen werden können und die Aufklärung von Haftungsfragen sowie eine Fortentwicklung der Methoden bei der Diagnostik der seltenen Krankheiten im Kindesalter möglich sind. Nach den Vorschlägen des Hessischen Sozialministeriums und des Screening-Zentrums sollen die Daten und Blutproben künftig 18 Jahre für Behandlungszwecke gespeichert bzw. aufbewahrt werden. Der lange Zeitraum wird insbesondere deshalb als erforderlich angesehen, weil manche der Erkrankungen erst spät sichtbar werden können. In den Fällen, in denen bei den gescreenten Kindern mit negativem Befund später doch Krankheiten auftreten (derartige Fälle sind in den vergangenen Jahren vorgekommen), ist eine Klärung der Ursachen (falsches Blut auf der Karte, falsche Personenzuordnung der Karte, falsche Messung im Labor, fehlerhaftes Messverfahren) nur mit Hilfe der Originalblutproben möglich. Die Ursachen können später nicht mittels einer erneuten Blutentnahme bei den Betroffenen geklärt werden, weil sich das Blut der Neugeborenen innerhalb kurzer Zeit verändert und die ursprünglichen Untersuchungen daher nicht wiederholt werden können.

Ich habe die Vorschläge akzeptiert unter der Bedingung, dass

- die medizinischen Daten und die Blutproben im Screening-Zentrum nach kurzer Frist pseudonymisiert werden,

- die persönlichen Daten aller Neugeborenen sich bei einem rechtlich, räumlich und personell von dem Screening-Zentrum getrennten Treuhänder befinden und
- die Zwecke, zu denen der Treuhänder depseudonymisieren darf, konkret und verbindlich festgelegt sind.

Als Zwecke, zu denen depseudonymisiert werden darf, kommen in erster Linie erneute Untersuchungen der Restblutprobe auf Wunsch der Eltern bzw. der Betroffenen selbst, z. B. in Erkrankungsfällen, in Betracht, ferner Forschungsvorhaben – insbesondere auch zur Verbesserung des Screening-Verfahrens –, bei denen auf der Grundlage einer Einwilligung der betroffenen Eltern auch die Restblutproben erneut getestet werden.

Nach 18 Jahren müssen die Restblutproben jahrgangsweise vernichtet werden, es sei denn, die Betroffenen haben einer längeren Lagerung mit definierter Frist zugestimmt.

Auch für die noch in Dillenburg gelagerten Altbestände an Daten und Restblutproben muss noch ein datenschutzgerechtes Verfahren festgelegt werden.

14.3
Prüfung des Klinikums Offenbach

Im Klinikum Offenbach muss die Ausgestaltung der Zugriffsrechte auf Patientendaten stärker differenziert werden. Die Maßnahmen zur Datensicherheit müssen vervollständigt werden.

Im Jahr 2002 hatte ich mit einer Prüfung der Datenverarbeitung im Klinikum Offenbach begonnen. Die Prüfung hatte in erster Linie die interne Verarbeitung personenbezogener Patientendaten zum Gegenstand, insbesondere die Ausgestaltung der Zugriffsrechte der Mitarbeiterinnen und Mitarbeiter und die technisch-organisatorischen Maßnahmen zur Datensicherheit.

Es verbietet sich, an dieser Stelle Einzelheiten zu den getroffenen Sicherheitsmaßnahmen zu beschreiben. Auf einige Punkte möchte ich jedoch exemplarisch hinweisen.

Die Zugriffe auf Patientendaten waren für den normalen Benutzer auf Netzwerk- bzw. Betriebssystemebene gesperrt. Nur über die dem einzelnen Benutzer freigegebenen Anwendungen war es möglich, auf die Patientendaten zuzugreifen. Deshalb mussten in den Anwendungen selbst differenzierte Sicherheitsmechanismen greifen. Dies galt sowohl für die Anmeldeprozedur mit Benutzerkennung und Passwort als auch für die Zugriffsrechte, die den Benutzern mit ihren verschiedenen Rollen zugeordnet waren. Bei einigen Anwendungen musste ich Defizite feststellen.

- Eine Anwendung in der Radiologie sah auch für Ärzte anderer Kliniken/Abteilungen umfassende Zugriffe auf Röntgenbilder und zugehörige Befunde vor. Eine nachträgliche Kontrolle war nur in Einzelfällen möglich.

  Dem Klinikum waren keine technischen Möglichkeiten bekannt, wie mit der Anwendung die Zugriffseinschränkungen umgesetzt werden können. Ich habe es aufgefordert mit dem Hersteller Kontakt aufzunehmen, um die Frage zu klären. Andernfalls ist es für einen datenschutzkonformen Betrieb nötig, die Nutzung der Anwendung einzuschränken.

- Es existierte ein Altverfahren, das Ärzten zu weit gehende, stationsübergreifende Zugriffsmöglichkeiten auf Patientendaten einräumte.
  Während der Prüfung war die Umstellung des o. a. Altverfahrens auf das Verfahren Kissmed im Gange, das zukünftig zur Patientendatenverwaltung dient. In Kissmed sollen die Zugriffsmöglichkeiten drastisch reduziert werden. Da es möglich ist, einem Arzt einer anderen Fachrichtung einen Fall dediziert zugänglich zu machen, ist es nicht mehr nötig, eine generelle Sicht auf Patienten einer anderen Fachrichtung einzuräumen. Die genauen Rollendefinitionen werden mir zur weiteren Prüfung noch zugeleitet.

- Die Passwörter und die zugehörigen Einstellungen genügten zum Teil nicht den Anforderungen des Grundschutzhandbuchs des Bundesamtes für Sicherheit in der Informationstechnik (BSI), die in Krankenhäusern als Basis zu sehen sind, auf die weitere Sicherheitsmaßnahmen aufbauen.

  Ich habe entsprechende Änderungen gefordert, die sich am Grundschutzhandbuch des BSI (www.bsi.bund.de) und meinen Ausführungen im 30. Tätigkeitsbericht, Ziff. 14 orientieren.

- Es gab teilweise nur rudimentäre Protokollierungsmöglichkeiten, deren Kontrolle auch nicht geregelt war.

  Für diesen und die folgenden Punkte habe ich das Klinikum aufgefordert, die Protokollierung den Erfordernissen anzupassen und die nötigen Regelungen hinsichtlich der Kontrolle zu treffen. Dies sollte sinnvollerweise in Form eines Revisionskonzepts geschehen. Generelle Anforderungen ergeben sich auch hier aus dem Grundschutzhandbuch und aus der "Orientierungshilfe Protokollierung" der Datenschutzbeauftragten des Bundes und der Länder (24. Tätigkeitsbericht, Ziff. 19.1).

- Die Datenbank- und Anwendungsbetreuung wurde durch externes Personal in den Räumen des Klinikums unterstützt. Die Betreuer hatten weitgehende Zugriffsmöglichkeiten auf Datenbankebene, die kaum kontrolliert werden konnten.

  Um die Tätigkeiten kontrollieren zu können, müssen aussagefähige Protokolle zur Verfügung stehen, die auszuwerten sind. Es handelt sich um einen Bestandteil des Revisionskonzepts.

In einer ersten Stellungnahme beschrieb das Klinikum Maßnahmen, die einige Probleme beseitigen. Hinsichtlich der Protokollierung und Revision sowie der Anforderungen an Passwörter konnte es jedoch keine befriedigende Lösung anbieten. Das liegt auch daran, dass Anfang 2004 eine Entscheidung getroffen werden soll, ob andere Softwareprodukte zur Verarbeitung von Patientendaten eingesetzt werden. Diese Produkte bieten andere, teilweise weitergehende technische Datensicherheitsfunktionen. Das Klinikum will sein weiteres Vorgehen beschreiben, wenn klar ist, welches Produkt eingesetzt wird und welche Maßnahmen ergriffen werden können.

Wenn mir die Informationen vorliegen werde ich prüfen, ob die vorgesehenen Maßnahmen ausreichen.

14.4
Prüfung der Vertrauensstelle des Hessischen Krebsregisters

Der Aufbau des Hessischen Krebsregisters hat begonnen. Bei meiner Prüfung der Vertrauensstelle des Krebsregisters in Frankfurt habe ich durch Startschwierigkeiten bedingte Probleme hinsichtlich der im Gesetz vorgesehenen Weiterverarbeitung der bereits gemeldeten bzw. übermittelten personenbezogenen Patientendaten festgestellt. Davon abgesehen wurden die datenschutzrechtlichen Anforderungen im Wesentlichen beachtet.

Da seit Frühjahr 2003 erstmals Meldungen an die Vertrauensstelle des Krebsregisters eingehen, habe ich mich vor Ort über die aktuelle Arbeitsweise informiert.

14.4.1
Trennung des Registers in Vertrauensstelle und Registerstelle

14.4.1.1
Rechtliche Vorgaben

Ende 2001 hat der hessische Gesetzgeber eine dauerhafte Nachfolgeregelung für das Ausführungsgesetz zum Krebsregistergesetz (AGKRG) vom 21. Oktober 1998 verabschiedet. Das Hessische Krebsregistergesetz (HKRG; GVBl. I, S. 582 ff.) hat die rechtliche Grundlage dafür geschaffen, dass jetzt epidemiologische Daten über Krebserkrankungen in einer definierten Bezugsbevölkerung gemeldet, aufbereitet und ausgewertet werden können. Ausgewählt wurde der Regierungsbezirk Darmstadt mit seinen ca. 3,6 Millionen Einwohnern (ca. 60 v.H. der hessischen Bevölkerung).

In Hessen - wie auch in anderen Bundesländern - wird aus Gründen des Datenschutzes kein zentrales personenbezogenes Register mit den Daten der Krebserkrankten aufgebaut, sondern im Gesetz ist ein so genanntes Treuhandmodell vorgesehen (s. §§ 2, 5 und 6 HKRG): Die Verarbeitung personenbezogener Daten im Krebsregister und damit auch die Gefahr eines Missbrauchs der Daten wird durch die Aufteilung auf zwei räumlich, organisatorisch und personell selbständige Stellen des Krebsregisters (Vertrauensstelle und Registerstelle) und eine Verschlüsselung der Identitätsdaten des Patienten auf ein Minimum reduziert. Der Arzt meldet die personenbezogenen Daten an die bei der Landesärztekammer in Frankfurt eingerichtete Vertrauensstelle. Die Daten werden aufgeteilt in die den Patienten identifizierenden Daten (Name, Anschrift, Geburtsdatum etc.) und die epidemiologischen Daten (Beruf, Tumordiagnose, Art der Therapie etc.). Die Vertrauensstelle verschlüsselt die Identitätsdaten. Die verschlüsselten Identitätsdaten und die epidemiologischen Daten werden zusammen mit einer gemeinsamen Kontrollnummer sowie den Angaben zu den meldenden Ärzten an die Registerstelle beim Staatlichen Untersuchungsamt Hessen übermittelt. Auf diese Weise können nachfolgende Meldungen zu demselben Patienten den vorhergehenden Meldungen zugeordnet werden. Die Registerstelle speichert die verschlüsselten Identitätsdaten und die epidemiologischen Daten dauerhaft. Die Registerstelle selbst kann keinen Personenbezug der Daten wiederherstellen. Bei der Vertrauensstelle müssen alle zu einer Meldung gehörenden personenbezogenen Patientendaten unverzüglich nach der abschließenden Bearbeitung der Daten durch die Registerstelle, spätestens jedoch drei Monate nach Übermittlung, gelöscht und die der Meldung zugrunde liegenden Unterlagen vernichtet werden. Eine Entschlüsselung der Identitätsdaten ist im Einzelfall durch die Vertrauensstelle für Maßnahmen des Gesundheitsschutzes und für wichtige, im öffentlichen Interesse stehende Forschungsaufgaben zulässig.

14.4.1.2
Aktueller Sachstand

Zur Zeit der Prüfung lagen in der Vertrauensstelle etwa 9.000 Meldungen von Krebserkrankungen aus dem Regierungsbezirk Darmstadt vor. Die Meldungen erfolgen überwiegend in Papierform, zwei Kliniken melden in elektronischer Form (s. hierzu noch unten). Da in der Vertrauensstelle noch die Datenbank für den Aufbau des Datenbestandes fehlt und auch personelle Engpässe bestehen, wurden die Meldungen bisher noch nicht digital erfasst, weiterverarbeitet und an die Registerstelle übermittelt. Entsprechend können auch die Papierbelege der Meldungen noch nicht vernichtet werden.

Wie im Gesetz vorgesehen, melden die 14 im Einzugsbereich des Krebsregisters befindlichen Gesundheitsämter die Inhalte aller Leichenschauscheine, pro Jahr etwa 35.000 (§ 4 Abs. 7 HKRG) zum Abgleich mit dem Krebsregister. Die Inhalte dieser Leichenschauscheine sind inzwischen in der Vertrauensstelle überwiegend digital erfasst. Da die Registerstelle zurzeit noch die Datenbank entwickeln lässt, wird der im Gesetz vorgesehene Abgleich derzeit nicht vorgenommen, alle Daten bleiben digital gespeichert und die Leichenschauscheine werden entsprechend aufbewahrt.

Insgesamt lagern daher zurzeit in der Vertrauensstelle in vom Treuhandmodell nicht vorgesehener Weise in größerem Umfang personenbezogene Daten. Ich habe mich davon überzeugt, dass die Daten sicher aufbewahrt werden (s. hierzu noch unten). Die Probleme müssen so bald wie möglich behoben werden. Ich gehe davon aus, dass die im Gesetz vorgesehene Verfahrensweise spätestens ab Frühjahr 2004 strikt eingehalten wird. Ich werde dies auch vor Ort erneut überprüfen.

14.4.2
Wahrung der Patientenrechte bei Meldungen durch Pathologen

Nach den gesetzlichen Regelungen dürfen personenbezogene Daten vom Arzt an das Register (Vertrauensstelle) ohne Einwilligung des Patienten gemeldet werden. Der Patient ist aber von der beabsichtigten Meldung zu unterrichten und kann der Meldung widersprechen. Unter bestimmten Voraussetzungen (insbesondere, wenn der Patient über die Diagnose nicht unterrichtet ist und die Gefahr einer Verschlechterung des Gesundheitszustandes droht) kann eine Unterrichtung des Patienten zunächst unterbleiben.

Von den derzeit in der Vertrauensstelle vorliegenden 9.000 Meldungen wurden ca. 3.000 Meldungen durch Pathologen übersandt. Da die Pathologen im Regelfall keinen direkten Kontakt mit den Patienten haben, stellt sich die Frage, wie die Patientenrechte bei diesen Meldungen gewahrt werden. Das Gesetz sieht vor, dass Pathologen auch ohne vorherige Unterrichtung der Patienten zur Meldung berechtigt sind. Sie müssen jedoch den meldepflichtigen Arzt, der das Präparat an sie eingesandt hat, von der Meldung unterrichten und ihn auf seine Pflicht hinweisen, den Patienten auf sein Widerspruchsrecht hinzuweisen. Andernfalls würden die Patientenrechte durch die Meldungen der Pathologen weitgehend unterlaufen. Widerspricht ein Patient der durch den Pathologen veranlassten Meldung, so müssen die Daten im Register gelöscht werden.

Vor und während der Prüfung habe ich Anhaltspunkte dafür gewonnen, dass dieses im Gesetz vorgesehene Verfahren durch die Pathologen in der Praxis noch nicht hinreichend umgesetzt wird. Ich habe mich daher mit der Vertrauensstelle des Krebsregisters, die mit den Meldepflichtigen regelmäßig Kontakt hat, darauf verständigt, dass sie die gesetzlichen Vorgaben für die Meldungen von Pathologen in die Gespräche einbringt. Als Hilfestellung für die Pathologen habe ich auch gemeinsam mit der Vertrauensstelle einen Textbaustein formuliert, den die Pathologen in die Befundmitteilung an den behandelnden Arzt integrieren können.

14.4.3
Maßnahmen zur Gewährleistung der Datensicherheit

Durch eine Alarmanlage und andere Sicherungsmaßnahmen waren die Rechner und die Räumlichkeiten gegen unbefugte Zutritte ausreichend gesichert.

Die IT-Struktur sah zwei Rechnernetze vor. Es gab ein internes Netz ohne Schnittstellen nach außen, in dem sich der Datenbank-Server der Vertrauensstelle mit den Patientendaten befand. Werden die Räume verlassen, so wird das interne Netz deaktiviert. Es gibt keine Möglichkeit mehr von Client-Rechnern auf den Server zuzugreifen. Ein weiteres, physikalisch getrenntes Netz hatte Übergänge ins Internet. Es war durch eine Firewall gesichert. Auf Rechnern in diesem Netz befanden sich keine Daten von Patienten.

Da nur wenige Mitarbeiter in der Vertrauensstelle arbeiten und diese sich gegenseitig vertreten, gab es bei den Zugriffsrechten keine Abstufung. Derzeit übertragen zwei Kliniken die Patientendaten elektronisch. Dabei werden die Daten verschlüsselt. Es wird als Algorithmus der Triple-DES eingesetzt. Der Algorithmus gilt als sicher (s. hierzu Ziff. 18.6 Orientierungshilfe Kryptografie). Ein Schlüssel ist zwischen der Vertrauensstelle und jeder Klinik einzeln vereinbart.

Insgesamt habe ich die Datensicherheitsmaßnahmen als ausreichend angesehen.

14.5
Automatisierung im öffentlichen Gesundheitsdienst

Gegen die Einführung automatisierter Datenverarbeitungssysteme im öffentlichen Gesundheitsdienst gibt es keine grundsätzlichen datenschutzrechtlichen Bedenken. Generell dürfen nur erforderliche Daten gespeichert werden. Wegen der strengen Zweckbindung müssen die einzelnen Fachbereiche gegeneinander abgeschottet sein. Da es sich regelmäßig um medizinische Daten handelt, sind wegen der ärztlichen Schweigepflicht besondere Anforderungen zu beachten. Außerdem dürfen besonders sensitive Daten - wie im Sozialpsychiatrischen Dienst –, die ohnehin nicht in andere Bereiche des Gesundheitsamtes gelangen dürfen, nicht in zentrale Verfahren des Gesundheitsamtes aufgenommen werden. Besonderer Wert ist auf die revisionsfähige Administration der Anwendung sowie die technischen und organisatorischen Maßnahmen nach § 10 Abs. 2 Hessisches Datenschutzgesetz zu legen.

14.5.1
Automation in den Gesundheitsämtern

Die Einführung automatisierter Verfahrensabläufe und die zentrale Speicherung der anfallenden Daten mit Hilfe spezieller Software-Programme in den hessischen Gesundheitsämtern hat mich bereits im Jahre 1998 beschäftigt (vgl. hierzu 27. Tätigkeitsbericht, Ziff. 7.6.). Seinerzeit habe ich mich mit dem Programm OCTOWARE der Firma easy-soft GmbH in Dresden befasst. Die von mir getestete Version des Programms hatte mich im Ergebnis dazu veranlasst, die datenschutzrechtliche Unbedenklichkeit festzustellen.

Im Verlauf der letzten Jahre haben eine ganze Reihe weiterer Gesundheitsämter die ihnen übertragenen gesetzlichen Aufgaben sowie die interne Organisation unter Zuhilfenahme spezieller Softwareprogramme automatisiert. In diesem Zusammenhang ist das Programm OCTOWARE nur eines von verschiedenen anderen Programmen, die mittlerweile bei den Gesundheitsämtern zur Anwendung kommen. So hat das Gesundheitsamt des Lahn-Dill-Kreises ein Produkt der Firma Mikroprojekt Computersysteme angeschafft. Mit den Möglichkeiten, die das Programm "Mikropro health" bietet, sollen die Verfahrensabläufe im Gesundheitsamt optimiert und die Leistungsfähigkeit erheblich gesteigert werden. Die Gesundheitsämter der

Kreise Eschwege und Fulda haben sich für ein Produkt der Firma unisoft mit Namen "Äskulab 21" entschieden. Dagegen wird beim Landkreis Kassel das Verfahren ISGA der Firma Computer Zentrum Binder & Karl GmbH eingesetzt.

14.5.2
Aufbau der Programme

Ich habe im Rahmen einer Prüfserie die Gesundheitsämter in Fulda, Eschwege, Wetzlar, Kassel und Dietzenbach aufgesucht, um mir einen Überblick über den derzeitigen Stand der Automatisierung zu verschaffen und bereits im Vorfeld Hinweise auf datenschutzkonforme Lösungen im Zusammenhang mit der Verarbeitung personenbezogener medizinischer Daten zu geben.

Alle Programme sind in ihrer Grundstruktur einander ähnlich, da sie in Form einzelner Module aufgebaut sind. So gibt es für die unterschiedlichen Aufgabenstellungen eines Gesundheitsamtes spezifische Module bzw. Arbeitsbereiche, welche die erforderlichen Verfahrensschritte, die gesetzliche Vorgaben zum Inhalt haben, abdecken. Beispielsweise werden die Verfahrensabläufe für die Meldungen nach den §§ 6 ff. Infektionsschutzgesetz an das Robert-Koch-Institut in Berlin von den Programmen so dargestellt, dass die zuständigen Sachbearbeiter die nach dem Gesetz meldepflichtigen Krankheiten innerhalb des Moduls abschließend bearbeiten können. Eine ähnliche Bearbeitung findet von der Ablauforganisation her in den anderen Fachbereichen des Gesundheitsamtes statt, sofern dort über die entsprechenden fachbezogenen Module verfügt wird.

14.5.3
Schwerpunkte der Prüfung bei den Gesundheitsämtern

Drei wesentliche datenschutzrechtliche Aspekte sind im Rahmen meiner Prüfungen der Programme OCTOWARE, ISGA, Äskulab 21 und Mikropro health mit den Amts- und Verwaltungsleitern und Sachbearbeitern diskutiert worden:

- Einrichtung der Zentraldatei
- Ausgestaltung der Zugriffsrechte und Administration
- Einbindung der Sozialpsychiatrischen Dienste

14.5.3.1
Zentraldatei

Bei der Zentraldatei handelt es sich im Einzelnen um einen Personenstammdatensatz, der dann angelegt wird, wenn ein Betroffener Kontakt mit dem Gesundheitsamt aufnimmt. Eine Ausnahme von dieser Verfahrensweise muss es allerdings beim sozialpsychiatrischen Dienst geben. In der Zentraldatei dürfen keine inhaltlichen Hinweise auf bestimmte Erkrankungen oder persönliche Lebensumstände eines Betroffenen enthalten sein. Die Aufgabe der Datei als Suchinstrumentarium ist dann erfüllt, wenn sich hieraus ausschließlich formale Informationen ergeben, ob z. B. eine Person bereits mit dem Gesundheitsamt zu tun hatte. Andererseits darf es keine inhaltlichen Hinweise auf z. B. bestimmte Krankheiten oder Beratungshinweise im Zusammenhang mit einer psychischen Erkrankung geben.

Bereits bei der in vielen Gesundheitsämtern manuell geführten Personenkartei gab es immer wieder Streitfragen im Hinblick auf deren Inhalt und den Zugriff durch Mitarbeiterinnen und Mitarbeiter. Vor allem kam es immer wieder vor, dass auf den Karteikarten Informationen zu einzelnen Besuchen bzw. Vorladungen vermerkt waren. Diese Diskussionen können mit der Einführung eines einheitlichen Personenstammdatensatzes ad acta gelegt werden. Jedes der Softwareprogramme sieht in seiner Grundstruktur das Anlegen eines Personenstammdatensatzes vor. Neben den Merkmalen Name, Vorname, Anschrift, Geburtsdatum und Staatsangehörigkeit ist es sinnvoll, den Fachbereich/Abteilung mit aufzuführen, in welcher der Betroffene ggf. bereits war. Damit wird es möglich, externe Anfragen gezielt an die Organisationseinheit weiterzuleiten, die mit dem Betroffenen befasst war. Dies schließt selbstverständlich jedoch zunächst aus, dass über die Fachabteilung hinaus Informationen ausgetauscht bzw. weitergeleitet werden. Vorstellbar ist im Rahmen der internen Organisation des Gesundheitsamtes eine Verknüpfung z. B. des amtsärztlichen und jugendärztlichen Dienstes mittels der Zentraldatei. Allerdings nicht dergestalt, dass extern anfragenden Personen oder Institutionen Inhaltsdaten zur Verfügung gestellt werden sollten. Vielmehr könnte über ein in der Zentralkartei gesetztes Merkmal die für eine bestimmte Person zuständige Sachbearbeiterin oder der Sachbearbeiter ermittelt und Anfrager auf diese Weise gezielt an die richtige Stelle geführt werden, um die klärungsbedürftigen Fragen zu stellen. Über allem steht dabei, keine Befunde, Gutachten oder sonstigen medizinischen Daten allgemein durch das System für das Personal des Gesundheitsamtes zugänglich zu machen.

Alle medizinischen Daten unterliegen nämlich der ärztlichen Schweigepflicht i. S. d. § 203 Strafgesetzbuch. Eine informationelle Einheit im Gesundheitsamt kann deshalb ebenso wenig wie bei den Krankenhäusern angenommen werden.

14.5.3.2
Technisches Umfeld, Zugriffsberechtigungen und Administration

Bei der vergleichenden Betrachtung der verschiedenen zum Einsatz kommenden Verfahren spielt die unterschiedliche Größe der einzelnen Gesundheitsämter sowie deren technische und organisatorische Einbettung in die jeweilige Verwaltung eine nicht unerhebliche Rolle. Die Ausgangssituation eines räumlich und technisch entkoppelten Gesundheitsamts ist eben nicht eins zu eins mit der eines vollständig in die Kreisverwaltung eingebetteten Gesundheitsamts zu vergleichen. Dabei kommt es im Wesentlichen darauf an, dass sich insgesamt ein angemessenes Datenschutzniveau ergibt. So müssen z. B. Schwächen der einzelnen Anwendung ggf. durch zusätzliche Maßnahmen auf der Betriebssystemebene kompensiert werden und bei einer Integration in das Netz der Kreisverwaltung steigen dementsprechend die Anforderungen an die Sicherheit dieses Netzes.

Insbesondere die folgenden Punkte wurden bei allen geprüften Verwaltungen bzw. Verfahren vergleichend betrachtet:

- **Art der Datenbank**
  Alle eingesetzten Anwendungen lassen sich hinsichtlich der verwendeten Datenbank in zwei Gruppen unterscheiden. Entweder wird die Datenbank, z. B. auf Access basierend, auf einem Dateiserver abgelegt oder das Verfahren setzt den Einsatz eines passenden Datenbankservers voraus. Insbesondere im ersten Fall ergeben sich für die Vertraulichkeit und Integrität der Daten höhere Risiken, denn alle Anwender des Verfahrens brauchen umfassenden Schreib-/Lese-Zugriff auf die Server-Verzeichnisse, auf denen die Datenbank abgelegt ist. Wenn dann ein Zugriff auf der Betriebssystemebene nicht durch geeignete Maßnahmen verhindert wird, kann die Datenbank unbefugt kopiert oder aber ganz gelöscht werden.

  Ein Teil der geprüften Stellen hat dieses Risiko durch entsprechende Einschränkungen der Benutzeroberflächen aufgefangen. Ein Zugriff auf die Datenbank außerhalb der Anwendung war damit wirkungsvoll ausgeschlossen. In den anderen Fällen können die Daten – eine ordnungsgemäße Administration vorausgesetzt – nur mit der Anwendung auf dem Datenbankserver gelesen werden. Hier greifen je nach Verfahren noch zusätzliche Verschlüsselungsmechanismen, die nicht nur die Daten, sondern auch die Passwörter der Anwender schützen.

- **Zugang zum Verfahren**
  In allen Fällen hatten nur berechtigte Anwender die Möglichkeit sich an den Verfahren anzumelden. Anderen Benutzern war der Zugang durch eine ordnungsgemäße Administration unmöglich. Die stichprobenhafte Überprüfung der dazu gehörenden Dokumentationen gab nur im Einzelfall Anlass zur Kritik. Die Einrichtung oder Änderung des Zugangs zum Verfahren wurde im Allgemeinen umfassend und in einem der Sensitivität der Daten entsprechenden Umfang schriftlich dokumentiert.

  Da es aber grundsätzlich berechtigten Nutzern in den meisten Fällen möglich ist, unabhängig von der Anmeldung am Betriebssystem, eine Anmeldung mit beliebiger Benutzerkennung am Verfahren durchzuführen, besteht hier die Gefahr, dass ein Anwender die Rolle im Verfahren wechselt bzw. Zugang zu anderen Modulen erhält. Der Schutz der Daten vor unbefugten Zugriffen ist somit von der Qualität der Verfahrensanmeldung bzw. des Passwortes abhängig.

  Daher sollten die Verfahren dazu in der Lage sein, eine Passwortlänge von mindestens acht Zeichen zu erzwingen und die Lebensdauer der Passworte ist auf längstens 60 Tage zu begrenzen, wie es auch bei Betriebssystemen üblich ist. Wenn diese Forderungen nicht durch die Verfahren sichergestellt werden können, ist die Umsetzung durch entsprechende Dienstanweisungen an Anwender und Administratoren zu erwirken.

- **Initialpasswort**
  Wird ein Benutzer in einem der Verfahren erstmals eingerichtet oder hat ein Benutzter sein zuletzt benutztes Passwort vergessen, ist durch den Anwendungsadministrator ein Initialpasswort einzurichten. Dabei sollte im Idealfall das Passwort frei zu wählen sein, und bei der ersten Anmeldung wird der Anwender gezwungen dieses zu wechseln, bevor er mit dem Programm arbeiten kann.

  Leider zeigen die Verfahren in diesem Zusammenhang ihre Schwächen. Programme die den sofortigen Passwortwechsel nicht erzwingen, erlauben es dem Anwender das Initialpasswort bis zum Fristablauf zu verwenden. Selbst wenn die Benutzer durch eine entsprechende Dienstanweisung zum sofortigen Wechsel des Passwortes aufgefordert werden, ist der Anwendungsadministrator in diesen Fällen gehalten, das Initialpasswort besonders aufwändig zu gestalten.

  Noch kritischer sind Verfahren, in denen das Initialpasswort fest vorgegeben ist, denn es ist allen Anwendern, gleich welche Rolle sie im Verfahren einnehmen, bekannt. Hier kommt der Forderung zum sofortigen Ändern des Passworts durch den Anwender besondere Bedeutung zu. Zur Durchsetzung dieser Forderung könnte ein Quittungsvermerk eingeführt werden, in dem der Anwender mit Datum und Uhrzeit die Änderung des Initialpasswortes bestätigt. Um ein verbleibendes Restrisiko technisch zu minimieren, sollte das Standardpasswort eine eng gefasste Gültigkeitsdauer z. B. 48 Stunden haben.

- **Risiken durch die Einbindung in E-Mail-Systeme bzw. Internet-Anbindung**
  Alle eingesetzten Systeme wurden, soweit eine Anbindung einzelner Arbeitsplätze an das Internet eingerichtet war, durch Firewalls abgesichert. Dabei reichte das Spektrum der eingesetzten Komponenten vom einfachen ISDN-Router mit Firewall-Funktionalität bis zum ausfallsicheren Firewall-Cluster mit integrierter Lastverteilung. Die eingesetzten Systeme entsprachen im Wesentlichen dem Schutzbedarf des jeweils nachfolgenden Netzes. Die Dienststellen wurden darauf hingewiesen, dass bestimmte Risiken nur durch sehr restriktive Browsereinstellungen, die den Zugriff auf aktive Elemente auf Internetseiten allerdings stark einschränken, ausgeschlossen werden (s. auch www.bsi-bund.de). Bei den E-Mail-Anbindungen wurden im Idealfall durch gestaffelte Virenscanner, die sowohl zentral auf dem Server als auch lokal bei Empfänger greifen, die notwendigen Schutzmechanismen eingerichtet.

- **Protokollierung und Revisionssicherheit**
  Die in den Anwendungen programmierten Protokollierungsoptionen werden, soweit vorhanden, wegen der entstehenden Speichervolumen nicht voll ausgeschöpft. Funktionen, die den letzten ändernden Zugriff zu einem Datensatz anzeigen, sind weitgehend in die Programme implementiert. Fehler bei der Administration der Module oder Fehlfunktionen des Programms werden u. U. so für berechtigte Anwender offensichtlich. Eine echte Revisionsfähigkeit, die die Historie aller Zugriffe leicht auswertbar, z. B. für einen behördlichen Datenschutzbeauftragten, ermöglicht, ist bei keinem Programm gegeben. Bei den datenbankbasierten Systemen entstehen allerdings die typischen protokollähnlichen

Datensätze, die für das Rekonstruieren der Datenbank nach einer Störung benötigt werden. Diese können im Einzelfall - bei besonderen Vorkommnissen - von Spezialisten durchsucht werden.

- **Fazit aus technischer Sicht**
  Wie bei vielen Anwendungsprogrammen, die in den hessischen Kommunalverwaltungen eingesetzt werden, gibt es mehr oder weniger ausgeprägte Probleme, weil die datenschutzrechtlichen Erfordernisse zunächst nicht im Vordergrund der Entwicklung stehen. Das führt angesichts des höheren Schutzbedarfs der hier verarbeiteten Daten dazu, dass Mängel mit zum Teil erheblichem zusätzlichem Aufwand auf der Ebene der Betriebssysteme und durch aufwändige organisatorische Regelungen kompensiert werden müssen.

14.5.3.3
Einbindung des sozialpsychiatrischen Dienstes

Der Sozialpsychiatrische Dienst (SpD) ist in vielen Gesundheitsämtern eine eigenständige Organisationseinheit. Rechtsgrundlagen für die Tätigkeit des Dienstes ist u. a. das Hessische Freiheits-Entziehungsgesetz. So werden beim SpD Stellungnahmen zu Unterbringungen gefertigt, die vom Ordnungsamt in Auftrag gegeben werden. Auch die Suchtberatung und Prävention sowie Beratungs- und Betreuungsplanung sind Aufgaben, die dem SpD obliegen.
Zu unterscheiden ist daher die freiwillige Kontaktaufnahme des Betroffenen mit dem SpD im Gesundheitsamt, die in der Regel mit einer Beratungsleistung verbunden ist. Andererseits wird der SpD auf Anfrage bzw. im Auftrag "von Amts wegen" tätig, um über Betroffene z. B. Gutachten zu fertigen, die ihre Wirkung durch konkretes Verwaltungshandeln der anfordernden Stelle erzielen.

Im Zusammenhang mit einer freiwilligen Beratung ist ohnehin die Frage zu stellen, ob deren Inhalte bzw. Ergebnisse im dafür vorgesehenen Modul hinterlegt werden müssen. Bei einer derartigen Konstellation mangelt es bereits an der notwendigen Erforderlichkeit i. S. v. § 11 Abs. 1 HDSG. Deshalb wäre es allenfalls akzeptabel, Inhaltsdaten ohne Personenbezug in das System einzustellen.

Auch wenn der SpD beauftragt wird und in diesem Zusammenhang Vorgänge zu einem Betroffenen entstehen, ist zweifelhaft, ob diese Personen im allgemeinen Personenstammdatensatz einer Zentraldatei abgespeichert werden können. Jeder „allgemein zugängliche“ Hinweis würde nämlich implizieren, dass der Betroffene im Zusammenhang mit einer Sucht- oder Drogenabhängigkeit bzw. auf Grund psychischer Probleme beim SpD bekannt wurde. Die Folge wäre im Zusammenhang mit einer amtsärztlichen Untersuchung, dass diese Organisationseinheit gezielt beim SpD nach aktenmäßigen Erkenntnissen nachsuchen würde. Um eine solche „Regelanfrage“ von vorneherein auszuschließen, darf die Information darüber, dass es im SpD Vorgänge gibt, nicht allgemein zugänglich sein. Zudem sollte vor jeder Datenübermittlung aus diesem Fachbereich eine Einwilligungserklärung des Betroffenen vorliegen.

Die organisatorische Konsequenz dessen, dass der SpD besonders sensitive Gesundheitsdaten verwaltet, muss demnach sein, dessen Einbindung in das automatisierte Verfahren auszuschließen. Bereits der Hinweis auf existente Akten dort, die allgemein zugänglich sind, könnte zu einer Stigmatisierung der Betroffenen und als weitere Folge dazu führen, dass man im konkreten Einzelfall in anderen Fachbereichen des Gesundheitsamtes nicht mehr vorurteilsfrei begutachtet bzw. handelt.

Das Problembewusstsein hierzu war in allen Häusern, die ich aufgesucht habe, vorhanden. Es hat auch ohne meine Mitwirkung dazu geführt, dass der SpD in der Regel nicht in den allgemeinen organisatorischen Betrieb eines Gesundheitsamtes eingebunden ist. Vielmehr wird, unabhängig von Fragen der Dienst- und Fachaufsicht, entsprechend der Sensibilität der Daten eine Abschottung der Datenbestände angestrebt.

14.5.4
Weiteres Verfahren

Ich habe die bislang aufgesuchten Gesundheitsämter angeschrieben und ihnen meine Vorstellungen erläutert, wie der Datensatz der Zentraldatei inhaltlich gestaltet sein könnte. Dabei kommt es darauf an, unabhängig von den einzelnen Anwendungen zu einer einheitlichen und klaren Definition dessen zu kommen, was als erforderlich anzusehen ist. Die Vorgabe eines von seinem Umfang her abschließenden Datensatzes, der Inhalt der Zentraldatei ist, ist datenschutzrechtlich erforderlich und für die Gleichbehandlung aller öffentlichen Stellen im Gesundheitsdienst notwendig. Nach der Auswertung der Rückmeldungen könnte es dann zu einem standardisierten Datensatz der Zentraldatei kommen, der für alle Gesundheitsämter gilt.

Was den SpD anbelangt, so werde ich - soweit das von den Gesundheitsämtern bislang nicht ohnehin bereits praktiziert worden ist - darauf hinwirken, dass eine vollständige Abschottung der Datenbestände auch im Hinblick auf Informationen in der Zentraldatei gewährleistet ist. Eine Datenübermittlung vom SpD zu einer anderen Stelle innerhalb des Gesundheitsamtes bedürfte ohnehin der schriftlichen Einwilligung des Betroffenen.

15. Sozialwesen

15.1
Existenzgrundlagengesetz

Die Datenverarbeitung der Vermittlungsagenturen ist im Gesetzentwurf datenschutzrechtlich nicht korrekt geregelt.

Die Hessische Landesregierung hat in den Bundesrat den Entwurf eines Gesetzes zur Sicherung der Existenzgrundlagen (EGG) eingebracht (BRDrucks. 654/03), der u. a. die Errichtung von Vermittlungsagenturen vorsieht (§§ 24 ff. EGG).

§ 30 des Entwurfs befasst sich mit der Datenerhebung, -verarbeitung und -nutzung der Vermittlungsagenturen. Die Vorschrift des Entwurfs hat folgenden Wortlaut:

§ 30 EGG-Entwurf

(1) Die Vermittlungsagenturen dürfen zur Wahrnehmung ihrer Aufgaben auf die Datenbanken der Arbeitsverwaltung zugreifen.
(2) Der Schutz der Sozialdaten richtet sich nach den Bestimmungen des Zehnten Buches.

Aus datenschutzrechtlicher Sicht ist die Regelung missverständlich.

Art. 1 EGG qualifiziert das EGG als Zwölftes Buch des Sozialgesetzbuches (SGB XII). Damit ist klar, dass das allgemeine Sozialdatenschutzrecht gilt, soweit nicht spezielles Sozialdatenschutzrecht im EGG normiert wird. Vor diesem Hintergrund ist § 30 EGG rechtssystematisch zweifelhaft konzipiert. So ist bei Abs. 1 dieser Norm, die verfügt, dass die Vermittlungsagenturen zur Wahrnehmung ihrer Aufgaben auf die Datenbanken zugreifen dürfen, unklar, ob materiellrechtlich der datenschutzrechtlich zentrale Erforderlichkeitsgrundsatz maßgebend sein soll und ob, weil erst Abs. 2 auf den allgemeinen Sozialdatenschutz verweist, der die Einrichtung automatisierter Abrufverfahren regelnde § 79 SGB X für den Zugriff der Vermittlungsagenturen auf die Datenbanken der Arbeitsverwaltung gelten soll. Dies hat insbesondere deshalb datenschutzrechtliche Relevanz, weil ich gemäß § 79 Abs. 3 SGB X vor der Einrichtung automatisierter Abrufverfahren zu unterrichten bin und dadurch die Möglichkeit habe, auf die datenschutzrechtliche Ausgestaltung des Verfahrens Einfluss zu nehmen. § 30 Abs. 2 EGG wirft darüber hinaus die Frage auf, ob die für den Sozialdatenschutz sehr wichtigen Bestimmungen in § 35 SGB I (Sozialgeheimnis) einschlägig oder etwa abbedungen sind, was wohl eher nicht gewollt ist. Da der Normtext des § 30 Abs. 2 EGG nur auf das SGB X verweist, könnte das gefolgert werden.

Vor diesem Hintergrund habe ich der Landesregierung aus datenschutzrechtlicher Perspektive folgenden Normtext für § 30 EGG vorgeschlagen:

> „Die Vermittlungsagenturen sind nach Maßgabe des § 79 Zehntes Buch befugt, auf die Datenbanken der Arbeitsverwaltung zuzugreifen, soweit das zur Erfüllung ihres gesetzlichen Auftrages erforderlich ist.“

§ 30 Abs. 2 kann ersatzlos entfallen.

Die Stellungnahme der Landesregierung steht bislang noch aus.

15.2
Sozialdatenschutz und Untersuchungsgrundsatz

Das Sozialdatenschutzrecht ist gegenüber dem sozialverwaltungsverfahrensrechtlichen Untersuchungsgrundsatz vorrangig.

Mit einer gewissen Regelmäßigkeit kommt es vor, dass sich Behörden, meistens im Zusammenhang mit dem Thema "Sozialleistungsmissbrauch", auf den Untersuchungsgrundsatz berufen. Danach ermittelt die Behörde den Sachverhalt von Amts wegen, und sie bestimmt Art und Umfang der Ermittlungen, § 20 Abs. 1 Sozialgesetzbuch X (SGB X).

Soweit es bei der Ermittlung des Sachverhalts um personenbezogene Daten geht, werden mit dem behördlichen Hinweis auf den Untersuchungsgrundsatz der Vorrang des Datenschutzrechts und die insofern nur subsidiäre Geltung des Untersuchungsgrundsatzes übersehen.

Schon im Hinblick auf den Geltungsbereich des Hessischen Datenschutzgesetzes (HDSG) hat der Gesetzgeber dessen Vorrang gegenüber dem allgemeinen Verwaltungsverfahrensrecht verfügt:

§ 3 Abs. 2 HDSG

Die Vorschriften dieses Gesetzes gehen denen des Hessischen Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

Exakt dieselbe Regelung hat der Bundesgesetzgeber im Bundesdatenschutz (BDSG) getroffen (§ 1 Abs. 4 BDSG), und insbesondere auch im Sozialgesetzbuch ist der Vorrang des Sozialdatenschutzrechts gegenüber den allgemeinen sozialverwaltungsverfahrensrechtlichen Regelungen ebenfalls gesetzlich verfügt (§ 37 Satz 3 SGB I).

§ 37 Satz 3 SGB I

Das Zweite Kapitel des Zehnten Buches geht dessen Erstem Kapitel vor, soweit sich die Ermittlung des Sachverhaltes auf Sozialdaten erstreckt.

Das Vorgehen des Zweiten Kapitels bedeutet im Klartext das Vorgehen des Sozialdatenschutzes.

Keineswegs bedeutet das, dass deswegen Leistungsmissbräuche nicht wirksam aufgedeckt werden könnten; bloß sind eben bei der Aufklärung des Sachverhalts die sozialdatenschutzrechtlichen Rahmenbedingungen einzuhalten, also die §§ 67 ff. SGB X und selbstverständlich auch die Grundnorm des Sozialdatenschutzes, § 35 SGB I.

Möchte beispielsweise ein Sozialamt personenbezogene Informationen vom Finanzamt einholen, ist dafür eine spezielle Rechtsgrundlage vonnöten (§ 67 Abs. 2 Nr. 2a SGB X). Eine solche ist - gerade was die Bekämpfung des Sozialleistungsmissbrauchs betrifft - § 31a Abgabenordnung (AO).

§ 31a AO

Die Offenbarung der nach § 30 geschützten Verhältnisse (Steuergeheimnis) der Betroffenen ist zulässig, soweit sie

1. für die Durchführung eines Strafverfahrens, eines Bußgeldverfahrens oder eines anderen gerichtlichen oder Verwaltungsverfahrens mit dem Ziel
   a) der Bekämpfung von illegaler Beschäftigung oder Schwarzarbeit oder
   b) der Entscheidung
      aa) über Erteilung, Rücknahme oder Widerruf einer Erlaubnis nach dem Arbeitnehmerüberlassungsgesetz oder
      bb) über Bewilligung, Gewährung, Rückforderung, Erstattung, Weitergewährung oder Belassen einer Leistung aus öffentlichen Mitteln

   oder
2. für die Geltendmachung eines Anspruchs auf Rückgewähr einer Leistung aus öffentlichen Mitteln erforderlich ist.

Ich betone gegenüber den Behörden regelmäßig, dass der Sozialdatenschutz einzuhalten ist, dass dies aber keineswegs bedeutet, Leistungsmissbrauch hinnehmen zu müssen, insofern ist auch im Sozialleistungsbereich Datenschutz keineswegs "Täterschutz". Nicht zu vergessen ist in diesem Zusammenhang insbesondere auch § 117 Bundessozialhilfegesetz, der eine ganze Fülle verschiedener Datenabgleiche zulässt.

§ 117 BSHG

(1) Die Träger der Sozialhilfe sind befugt, Personen, die Leistungen nach diesem Gesetz beziehen, auch regelmäßig im Wege des automatisierten Datenabgleichs daraufhin zu überprüfen,

1. ob und in welcher Höhe und für welche Zeiträume von ihnen Leistungen der Bundesanstalt für Arbeit (Auskunftsstelle) oder der Träger der gesetzlichen Unfall- oder Rentenversicherung (Auskunftsstellen) bezogen werden oder wurden und
2. ob und in welchem Umfang Zeiten des Leistungsbezuges nach diesem Gesetz mit Zeiten einer Versicherungspflicht oder Zeiten einer geringfügigen Beschäftigung zusammentreffen, und
3. ob und welche Daten nach § 45d Abs. 1 des Einkommensteuergesetzes dem Bundesamt für Finanzen (Auskunftsstelle) übermittelt worden sind,
4. ob und in welcher Höhe ein Kapital nach § 88 Abs. 2 Nr. 1a nicht mehr dem Zweck einer geförderten zusätzlichen Altersvorsorge im Sinne des § 10a oder des Abschnitts XI des Einkommensteuergesetzes dient.

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

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

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

(3) Die Träger der Sozialhilfe sind befugt, zur Vermeidung rechtswidriger Inanspruchnahme von Sozialhilfe Daten von Personen, die Leistungen nach diesem Gesetz beziehen, bei anderen Stellen ihrer Verwaltung, bei ihren wirtschaftlichen Unternehmen und bei den Kreisen, Kreisverwaltungsbehörden und Gemeinden zu überprüfen, soweit diese für die Erfüllung dieser Aufgaben erforderlich sind. Sie dürfen für die Überprüfung die in Absatz 1 Satz 2 genannten Daten übermitteln. Die Überprüfung kann auch regelmäßig im Wege des automatisierten Datenabgleichs mit den Stellen durchgeführt werden, bei denen die in Satz 4 jeweils genannten Daten zuständigkeitshalber vorliegen. Nach Satz 1 ist die Überprüfung folgender Daten zulässig:

a) Geburtsdatum und -ort;
b) Personen- und Familienstand;
c) Wohnsitz;
d) Dauer und Kosten von Miet- oder Überlassungsverhältnissen von Wohnraum;
e) Dauer und Kosten von bezogenen Leistungen über Elektrizität, Gas, Wasser, Fernwärme oder Abfallentsorgung;
f) Eigenschaft als Kraftfahrzeughalter.

Die in Satz 1 genannten Stellen sind verpflichtet, die in Satz 4 genannten Daten zu übermitteln. Sie haben die ihnen im Rahmen der Überprüfung übermittelten Daten nach Vorlage der Mitteilung unverzüglich zu löschen. Eine Übermittlung durch diese Stellen unterbleibt, soweit ihr besondere gesetzliche Verwendungsregelungen entgegenstehen.

Ich weise regelmäßig die Behörden auch auf diese Möglichkeiten der Datenabgleiche zur Verhinderung des Sozialleistungsmissbrauchs hin.

15.3
Opferschutz und Jugendgerichtshilfe

Jugendhilferechtliche Maßnahmen zur Förderung einer positiven Entwicklung Jugendlicher, die sich kriminell verhalten haben, müssen das informationelle Selbstbestimmungsrecht der geschädigten Person beachten.

Die Eingabe einer Beschwerdeführerin betraf das Verhalten eines Jugendamts (Jugendgerichtshilfe). Hintergrund war, dass die Beschwerdeführerin von einem der jugendlichen Täter, der sie zusammen mit anderen überfallen hatte (versuchter Handtaschenraub), ein Entschuldigungsschreiben erhielt und sie sich nicht erklären konnte, woher der Täter ihren Namen und ihre Anschrift kannte. Im Zuge ihrer Recherchen stellte sich heraus, dass das zuständige Jugendamt bei dem Jugendlichen ein Entschuldigungsschreiben angeregt hatte und in diesem Zusammenhang dem Jugendlichen Name und Anschrift der betroffenen Bürgerin bekannt gegeben hatte, ohne deren Einwilligung hierfür einzuholen.

Diese Vorgehensweise ist datenschutzrechtlich nicht zulässig gewesen. Das informationelle Selbstbestimmungsrecht der betroffenen Bürgerin verlangt, dass entweder vor einer solchen Bekanntgabe ihrer Daten ihre Einwilligung hätte eingeholt werden müssen oder dass in einer solchen Konstellation ein Entschuldigungsschreiben vom Jugendamt versandt worden wäre, ohne dass dem Täter vorher der Name und die Anschrift bekannt gegeben worden wäre. Der Täter braucht den Namen und die Anschrift des Opfers nicht zu kennen, um sich schriftlich zu entschuldigen. Diese Daten können auch erst nachträglich auf den Brief vom Jugendamt hinzugefügt werden. Mit dem Jugendamt wurde für die Zukunft ein dementsprechendes Verfahren festgelegt.

16. Personalwesen

16.1
Personalaktenregistratur im Schulbereich

Es ist datenschutzrechtlich nicht akzeptabel, wenn der Aufbewahrungsort von Personalakten ungewiss ist.

Eine ehemalige Lehramtsreferendarin beschwerte sich bei mir darüber, dass sie keine Möglichkeit habe, Einsicht in ihre vollständigen Personalaktenunterlagen zu nehmen, sie seien bei der Schulverwaltung nicht auffindbar. So teilte ihr das Regierungspräsidium Darmstadt mit, dass sich ihre Prüfungsniederschrift im Staatsarchiv befinde; dieses wiederum verwies die Eingeberin an das Staatliche Schulamt Gießen, ebenfalls ohne Erfolg.

Aus datenschutzrechtlicher Sicht ist es zwingend, dass der jeweilige Aufbewahrungsort einer Personalakte oder einzelner zur Personalakte gehörenden Unterlagen transparent ist. Nur so kann gewährleistet werden, dass die personalaktenrechtlichen Vorschriften beachtet und die damit verbundenen Rechte der Betroffenen, wie etwa das Einsichtsrecht (§ 107c HBG), wahrgenommen werden können.

Nach von mir veranlassten Recherchen in der Schulverwaltung stellte sich heraus, dass sich die Personalakte beim Amt für Lehrerausbildung in Frankfurt befand.

Ich habe den Vorgang zum Anlass genommen, die Personalaktenverwaltung im Amt für Lehrerausbildung in Frankfurt zu prüfen.

Das Amt für Lehrerausbildung ist Ende 2001 errichtet worden; in der Folgezeit erhielt es von den aufgelösten Schulabteilungen der Regierungspräsidien und Staatlichen Schulämtern in großer Zahl unsortiert Personalakten. Ich konnte mich vor

Ort davon überzeugen, dass das (mit einer Nebenstelle in Kassel) für ganz Hessen zuständige Amt für Lehrerausbildung in Frankfurt mittlerweile deutlich fortgeschritten ist, die Situation zu bereinigen. Dies liegt insbesondere auch daran, dass speziell für die Aktenregistratur eine Arbeitskraft eingestellt wurde, die die vorhandenen Akten sichtet und registriert. Diesem Umstand ist auch zu verdanken, dass die Personalakten der Eingeberin mittlerweile vollständig vorliegen. Die Beschwerdeführerin wurde unverzüglich vom Auffinden der Akte unterrichtet und ihr wurde Gelegenheit zur Akteneinsicht gegeben.

16.2
Vereitelung von Akteneinsichtsrechten durch Vernichtung von Unterlagen

Bedienstete haben, auch nach Beendigung ihres Beschäftigungsverhältnisses, einen Anspruch auf Einsicht in Unterlagen ihres Dienstherrn, die personenbezogene Daten über sie enthalten. Weder dieser Anspruch noch mein eigenes Einsichtsrecht in solche Unterlagen darf durch deren rechtswidrige Vernichtung vereitelt werden.

Eine ehemalige Bedienstete des Landeswohlfahrtsverbandes (LWV) hat Beschwerde darüber erhoben, dass ihr der Verband keine Einsicht in ein Schlussgutachten gewähre, das von einer externen Sachverständigen im Auftrag des LWV angefertigt worden war; das Schlussgutachten war das Resultat eines so genannten Coaching-Verfahrens, das wegen verbandsinterner Konflikte, in die auch die Beschwerdeführerin involviert war, vom LWV eingeleitet worden war.

16.2.1
Akteneinsichtsrecht

Der LWV verweigerte der Beschwerdeführerin die Akteneinsicht in das Schlussgutachten u. a. mit der Begründung, es handele sich bei den Unterlagen nicht um solche, die zur Personalakte gehören, und es seien auch evtl. vertrauensschutzbedürftige Belange Dritter betroffen, was einer Einsicht durch die Beschwerdeführerin ebenfalls entgegenstehe. Das Schlussgutachten werde im Übrigen nicht zur Grundlage weiterer Entscheidungen des LWV gemacht. In der Folgezeit wurde der befristete Anstellungsvertrag mit der Beschwerdeführerin nicht verlängert.

Die Verweigerung der Akteneinsicht durch den LWV verstieß gegen das Einsichtsrecht der Bediensteten gewährleistenden § 107c HBG; diese Vorschrift gilt wegen § 34 Abs. 1 Satz 2 HDSG auch für Bedienstete, die nicht Beamte sind.

§ 107c HBG

(1) Der Beamte hat, auch nach Beendigung des Beamtenverhältnisses, ein Recht auf Einsicht in seine vollständige Personalakte.

(2) Einem Bevollmächtigten des Beamten ist Einsicht zu gewähren, soweit dienstliche Gründe nicht entgegenstehen. Dies gilt auch für Hinterbliebene, wenn ein berechtigtes Interesse glaubhaft gemacht wird, und deren Bevollmächtigte. Für Auskünfte aus der Personalakte gelten Satz 1 und 2 entsprechend.

(3) Die personalaktenführende Behörde bestimmt, wo die Einsicht gewährt wird. Soweit dienstliche Gründe oder Rechte Dritter nicht entgegenstehen, können Auszüge, Abschriften, Ablichtungen oder Ausdrucke gefertigt werden; dem Beamten ist auf Verlangen ein Ausdruck der zu seiner Person automatisiert gespeicherten Personalaktendaten zu überlassen.

(4) Der Beamte hat ein Recht auf Einsicht auch in andere Akten, die personenbezogene Daten über ihn enthalten und für sein Dienstverhältnis verarbeitet oder genutzt werden, soweit gesetzlich nichts anderes bestimmt ist; dies gilt nicht für Sicherheitsakten. Die Einsichtnahme ist unzulässig, wenn die Daten des Betroffenen mit Daten Dritter oder geheimhaltungsbedürftigen nichtpersonenbezogenen Daten derart verbunden sind, dass ihre Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist. In diesem Fall ist dem Beamten Auskunft zu erteilen.

§ 34 Abs. 1 Satz 2 HDSG

Die für das Personalaktenrecht geltenden Vorschriften des Hessischen Beamtengesetzes sind, soweit tarifvertraglich nichts anderes geregelt ist, auf Angestellte und Arbeiter im öffentlichen Dienst entsprechend anzuwenden.

Von Bedeutung ist zunächst, dass das Einsichtsrecht nicht nur während, sondern auch nach Beendigung des Beschäftigungsverhältnisses fortbesteht (§ 107c Abs. 1 HBG), was der LWV angezweifelt hat. Die vom LWV geäußerte Ansicht, das Schlussgutachten sei eine so genannte Sachakte und habe keine Personalaktenqualität, ist schon angesichts des in § 107 Abs. 1 HBG verankerten weiten, materiellen Personalaktenbegriffs zweifelhaft; letztlich kommt es aber darauf nicht entscheidend an, weil das Einsichtsrecht auf Sachakten, die Bedienstetendaten betreffen, gesetzlich ausgedehnt worden ist (§ 107c Abs. 4 HBG). Der vom LWV vorgetragene Einwand, das Schlussgutachten sei hinsichtlich des Dienstverhältnisses nicht verwertet worden, überzeugt nicht angesichts des Umstandes, dass der LWV sich mit dem Schlussgutachten auseinander gesetzt hat und der Vertrag mit der Eingeberin nicht verlängert worden ist.

Das Problem "Daten Dritter" im Schlussgutachten hätte sich durch teilgeschwärzte Kopien bzw. Auskunftserteilung lösen lassen.

Ich hatte den LWV auf die Rechtslage hingewiesen. Der LWV hat mir mitgeteilt, dass er sich meiner Auffassung nicht anschließt. Ohne Rücksprache mit mir hat er sodann das Schlussgutachten vernichtet.

16.2.2
Rechtswidrige Aktenvernichtung

16.2.2.1
Rechte der Betroffenen

Im Hinblick auf die Eingeberin verstößt die Vernichtung des Gutachtens gegen § 19 Abs. 3 Satz 3 HDSG, weil die Möglichkeit zur Kenntnisnahme des Gutachtens Voraussetzung dafür ist, sich gegen dessen Inhalte gegebenenfalls zur Wehr setzen zu können. Insofern wurden durch die Vernichtung schutzwürdige Belange der Eingeberin beeinträchtigt.

§ 19 Abs. 3 HDSG

Personenbezogene Daten sind unverzüglich zu löschen, sobald feststeht, dass ihre Speicherung nicht mehr erforderlich ist, um die Zwecke zu erfüllen, für die sie erhoben worden sind oder für die sie nach § 13 Abs. 2 und 4 weiterverarbeitet werden dürfen. Wenn bei der Speicherung nicht absehbar ist, wie lange die Daten benötigt werden, ist nach einer auf Grund der Erfahrung zu bestimmenden Frist zu prüfen, ob die Erforderlichkeit der Speicherung noch besteht. Satz 1 findet keine Anwendung, wenn Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden.

16.2.2.2
Rechte des Hessischen Datenschutzbeauftragten

Ganz unabhängig davon ist durch den LWV mein eigenes Einsichtsrecht nach § 29 Abs. 1 Nr. 1 HDSG verletzt worden; dass eine Behörde Unterlagen vernichtet, die Gegenstand einer noch nicht abgeschlossenen Kontroverse mit meinem Haus sind, und dadurch meine Befugnisse zur Einsichtnahme durch vollendete Tatsachen zunichte macht, ist eine eklatante Missachtung meiner Informationsrechte im Sinne von § 29 Abs. 1 HDSG.

§ 29 Abs. 1 HDSG

Alle datenverarbeitenden Stellen und ihre Auftragnehmer sind verpflichtet, den Hessischen Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen. Ihm ist dabei insbesondere

1. Auskunft zu seinen Fragen sowie Einsicht in alle Unterlagen zu gewähren, die in Zusammenhang mit der Verarbeitung personenbezogener Daten stehen,
2. Zutritt zu allen Diensträumen zu gewähren.

Da es sich bei besagter Vernichtung des Schlussgutachtens durch den LWV um einen gravierenden Verstoß gegen das Datenschutzrecht handelt, habe ich eine Beanstandung nach § 27 HDSG ausgesprochen und den LWV aufgefordert, dafür zu sorgen, dass sich vergleichbare Vorfälle in Zukunft nicht wiederholen. Außerdem habe ich das Hessische Innenministerium als zuständige Aufsichtsbehörde über die Angelegenheit unterrichtet.

§ 27 Abs. 1 und 4 HDSG

(1) Stellt der Hessische Datenschutzbeauftragte Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Datenschutzbestimmungen oder sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so beanstandet er dies

1. bei der Landesverwaltung gegenüber der zuständigen obersten Landesbehörde,
2. bei den Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie bei Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gegenüber dem Vorstand oder dem sonst vertretungsberechtigten Organ

und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf.
In den Fällen von Satz 1 Nr. 2 unterrichtet der Hessische Datenschutzbeauftragte gleichzeitig auch die zuständige Aufsichtsbehörde.

(4) Die gemäß Abs. 1 abzugebende Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die auf Grund der Beanstandung des Hessischen Datenschutzbeauftragten getroffen worden sind. Die in Abs. 1 Satz 1 Nr. 2 genannten Stellen leiten der zuständigen Aufsichtsbehörde eine Abschrift ihrer Stellungnahme an den Hessischen Datenschutzbeauftragten zu.

Das Hessische Ministerium des Innern und für Sport hat infolge meiner Unterrichtung über die Angelegenheit bestätigt, dass die Aktenvernichtung rechtswidrig gewesen ist und hat den LWV aufgefordert, solche Rechtsverstöße zukünftig zu unterlassen.

17. Recht der Presse, Medien- und Teledienste

17.1
Neuordnung der Rundfunkfinanzierung

Eine Realisierung der Vorstellungen der Landesrundfunkanstalten zur Novellierung des Rundfunkgebührenstaatsvertrages würde zu einer erheblichen Verschlechterung des Datenschutzes führen.

17.1.1
Hintergrund der geplanten Neuregelung

Am 31. Dezember 2004 endet für Computer, die über Internet Rundfunkprogramme empfangen können, die vorläufige Freistellung von der Gebührenpflicht (§ 5a Rundfunkgebührenstaatsvertrag; RGebStV). Das bevorstehende Ende des Moratoriums hat die Landesregierungen dazu veranlasst, über eine grundsätzliche Neuordnung der Rundfunkfinanzierung nachzudenken. Im Zentrum der Überlegungen steht eine Umstellung von der Gebührenpflicht des Rundfunkteilnehmers auf eine Gebührenpflicht des Haushalts. Beratungsgrundlage sind dabei Vorstellungen der öffentlich-rechtlichen Rundfunkanstalten. Auf Wunsch der Staatskanzlei und des Hessischen Ministeriums für Wirtschaft, Verkehr und Landesentwicklung habe ich zu den von den Rundfunkanstalten unterbreiteten Vorschlägen zur Neustrukturierung der Rundfunkfinanzierung Stellung genommen. Zu kritisieren sind besonders die vorgeschlagenen Datenübermittlungen an die Landesrundfunkanstalten.

17.1.2
Datenübermittlungen der Einwohnermeldeämter

Die Vorschläge der Rundfunkanstalten sehen vor, dass sämtliche Einwohnermeldeämter zu einem Stichtag der Gebühreneinzugszentrale (GEZ) Daten aller über 16-jährigen Personen zur Verfügung stellen, wobei offen gelassen wird, welche Daten genau mitgeteilt werden sollen. Die GEZ verarbeitet die Daten im Auftrag der Landesrundfunkanstalten, so dass rechtlich gesehen die Daten nicht an die GEZ, sondern an diese übermittelt werden.

Der Nutzen dieser Datenübermittlung für die Feststellung der Rundfunkgebührenpflicht ist mehr als fraglich. Die Gebührenpflicht soll pro Wohnung/Haushalt bestehen. Abgesehen von den rundfunkgebührenrechtlichen Problemen, die der Wechsel vom gebührenpflichtigen Rundfunkteilnehmer (§ 2 Abs. 2 RGebStV) zum gebührenpflichtigen Haushalt bereiten dürfte (Soll ein einzelnes zu benennendes Haushaltsmitglied gebührenpflichtig sein oder sollen die Haushaltsmitglieder gesamtschuldnerisch haften?), entstehen durch die anscheinend beabsichtigte Gleichsetzung von Haushalt und Wohnung Erhebungsprobleme. Die Gleichsetzung ist insofern verständlich, als im Einwohnermelderegister zwar das Merkmal Wohnung (Haupt- und Nebenwohnung) nicht aber das Merkmal Haushalt erfasst wird (§ 3 Hessisches Meldegesetz; HMG). In einer Wohnung können allerdings mehrere Haushalte existieren, wie nicht zuletzt ein Blick in das Mikrozensusgesetz zeigt. Nach § 2 Abs. 1 Mikrozensusgesetz bilden alle Personen, die gemeinsam wohnen und wirtschaften, einen Haushalt. Daher wird beim Mikrozensus auch nach der Zahl der Haushalte in der Wohnung gefragt (§ 4 Abs. 1 Nr. 1a Mikrozensusgesetz). Die Angaben aus dem Einwohnermelderegister erlauben mithin keine verlässliche Zuordnung der Person zu einem Haushalt.

Seit 1993 erhält die GEZ im Auftrag des Hessischen Rundfunks (HR) auf der Grundlage des § 18 Abs. 1 Meldedaten-Übermittlungsverordnung von den hessischen Meldebehörden bei An- und Abmeldungen und Ableben volljähriger Einwohner folgende Daten: Familiennamen, Vornamen, Tag der Geburt, gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung, Tag des Ein- und Auszugs, Sterbetag. Die Datenübermittlung erfolgt monatlich im automatisierten Verfahren. Der HR hat somit in den letzten zehn Jahren bereits in beträchtlichem Umfang Meldedaten erhalten und erhält sie weiterhin. Er ist also schon durch das bestehende Melderecht privilegiert, denn er erhält als einzige öffentliche Stelle zum Zwecke der Überprüfung, ob ein Bürger seiner Gebührenpflicht nachkommt, sämtliche Veränderungsdaten aus den Melderegistern. In den meisten anderen Bundesländern existieren ähnliche Regelungen.

Bereits die Verhältnismäßigkeit der gegenwärtigen Datenübermittlungen ist zweifelhaft. Ein großer Teil der Meldedaten, welche die Landesrundfunkanstalten nach geltendem Recht erhalten, betrifft Personen, die keiner Gebührenpflicht unterliegen, z. B. weil es sich um Ehegatten oder Personen handelt, welche mit dem Rundfunkteilnehmer in häuslicher Gemeinschaft leben (§ 5 Abs. 1 RGebStV). Weit größer würde das Missverhältnis, erhielten die Landesrundfunkanstalten stichtagsbezogen die Meldedaten aller Einwohner, die über 16 Jahre alt sind. Die Rundfunkanstalten gehen davon aus, dass der Gebührenausschöpfungsgrad bei den privaten Haushalten derzeit bei durchschnittlich 94 v.H. liegt. Durch die stichtagsbezogenen Meldedaten erhoffen sie sich eine Steigerung um zwei Prozentpunkte. Zu diesem Zweck sollen die Daten von ca. 66 Millionen Einwohnern an die Landesrundfunkanstalten übermittelt werden. In der vom Hauptausschuss des Hessischen Landtags am 6. März 2002 durchgeführten Anhörung zur Zukunft der Rundfunkgebühren hat der Geschäftsführer der GEZ die Zahl der zurzeit von der GEZ verwalteten Teilnehmerkonten auf 39 Millionen beziffert (HHA 15/39 S. 25). Die GEZ unterhält ca. 1,88 Millionen nichtprivate (geschäftliche) Teilnehmerkonten. Demnach führt sie etwa 37 Millionen Konten von Rundfunkteilnehmern aus privaten Haushalten. Da dies einem Gebührenausschöpfungsgrad von 94 v.H. entspricht, läge die maximal zu erreichende Kontenzahl (100 v.H.) bei ca. 39,5 Millionen. Das bedeutet, von ca. 26,5 Millionen Einwohnern, die keiner Gebührenpflicht unterliegen, würden Meldedaten an die GEZ übermittelt.

Bei der GEZ entstünde faktisch ein bundesweites Register aller über 16-jährigen Personen mit Informationen über deren soziale Verhältnisse (wie Partnerschaften, gesetzliche Vertretungen, Haushaltszugehörigkeit und Empfang von Sozialleistungen). Ein großer Teil dieser Daten ist jedoch zu keiner Zeit für den Einzug der Rundfunkgebühren erforderlich.

17.1.3
Datenübermittlungen weiterer Stellen

Das von den Rundfunkanstalten zur Verbesserung des Gebührenausschöpfungsgrades im nicht privaten (geschäftlichen) Bereich geäußerte Interesse an Daten aus den Gewerbeanzeigen und der Wunsch nach Zugriff auf Mitgliederdaten der Kammern (IHK, Handwerkskammern, Ärztekammern, Rechtsanwaltskammern usw.) und auf Daten des Kraftfahrt-Bundesamtes müssen sich ebenfalls am Verhältnismäßigkeitsgrundsatz messen lassen. Eine Übermittlung der Gesamtdatenbestände irgendeiner der genannten Stellen scheidet deshalb mit Sicherheit aus. So wäre es offensichtlich unverhältnismäßig, den Landesrundfunkanstalten die beim Kraftfahrt-Bundesamt im Zentralen Fahrzeugregister gespeicherten 53 Millionen Fahrzeug- und Halterdatensätze zur Verfügung zu stellen, damit die Anstalten überprüfen können, für welches Rundfunkgerät in geschäftlich genutzten Fahrzeugen keine Gebühr entrichtet wird. Nicht ausgeschlossen ist dagegen, dass auf Einzelfälle bezogene Datenübermittlungen an die Landesrundfunkanstalten gesetzlich erlaubt werden könnten. Dazu müssten die Landesrundfunkanstalten ihre Informationswünsche allerdings zunächst konkretisieren und begründen.

17.2
Erwerb von Adressen durch die Gebühreneinzugszentrale

Im Auftrag des Hessischen Rundfunks beschafft sich die Gebühreneinzugszentrale bei Adresshändlern Anschriften für Briefaktionen, mit denen Schwarzhörer und -seher zur Zahlung der Rundfunkgebühren bewegt werden sollen. Der Erwerb der Adressen verstößt gegen das Hessische Datenschutzgesetz.

17.2.1
Briefaktionen der Gebühreneinzugszentrale

Die Gebühreneinzugszentrale (GEZ) erwirbt im Auftrag der Rundfunkanstalten im Adresshandel regelmäßig Anschriften und nutzt sie für Briefaktionen, mit denen Schwarzhörer und -seher zur Anmeldung ihrer Rundfunkgeräte bewegt werden sollen. In einem ersten Anschreiben werden die Empfänger aufgefordert, zu überprüfen, ob sie ihrer gesetzlichen Verpflichtung zur Anmeldung von Rundfunkgeräten nachkommen. Geht das Schreiben an Privatpersonen, schildert die GEZ verschiedene Konstellationen, in denen im Privathaushalt Rundfunkgebühren entstehen (Nichteheliche Lebensgemeinschaften, Kinder im Haushalt der Eltern, Eltern im Haushalt der Kinder, Rundfunk am Arbeitsplatz, Zweit- oder Ferienwohnung). Selbständige oder Gewerbetreibende erhalten ein ähnliches Schreiben, in dem Tatbestände geschildert werden, die in diesen Bereichen zur Rundfunkgebührenpflicht führen. Die Empfänger werden unter Fristsetzung aufgefordert, auch dann zu antworten, wenn sie keine Rundfunkgeräte anzumelden haben. Sie würden sich dadurch eine "Erinnerung" ersparen. Wer nicht antwortet, erhält einen Monat später eine "Freundliche Erinnerung", wiederum verbunden mit einer Frist für die Beantwortung. Wer auch diese Frist verstreichen lässt, erhält eine "Letzte Erinnerung", die den Hinweis enthält, dass eine Verletzung der Anmeldepflicht mit einer Geldbuße bis zu 1.000 € geahndet werden könne und sich durch eine fristgemäße Antwort Unannehmlichkeiten vermeiden ließen.

Bei den Aktionen werden zwangsläufig viele Personen angeschrieben, die bereits Gebühren zahlen oder keiner Gebührenpflicht unterliegen. Je nach Qualität des Adressmaterials sind Kuriositäten dabei nicht auszuschließen. So werden Personen, die ihre Zulassung als Rechtsanwalt schon vor Jahrzehnten zurückgegeben haben, als Rechtsanwalt angeschrieben und zur Anmeldung ihrer Rundfunkgeräte in geschäftlich genutzten Fahrzeugen aufgefordert. Auch Tote erhalten mitunter Post von der GEZ, was bei manchen Angehörigen besondere Empörung hervorruft.

Es ist daher kaum verwunderlich, dass zu den Briefaktionen der GEZ häufig Beschwerden bei mir eingehen. Oft bezweifeln die Betroffenen nicht nur die datenschutzrechtliche Zulässigkeit, sondern geben auch an, dass sie sich durch die Briefe der GEZ bedroht und belästigt fühlen.

17.2.2
Verstoß gegen das Hessische Datenschutzgesetz

Trotz eines längeren Briefwechsels konnte ich den Hessischen Rundfunk (HR) nicht davon überzeugen, dass der Erwerb der Adressen gegen das Hessische Datenschutzgesetz verstößt. Öffentliche Stellen dürfen personenbezogene Daten grundsätzlich nur beim Betroffenen erheben. Bei Dritten außerhalb des öffentlichen Bereichs dürfen Daten ohne Kenntnis der Betroffenen erhoben werden, wenn der Schutz von Leben und Gesundheit oder die Abwehr einer erheblichen Gefährdung der natürlichen Lebensgrundlagen dies im Einzelfall gebietet oder eine Rechtsvorschrift dies vorsieht oder, soweit es sich um eine Rechtsvorschrift des Bundes handelt, zwingend voraussetzt (§ 12 Abs. 1 und 3 Hessisches Datenschutzgesetz [HDSG]).

§ 12 Abs. 1 und 3 HDSG

(1) Personenbezogene Daten sind grundsätzlich bei dem Betroffenen mit seiner Kenntnis zu erheben. Werden Daten nicht über eine bestimmte Person, sondern über einen bestimmbaren Personenkreis, etwa durch Videoüberwachung, erhoben, dann genügt es, wenn er die seinen schutzwürdigen Belangen angemessene Möglichkeit zur Kenntnisnahme hat.

(3) Beim Betroffenen und bei Dritten außerhalb des öffentlichen Bereichs dürfen Daten ohne seine Kenntnis nur erhoben werden, wenn der Schutz von Leben und Gesundheit oder die Abwehr einer erheblichen Gefährdung der natürlichen Lebensgrundlagen dies im Einzelfall gebietet oder eine Rechtsvorschrift dies vorsieht oder, soweit es sich um eine Rechtsvorschrift des Bundes handelt, zwingend voraussetzt.

Die Erhebung der Adressdaten bei privatwirtschaftlichen Adressverlagen ohne Kenntnis der Betroffenen lässt sich auf keine dieser Ausnahmeregelungen stützen. Der HR sieht dagegen keinen Verstoß gegen das Datenschutzrecht und hat dementsprechend auch meine Forderung, die Briefaktionen bis zur Schaffung einer ausreichenden Rechtsgrundlage einzustellen, abgelehnt.

Im Verlauf meiner Prüfung wurden unterschiedliche Argumente genannt, die alle einer rechtlichen Prüfung nicht standhalten.

17.2.3
Rechtfertigungsversuch der Gebühreneinzugszentrale

Die GEZ hatte in Antwortschreiben auf Beschwerden die Adressenbeschaffung als eigene Datenerhebung eingeordnet, die durch das Bundesdatenschutzgesetz (BDSG) gerechtfertigt sei. Dem steht jedoch der Rundfunkgebührenstaatsvertrag entgegen. § 8 Abs. 2 Satz 1 Rundfunkgebührenstaatsvertrag stellt klar, dass die GEZ die beim Gebühreneinzug anfallenden personenbezogenen Daten als Auftragnehmerin für die Landesrundfunkanstalten verarbeitet. Wie aus der Begründung des Staatsvertrages zu entnehmen ist, bedeutet die Formulierung nicht, dass die Datenverarbeitung im Zusammenhang mit individuellen Einzugsmaßnahmen stehen muss, es genügt jede auf den Gebühreneinzug gerichtete Tätigkeit (Begründung des Staatsvertrages über den Rundfunk im Vereinten Deutschland, S. 143 - Hessischer Landtag Drucks. 13/3518 vom 4. Dezember 1992). Nach der Definition des Rundfunkgebührenstaatsvertrages erfolgt somit auch die mit den Briefaktionen verbundene Verarbeitung personenbezogener Daten im Auftrag der Landesrundfunkanstalten. Soweit die GEZ hessische Adressen für Briefaktionen erhebt und nutzt, ist datenverarbeitende Stelle der HR. Für dessen Datenverarbeitung ist nicht das Bundesdatenschutzgesetz maßgeblich, sondern mangels einer besonderen Regelung im Rundfunkgebührenstaatsvertrag allein das Hessische Datenschutzgesetz.

17.2.4
Hessischer Rundfunk als Wettbewerbsunternehmen?

Der HR erkannte zwar an, dass er datenverarbeitende Stelle sei, war aber dennoch der Meinung, dass für die Briefaktionen nicht das HDSG, sondern das BDSG gelte, da er ein öffentlich-rechtliches Wettbewerbsunternehmen sei. Für diese sind gem. § 3 Abs. 6 HDSG nicht die materiellrechtlichen Verarbeitungsvorschriften des HDSG, sondern die Regelungen des BDSG für die Datenverarbeitung nicht öffentlicher Stellen maßgeblich. Diese Selbstcharakterisierung des HR überrascht und verwundert gleichermaßen. Seit der Novellierung des HDSG im Jahr 1986 bestand Konsens zwischen dem Hessischen Datenschutzbeauftragten und dem HR, dass für die Verwaltungsdatenverarbeitung die Vorschriften des HDSG uneingeschränkt gelten.

Die Frage des anzuwendenden Rechts ist eindeutig in § 3 Abs. 5 HDSG geregelt.

§ 3 Abs. 5 HDSG

Soweit der Hessische Rundfunk personenbezogene Daten ausschließlich zu eigenen journalistischen-redaktionellen Zwecken verarbeitet, gelten von den Vorschriften dieses Gesetzes nur die §§ 10 und 37. Im Übrigen gelten die Vorschriften dieses Gesetzes.

Zwar ist die Anwendbarkeit des HDSG für die journalistisch-redaktionelle Datenverarbeitung des HR dort weitgehend eingeschränkt. Für den übrigen Bereich ist klar und eindeutig geregelt, dass das HDSG in vollem Umfang gilt. Auch eine systematische Betrachtung bestätigt dies, denn Satz 2 wäre schlicht sinnlos, wenn der Gesetzgeber den HR als Wettbewerbsunternehmen i.S.v. § 3 Abs. 6 HDSG angesehen hätte.

Andere öffentlich-rechtliche Rundfunk- und Fernsehanstalten unterliegen ähnlichen Regelungen. Soweit die Deutsche Welle in Verwaltungsangelegenheiten personenbezogene Daten verarbeitet, unterliegt sie unbestritten den BDSG-Vorschriften über die Datenverarbeitung öffentlicher Stellen (§ 41 Abs. 4 BDSG). Gemäß § 16 ZDF-Staatsvertrag sind für den Datenschutz beim Zweiten Deutschen Fernsehen (ZDF) die jeweils geltenden Vorschriften des rheinland-pfälzischen Datenschutzgesetzes anzuwenden. Die Begründung zu § 36 Abs. 1 des Staatsvertrages über die Errichtung einer gemeinsamen Rundfunkanstalt der Länder Berlin und Brandenburg enthält den Hinweis, dass für den wirtschaftlich-administrativen Bereich das Landesdatenschutzgesetz des Landes Berlin gelte, was dem bisherigen Rechtszustand sowohl in Berlin als auch in Brandenburg entspreche.

In der Literatur ist unbestritten, dass für die Verwaltungsdatenverarbeitung der öffentlich-rechtlichen Rundfunkanstalten die jeweiligen Datenschutzgesetze gelten. Die Kommentarliteratur zum HDSG erwähnt ausdrücklich die Auftragsdatenverarbeitung der GEZ als Beispiel für die uneingeschränkte Anwendung des HDSG.

In diesem Zusammenhang sei angemerkt, dass die Gebührenfinanzierung des der Grundversorgung verpflichteten öffentlich-rechtlichen Rundfunks nicht mehr legitimiert werden könnte, wollte man diesen schwerpunktmäßig als Wettbewerbsunternehmen qualifizieren.

Angesichts der eindeutigen Rechtslage erwähnt der HR daher folgerichtig in den Anschreiben der Briefaktionen seine Informationspflicht nach dem HDSG.

Selbst wenn man unterstellte, der HR sei ein öffentlich-rechtliches Wettbewerbsunternehmen, weil er mit privaten Rundfunkveranstaltern im Wettbewerb um Werbeeinnahmen stehe, würde dies im vorliegenden Fall nicht zur eingeschränkten

Anwendung des HDSG führen. Wettbewerbsunternehmen sind nämlich nicht generell von der Anwendung der materiellrechtlichen Vorschriften des HDSG ausgenommen, sondern nur insoweit, wie sie als Wettbewerbsunternehmen tätig werden, denn nur dann könnten sich die landesgesetzlichen Datenschutzvorschriften wettbewerbsverzerrend auswirken. Deswegen gelte etwa die Vorschrift des HDSG zum Arbeitnehmerdatenschutz auch für Wettbewerbsunternehmen. Man wird jedoch nicht behaupten können, der HR stehe bei der Erhebung von Rundfunkgebühren im Wettbewerb mit privatwirtschaftlichen Rundfunkveranstaltern und der Umstand, dass die im Zusammenhang mit dieser Aktivität stehende Verarbeitung personenbezogener Daten den materiellrechtlichen Vorschriften des HDSG unterliege, wirke sich wettbewerbsverzerrend aus.

17.2.5
Adressverlage als allgemein zugängliche Datenquellen?

Darüber hinaus ist der HR der Ansicht, dass es sich bei privatrechtlichen Adressverlagen um allgemein zugängliche Quellen handele. Für Daten, die in allgemein zugänglichen Quellen gespeichert sind, gilt das HDSG nicht (§ 3 Abs. 4 HDSG). Die Auffassung des HR ist nicht nur mit der Rechtsprechung des Bundesverfassungsgerichts unvereinbar, sie widerspricht auch der in der datenschutzrechtlichen Literatur einhellig vertretenen Meinung.

Allgemein zugänglich ist eine Datenquelle, wenn sie technisch geeignet und bestimmt ist, der Allgemeinheit, d. h. einem individuell nicht bestimmbaren Personenkreis, Informationen zu verschaffen (BVerfGE 27, 71 [83]). Als Beispiele für allgemein zugängliche Quellen werden in der Literatur genannt: Bücher, Zeitungen, Zeitschriften, Adress- und Telefonverzeichnisse, Flugblätter, Kataloge, öffentliche Aushänge, Kino, Hörfunk und Fernsehen, öffentliche Veranstaltungen und öffentliche Register ohne Zugangsbeschränkung, wie z. B. das Handels- oder Vereinsregister.

Es ist offensichtlich, dass die Dateien privatwirtschaftlicher Adressverlage die vom Bundesverfassungsgericht formulierten und in der datenschutzrechtlichen Literatur allgemein anerkannten Kriterien für allgemein zugängliche Quellen nicht erfüllen. Das Adressmaterial der Adresshändler steht der Allgemeinheit nicht uneingeschränkt zur Verfügung, sondern der Händler entscheidet, wem er die Daten unter welchen Bedingungen überlässt. Er ist nicht verpflichtet, die Adressen der Allgemeinheit, d. h. einem individuell nicht bestimmbaren Personenkreis, zur Verfügung zu stellen.

Dass die Datenbestände der Adressverlage keine allgemein zugänglichen Datenquellen sind, zeigt außerdem § 29 Abs. 1 BDSG, der die Datenübermittlung des Adresshandels besonders regelt.

17.2.6
Ausnahme vom Grundsatz der Datenerhebung beim Betroffenen

Nicht nachvollziehbar ist das vom HR in der langwierigen Auseinandersetzung zuletzt vorgebrachte Argument, die Beschaffung der Adressen bei Adressverlagen sei eine zulässige Ausnahme vom Grundsatz der Datenerhebung beim Betroffenen. Das HDSG lässt zwar Ausnahmen zu, regelt diese aber abschließend in § 12 Abs. 2 und 3. Für die Datenerhebung bei privaten Personen oder Stellen hat der hessische Gesetzgeber in § 12 Abs. 3 HDSG besondere Restriktionen vorgesehen (s. 17.2.2). Die Erhebung der Adressdaten bei Adresshändlern erfüllt diese Voraussetzungen nicht. Eine darüber hinausgehende Ermächtigung zur Datenerhebung könnte sich nur aus einer landes- oder bundesgesetzlichen bereichsspezifischen Regelung ergeben. Weder der Rundfunkgebührenstaatsvertrag noch eine andere landesgesetzliche Vorschrift oder ein Bundesgesetz erlauben jedoch dem HR eine über die im HDSG festgelegten Ausnahmen hinausgehende Datenerhebung bei privaten Stellen.

17.2.7
Fazit

Selten ist ein Sachverhalt so eindeutig gesetzlich geregelt, wie im vorliegenden Fall: Der Erwerb der Adressen ist rechtswidrig. Diese Wertung ist keineswegs einem übertriebenen Gesetzespositivismus geschuldet, wie der HR zu meinen scheint. Es geht nicht an, die klaren Vorgaben des hessischen Gesetzgebers zu umgehen. Im Gegensatz zur Meinung des HR ist die Datenerhebung für die Betroffenen im Übrigen keineswegs belanglos. Sie führt, wenn die Empfänger auf die Anschreiben nicht reagieren – wozu sie, falls keine Gebührenpflicht besteht, nicht verpflichtet sind –, zu drei im Ton immer bestimmter werdenden Schreiben mit Fristsetzung. Die Zulässigkeit der Fristsetzung sei hier dahingestellt. In den Beschwerden, die ich erhalte, betonen die Betroffenen besonders, dass sie sich durch die Briefaktionen belästigt fühlen und das nicht nur, weil die Beantwortung in jedem Fall mit Zeit, Mühen und Kosten verbunden ist.

Deshalb sollte der HR bis zur Schaffung einer ausreichenden Rechtsgrundlage die Briefaktionen aussetzen. Der Intendant des HR lehnt dies ab, hat mir allerdings mitgeteilt, dass er bei einem Fortbestehen des Dissenses eine gesetzliche Regelung befürworte.

17.3
Online-Bestellung von Newslettern

Das Doppelte Opt-in-Verfahren zur Bestellung von Newslettern kann so ausgestaltet werden, dass es sich mit dem Datenschutzrecht vereinbaren lässt.

Veranlasst durch eine Entscheidung des Landgerichts Berlin, in der das Gericht das bei der Bestellung von Newslettern im Internet häufig praktizierte so genannte Doppelte Opt-in-Verfahren beanstandet hat, bat mich ein Anbieter eines Newsletters um datenschutzrechtliche Beurteilung eines von ihm vorgeschlagenen modifizierten Anmeldeverfahrens.

17.3.1
Unerwünschte Werbe-Mails

Unverlangte Zusendungen von E-Mails mit Werbeinhalten (spamming) sind sowohl nach Art. 13 der EU-Datenschutzrichtlinie für elektronische Kommunikation vom 12. Juli 2002 (ABl. 201 vom 31. Juli 2002, S. 37) als auch nach der deutschen Rechtsprechung unzulässig. Das unaufgeforderte Zusenden von Werbemails an Geschäftsleute werten die Gerichte als rechtswidrigen Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb. Geht die Werbemail an Privatpersonen, sieht die Rechtsprechung darin eine Verletzung des allgemeinen Persönlichkeitsrechts. In beiden Fällen räumt sie den Empfängern einen Unterlassungsanspruch gegenüber dem Versender der E-Mail ein. Eine entsprechende bundesgesetzliche Verbotsregelung steht kurz bevor: § 7 Abs. 2 Nr. 3 des von der Bundesregierung am 22. August 2003 im Bundestag eingebrachten Entwurfs eines Gesetzes gegen den unlauteren Wettbewerb (BTDrucks. 15/1487) sieht ein grundsätzliches Verbot der unerbetenen E-Mail-Werbung vor.

17.3.2
Doppeltes Opt-in-Verfahren

Als Konsequenz aus dieser Rechtslage verwenden die Anbieter von Newslettern für die Online-Anmeldung häufig das so genannte Doppelte Opt-in-Verfahren (Doppelte Einwilligung). Nach der Anmeldung per Webformular (erste Einwilligung) schickt der Anbieter an die im Formular angegebene E-Mail-Adresse eine Bestätigungs-Mail mit einem Aktivierungslink. Erst nachdem der Besteller den Aktivierungslink angeklickt hat (zweite Einwilligung), wird er in den Newsletter-Verteiler aufgenommen. Mit Bestätigungs-Mail und Aktivierungslink wollen die Newsletter-Diensteanbieter die Eingaben im Webformular verifizieren und verhindern, dass ein Empfänger ohne Einwilligung einen Newsletter erhält. Das Landgericht Berlin (Az.: 16 O 515/02) sieht jedoch auch in der Bestätigungs-Mail mit Aktivierungslink eine unerwünschte Werbung, wenn der Diensteanbieter nicht beweisen kann, dass der Empfänger die Aufnahme in den Verteiler selbst beantragt oder den Antrag veranlasst hat. Die Folge: Online-Bestellungen sind unter diesen Voraussetzungen nur dann rechtlich unproblematisch, wenn derjenige, der den Newsletter anfordert, seine Identität nachweist. Das könnte z. B. mittels digitaler Signatur geschehen, die bislang allerdings nur sehr wenig verbreitet ist. Sollten sich andere Gerichte der Auffassung des Landgerichts Berlin anschließen, wären Online-Bestellungen faktisch kaum mehr möglich, Newsletter müssten stattdessen in erster Linie per Post bestellt werden.

17.3.3
Verfahrensvorschlag

Um das Online-Bestellverfahren auch unter den vom Landgericht Berlin formulierten Bedingungen weiterführen zu können, regte der Anbieter eines Newsletters eine Modifizierung des Doppelten Opt-in-Verfahrens an und bat mich um eine datenschutzrechtliche Bewertung. Der Vorschlag sieht vor, die Bestätigungsmail als datenschutzrechtliche Benachrichtigung auszugestalten. Nachdem eine Bestellung per Webformular eingegangen ist, sendet der Anbieter des Newsletter-Dienstes an die im Formular eingetragene E-Mail-Adresse eine E-Mail, die über die Datenspeicherung informiert. Der Anbieter soll dem Empfänger darüber hinaus mitteilen, dass er die Daten nach einer kurzen definierten Frist löschen werde, falls nicht bis dahin eine Bestätigungsnachricht eingehe.

17.3.4
Datenschutzrechtliche Benachrichtigungspflicht

Diensteanbieter, die ohne Kenntnis des Betroffenen dessen E-Mail-Adresse in einen Verteiler aufnehmen, haben eine Benachrichtigungspflicht. Das Bundesdatenschutzgesetz (BDSG) verpflichtet Stellen, die erstmals personenbezogene Daten für eigene Zwecke ohne Kenntnis des Betroffenen speichern, den Betroffenen von der Speicherung, der Art der Daten, der Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und der Identität der verantwortlichen Stelle zu benachrichtigen (§§ 19a und 33 BDSG). Das Hessische Datenschutzgesetz (HDSG) enthält in § 18 Abs. 1 eine ähnlich lautende Regelung. Die Vorschriften gelten auch für Anbieter von Tele- oder Mediendiensten, denn gem. § 1 Abs. 2 Teledienstedatenschutzgesetz (TDDSG) und § 16 Abs. 3 Mediendienste-Staatsvertrag (MDStV) sind neben den besonderen Regelungen des TDDSG und des MDStV die allgemeinen Datenschutzvorschriften ergänzend anwendbar. Auf die Benachrichtigung kann zwar unter bestimmten gesetzlich festgelegten Umständen verzichtet werden. Im Fall von Newsletter-Diensten ist jedoch keiner der in den §§ 19a Abs. 2 und 3 und 33 Abs. 2 BDSG geregelten Ausnahmetatbestände erfüllt. Das gilt auch für die Ausnahmeregelung in § 33 Abs. 2 Nr. 7a BDSG, wonach die Benachrichtigungspflicht entfällt, wenn die für eigene Zwecke gespeicherten Daten aus allgemein zugänglichen Quellen entnommen sind und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist. Die elektronische Benachrichtigung selbst einer großen Zahl von Personen erfordert keinen besonderen Aufwand.

Beim Doppelten Opt-in-Verfahren besteht keine Benachrichtigungspflicht, soweit der Besteller selbst gehandelt hat und der Anbieter des Newsletter-Dienstes ihn gemäß § 4 Abs. 1 TDDSG und § 6 Satz 1 Nr. 1 TDG bzw. §§ 10 Abs. 1 und 18 Abs. 1 MDStV zu Beginn des Bestellvorgangs unterrichtet hat. Die Daten werden in diesem Fall nicht ohne Kenntnis des Betroffenen erhoben. Eine Pflicht zur Benachrichtigung existiert nur, soweit Dritte ohne Wissen des Betroffenen die Bestellung vornehmen. Bis auf den praktisch seltenen Fall, in dem die Bestellung mit qualifizierter elektronischer Signatur erfolgt, kann der Diensteanbieter nie sicher sein, dass das Webformular nicht von Dritten ausgefüllt und abgeschickt worden ist. Das vorgeschlagene Verfahren gibt ihm die Gewähr, dass er seine Benachrichtigungspflicht in jedem Fall erfüllt und ist daher eine datenschutzrechtlich akzeptable Lösung. Ob freilich auch diese - datenschutzrechtlich gebotene - Benachrichtigung eine unerbetene und damit unzulässige Werbung darstellt, müssen der Gesetzgeber oder die Gerichte entscheiden.

18. Entwicklungen und Empfehlungen im Bereich der Technik

18.1
TCPA

Im letzten Jahr hat es eine hitzige Diskussion gegeben, welche Risiken sich aus Initiativen der Industrie ergeben, die unter dem Stichwort TCPA und Palladium Verbesserungen der Sicherheit beim IT-Einsatz erreichen wollen. Dabei gibt es noch kein klares Bild der Entwicklung.

18.1.1
Die Ausgangslage

Der IT-Einsatz ist derzeit mit vielen Risiken verbunden. Durch Schadprogramme wie Würmer, Viren oder trojanische Pferde können Daten verfälscht, ausspioniert oder gelöscht werden. Unbefugte können auf Rechner eindringen und die Datenverarbeitung sabotieren. Es geschieht aber auch, dass Benutzer entgegen dem Lizenz- und Urheberrecht Daten verarbeiten. Mit der heutigen Technik ist es faktisch nicht möglich ein System aufzubauen, in dem man sicher sein kann, dass Daten korrekt und verfügbar sind und nur im zulässigen Umfang genutzt werden können. Für diese Probleme will die Industrie Lösungen finden.

Als Ursache der Probleme wird dabei angesehen, dass es die jetzt vorhandene Technik des Personal-Computers erlaubt beliebige Programme einzusetzen, auch solche, die unzulässige „Nebenwirkungen“ haben und unbefugten Dritten ermöglichen, Programme oder Schadroutinen zu installieren und zur Ausführung zu bringen.

Es gibt mehrere Ansätze und Ziele, um die bestehende Situation zu ändern. Als Stichwörter fallen dabei die Begriffe TCPA, Palladium und DRM.

18.1.2
Technische Ansätze

18.1.2.1
TCPA / TCG

TCPA steht für "Trusted Computing Platform Alliance". Es handelte sich um eine Allianz von Industrieunternehmen, die eine Spezifikation für eine Hardware-Sicherheitsplattform für Personal-Computer entwickelte. Mitte des Jahres 2003 wurde eine Nachfolgeorganisation, die TCG (Trusted Computing Group) gegründet. Herzstück der Sicherheitsplattform ist das TPM (Trusted Platform Module), ein Stück Hardware, das kryptografische Funktionen, sichere Boot-Funktionen sowie Initialisierungs- und Management-Funktionen zur Verfügung stellt. In den bisher vorgestellten Lösungen war es ein fest mit dem Rechner verbundener Chip.

Mit dieser Spezifikation soll insbesondere erreicht werden, dass sich eine externe Instanz überzeugen kann, dass ein Rechner sich zu einem bestimmten Zeitpunkt in einem vorgegebenen Zustand befindet, d. h. keine Manipulationen gegenüber dem vorgegebenen Zustand vorhanden sind. Damit ist es beispielsweise möglich, dem Rechner dahingehend zu vertrauen, dass keine Schadprogramme im Augenblick aktiv sind. Kryptografische Funktionen ermöglichen es, den Rechner bzw. das TPM zu identifizieren. Damit wird die Technik für Firmennetzwerke interessant, denn die Datensicherheit von VPN (Virtual Private Network), RAS (Remote Access Service) und WLAN (Wireless Local Area Network) lässt sich erhöhen. Außerdem können sensitive Daten wirksamer geschützt werden, da kryptografische Schlüssel im TPM sicher gespeichert sind und Daten einfacher und besser verschlüsselt gespeichert werden können.

Die Technik kann aber auch für andere, eher datenschutzfeindliche Zwecke genutzt werden. Hier sind einige Problembereiche zu nennen:

- Digital Rights Management-Systeme (DRM),
- Einschränkung der Nutzung von Software,
- Abhängigkeit von externen Zertifizierungsstellen,
- die Bindung an einen Hersteller,
- eine - je nach Implementierung - einheitliche Serien-Nummer des TPM, die dann im Internet die Aktivitäten mit einem Rechner eventuell nachvollziehbar macht.

18.1.2.2
Palladium / NGSCB

Die Firma Microsoft ist Mitglied der TCPA/TCG und hat parallel dazu ein Projekt gestartet, um ein "vertrauenswürdiges Betriebssystem" zu entwickeln. Der Name des Projekts war Palladium. Nach den teilweise heftigen Diskussionen über die Nachteile des Konzepts, hat Microsoft Palladium in NGSCB (Next Generation Secure Computing Base) umbenannt. Es soll ein integraler Bestandteil zukünftiger Betriebssysteme der Firma Microsoft sein.

Die NGSCB soll auch Funktionen nutzen, die vom TPM bereitgestellt werden. Nicht zuletzt deshalb tauchen in den Diskussionen auch immer wieder beide Begriffe zusammen auf. Die NGSCB soll den Computer sicherer machen. Dies soll auch dadurch geschehen, dass der Benutzer in seinen Möglichkeiten beschränkt wird. Mit diesem sicheren Computer, der den Benutzer kontrolliert, kann dann erzwungen werden, dass Daten nur mit bestimmten Anwendungen und nach vorgegebenen Regeln verarbeitet werden.

18.1.2.3
Digital Rights Management-Systeme

Für DRM-Systeme, also Systeme, die beispielsweise das Abspielen und Kopieren von Musikstücken kontrollieren sollen, sind Funktionen, wie sie die NGSCB bietet, nicht nur wünschenswert, sondern geradezu unverzichtbar. Die NGSCB wiederum baut teilweise auf dem TPM auf.

Um TCPA-konforme Hardware für ein DRM-System nutzen zu können, sind ein passendes DRM-BIOS und ein DRM-unterstützendes Betriebssystem nötig. Außerdem sind noch einige Änderungen am aktuellen Stand des TPM nötig. Bisher sind diese Voraussetzungen nicht gegeben. Die Kritiker des TCPA-Ansatzes weisen aber darauf hin, dass nach einer weitgehenden Marktdurchdringung mit TCPA-konformer Hardware, die fehlenden Ergänzungen der Komponenten vergleichsweise schnell vorgenommen werden könnten.

18.1.2.4
Folgerungen

Problematisch werden die Sicherheits- und Kontrollmechanismen eines DRM-Systems, eines Betriebssystems oder eines Rechners, wenn sie für den Benutzer nicht transparent sind und die Funktionen oder Funktionsfähigkeit des Computers von externen Stellen ganz oder teilweise gesteuert wird. Damit würde es dann möglich, Personen in ihrem Recht auf Informationsfreiheit und informationelle Selbstbestimmung zu beschränken.

Im Bereich der Datensicherheit bieten die vorgeschlagenen Lösungen aber auch interessante Perspektiven.

18.1.3
Stand der Diskussion

In der öffentlichen Diskussion wurden von Kritikern der Ansätze Szenarien beschrieben, die zu schwerwiegenden Folgen für das Recht auf informationelle Selbstbestimmung geführt hätten. Die Datenschutzbeauftragten sahen es daher als nötig an, in einer Entschließung (vgl. Ziff. 20.2) explizit die Grenzen aufzuzeigen, innerhalb derer sich die Technik bewegen muss. Ferner hat der Landesbeauftragte für den Datenschutz und das Recht auf Akteneinsicht Brandenburg in seinem Internetangebot ein Papier veröffentlicht, in dem die Techniken erläutert werden und auf die verschiedenen Aspekte detaillierter eingegangen wird. Man kann feststellen, dass es neben den Risiken auch positive Aspekte gibt, es müssen aber die Grenzen eingehalten werden.

Die Einführung der neuen Technik ist jedoch nicht nur aus Datenschutzsicht problematisch. Sie hat die Bundesregierung und den Bundestag beschäftigt. In einer Anfrage (BTDrucks. 15/660) wurde die Bundesregierung aufgefordert, zu den Auswirkungen des "Trusted Platform Module" und der Software "Palladium" zu berichten. Mit der BTDrucks. 15/795 vom 7. April 2003 antwortete die Bundesregierung auf die 29 Fragen. Interessant ist in diesem Zusammenhang, dass beim Bundesamt für Sicherheit in der Informationstechnik eine 17 Mitarbeiter umfassende Projektgruppe seit August 2002 die Entwicklungen und Folgerungen aus "TPM/Palladium" beobachtet und kritisch prüft. Sobald belastbare Erkenntnisse vorliegen, wird sie die Bundesregierung in geeigneter Form veröffentlichen.

Die Datenschutzbeauftragten werden die Entwicklung ebenfalls weiter kritisch verfolgen.

18.2
SPAM - die neue Gefahr für die Integrität des Internets

Immer mehr unverlangt zugesendete Mails, so genannte "Spam" verstopfen die Postfächer von Privatleuten und Unternehmen. Aber auch die öffentliche Verwaltung klagt über eine stetig zunehmende Flut unerwünschter Mails und sucht nach Abwehrmöglichkeiten.

18.2.1
Was ist Spam?

Der Begriff Spam, Spiced Pork and Meat (engl.: Dosenfleisch), leitet sich vom Hauptrequisit eines Monty-Python-Sketches ab.

Aus Sicht des Nutzers sind Spam mehr als nur unerwünschte E-Mails, sondern all das, was er in seinem Postfach findet und nicht haben möchte.

Aus Sicht des Juristen sind es unerwünschte Mails mit "Werbendem Inhalt". Es besteht kein geschäftlicher Kontakt zwischen Versender und Empfänger (z. B. Werbe-Newsletter). Das Einverständnis des Empfängers kann nicht ausnahmsweise vermutet werden (strittig, eng auszulegen). Sie sind unerwünscht, wenn der Empfänger nicht vorher ausdrücklich Informationen angefordert hat.

Aus Sicht des Technikers wird Spam als Unsolicited Commercial Email (UCE) oder Unsolicited Bulk Email (UBE) bezeichnet.

Spam beginnt die Integrität der E-Mail-Systeme zu untergraben und führt zu Einschränkungen der Internetnutzung. Allein beim Microsoft Online Dienst MSN werden täglich 2,4 Milliarden Spam-Mails abgefangen, was 80 v.H. des gesamten

Mailaufkommens bei MSN entspricht (Schreiben des Vorsitzenden der Geschäftsführung Microsoft Deutschland GmbH vom 30. Juli 2003 zum Microsoft Politik-Report Juli 2003). Bereits im Laufe dieses Jahres habe ich auf meiner Homepage aktuelle Hinweise zu diesem Thema gegeben. Spammer und ihre Gegner liefern sich ein Wettrüsten ohne erkennbares Ende. Letztlich geht es hier um die Zukunft der Kommunikation via Internet.

Der nachfolgende Beitrag beleuchtet neben der Entstehungsgeschichte auch die technischen und rechtlichen Fragestellungen zu dieser Thematik und zeigt Lösungen zur Vermeidung und Reduzierung von Spam auf.

18.2.2
E-Mail-Systeme, die Infrastruktur für Spam

E-Mail ist das Kommunikationsmittel für die moderne Gesellschaft. Die vielfältigen Vorteile liegen auf der Hand:

Schnelle Übermittlung, primär niedrige Kosten für die Übertragung, leichte Antwortmöglichkeit, internationale Verfügbarkeit, einfacher Versand mit Anhängen, bequemer Mehrfachversand, schnelle Erstellung und Zustellung, einfache Archivierung, keine strengen Formvorschriften etc.

Dem stehen Nachteile gegenüber:

Schwer zu regulierende Informationsflut (viele uninteressante und überflüssige Informationen werden versendet), hoher Zeitaufwand zum Lesen, sensible Daten in unverschlüsselten E-Mails, unerwünschte Anhänge (zum Teil schadstoffbehaftete E-Mail-Anhänge mit Viren, Trojanischen Pferden und Active Contents).

Hieraus ergeben sich altbekannte Probleme:

Stetig wachsende Anforderungen an Organisation und Technik der Infrastruktur, Sicherheitsrisiken bei unverschlüsselter E-Mail-Übertragung, mangelnde Rechtsverbindlichkeit der Kommunikation, mangelnde Beweiskraft, Produktivitätsverluste bei Kettenbriefen und privater Nutzung am Arbeitsplatz, Haftungsrisiken und Imageverlust bei pornografischen und diskriminierenden E-Mails, Informationsverlust sowie Verstöße gegen gesetzliche Archivierungsvorschriften.

Mit der exponentiellen Zunahme von Spam ist ein neues schwerwiegendes Sicherheitsrisiko hinzugekommen, das sich auf Grund der verwendeten offenen Infrastruktur hervorragend entwickeln konnte, indem es vorhandene Schwachstellen, fehlende Authentifikations-Möglichkeiten und die nutzungsunabhängige Abrechnung der Dienste ausnutzt.

18.2.3
Lösungsansätze zum Umgang mit Spam

Zur Vermeidung von Spam sind organisatorische und technische Maßnahmen unter Berücksichtigung der rechtlichen Rahmenbedingungen erforderlich.

Die Lösungsansätze reichen vom Einsatz von Filtertechnologien, über das Definieren von rechtlichen Ausschlussklauseln (Legal Disclaimer) hin bis zu gültigen Richtlinien im Umgang von E-Mails (E-Mail-Policys).

18.2.3.1
Organisatorische Maßnahmen

Wie mit Spam umgegangen wird, ist auch eine organisatorische Frage. Der Einsatz spezieller Filtertechnologien erfordert ebenso wie alle anderen Sicherheitsfunktionen Aufwand in den Bereichen Infrastruktur, Verkabelung und Personal. Hier entstehen Kosten für Benutzerunterstützung, Administration, System-Ressourcen und benötigte größere Bandbreite der Kabel. Insbesondere sind hier die Pflege und Kontrolle der IP-Listen (Black- und White-Listen), Bearbeitung von Nutzeranfragen bei Spam-Alarm und Weiterentwicklung von Anti-Spam-Maßnahmen zu erwähnen. Die erforderlichen Maßnahmen müssen von den Verantwortlichen beschrieben, von der Geschäftsleitung in einer Policy festgeschrieben und in Dienstanweisungen in Absprache mit dem Personalrat festgelegt werden.

- **Black-Lists**
  bestehen aus Internet-Protokoll-Adressen, Domain-Namen und Server-Farmen, die bei Spam-Aktionen mitgewirkt haben und ausgeschlossen werden sollen.

- **White-List**
  bezeichnet ein Adress-Buch mit dem vom Nutzer ohne Prüfung freigegebenen (akzeptierten) Absendern.

18.2.3.2
Technische Maßnahmen

Die erforderlichen Maßnahmen sind in das Sicherheitskonzept zu integrieren.

Bei den Lösungsansätzen gibt es eine Parallele zu dem Problem der Viren. Sowohl virenverseuchte E-Mails als auch Spam-Mails müssen erkannt werden, bevor sie den Adressaten erreichen. Je nach Gestaltung der Mail-Systeme befinden sich die Scanner und Filtertechnologien auf Server- und/oder Client-Seite. Der Einsatz von Virenscannern ist Stand der Technik. Programme zur Filterung von Spams haben sich im Laufe dieses Jahres fast überall etabliert. Welches Produkt und welches

Vorgehen am besten sind, hängt vom Einzelfall ab. Interessant ist hier zum einen der Prozentsatz, zu dem unerwünschte Mails im Filter hängen bleiben und zum anderen die „False Positive“-Quote, der Anteil von erwünschten Mails, die vom System fälschlich als Spam identifiziert werden.

Auf Serverebene haben sich folgende Funktionalitäten der Filter mit dem Ergebnis einer globalen Spam-Erkennung als sinnvoll erwiesen:

- Sperrung einschlägig bekannter Netze
- Absender- bzw. Empfänger filtern
- Analyse der Mail-Header
- Analyse des Mail-Inhalts
- Verhinderung des Scannens von Adressen

Auf Client-Ebene haben sich folgende Techniken zur nutzerbezogenen individuellen Spam-Erkennung als praktikabel erwiesen:

- nutzerdefinierte E-Mail-Filter
- nutzerdefinierte Spam-Filter
- White Lists

18.2.3.3
Rechtliche Aspekte

Die Aussichten auf ein erfolgreiches Vorgehen gegen Versender von Werbemails sind je nach Herkunftsland der E-Mails unterschiedlich. Werden die E-Mails von außerhalb der EU abgeschickt, bestehen kaum Erfolgsaussichten. Gegen Versender aus den USA könnte demnächst die dortige Federal Trade Commission mobilisiert werden. Der US-Kongress hat am 8. Dezember 2003 ein Anti-Spam-Gesetz verabschiedet, das am 1. Januar 2004 in Kraft getreten ist (Controlling the Assault of Non-Solicited Pornography and Marketing Act - CAN-SPAM Act of 2003). Das Gesetz sieht für Spamming Freiheits- und Geldstrafen vor. Gegen Absender von Werbemails können jedoch nicht die Empfänger unmittelbar vorgehen, sondern in erster Linie die Federal Trade Commission (FTC), aber auch andere Behörden, wie z. B. die Federal Communications Commission (FCC) oder die Securities Exchange Commission (SEC - Börsenaufsicht), Strafverfolgungsbehörden und Diensteanbieter.

Bessere Chancen, E-Mail-Werbung zu unterbinden, bieten sich in der Europäischen Union. Art. 13 der EU-Datenschutzrichtlinie für elektronische Kommunikation vom 12. Juli 2002 (ABl. L 201 vom 31. Juli 2002, S. 37) lässt E-Mail-Werbung grundsätzlich nur zu, wenn der Empfänger zuvor eingewilligt hat (Opt-in-Verfahren).

Die Richtlinie hätte von den Mitgliedstaaten bis zum 31. Oktober 2003 in nationales Recht umgesetzt werden müssen (Art. 17). Gegenüber Werbetreibenden aus Mitgliedstaaten, welche die Umsetzungsfrist bislang nicht eingehalten haben, kann sich der Empfänger nach der Rechtsprechung des Europäischen Gerichtshofs unmittelbar auf die EU-Richtlinie berufen.

In Deutschland soll Art. 13 der EU-Datenschutzrichtlinie für elektronische Kommunikation im Wettbewerbsrecht, nämlich im Gesetz gegen den unlauteren Wettbewerb (UWG) umgesetzt werden. § 7 Abs. Abs. 2 Nr. 3 des von der Bundesregierung am 22. August 2003 im Bundestag eingebrachten Entwurfs (BTDrucks. 15/1487) sieht in unerbetener E-Mail-Werbung eine unzulässige Wettbewerbsverfälschung. Dagegen sollen allerdings nur Wettbewerber, Verbraucherverbände und Industrie- und Handelskammern gerichtlich vorgehen können, nicht jedoch die Empfänger der E-Mail oder - wie in den USA vorgesehen - der Diensteanbieter. Der Gesetzentwurf verzichtet bewusst auf ein Klagerecht des einzelnen Verbrauchers. Begründet wird dies damit, dass bei Gewährung individueller Rechte des Verbrauchers bei Verstößen gegen das UWG das hohe Schutzniveau des Gesetzes in Frage gestellt werden müsse. Denn bei dem im Entwurf vorgesehenen hohen Schutzniveau müsse der Unternehmer jederzeit mit einer Vielzahl von Klagen einzelner Verbraucher rechnen, was zu einer erheblichen Belastung für die Wirtschaft führe und einen Standortnachteil zur Folge habe. Um die Belastung der Wirtschaft erträglich zu gestalten, müsse bei einem individuellen Klagerecht der Verbraucher zur Verringerung des Prozessrisikos der Unternehmer entsprechend das Schutzniveau abgesenkt werden (a.a.O. S. 45). Die Einschätzung mag auf das Unlauterkeitsrecht insgesamt zutreffen, trägt aber nicht als Argument gegen eine Verbesserung der Individualrechtsposition der Verbraucher im speziellen Falle unverlangter E-Mail-Werbung. Das Schutzniveau ist hier zumindest in der EU einheitlich und darf durch nationales Recht nicht unter das Niveau der Datenschutzrichtlinie für elektronische Kommunikation abgesenkt werden. Bei einheitlicher Umsetzung der Richtlinie in der EU entstehen keine Standortnachteile.

Unabhängig von der zu erwartenden gesetzlichen Regelung hat der Empfänger unerbetener E-Mail-Werbung bereits nach geltendem Recht die Möglichkeit, sich zu wehren. Es gibt zwar in Deutschland bislang kein ausdrückliches gesetzliches Verbot dieser Werbeform, in der Rechtsprechung und Literatur herrscht jedoch Einigkeit, dass unerbetene E-Mail-Werbung rechtswidrig ist. Die Gerichte sehen in dem unaufgeforderten Zusenden von Werbemails an Geschäftsleute einen unzulässigen Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb, soweit Privatpersonen angeschrieben werden, eine Verletzung des allgemeinen Persönlichkeitsrechts und räumen den Empfängern gemäß § 823 Abs. 1 und § 1004 BGB einen Unterlassungsanspruch gegenüber dem Versender der E-Mail ein.

Wirksamer als rechtliche Abwehrmaßnahmen dürften allerdings technische Vorkehrungen sein, die verhindern, dass E-Mail-Werbung den Empfänger erreicht. In Frage kommen dafür z. B. Spam-Filterprogramme. Welche rechtlichen Anforderungen beim Einsatz von Spam-Filtern zu beachten sind, hängt davon ab, ob in der Behörde neben der dienstlichen auch die private E-Mail-Nutzung zugelassen ist.

Ist die private Nutzung untersagt, richtet sich die Zulässigkeit des automatisierten Filterns nach § 11 Abs. 1.

§ 11 Abs. 1 HDSG

Die Verarbeitung personenbezogener Daten ist nach Maßgabe der nachfolgenden Vorschriften zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der datenverarbeitenden Stelle liegenden Aufgaben und für den jeweils damit verbundenen Zweck erforderlich ist. Die Erforderlichkeit einer Datenübermittlung muss bei einer der beteiligten Stellen vorliegen.

Unerwünschte Werbemails können nicht unerheblich Speicherkapazität auf dem Mailserver der Dienststelle belegen und Mailboxen verstopfen. Die Beschäftigten müssen Zeit und Arbeitskraft aufwenden, um die Werbemails aufzurufen, evtl. durchzuschauen und zu löschen. In dem Wust von Werbung können leicht relevante Schreiben untergehen. Gegen den Einsatz von Filterprogrammen bestehen daher keine datenschutzrechtlichen Bedenken.

Hat die Dienststelle die private E-Mail-Nutzung erlaubt, wird sie zum Anbieter eines Telekommunikations- bzw. Teledienstes und ist verpflichtet, das Fernmeldegeheimnis zu wahren. Die E-Mails unterliegen in diesem Fall dem Fernmeldegeheimnis (§ 85 Telekommunikationsgesetz). Der Einsatz eines Spam-Filters ohne Einwilligung der Empfänger wäre nach § 206 Abs. 2 Nr. 2 Strafgesetzbuch (StGB) strafbar.

§ 206 Abs. 1 und Abs. 2 Nr. 2 StGB

(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekannt geworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines in Absatz 1 bezeichneten Unternehmens unbefugt

2. eine einem solchen Unternehmen zur Übermittlung anvertraute Sendung unterdrückt oder …

Die Beschäftigten müssen deshalb über den geplanten Einsatz des Filters informiert werden und ausdrücklich einwilligen. Es dürfte außerdem sinnvoll sein, den Empfängern einen Zugriff auf die aussortierten E-Mails einzurichten. Das würde die Gefahr minimieren, dass auch erwünschte E-Mails automatisiert aussortiert und gelöscht werden, mit u. U. negativen Folgen für die Behörde.

18.2.4
Ausblick

Spam ist ein Problem, dem mit den beschriebenen technischen und organisatorischen Maßnahmen begegnet werden muss.

Solange die Versendung von Mails kostenlos und eine eindeutige Identifikation und Authentifizierung der Teilnehmer nicht möglich ist, wird sich am eigentlichen Problem jedoch nicht viel ändern. Die Einführung der Rückverfolgbarkeit erfordert aber fundamentale Änderungen an dem Protokoll, das den gesamten E-Mail-Verkehr regelt. Wenn alle E-Mail-Provider auf ein authentifiziertes SMTP (Simple Mail Transport Protokoll) umsteigen würden, würden nur noch Mails von überprüften Adressen den gewünschten Empfänger erreichen. Es existieren technische Lösungen mit Hilfe der digitalen Signatur und sicherem IP-Protokoll. Ihr Einsatz hat sich aber noch nicht im erforderlichen Umfang durchgesetzt. Auch in Zukunft wird man daher nur die Symptome behandeln und nicht die Ursache beheben können.

18.3
Automatische Software-Updates

Es gibt eine zunehmende Tendenz von Herstellern, Software-Updates zu automatisieren. Diese Funktion ist eine Datenverarbeitung im Auftrag. Je nach technischer und organisatorischer Ausgestaltung kann sie datenschutzrechtlich unzulässig sein.

18.3.1
Gründe für automatische Software-Updates

In letzter Zeit haben Softwarehersteller zunehmend Probleme, Software-Updates zeitnah dem Anwender zur Verfügung zu stellen. Besonders augenfällig ist das Problem, wenn durch das Software-Update Sicherheitslücken geschlossen werden sollen. Der Rechner wird gegenüber Angriffen umso anfälliger, je länger eine Sicherheitslücke bekannt ist und keine Gegenmaßnahmen ergriffen werden. Es handelt sich um ein Problem, das nicht nur private Anwender betrifft, sondern auch die professionelle Datenverarbeitung. Gerade die rasante Ausbreitung von Würmern und Viren wie "Code Red", die bekannte Sicherheitslücken von Servern ausnutzen konnten, obwohl seit Monaten Patches und Updates zur Verfügung standen, belegen dies. Vor diesem Hintergrund erscheint es sinnvoll, die Updates schnell einzuspielen, ohne dass Eingriffe seitens des Kunden nötig sind.

Ein weiterer Grund für Hersteller, automatische Updates verstärkt anzubieten, liegt in der Kosteneinsparung. Es ist beispielsweise nicht mehr nötig, Datenträger zu erstellen und zu verteilen. Der Kunde holt sich das Update selbst, wenn er es braucht. Damit sich der Aufwand für den Kunden in Grenzen hält, ist die logische Folgerung, diesen Vorgang zu automatisieren.

18.3.2
Problembereiche beim automatischen Software-Update

Der Ansatz, Software-Updates zu automatisieren, ist folgerichtig. Es ergeben sich in der Praxis jedoch schwerwiegende Fragen.

- **Welche Daten werden an den Hersteller übertragen?**
  Bei einem automatisierten Update werden Daten vom Kundenrechner zum Hersteller übertragen. In aller Regel ist nicht bekannt, welche Daten übertragen werden. Zumindest bei einem großen Hersteller wird immer wieder der Verdacht geäußert, dass nicht nur Konfigurationsdaten, sondern auch weitere personenbezogene Daten unzulässigerweise bekannt werden.

- **Wer entscheidet, ob und wann ein Update erfolgt?**
  Auch wenn es nach Ansicht des Herstellers sinnvoll ist, ein Update einzuspielen, hat der Kunde vielleicht gute Gründe, die Anpassung später oder gar nicht vorzunehmen.

- **Wird die Funktionsfähigkeit des Rechners durch das Update beeinträchtigt?**
  Mit jeder Softwareänderung ist das Risiko verbunden, dass der Rechner anschließend ganz oder teilweise nicht mehr funktioniert. Deshalb sollten Softwareänderungen vor der Übernahme in Produktion immer getestet werden. Diese Vorgehensweise ist im professionellen Umfeld zwingend erforderlich.

- **Widersprechen die technischen Voraussetzungen für das Update Sicherheitsrichtlinien oder anderen Vorgaben des Kunden?**
  In der Regel wird das automatische Update über das Internet vorgenommen. Es kann aber nicht akzeptiert werden, dass nur zu diesem Zweck Rechner eine Anbindung an das Internet erhalten und damit potenziell Angriffen ausgesetzt werden. Je nach technischer Ausgestaltung müssen eventuell auch in einer Firewall Ports und Dienste freigeschaltet werden, die der Sicherheitspolitik des Betreibers widersprechen.

Während es bei einem einzelnen PC oft keine Alternative zum Einspielen der Updates im "produktiven" Betrieb gibt, stellt sich die Situation bei größeren Installationen differenzierter dar. Viele Hersteller, wie z. B. auch Microsoft, bieten die Hilfsmittel an, um in einem Netz Updates von einem internen Server aus zu verteilen. In diesem Fall kann ein Update aus dem Internet heruntergeladen und zunächst getestet werden, um es dann über den Server intern zu verteilen.

18.3.3
Datenschutzrechtliche Einordnung

Das Einspielen von Software-Updates ist eine Wartungstätigkeit. Datenschutzrechtlich sind Wartungstätigkeiten nach § 4 HDSG als Datenverarbeitung im Auftrag zu werten. Ein automatisches Software-Update entspricht weitgehend einer Fernwartung. In meinem 24. Tätigkeitsbericht, Ziff. 17.4 habe ich datenschutzrechtliche Anforderungen hierzu formuliert. Eine Orientierungshilfe ist ebenfalls im 24. Tätigkeitsbericht unter Ziff. 19.2 zu finden. Insgesamt ergeben sich für datenverarbeitende Stellen bei einer Fernwartung eine Reihe von Forderungen, die ich noch einmal kurz wiederholen will.

Von den Abläufen her können drei Phasen mit verschiedenen Aktivitäten unterschieden werden.

Die Planung der Fernwartung:

- Die Rechte und Pflichten müssen verbindlich festgelegt werden.
- Der Umfang der Zugriffsrechte ist zu bestimmen.
- Die Systemverwalter sind zu schulen.
- Technische Maßnahmen zur Verringerung des Netzrisikos müssen ergriffen werden; wenn technisch umsetzbar, sind die übertragenen Daten zu verschlüsseln.
- Es müssen technische Maßnahmen beim Rechner umgesetzt werden, damit ausschließlich zugelassene Personen arbeiten können, Zugriffe nur im beabsichtigten Umfang auf Daten und Programme erfolgen und die Revisionsfähigkeit gegeben ist.

Der Ablauf der jeweiligen Fernwartung:

- Die Fernwartung muss vom Betreiber eingeleitet werden.
- Die systemseitigen Sicherungsmaßnahmen müssen vom Wartungspersonal durchlaufen werden.
- Die Fernwartung ist vom Betreiber zu überwachen. Er muss wissen, welche Aktionen während der Wartung auf dem Rechner vorgenommen werden, bei Unregelmäßigkeiten muss er die Fernwartung abbrechen und, wenn erforderlich, Freigaben erteilen.
- Nach Abschluss der Wartung sind offenbarte Passwörter zu ändern.

Die Revision der Fernwartung:

- Es muss bekannt sein, wer wann von wo mit welchen Mitteln was veranlasst und worauf zugegriffen hat.

Bei automatischen Software-Updates sind diese Anforderungen oft nicht erfüllt. Gerade die Planung wird nur vom Hersteller bei der Konzeption vorgenommen und der Kunde kann die Rahmenbedingungen nur akzeptieren oder auf die Möglichkeit verzichten. Ein automatisches Software-Update wird auch nicht vom Betreiber eingeleitet und systemseitige Siche-

rungsmaßnahmen kann es nur dann geben, wenn das Update nicht das Betriebssystem betrifft. In der Regel ist auch eine Überwachung nicht möglich. Insgesamt ergibt sich eine Situation mit vielen Risiken.

Vor diesem Hintergrund hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Entschließung gefasst (Text s. Ziff. 20.11), in der die folgenden Forderungen erhoben werden:

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Software-Hersteller auf,

- überprüfbare, benutzerinitiierte Update-Verfahren bereitzustellen, die nicht zwingend einen Online-Datenaustausch mit dem Zielrechner erfordern.
- Weiterhin sollten datenträgerbasierte Update-Verfahren angeboten werden, bei denen lediglich die für den Datenträgerversand erforderlichen Daten übertragen werden.
- Automatisierte Online-Update-Verfahren sollten nur wahlweise angeboten werden. Sie sind so zu modifizieren, dass sowohl der Update- als auch der Installationsprozess transparent und revisionssicher sind.
- Software-Updates dürfen in keinem Fall davon abhängig gemacht werden, dass den Anbietern ein praktisch nicht kontrollierbarer Zugriff auf den eigenen Rechner gewährt werden muss.
- Personenbezogene Daten dürfen nur dann übermittelt werden, wenn der Verwendungszweck vollständig bekannt ist und in die Verarbeitung ausdrücklich eingewilligt wurde. Dabei ist in jedem Fall das gesetzlich normierte Prinzip der Datensparsamkeit einzuhalten.

Unter diesen Bedingungen haben die Betreiber die Möglichkeit, ein datenschutzkonformes Software-Update für ihre Belange einzurichten.

18.4
Sicherheitsprobleme beim Einsatz von USB-Geräten

Durch die sprunghafte Entwicklung von USB-Geräten, insbesondere im Bereich der Massenspeichergeräte (so genannte Memory-Sticks), ist die Auseinandersetzung mit dieser Thematik besonders in sicherheitssensitiven Bereichen dringend erforderlich. Da diese vom System automatisch als neue Laufwerke erkannt und installiert werden, stellen sie eine schwer zu kontrollierende Möglichkeit dar, Daten aus und in sensitive Bereiche zu transportieren.

18.4.1
Vorbemerkung

Durch die Zunahme von USB-Schnittstellen und -geräten am Markt und die Verdrängung herkömmlicher Schnittstellen sind Sicherheitsprobleme entstanden. Hierzu hat der Arbeitskreis "Technische und organisatorische Datenschutzfragen" der Datenschutzbeauftragten des Bundes und der Länder eine Orientierungshilfe erarbeitet, die auf meiner Internetseite (www.datenschutz.hessen.de) veröffentlicht ist. Dieser Beitrag stellt die Problemlage und Lösungsmöglichkeiten dar. Er beruht auf Ergebnissen aktueller Prüfungen und auf Projekten, die beratend begleite.

18.4.2
Entwicklung und Markteinführung

Der Universal Serial Bus (USB), eine Technologie zur Anbindung von Peripheriegeräten an PC-Systeme hat sich in den letzten Jahren zur bevorzugten Schnittstelle entwickelt. Die Erstentwicklung (USB-Version 1.0 bzw. 1.1) verbreitete sich zunächst schleppend. Die technische Entwicklung stagnierte zwar zeitweilig, das Aufkommen von Konkurrenzprodukten (z. B. Firewire) beschleunigte aber die Weiterentwicklung der USB-Schnittstelle, insbesondere im Bereich der Übertragungsgeschwindigkeit. Waren vor wenigen Jahren nur einzelne Geräte (z. B. Modems) mit USB-Schnittstelle verfügbar, ist die USB-Version 2.0 nunmehr dabei, die bisherigen Standardschnittstellen PS/2 (Tastatur, Maus), den Parallel-Port (Drucker) und die SCSI-Schnittstelle (Scanner) zu verdrängen. Für den Heimanwender-Bereich sind z. B. derzeit kaum mehr Drucker mit Parallel-Port-Anschluss verfügbar. Die Palette der verfügbaren Gerätetypen und deren Kapazität nehmen außerdem kontinuierlich zu, insbesondere im Bereich der Speicherkarten und Memory-Sticks. Hauptvorteil ist neben der standardisierten Schnittstelle die einfache (Selbst-)Installation, die nur in besonderen Konstellationen (ältere Betriebssystemvarianten) einen Benutzereingriff (Installations-CD) erfordert.

Das Problem, plötzlich unkontrollierbare Datentransportmöglichkeiten geschaffen zu haben, wurde lange Zeit nicht gesehen.

18.4.3
Generelle Problemlage

Behörden bzw. Unternehmen, haben erhebliche Investitionen im Sicherheitsbereich getätigt:

- Das Eindringen in Netze, Einschleusen von Schadprogrammen (Viren, Trojanische Pferde usw.) bzw. Diebstahl von Daten lässt sich zentral über abgesicherte Netzbereiche, Firewalls und zentrale Virenprüfung verhindern.
- Sensitive Arbeitsplatzrechner lassen sich durch technische Maßnahmen, z. B. Ausbau des CD-ROM-Laufwerks oder abschließbare Diskettenlaufwerke sichern.
- Methoden, den Zugriff auf Bereiche des Betriebssystems zu verhindern, sind ebenso vorhanden (Sperren der DOS-Eingabeaufforderung, Ausblenden von Laufwerken aus dem Windows-Explorer usw.)

In diesem Gesamtkontext konnte die USB-Problematik bisher durch deaktivieren im Basic Input/Output-System (BIOS) ausgeschlossen werden. Änderungen im BIOS lassen sich durch einen - wenn auch einfachen - Passwortschutz weitestgehend ausschließen.

Dies kann aber auf Dauer nicht aufrechterhalten werden, da USB-Geräte auch ihren Einzug in sicherheitsrelevante Bereiche haben und zukünftig verstärkt haben werden. Damit entsteht eine nicht zu unterschätzende Sicherheitslücke.

Diese Probleme werden noch durch die „Uniformität“ der USB-Technologie verschärft: USB kennt nur das "Gerät" an sich, eine weitergehende Differenzierung, (z. B. Scanner, Drucker, Massenspeichergeräte usw.) ist nicht vorhanden und auch seitens der Betriebssysteme nicht vorgesehen.

Eine grundsätzliche Unterscheidung der Geräte ist z. B. unter Windows über die Einträge in der Systemregistrierung (Schlüssel "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB" bzw. "HKEY_LOCAL_MACHINE\-SYSTEM\CurrentControlSet\Enum\USBSTOR") möglich: Die Einträge "VendorID" (Hersteller), "ProductID" oder "DeviceDesc" (Gerätebeschreibung) lassen eine Klassifizierung der installierten Geräte zu. Inwieweit diese aber schlüssig und letztendlich aussagekräftig und -fähig für eine automatisierte Prüfung und Unterscheidung sind, kann nicht abschließend beurteilt werden, da sie nicht standardisiert sind und vom Hersteller festgelegt werden. Fehlen spezielle Treiber, werden zudem die (Windows-) Standardtreiber (mit Standardwerten in diesen Feldern) verwendet. Damit ist – und wird – es sehr schwierig, erlaubte von nicht erlaubten USB-Geräten zu unterscheiden.

18.4.4
Betriebssystemspezifische Betrachtungen

18.4.4.1
USB unter Windows

18.4.4.1.1
Windows 95 und Nachfolgeversionen

Für den Betrieb von USB-Geräten waren unter Windows 95 und 98 noch spezielle Treiber erforderlich. Mit Windows 98 SE (Second Edition) und Windows ME (Millennium Edition) fand die USB-Technologie ihren endgültigen Platz im Windows-Betriebssystem. Da diese Betriebssysteme keine Sicherheitskomponenten (d. h. unterschiedliche Rechte für Benutzer) kennen, lassen sich hier kaum Mechanismen einbauen, da sie von jedem Benutzer (der ja alle Rechte hat) wieder umgangen bzw. deaktiviert werden können.

18.4.4.1.2
Windows NT und Nachfolgeversionen

Die professionelle Windows-Version NT (New Technology) brachte aufgrund der Betriebssystem-Konzepte keine USB-Unterstützung mit. Dennoch war (und ist) der Betrieb von USB-Geräten unter NT möglich, nur entwickelten die wenigsten Hersteller von Geräten den hierfür nötigen speziellen NT-Treiber. Die hierfür erforderliche Installation des Treibers kann aber nur von berechtigten Personen (in der Regel die Administratoren) vorgenommen werden, sodass hier eine Kontrollmöglichkeit gegeben ist.

Mit der Verschmelzung und gemeinsamen Weiterentwicklung der Windows-Betriebssysteme als einheitliche Reihe nimmt USB nunmehr auch seinen Platz im professionellen Bereich der Windows-Anwender ein. War (und ist) dort Windows NT der Standard, ist diese Problematik nicht relevant, da USB-Treiber selten verfügbar sind (s. o.).

Steht eine Migration nach Windows XP, 2000 oder 2003 an oder ist sie bereits erfolgt, ist eine Auseinandersetzung mit dem Thema erforderlich.

18.4.4.1.3
Lösungsansätze

Unter Windows werden verschiedene Lösungsansätze diskutiert:

- **Einsatz von Überwachungssoftware**
  Kommerzielle Software, die in der Lage ist, den Aufruf von Objekten zu überwachen und ggf. zu verhindern, ist am Markt verfügbar. Damit lassen sich Zugriffe auf sämtliche Systemobjekte (unter anderem die Peripheriegeräte des Rechners) überwachen und steuern.

  Microsoft selbst stellt mit dem DDK (Device Development Kit) dem Programmierer die erforderlichen Dokumentationen und Lösungen bereit. Dieser Weg scheidet jedoch für die meisten Anwender aus, da Programmierkenntnisse und -umgebungen weitestgehend fehlen (s. u. "ACL").

  Denkbar sind auch selbstgeschriebene Skripte, die den Programmaufruf (Schlüssel "HKEY_CLASSES_ROOT\exefile\shell\open\command2) überwachen und diesen z. B. nur von lokalen Laufwerken (z. B. C:\) zulassen. Diese können auch beliebig für den Eigenbedarf erweitert werden, beispielsweise den Aufruf von Dateien unterbinden, die Zeichenfolgen wie "Setup", "Install" oder "Update" enthalten.

- **Access Control Lists (ACL)**
  ACL sind mächtige Funktionen des Betriebssystems, die Zugriffe auf Systemobjekte bereitstellen.

  Da der Zugriff nur über das Windows-API (Application Program Interface) möglich ist und die Dokumentation nur im Microsoft DDK (Device Development Kit) verfügbar ist, steht dieser Weg – mangels momentan verfügbarer Programme dieser Kategorie – nur Programmierern offen. [1] – [3].

- **Manipulation/Überwachung der Registry**
  Ansätze zum Erstellen eigener Software sind in der Fachpresse bereits diskutiert [4], [5]. Der Ansatz beruht auf der Überwachung des Registrierungsschlüssels "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB", in dem alle registrierten USB-Geräte eingetragen sind.

  Diese werden mit einer Positivliste verglichen und bei unzulässigen Einträgen können Maßnahmen vorgesehen werden. Die selbstständige Deaktivierung bzw. Entfernung dieser Geräte aus dem System scheidet hierbei aus, da hierfür nur der Weg über die Windows-API in Frage kommt.

  Die Frage, inwieweit die Manipulation der Systemregistrierung - etwa die Einschränkung der Rechte auf diesen Schlüssel für das Betriebssystem (Benutzer "System") - nutzbringend ist, ohne ggf. die Systemstabilität zu gefährden, kann an dieser Stelle nicht abschließend beantwortet werden.

18.4.4.2
Linux

18.4.4.2.1
USB unter Linux

Linux verfolgt in der Standardinstallation durchgängig das modulare Konzept: alle Treiber werden bei Bedarf dynamisch zum Kernel hinzugeladen und ausgeführt.

Im Server-Bereich sollte ein statischer Kernel zum Standard gehören (vgl. 31. Tätigkeitsbericht, Ziff. 12.4). Damit stellt sich die Modulproblematik nicht, da Module, die bei der Erstellung des Kernels nicht berücksichtigt wurden, auch nicht verfügbar sind.

18.4.4.2.2
Lösungsansätze

Scheidet bei Linux-Rechnern die Kernelerstellung aus, kommen zwei Lösungsansätze in Betracht:

- **Löschen der USB-Module in /lib/modules**
  Dies ist die einfachste Methode, das Laden von Modulen zum Linux-Kernel zu verhindern.

- **Anpassung des Hotplug-Daemons, der für die Geräteverwaltung zuständig ist**
  Dieser kann in den entsprechenden Runlevels (Betriebssystemmodus eines Linux-Systems, z. B. Text- oder grafische Oberfläche) vollständig deaktiviert werden. Ist dies nicht möglich oder nicht gewollt, lassen sich die erlaubten (USB-)Module in der Datei "/etc/hotplug/usb*.map" eintragen, die nicht erlaubten in "/etc/hotplug/blacklist".
  Dies ist sicherlich der arbeits- und zeitintensivere Weg, wird aber in Anbetracht der Zunahme an verfügbaren USB-Geräten bzw. dem Mangel alternativer Geräte nicht zu umgehen sein.

18.4.5
Dienstanweisungen

Sind USB-Anschlüsse verfügbar, ist es dringend angeraten, den Betrieb von USB-Geräten, die nicht für den Dienstbetrieb erforderlich sind und nicht dienstlich bereitgestellt werden, durch eine Dienstanweisung zu untersagen.

Sind Massenspeichergeräte im Einsatz, ist Art und Umfang des Datentransfers zu regeln, in diesem Fall unter dem besonderen Aspekt eines möglichen Verlusts des Datenträgers.

Quellen

[1] Mark Russinovich – Documentation for NT 4.0 ACL Editors
http://www.sysinternals.com/ntw2k/info/acledit.shtml
[2] Mark Russinovich – Device Object Security
http://www.sysinternals.com/ntw2k/info/devsec.shtml
[3] WinObj – NT Object Manager von Mark Russinovich
http://www.sysinternals.com/ntw2k/freeware/winobj.shtml
[4] R. Hohmann, USB-Wächter - Digitaler Keuschheitsgürtel aus VBScript für die USB-Schnittstelle, c't Magazin für Computertechnik 08/2003, S. 190 ff., Heise Verlag, Hannover
[5] M. Withopf, Geordneter Rückzug - Geräte unter Windows automatisch abmelden, c`t Magazin für Computertechnik 16/2003, S. 208, Heise Verlag, Hannover

18.5
Elektronische Authentisierung mit Schlüsseln

Für den Einsatz von Signaturschlüsseln und Authentisierungsschlüsseln gibt es unterschiedliche Anwendungsfelder.

18.5.1
Einleitung

Auf den meisten Signaturkarten für qualifizierte Signaturen sind drei verschiedene Schlüsselpaare (je ein persönlicher/privater und ein zugehöriger öffentlicher Schlüssel) enthalten, von denen eines zur Signatur (vgl. 30. Tätigkeitsbericht, Ziff. 4 und 24. Tätigkeitsbericht Ziff. 17.1), eines zur Verschlüsselung im Sinne von Geheimhaltung (vgl. Ziff. 18.6 Orientierungshilfe Kryptografie) und das dritte zur Authentisierung (vgl. 30. Tätigkeitsbericht, Ziff. 14.1 zur Authentisierung ohne Schlüssel) verwendet werden kann.

Technisch sind der Aufbau und die Anforderungen an diese drei Schlüsselpaare identisch, sodass – einen geeigneten Verschlüsselungsalgorithmus vorausgesetzt – jedes grundsätzlich für jeden dieser drei Zwecke gleichgut einsetzbar ist. Die Festlegung, welches Schlüsselpaar für welchen Zweck verwendet wird, ergibt sich aus dem zugehörigen Zertifikat eines Zertifizierungsdienstanbieters (ZDA) bzw. einer Public Key Infrastruktur (PKI). Das Zertifikat muss u. a. folgende Angaben enthalten:

- den Namen des Karten- bzw. Schlüsselinhabers,
- den öffentlichen Schlüssel zum Prüfen bzw. Entschlüsseln,
- die Bezeichnung der Algorithmen, mit denen das Schlüsselpaar genutzt werden kann,
- den Gültigkeitszeitraum des Zertifikats,
- den Namen des ZDA bzw. der PKI,
- ggf. Angaben darüber, ob die Nutzung des Schlüssels auf bestimmte Anwendungen nach Art und Umfang beschränkt ist.

Organisatorisch und rechtlich gibt es fundamentale Unterschiede beim Einsatz von Schlüsseln zur Geheimhaltung und zur Signatur.

Der persönliche Signaturschlüssel muss gemäß § 2 Abs. 3 Signaturgesetz (SigG) unter der alleinigen Verfügungsgewalt des Schlüsselinhabers stehen und er darf ihm selbst nicht bekannt sein. Ferner können beim Einsatz eines Signaturschlüssels allein durch die Verbindung eines elektronischen Dokuments mit der (qualifizierten) elektronischen Signatur gemäß § 2 Nr. 3 SigG bestimmte Rechtsfolgen wie die Gleichsetzung der elektronischen mit der Schriftform (§§ 126 Abs. 3, 126a BGB; § 3a Verwaltungsverfahrensgesetz) oder der Anscheinsbeweis bei elektronischen Dokumenten (§ 292a ZPO) ausgelöst werden. Eine Verschlüsselung zur Geheimhaltung erzielt diese Rechtsfolgen nicht.

Der "persönliche" Verschlüsselungsschlüssel kann u. U. auch von einer Gruppe von Personen, z. B. einer Behörde oder einer Abteilung zur Entschlüsselung von eingehenden, mit dem zugehörigen öffentlichen Schlüssel verschlüsselten Nachrichten genutzt werden. Selbst wenn er nur für die Nutzung durch eine einzige natürliche Person gedacht ist, kann es sein, dass er z. B. für den Fall des Ausscheidens oder bei längerer Krankheit eines Mitarbeiters hinterlegt wird oder dass er aus anderen rechtlichen Gründen, z. B. um evtl. Informationsansprüche Dritter zu befriedigen (Kryptokontroverse) hinterlegt werden muss. Um einen Schlüsselverlust und damit Verlust aller mit dem Schlüssel verschlüsselten Informationen zu vermeiden, wurden so genannte Key-Recovery-Verfahren entwickelt. Bei diesen Verfahren werden Schlüsselteile oder Parameter der Schlüsselerzeugung hinterlegt, um ggf. den persönlichen Schlüssel zur Entschlüsselung wiederherstellen zu können.

Diese grundsätzlichen Unterschiede hatten folgerichtig zunächst dazu geführt, dass für Zwecke der Geheimhaltung ein anderes Schlüsselpaar eingesetzt wird als zur Signatur.

Inzwischen ist auf den meisten Signaturkarten noch ein weiteres Schlüsselpaar zur Authentisierung enthalten. Zu diesen Authentisierungsschlüsseln erreichen mich immer wieder die folgenden beiden Fragen:

1. Wofür und wie können Authentisierungsschlüssel eingesetzt werden?
2. Warum sollte man zur Authentisierung in der Regel weder den Signaturschlüssel noch den Verschlüsselungsschlüssel verwenden?

18.5.2
Begriffe

Da die Terminologie in der Literatur keineswegs einheitlich ist, werden zunächst die wichtigsten Begriffe definiert, um die Voraussetzung für ein gemeinsames Verständnis zu schaffen.

Authentisierung

Unter einer Authentisierung (engl. *authentication*[1)] versteht man die Vorlage eines Nachweises eines Kommunikationspartners, in dem bestätigt wird, dass er tatsächlich derjenige ist, der er vorgibt zu sein.

Authentisierungs-Daten

Authentisierungs-Daten (engl. *authentication data*) sind diejenigen Daten, die ein Kommunikationspartner benötigt, um sich zu authentisieren.

Authentifizierung

Unter einer Authentifizierung (engl. *authentication*[1)]) versteht man die Prüfung einer *Authentisierung*, d. h. die Überprüfung, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein.

Identifikation bzw. Identifizierung

Unter dem Begriff Identifikation bzw. Identifizierung[2)] (engl. *identification*) versteht man die Feststellung der Identität einer Person anhand eines eindeutigen Unterscheidungsmerkmals.

[1)] Im Englischen wird der Begriff "authentication" sowohl für die Authentisierung als auch für die Authentifizierung verwendet.

[2)] Die Begriffe Identifikation und Identifizierung beziehen sich immer auf die Überprüfung der Identität einer Person im Rahmen einer Registrierung; bei der Kommunikation im Fachverfahren spricht man von der Authentisierung eines Kommunikationspartners.

(Quelle: BSI: E-Government-Handbuch)

18.5.3
Authentisierung mit Authentisierungsschlüssel

18.5.3.1
Allgemeine Authentisierung

Wie beim Signaturschlüssel handelt es sich auch beim Authentisierungsschlüssel um ein Schlüsselpaar. Der private Schlüssel ist auf der (Signatur-) Chipkarte und dient zum Authentisieren, der zugehörige öffentliche Prüfschlüssel steht in einem Zertifikat eines Zertifizierungsdienstesanbieters bzw. einer Public Key Infrastruktur (PKI) und ggf. in einem von diesem geführten öffentlichen Verzeichnis.

Damit lässt sich die erste Frage prinzipiell beantworten: Den persönlichen Authentisierungsschlüssel kann man benutzen, um sich gegenüber Kommunikationspartnern oder Rechnern zu authentisieren. Den öffentlichen Schlüssel kann der Kommunikationspartner bzw. Rechner nutzen, um die Authentisierung des Absenders zu prüfen, ihn also zu authentifizieren.

Das Authentisierungszertifikat mit dem Prüfschlüssel kann vom Absender seiner Authentisierungsnachricht beigefügt werden; aber nur der Weg über eine Prüfung oder eine Abfrage beim Zertifizierungsdiensteanbieter bringt Sicherheit über die aktuelle Gültigkeit des Zertifikats.

18.5.3.2
Einsatzmöglichkeiten

Dieses Verfahren lässt sich sowohl für die Kommunikation einer Person mit einem System oder einer Systemkomponente als auch für die elektronische Kommunikation zwischen zwei Personen einsetzen.

- zur Benutzeranmeldung am PC, an Servern oder Systemkomponenten genutzt, z. B. über die Verwendung von Zufallszahlen oder Datum und Uhrzeit, die nach Eingabe der Authentisierungs-PIN mit dem Authentisierungsschlüssel authentisiert werden. Der Empfänger (Rechner) prüft mit dem Authentisierungs-Prüfschlüssel und gewährt bei positivem Ergebnis Zugriff auf die Anwendung bzw. Systemkomponente, für die der Benutzer berechtigt ist.

  Gegenüber einer Benutzeranmeldung mit Passwort bietet die Verwendung von Authentisierungsschlüsseln höhere Sicherheit. Denn ein Passwort - auch wenn es (mit immer dem gleichen Schlüssel) verschlüsselt übertragen wird, eröffnet die Möglichkeit von Replay-Attacken (vgl. 30. Tätigkeitsbericht, Ziff. 14.1), d. h. ein Angreifer kann diese Information abfangen und wieder einspielen, um selbst die entsprechenden Berechtigungen des Benutzers missbräuchlich zu nutzen.

  Single-Sign-On-Verfahren sind Anmelde-Verfahren, bei denen der Benutzer nach einer erfolgreichen Authentifizierung Zugriff auf alle Anwendungen und Systemkomponenten bekommt, für die er berechtigt ist. Für den Benutzer ist das bequem, bei Missbrauch ist der Schaden aber auch wesentlich höher, deshalb sollten hierfür nur "starke" Authentisierungsverfahren verwendet werden. Dies ist mit Challenge-Response-Verfahren möglich, die die wechselseitige Authentifizierung von Benutzern, Servern, Systemkomponenten etc. ermöglichen.

- *Elektronische Kommunikation zwischen Personen*
  Hier geht es um die Kommunikation zwischen zwei Personen – auch als Mitarbeiterinnen bzw. Mitarbeiter in einer Institution (Behörde, Firma) –, bei der es nicht auf Rechtsverbindlichkeit bzw. Schriftform ankommt.

Rechtlich ist es unwichtig, welchen konkreten Inhalt man nach Eingabe seiner Authentisierungs-PIN und eventueller Prüfung biometrischer Merkmale mit Hilfe seines Authentisierungsschlüssels authentisiert. Ob es sich beispielsweise um eine Zufallszahl, eine vom Rechner gesendete Aufforderung für ein Challenge-Response-Verfahren oder um persönliche Identifikationsdaten handelt. Letztere sollten dann aber stets verschlüsselt sein.

Bei einer Authentisierung wird der Inhalt der authentisierten Zeichenfolge weder geprüft noch bestätigt. Häufig werden Zeichenfolgen ohne semantischen Inhalt wie z. B. Zufallszahlen verwendet. Weil an die elektronische Authentisierung im Gegensatz zur qualifizierten elektronischen Signatur keine weiteren Rechtsfolgen geknüpft sind (s. o. Ziff. 18.5.1), braucht man sich keine Gedanken darüber machen, ob zu dem vom Rechner gesendeten Challenge oder zu der Zufallszahl (unabhängig davon, ob sie auf dem eigenen oder dem Zielsystem generiert wurde) ein Dokument existiert, das genau diesen Hashwert hat, den man jetzt authentisiert. Wer an dieser Stelle statt des Authentisierungsschlüssels den Signaturschlüssel verwendet, kann nicht ausschließen, von seinem Kommunikationspartner einen Datensatz bzw. ein Dokument präsentiert zu bekommen, dessen Inhalt er nicht sehen bzw. erkennen kann, der ihm aber allein durch die Verwendung des Signaturschlüssels zugerechnet wird. Das könnte z. B. bedeuten, dass ungewollt eine wie auch immer geartete Willenserklärung signiert (rechtlich betrachtet: "unterschrieben") wird.

18.5.4
Authentisierung mit elektronischer Signatur

Aus dem Vorangegangenen folgt, dass eine Authentisierung mittels elektronischer Signatur nur in den Fällen vorgenommen werden sollte, in denen ein verbindlicher Antrag mit persönlichen Identifikationsdaten an den Kommunikationspartner (z. B. eine Behörde im Rahmen von E-Government) übersandt werden muss, mit dem ein dem Absender eindeutig zugeordneter Datensatz beim Empfänger ausfindig gemacht werden soll. In diesem Fall ist mit dem qualifiziert signierten Antrag und seinen (erwünschten) Rechtsfolgen die Authentisierung mit erledigt; an dieser Stelle sei auch darauf hingewiesen, dass die Identifikationsdaten sinnvollerweise verschlüsselt und gegen Replay-Attacken geschützt werden sollten. Letzteres ist beispielsweise dadurch möglich, dass man die Daten mit einem Zeitstempel versieht.

Sofern es also nicht um einen verbindlichen Antrag, sondern lediglich um die Übersendung von Authentisierungsdaten geht, sollte die Authentisierung mit einem Authentisierungsschlüssel gewählt werden, um evtl. unerwünschte Rechtsfolgen zu vermeiden.

18.5.5
Authentisierung und Verschlüsselung

Umgekehrt sollte auch der (private) Authentisierungsschlüssel selbstverständlich „unter der alleinigen Verfügungsgewalt des Schlüsselinhabers“ sein und bleiben. Deshalb kann dieser in der Regel nicht zur Geheimhaltung verwendet werden. Denn bei der Hinterlegung bzw. beim Key-Recovery wird ja gerade der private Schlüssel (des Empfängers) hinterlegt bzw. rekonstruiert, um das Dokument, das mit dem zugehörigen öffentlichen Schlüssel (des Empfängers) verschlüsselt wurde, zu entschlüsseln.

Ferner sind Gruppenschlüssel zur Geheimhaltung auf keinen Fall zur Authentisierung einer einzelnen Person geeignet, weil der private Schlüssel ja allen Gruppenmitgliedern zur Entschlüsselung zur Verfügung steht.

18.5.6
Rahmenbedingungen

18.5.6.1
Zertifizierungs-Infrastruktur für Authentisierungszertifikate

Es gibt derzeit noch keine allgemeinen Regelungen für Authentisierungs-Zertifikate.

Für natürliche Personen wäre denkbar, dass die Zertifizierungsdiensteanbieter für qualifizierte Signaturen im Rahmen des Antrags für eine Signaturkarte oder auch später - mit einem getrennten Formular - einen Antrag für ein Authentisierungs-Zertifikat entgegennehmen zu einem Authentisierungsschlüssel, der sich bereits auf der Signaturkarte befindet. Auf der Grundlage des Identifikationsverfahrens nach § 5 Abs. 1 SigG, das für die Signatur ohnehin durchgeführt wird, kann man von einer hohen Qualität der getroffenen technischen und organisatorischen Maßnahmen – insbesondere bei den akkreditierten Anbietern – ausgehen. Der Zusatzaufwand ist gering, sodass keine hohen zusätzlichen Kosten zu erwarten sind. Hier ist abzuwarten, welche Geschäftsmodelle die Zertifizierungsdiensteanbieter entwickeln und wie Aufbau und Prüfung bzw. Abrufbarkeit der Authentisierungszertifikate genau geregelt werden. Die Regelungen für qualifizierte Zertifikate gemäß § 2 Nr. 7 SigG lassen sich zumindest als Leitlinien verwenden.

Für juristische Personen besteht die Möglichkeit im Rahmen einer Vertretungsregelung entsprechende Angaben in das Zertifikat bzw. Attribut-Zertifikat einer natürlichen Person aufzunehmen.

Zu klären ist, ob und wie man Authentisierungszertifikate ähnlicher Qualität für Systeme und Systemkomponenten erstellen kann.

Bedauerlich wäre es aus meiner Sicht, wenn es wegen einer Vielzahl unterschiedlich definierter Qualitäten und Abläufe für elektronische Authentisierung und Authentisierungszertifikate zu ähnlich zögerlichem Einsatz und Verunsicherung der Kunden käme wie bei der elektronischen Signatur.

18.5.6.2
Authentisierung zwischen zwei Partnern mit gemeinsamem Geheimnis

Wenn es sich lediglich um zwei bestimmte Partner handelt, kann die Authentisierung eventuell auch über ein gemeinsames Geheimnis erfolgen, das aus dem oder – bei wechselseitiger Authentifizierung – den Authentisierungs-Prüfschlüsseln besteht. Hier kann dann – sichere Generierung der Schlüsselpaare und sicheren Austausch und gesicherte Aufbewahrung der Prüfschlüssel etc. vorausgesetzt – ggf. auf allgemeine Zertifikate eines Zertifizierungsdiensteanbieters verzichtet werden.

18.5.6.3
Risikoanalyse

Generell ist auch für den Einsatz von Authentisierungsverfahren eine Risikoanalyse durchzuführen.

Dabei muss unter anderem geklärt und berücksichtigt werden, ob

- die verwendeten Geräte identifizierbar und/oder zertifiziert sind
- ob die verwendete Software zertifiziert ist
- in welcher Umgebung mit welchen Risiken das Verfahren laufen soll
- ob und welcher Zertifizierungsdiensteanbieter bzw. welche PKI mit welcher Policy und welchen konkreten technischen, organisatorischen und rechtlichen Rahmenbedingungen genutzt werden soll.

Ferner ist für jeden konkreten Geschäftsprozess eine eigene Restrisikobetrachtung durchzuführen.

Nur so – durch die Betrachtung des gesamten konkreten Einsatzbereiches – kann die Frage nach den angemessenen Maßnahmen zutreffend beantwortet werden.

18.6
Orientierungshilfe Kryptografie - Technische Grundlagen

Die Datenschutzbeauftragten des Bundes und der Länder haben eine Orientierungshilfe zu Fragen des Einsatzes kryptografischer Verfahren, insbesondere von Verschlüsselungstechniken, erarbeitet.

Bei der Entwicklung neuer Verfahren und wenn es gilt Datensicherheit zu gewährleisten, spielen kryptografische Verfahren eine immer größere Rolle. Beispielsweise kann bei der Datenübertragung im Internet oder zum Schutz gespeicherter sensibler Daten gegen unbefugte Kenntnisnahme auf die Datenverschlüsselung nicht verzichtet werden. Wegen der komplexen Fragestellungen, die beim Einsatz von Verschlüsselungsverfahren beachtet werden müssen, haben die Datenschutzbeauftragten des Bundes und der Länder eine Orientierungshilfe erstellt, die dem Anwender Hinweise zur Lösung seiner Probleme geben soll. Folgende Bereiche werden angesprochen:

- **Datenschutzrechtliche Grundlagen**
  Es werden die Schutzziele genannt und auf Datenkategorien mit besonderem Schutzbedarf wie Gesundheitsdaten, Daten über Dienst- und Arbeitsverhältnisse (Personaldaten) und Sozial- sowie Steuerdaten eingegangen.

- **Technische Grundlagen der Kryptografie**
  Dieses Kapitel ist unten abgedruckt, da es einen generellen Überblick über Fragen zur Kryptografie gibt.

- **Grundszenarien der Nutzung der Informationstechnik im Zusammenhang mit ihrer Absicherung mit kryptografischen Verfahren**
  Die Verschlüsselung bei der Speicherung von Daten wird für die Zugriffskontrolle, die Weitergabekontrolle beim Datenträgeraustausch und bei der Speicherverschlüsselung dargestellt.

- **Allgemeine Lösungsansätze**
  Es wird auf das Tunneling, die elektronische Signatur, Challenge-Response-Verfahren, Leitungs- und Ende-zu-Ende-Verschlüsselung, Kryptoboxen sowie Verschlüsselungskomponenten von Standardsoftware eingegangen.

- **Szenarien - Infrastrukturen**
  Am Beispiel des Internet, von Landesnetzen, Corporate und Virtual Private Networks (VPN), lokalen Netzen und von Sprachkommunikation und Telefax werden Infrastrukturen beschrieben.

- **Szenarien - ausgesuchte Anwendungsfälle**
  Als ausgesuchte Anwendungsfälle werden die Abschottung der Systemadministration, E-Commerce - Elektronischer Handel, elektronische Bürgerdienste, elektronische Post, externe Archivierung, Fernwartung, mobile Geräte und Datenträger, Outsourcing sowie Außendienst und Telearbeit detailliert behandelt.

- Ferner ist ein Glossar, ein Abkürzungsverzeichnis und ein Literaturverzeichnis Bestandteil der Orientierungshilfe.

Der vollständige Text der Orientierungshilfe steht auf meiner Homepage (www.datenschutz.hessen.de) zur Verfügung. Den Teil, in dem die technischen Grundlagen der Kryptografie dargestellt werden, möchte ich jedoch auch an dieser Stelle veröffentlichen. Es muss dabei beachtet werden, dass es sich um Aussagen aus dem September 2003 handelt. Gerade Ausführungen zu Schlüssellängen stehen unter dem Vorbehalt, dass es keine wesentlichen mathematischen oder technischen Fortschritte gegeben hat. Um sich ein aktuelles Bild zu machen, können die Angebote des Bundesamtes für Sicherheit in der

Informationstechnik (BSI) oder der Regulierungsbehörde für Telekommunikation und Post (RegTP) weiterhelfen. Während die RegTP auf die Fundstellen hinweist, in denen für die digitale Signatur geeignete Algorithmen genannt werden, bietet das BSI allgemeine Informationen zu Fragen der Kryptografie (www.bsi.bund.de).

18.6.1
Was kryptografische Verfahren leisten – und nicht leisten können

Kryptografische Verfahren sind Realisierungen von mathematischen Rechenvorgängen, sog. Algorithmen. Sie sind im Prinzip geeignet, die folgenden Ziele zu erreichen:

- Unbefugte Personen können die Daten nicht zur Kenntnis nehmen. (**Vertraulichkeit)**
- Unbefugte Änderungen von Daten können erkannt werden. (**Integrität)**
- Es kann nachgewiesen werden, wer der Kommunikationspartner ist (Identitätsnachweis), und es kann nachgewiesen werden, von wem eine Nachricht stammt (Nachrichtenauthentisierung). (**Authentizität)**
- Dritten gegenüber kann nachgewiesen werden, dass eine Kommunikation zwischen bestimmten Partnern stattgefunden hat. (**Nichtabstreitbarkeit)**

Die Vertraulichkeit wird durch Verschlüsselung erreicht. Eine Verschlüsselung basiert auf einem Algorithmus, der unter Verwendung eines Schlüssels die Ursprungsdaten so "verquirlt", dass es für jeden, ausgenommen die autorisierten Empfänger, extrem schwierig ist, die Ursprungsdaten wieder herzustellen. Die Methoden, die der Gewährleistung von Integrität, Authentizität und Nichtabstreitbarkeit zugrunde liegen, sind Message Authentication Codes, Hashfunktionen, digitale Signaturen und kryptografische Protokolle. Digitale Signaturen verbinden Hashfunktionen mit asymmetrischen Verschlüsselungsverfahren. Sie erlauben es festzustellen, wer eine Nachricht erzeugt hat und es ist überprüfbar, ob die signierte Datei mit der vorliegenden Datei übereinstimmt.

Verschlüsselungsverfahren und digitale Signaturen haben, auch wenn sie gleiche oder ähnliche Algorithmen verwenden, stark differierende Eigenschaften. Verschlüsselte Daten können nur die Kommunikationsteilnehmer entschlüsseln, die den geheimen Schlüssel kennen. Eine gesicherte Aussage, wer Urheber einer Nachricht ist, kann - zumindest bei asymmetrischen Verschlüsselungsverfahren - jedoch nicht getroffen werden. Demgegenüber kann eine digitale Signatur nur vom Inhaber des passenden geheimen Schlüssels erzeugt worden sein, aber jeder kann sie lesen und verifizieren.

Kryptografische Verfahren können nicht verhindern, dass Nachrichten unterdrückt oder verändert werden; sie können jedoch helfen, solche (gezielte oder ungezielte) Störungen zu erkennen. Sie sind ebenfalls nicht geeignet, eine Verkehrsanalyse ("wer kommuniziert wann mit wem?") zu verhindern, können jedoch dazu beitragen, deren Aussagekraft zu minimieren.

Kryptografie ist kein Allheilmittel für alle Probleme des Datenschutzes und der Datensicherheit. Doch in einer Reihe von Situationen gibt es aus heutiger Sicht keine Alternative.

18.6.2
Klassen von Verschlüsselungsverfahren

Es gibt drei Klassen von Verschlüsselungsverfahren: symmetrische, asymmetrische und, als Kombination beider, hybride Verfahren.

Symmetrische Verschlüsselungsverfahren benutzen denselben Schlüssel für die Ver- und die Entschlüsselung. Beispiele sind DES, IDEA, Triple-DES, RC5 und der derzeitige Verschlüsselungsstandard AES (Advanced Encryption Standard).

Asymmetrische Verschlüsselungsverfahren arbeiten im Unterschied zu symmetrischen Verfahren mit einem Schlüsselpaar. Das Schlüsselpaar besteht aus einem allgemein zugänglichen öffentlichen Schlüssel (Public Key) und einem geheimen Schlüssel (Private Key). Wird eine Nachricht mit dem öffentlichen Schlüssel verschlüsselt, so kann die Nachricht nur mit dem passenden geheimen Schlüssel entschlüsselt werden. Bekannte Verfahren sind RSA, ElGamal und ECC.

Symmetrische und asymmetrische Verfahren haben spezifische Vor- und Nachteile. Symmetrische Verfahren erreichen einen hohen Durchsatz und sind daher besser geeignet, Daten zu verschlüsseln, wenn die Anwendung, wie im Fall der Kommunikation über Netze, zeitkritisch ist. Demgegenüber ist die Schlüsselverteilung bei asymmetrischen Verfahren einfacher. Die öffentlichen Schlüssel können auf allgemein zugänglichen Servern vorgehalten werden, während bei symmetrischen Verfahren die Schlüssel so ausgetauscht werden müssen, dass sie kein Unbefugter zur Kenntnis nehmen kann. Auch müssen bei symmetrischen Verfahren sämtliche Schlüssel geheim gehalten werden, während bei asymmetrischen Verfahren jeder Teilnehmer nur seinen eigenen Schlüssel geheim halten muss (s. Ziff. 18.6.4).

Um die Vorteile beider Klassen zu kombinieren, wurden Hybridverfahren entwickelt. Dabei wird für jede Sitzung ein Schlüssel (Session Key) zufällig generiert und asymmetrisch verschlüsselt ausgetauscht. Die Daten selbst werden dann durch einen schnellen symmetrischen Algorithmus mit dem Session Key verschlüsselt.

18.6.3
Schlüssellängen und ihre Bedeutung

Im Zusammenhang mit der Qualität kryptografischer Verfahren ist immer wieder von der Länge der verwendeten Schlüssel die Rede, wobei je nach Zusammenhang sehr unterschiedliche Werte genannt werden. Einer Analyse aus Sicht des Datenschutzes muss vorausgeschickt werden, dass eine zu geringe Schlüssellänge zu einer nicht ausreichenden Sicherheit führt, die Frage der Schlüssellänge aber nicht als alleiniges Kriterium zur Bewertung eines Verschlüsselungsverfahrens dienen kann. Letztlich dient sie zur Ermittlung der Obergrenze für den Aufwand, der erforderlich ist, um ein Verfahren zu brechen (s. Ziff. 18.6.5). Sofern ein Verfahren jedoch auf andere Weise angegriffen werden kann, spielt die Schlüssellänge u. U. eine unwesentliche Rolle.

- **Schlüssellängen bei symmetrischen und asymmetrischen Verfahren**
  Zwischen beiden Verfahren muss bei der Betrachtung der Schlüssellänge unterschieden werden. Da es bei der Betrachtung der Schlüssellänge um den Aufwand geht, der für ein Brechen des Verfahrens höchstens erforderlich ist, müssen die jeweiligen mathematischen Methoden, die den Verfahren zugrunde liegen, berücksichtigt werden. Dabei ergibt sich folgende Gegenüberstellung in etwa aufwandsäquivalenter Schlüssellängen [Schneier96, S. 194]:

symmetrisch	asymmetrisch (Beispiel RSA)
56 Bit	384 Bit
64 Bit	512 Bit
80 Bit	768 Bit
128 Bit	2.304 Bit

- **Zeitliche Relativität der Schlüssellängen**
  Aussagen zur (ausreichenden) Länge von kryptografischen Schlüsseln sind immer im Zusammenhang mit dem angenommenen Aufwand zu betrachten, der einem potenziellen Angreifer unterstellt wird. Dieser ist vom Stand der Technik und von dessen finanziellen und zeitlichen Ressourcen abhängig. Allein durch die Weiterentwicklung der Computertechnik werden daher die Anforderungen an Schlüssellängen immer größer. Dabei spielt nicht nur die durch ein einzelnes Gerät zur Verfügung gestellte Leistung eine Rolle, sondern in zunehmendem Maße auch die Vernetzung, die es ermöglicht, eine umfangreiche Entschlüsselungsaufgabe durch viele Geräte arbeitsteilig in kurzer Zeit zu lösen.

- **Theoretische Obergrenzen**
  Gleichwohl sind auch bei weiterhin steigenden Rechenkapazitäten den Möglichkeiten der Entschlüsselung physikalische Grenzen gesetzt. Aus Erwägungen der Thermodynamik heraus lässt sich folgern, dass symmetrische Verfahren ab ca. 256 Bit Schlüssellänge in konventioneller Technik nicht mehr mit Brute-Force-Methoden attackierbar sind, da hierfür schlichtweg die Energie des gesamten Universums nicht ausreichen würde [Schneier96, S. 185]. Neuartige Computertechniken (Stichwort: Quantencomputer) könnten diese Aussage allerdings relativieren.

- **Verwendungsspezifische Erwägungen**
  Bei der Überlegung, mit welchem Aufwand durch einen Angreifer zu rechnen ist, spielt es u. a. eine Rolle, für welche Zeitdauer die Daten geheim bleiben müssen. Daten mit kurzem Geheimhaltungsbedarf können schwächer (mit kürzeren Schlüssellängen) verschlüsselt werden als Daten mit langem Schutzbedarf (z. B. im Rahmen der Archivierung). Eine unberechtigte Entschlüsselung kann hingenommen werden, wenn die Daten bereits nicht mehr schützenswert oder aus anderen Gründen uninteressant geworden sind.

  Allerdings kommt dieser Unterscheidung im Datenschutzumfeld eine geringe Bedeutung zu, da bei personenbezogenen Daten generell von einem Langzeitschutzbedarf auszugehen ist. Daher kommt es hier in der Hauptsache auf die Sensibilität der Daten an.

- **Empfehlungen aus Datenschutzsicht**
  Unter Berücksichtigung der datenschutzrechtlichen Hintergründe ist die Wahl der Verschlüsselungsverfahren und deren Parameter unter dem Aspekt des angemessenen Aufwands zu betrachten. Dabei liegt der wesentliche Faktor nicht so sehr im Aspekt des Rechenaufwandes bei einer Verschlüsselung, der für höhere Schlüssellängen zu leisten ist (dieser ist vergleichsweise gering), sondern aufgrund der Marktsituation vielmehr in der Beschaffung von Produkten, die mit geeigneten Schlüssellängen operieren können (s. hierzu Ziff. 18.6.9). Für den symmetrischen Bereich lässt sich beim jetzigen Stand der Technik folgende Bewertung vornehmen:

Effektive Schlüssellänge	**datenschutzrechtliche Bewertung**	**datenschutzrechtliche Empfehlung**
40 bis 55 Bit	Schutz gegen zufällige Kenntnisnahme	Einsatz bei nicht sensiblen personenbezogenen Daten, wenn ein gezielter Angriff unwahrscheinlich ist.
ab 56 Bit	Schutz von Daten mit niedrigem bis mittlerem Schutzbedarf	Einsatz bei nicht sensiblen personenbezogenen Daten oder in solchen Fällen, in denen ein Angriff mit hohem Aufwand aus anderen Gründen unwahrscheinlich ist (z. B. geschlossenes Netz). Zukünftige Sicherheitsprobleme sind jedoch zu erwarten.
ab 80 Bit	Schutz von Daten mit mittlerem bis hohem Schutzbedarf	Einsatz uneingeschränkt außer bei Daten mit sehr hohem Schutzbedarf; bei Archivierung generell höhere Schlüssellängen
ab 112 Bit	Schutz von Daten mit sehr hohem Schutzbedarf	Einsatz uneingeschränkt

In jedem Fall sollten möglichst hohe Schlüssellängen eingesetzt werden, um einen ausreichenden Schutz gegen Brute-Force-Angriffe (s. Ziff. 18.6.5) zu erhalten. Da ein einmal installiertes Verschlüsselungssystem sich in der Regel nicht ohne erheblichen Aufwand mit anderen Schlüssellängen oder Algorithmen versehen lässt, sollten für neue Anwendungen nur Algorithmen mit Schlüssellängen ab 112 Bit zum Einsatz kommen. Dieses entspricht auch dem aktuellen Stand der Technik: Aktuelle Produkte erreichen diesen Mindeststandard in jedem Falle.

Die empfohlenen Schlüssellängen bei asymmetrischen Algorithmen differieren in Abhängigkeit vom gewählten Algorithmus. Der bekannteste und auch verbreitetste Algorithmus ist derzeit der RSA-Algorithmus. Da er gleichzeitig Objekt intensiver und erfolgreicher Forschung zur Kryptoanalyse ist, kann er heute nicht mehr als hinreichend angesehen werden, wenn die Schlüssellänge 1.024 Bit verwendet wird. Es sollten daher RSA-Schlüssel von mindestens der Länge von 2.048 Bit eingesetzt werden [Weis/Lucks/Bogk03].

18.6.4 Schlüsselverwaltung

Erfolgt die Verschlüsselung nur zwischen zwei oder wenigen Beteiligten, bereitet die Verwaltung der Schlüssel keine nennenswerten Probleme. Bei der Verwendung symmetrischer Verfahren steigt die Komplexität jedoch mit höherer Benutzerzahl rasch an. Um eine jeweils bilateral sichere Kommunikation zu ermöglichen, sind bei n Teilnehmern ca. $n^2/2$ Schlüssel zu verwalten, d. h. zu erzeugen, zu verteilen, zu verifizieren und nach gewisser Zeit wieder zu ersetzen. Daher wird auf zwei- oder mehrstufige Verfahren ausgewichen, bei denen die eigentlichen Schlüssel - durch besondere Schlüssel (key-encryption keys) verschlüsselt - sicher elektronisch übermittelt werden können. Nur die Schlüssel höherer Ordnung müssen dann aufwändig auf besonderem Weg verteilt werden (vgl. X9.17-Standard).

Die asymmetrische Verschlüsselung hingegen erfordert zum einen weniger Schlüssel (n Schlüssel bei n Teilnehmern), zum anderen ist deren Versand selbst weniger sicherheitskritisch. Gleichwohl stellen sich auch hier Fragen der Schlüsselverwaltung. Das wesentliche Sicherheitsproblem bei öffentlichen Schlüsseln liegt in der korrekten Zuordnung eines öffentlichen Schlüssels zu dem zugehörigen Eigentümer. Diese Aufgabe übernehmen typischerweise besondere Stellen, für die sich im deutschen Sprachraum der Begriff „Trust Center“ (TC) etabliert hat. Im Englischen wird dabei von "Certification Authority" (CA) gesprochen.

TC bzw. CA stellen öffentliche Schlüssel zur Verfügung und belegen zugleich mit Hilfe eines kryptografischen Zertifikats die Korrektheit des Schlüssels sowie dessen Zugehörigkeit zu dem angegebenen Eigentümer. Als technisches Rahmenwerk für solche Zertifikate hat sich der X.509-Standard etabliert (siehe hierzu die Orientierungshilfe Verzeichnisdienste des AK Technik). Die Verwendung eines solchen Schlüssels setzt also das Vertrauen in diese Stelle voraus. Durch eine baumartige Hierarchie von CA kann das Vertrauen jedoch auf eine höhere Instanz gestützt werden, wobei am oberen Ende im Idealfall eine Stelle angesiedelt ist, der alle Beteiligten vertrauen. In diesem Zusammenhang wird von einer PKI (Public Key Infrastructure) gesprochen.

Neben diesem hierarchischen Modell hat sich durch das weit verbreitete E-Mail-Verschlüsselungsprogramm PGP ein vermaschtes Vertrauensmodell (so genanntes "web of trust") etabliert. Bei diesem bestimmt jeder Benutzer selbst, in welchem Maße er oder sie einem Zertifikat traut, wobei sowohl die eigene Einschätzung eines Ausstellers als auch das Vertrauen Dritter einfließen können. Das Vertrauen in einen PGP-Schlüssel hängt dabei nicht nur vom Aussteller allein ab, sondern vom Distributionsweg und von der Korrektheit des zugehörigen Hashwerts (so genannter Fingerprint).

18.6.5
Attacken

Als Gegenpart zur Kryptografie ist die Kryptoanalyse zu sehen. Hierbei handelt es sich um die Kunst, ohne Kenntnis des geheimen Schlüssels möglichst viele Informationen über den Klartext zu gewinnen, der einer Verschlüsselung zugrunde lag. Es gibt eine Reihe von Angriffsmöglichkeiten auf einen Algorithmus, die Kryptologen zur Verfügung stehen [Wobst97, Kapitel 3].

Ein häufiger Angriff ist die so genannte Brute-Force-Attacke, bei der alle möglichen Schlüssel ausprobiert werden. Die Empfehlungen zur Schlüssellänge von symmetrischen Verfahren in Ziff. 18.6.3 sind Einschätzungen, inwieweit dieser Angriff derzeit eine realistische Gefahr darstellt. Dabei muss man sich vor Augen halten, in welcher zeitlichen Relation ein Brechen der Schlüssel steht. Wenn man hypothetisch annimmt, ein 56-Bit-Schlüssel könnte in einer Stunde ausgeforscht werden, so benötigt man für einen 80-Bit-Schlüssel mehr als 1.900 Jahre. Bei einem 112-Bit-Schlüssel kommt man auf die nicht mehr vorstellbare Dauer von mehr als 8.000 Milliarden Jahren; ein Vielfaches der Existenzdauer des Universums. Um auch in der überschaubaren Zukunft gegen diesen Angriff gesichert zu sein, insbesondere wenn es darum geht, archivierte Daten gegen unberechtigte Kenntnisnahme zu schützen, sind Schlüssellängen ab 112 Bit als ausreichend sicher anzusehen. Da die meisten heute verfügbaren Algorithmen Schlüssellängen von mindestens 112 Bit haben, können sie nicht mit Brute-Force-Attacken allein, sondern nur zusammen mit anderen Methoden geknackt werden.

Die Ansatzpunkte für Angriffe auf Verschlüsselungsverfahren sind daher weniger in unzureichenden Schlüssellängen zu suchen, als in Schwächen des Algorithmus und bei der Implementierung.

Es könnten in einen Algorithmus mathematische Schwachstellen vorhanden sein, die ihn gegenüber bestimmten Analysemethoden angreifbar machen. Um derartige Schwachstellen aufzuzeigen und eventuell Gegenmaßnahmen zu treffen, bietet sich eine öffentliche Diskussion unter Experten an. Der FEAL-Algorithmus bietet ein gutes Beispiel für Analysen und eine offene Diskussion darüber [Wobst97, S. 228]. Bei asymmetrischen Verfahren tritt ein vergleichbares Problem auf. Die Sicherheit beruht auf mathematischen Problemen, beim RSA z. B. die Faktorisierung großer Zahlen, die schwer zu lösen sind. Wenn die mathematische Forschung Fortschritte macht, die bestimmte Algorithmen unsicher werden lässt, kann das nur bei offen gelegten Algorithmen publik werden. Für diesen Fall müssen Ersatzalgorithmen vorhanden sein, die auf anderen mathematischen Fragestellungen beruhen. Anderenfalls profitieren zwar die Stellen, die den Algorithmus kennen, der Bürger wiegt sich aber in einer nicht vorhandenen Sicherheit. Aus diesem Grund bewirkt die Geheimhaltung von Kryptoalgorithmen in der Regel keine Verbesserung der Sicherheit.

Ein großes Problem stellt die sichere Implementierung dar. Dazu gehören Details wie Passworteingabe, Verwaltung geheimer Daten, Größe des Schlüsselraums oder Betriebsart. Zwei Beispiele sollen das illustrieren:

Bei der Implementierung eines Verschlüsselungsverfahrens in Hard- oder Software kann eine Hintertür eingebaut werden, die beispielsweise Teile des Schlüssels im Geheimtext oder im Kommunikationsprotokoll versteckt. Ein kundiger Angreifer kann den Text sofort entziffern oder muss nur noch einen kleinen Teil der möglichen Schlüssel testen. In Exportversionen vieler Produkte amerikanischer Hersteller ist für denjenigen eine effektive Schlüssellänge von 40 Bit implementiert, der die Hintertür kennt. Alle anderen Angreifer sehen sich einer Schlüssellänge von 56 und mehr Bit gegenüber.

Eine weitere wichtige Komponente in einem Verschlüsselungssystem ist ein Zufallszahlengenerator. Er ist unverzichtbar, wenn Schlüssel erzeugt werden. Wenn der Generator aber, absichtlich oder irrtümlich, nicht alle möglichen Schlüssel generiert, reduziert das die Zahl der möglichen Schlüssel. Eine Brute-Force-Attacke kann dann trotz eigentlich ausreichender Schlüssellänge machbar sein. Ein Beispiel hierzu lieferte Netscape, das in einer alten Version des Navigator Zufallszahlen in Abhängigkeit von der Systemzeit und anderen Informationen des Rechners erzeugte [Wobst97, S. 187]. Mit diesen Informationen wurde die Zahl der möglichen Schlüssel stark reduziert.

Neben Versuchen, den Algorithmus selbst zu knacken oder Schlüssel auszuforschen, gibt es Angriffe auf die Kommunikation und den Schlüsselaustausch. So sind Angriffe denkbar, bei denen keine Daten entschlüsselt werden, sondern Daten eingefügt oder Nachrichten wiederholt werden. Der bekannteste Angriff auf den Schlüsselaustausch wird "Mann in der Mitte" (Man in the middle) genannt. Dabei gibt sich der Angreifer M gegenüber dem Teilnehmer A als Teilnehmer B aus und umgekehrt. Wenn nun A an B verschlüsselte Daten senden will, schickt A sie tatsächlich an M. Der entschlüsselt die Daten und schickt sie dann an B weiter, wobei er sich als A ausgibt. Durch ein entsprechendes Design der Kommunikation können diese Angriffe unterbunden werden.

In vielen Fällen werden solche Lücken nicht vorsätzlich eingebaut, sondern sind durch Fehler im Entwurf oder der Umsetzung entstanden.

18.6.6
Recovery

Wenn Daten verschlüsselt gespeichert oder übertragen werden, gibt es zwei Szenarien, die eine Entschlüsselung durch Dritte erforderlich machen können. Es kann der geheime Schlüssel verloren gegangen sein oder es soll (ohne Mitwirkung des Schlüsselinhabers) Dritten ein Zugriff auf die Originaldaten ermöglicht werden. Dritter kann beispielsweise der Arbeitgeber oder eine staatliche Stelle sein.

Um einen Zugang zu den Originaldaten zu ermöglichen, sind verschiedene Lösungen denkbar. Es könnte der geheime Schlüssel bereitgestellt werden, der zur Entschlüsselung benötigt wird (Key-Recovery). Die Konsequenz wäre dann, dass

auch alle anderen Daten entschlüsselt werden könnten, die mit diesem Schlüssel gesichert wurden oder zukünftig gesichert werden. Bei einer anderen Lösung werden die Daten mit einem zufälligen Schlüssel verschlüsselt. Der Zufallsschlüssel wird dann für jeden potenziellen Zugriffsberechtigten getrennt verschlüsselt und den Daten hinzugefügt. Dadurch können mehrere Benutzer die Originaldaten erhalten, ohne geheime Schlüssel anderer Beteiligter kennen zu müssen (Data-Recovery).

Bei den Überlegungen, welche Lösung sinnvoll sein kann, lassen sich folgende Fälle unterscheiden:

- **Verschlüsselte Kommunikation**
  Um Übertragungsfehler zu korrigieren, ist in der Regel kein Zugriff auf Schlüssel nötig, weil die Übertragung wiederholt werden kann. Als Privatperson sollte man in der jetzigen Situation keine Zugriffsmöglichkeit durch Dritte akzeptieren. Das gilt nicht für Arbeitnehmer. Der Arbeitgeber hat das Recht zu wissen, welche Daten in seinem Namen übertragen wurden. Er darf die Daten lesen, die ein Mitarbeiter verschlüsselt hat, soweit dabei die rechtlichen Vorgaben eingehalten werden.

- **Verschlüsselte Speicherung**
  Es ergeben sich enorme Risiken für die Verfügbarkeit, wenn auf verschlüsselt gespeicherte Daten nicht mehr zugegriffen werden kann. Daher muss eine Möglichkeit vorgesehen werden, die Originaldaten zu rekonstruieren. Als Privatperson kann man den Schlüssel an einer sicheren Stelle hinterlegen. Im beruflichen Umfeld sollten Regelungen existieren, die eine Rekonstruktion unabhängig von bestimmten Personen erlauben. Es muss aber ein unkontrollierter Zugriff verhindert werden. Dem kann zum Beispiel durch "Data-Recovery" oder das Hinterlegen von Schlüsseln nach einem "Secret Splitting" (Das Geheimnis, mit dessen Kenntnis der Schlüssel rekonstruiert werden kann, wird so auf mehrere Personen oder Institutionen verteilt, dass nur alle zusammen den Schlüssel rekonstruieren können.) oder "Secret Sharing" (Das Geheimnis wird auf mehrere Personen oder Institutionen so verteilt, dass mehrere, die Zahl kann vorgegeben werden, kooperieren müssen, um den Schlüssel rekonstruieren zu können.) Rechnung getragen werden. Auf keinen Fall darf ein Hersteller oder ein anderer Dritter einen Generalschlüssel haben, der es erlaubt auf die Daten zuzugreifen.

- **Digitale Signatur**
  Es gibt keinen Grund, einen Signierschlüssel zu hinterlegen oder einer anderen Person zugänglich zu machen. Wenn der Schlüssel verloren geht, können keine Dokumente mehr signiert werden, aber alle bereits signierten Dokumente können weiterhin verifiziert werden. Der einzige Schaden kann darin bestehen, dass bis zum Erhalt des neuen Schlüssels keine Signaturen erfolgen können. Er ist aber nicht vergleichbar mit dem Schaden, der entstehen würde, wenn unberechtigte Personen mit einem hinterlegten Schlüssel statt des Eigentümers Dokumente signieren können.

18.6.7
Filterung und Virenschutz beim Einsatz von Verschlüsselung

Durch den Einsatz von Verschlüsselungsverfahren kann sich hinsichtlich der Datensicherheit ein Zielkonflikt ergeben. Denn nicht nur die unberechtigte Kenntnisnahme von Inhalts- und Verbindungsdaten wird dadurch unmöglich gemacht, sondern ebenso eine mitunter erwünschte zentrale Kontrolle auf enthaltene Schadensprogramme (Viren etc.) und u. U. auch eine Adress- und Port-Filterung durch Firewalls. Inwieweit ein solcher Konflikt besteht, hängt von der eingesetzten Technik wesentlich ab; dies sollte daher im Rahmen eines Einsatzkonzeptes berücksichtigt werden.

Grundsätzlich lässt sich das Problem dadurch vermeiden, dass die Verschlüsselung erst jenseits der in Frage stehenden zentralen Komponenten (Firewall, Virenscanner) ansetzt, z. B. durch Einsatz einer Verbindungsverschlüsselung am Übergang zum Internet oder Corporate Network. Allerdings kann das Problem auch in diesem Szenario durch eine zusätzliche Ende-zu-Ende-Verschlüsselung (z. B. im E-Mail-Verkehr oder beim Dateiversand) auftreten.

Da sich die Verschlüsselung in der Regel auf die Inhaltsdaten bezieht, ergeben sich für die Filterung nur dann Probleme, wenn diese auch inhaltliche Teile einbezieht (z. B. Webadressen oder Elemente von Protokollen auf Anwendungsebene). TCP/IP-Adressen und -Ports hingegen sind auch bei verschlüsselten Daten (z. B. beim Einsatz von SSL) auswertbar, sofern nicht besondere Tunnelungsverfahren eingesetzt werden, die (etwa bei IPSec) die eigentlichen Adressdaten verbergen. In diesem Fall allerdings läuft eine Filterung nahezu vollkommen ins Leere.

Mehr Probleme entstehen für den Fall einer zentralen inhaltlichen Überprüfung. Hier scheitert u. U. bereits die Feststellung, ob z. B. eine verschlüsselte E-Mail Anhänge enthält, die aus Sicht einer Virenkontrolle von Bedeutung sind. Sofern nicht durch eine entsprechende Schlüsselinfrastruktur eine zentrale Entschlüsselungsmöglichkeit (mit all ihren Problemen, s. Ziff. 18.6.6) eröffnet werden soll, ist mit dieser Einschränkung zu leben. Dies bedeutet, dass neben einer zentralen auch eine dezentrale Virenkontrolle (die sich auch aus anderen Gründen empfiehlt) erfolgen muss. Der Versuch, den Zielkonflikt dadurch zu vermeiden, dass die Verschlüsselung unterdrückt wird (z. B. durch Nichtweiterleitung eingehender verschlüsselter E-Mails), ist aus Sicht des Datenschutzes jedenfalls keine sinnvolle Lösung.

18.6.8
Verschlüsselung durch Auftragnehmer

Während die Verschlüsselung typischerweise eingesetzt wird, um Dritte von der Kenntnisnahme und der Manipulation von Daten auszuschließen, ist gleichwohl eine Übertragung der Kryptografie auf einen Dienstleister denkbar. Insbesondere im Zusammenhang mit der Bereitstellung von Netzwerkdiensten bietet sich als zusätzlicher Dienst die kryptografisch gesicherte Übertragung an. Typischer Fall einer solchen Konstruktion wäre die Bereitstellung eines VPN (Virtuellen Privaten Netz-

werks) durch einen Provider, mit dessen Hilfe verteilte Standorte über offene Netze wie das Internet sicher miteinander verbunden werden können.

Da der Sicherheits-Dienstleister bei einer solchen Konstruktion prinzipiell über die Möglichkeit verfügt, die Daten im Klartext zur Kenntnis zu nehmen, muss diesem ausreichendes Vertrauen entgegengebracht werden, und die Dienstleistungsverträge sind so zu gestalten, dass ein Missbrauch weitgehend ausgeschlossen ist.

Eine solche Verschlüsselungsinfrastruktur kann zudem als Grundschutz eingesetzt werden, um ein ausreichendes Schutzniveau bei der Übermittlung nicht sensibler Daten zu gewährleisten. Die im Einzelfall übertragenen sensiblen Daten können dann mit zusätzlichen Verschlüsselungsverfahren, ggf. anwendungsbezogen, auch gegen eine Kenntnisnahme durch den Provider geschützt werden.

18.6.9
Kryptokontroverse und Exportkontrolle

Seit einigen Jahren gibt es immer wieder Bestrebungen, den Einsatz von Verschlüsselungssystem zu reglementieren, weil die Verfahren immer schwerer zu brechen sind. Dabei wird auf kriminelle Organisationen verwiesen, die sich durch Verschlüsselung einer staatlichen Überwachung entziehen können. Die Diskussion, inwieweit ein Zugriff staatlicher Stellen auf eine verschlüsselte Kommunikation zulässig und sinnvoll ist, ist als Kryptokontroverse bekannt.

Befürworter einer Überwachung schlagen als technische Lösung Key-Recovery-Systeme vor, wie sie erstmals als Reaktion auf die Clipper-Initiative der US-Regierung 1993 öffentlich diskutiert wurden. Demgegenüber weisen Gegner darauf hin, dass es Möglichkeiten gibt, sich der Überwachung zu entziehen. Außerdem halten sie die vorgeschlagenen Systeme für unbeherrschbar, sowohl vom Betrieb her als auch hinsichtlich der Gefahren für die Bürger [Abelson98]. Die Datenschutzbeauftragten teilen die Vorbehalte. In ihrem Eckpunktepapier zur Kryptopolitik vom 2. Juni 1999 hat die Bundesregierung einen vorläufigen Schlussstrich gezogen. Sie stellt fest, dass solche Eingriffe zurzeit nicht geplant sind. Abhängig von zukünftigen Erfahrungen behält man sich jedoch vor, diese Aussage zu revidieren.

Mit dem Ziel, starke Verschlüsselungsverfahren nur kontrolliert zu verbreiten, haben praktisch alle Staaten Regelungen zum Export und Import getroffen ([Beucher/Schmoll99], [Roth98]). Am bekanntesten sind die Exportrestriktionen der USA, weil sie wegen der Dominanz amerikanischer Software die größten Auswirkungen haben. Die Beschränkungen waren früher sehr restriktiv und führen teilweise noch immer dazu, dass exportierte Produkte nur unzureichende Verschlüsselungsmöglichkeiten bieten (vgl. Ziff. 18.6.5). Inzwischen sind die Restriktionen deutlich gelockert, so dass heute aus diesem Grund bei keinem Hersteller bzw. Produkt auf eine starke Verschlüsselung verzichtet werden muss.

Quellen

[Schneier96]	B. Schneier: Angewandte Kryptografie, 1996
[Weis/Lucks/Bogk03]	R. Weis, S. Lucks, A. Bogk: Sicherheit von 1024 bit RSA-Schlüsseln gefährdet; DuD 2003, S. 360
[Wobst97]	R. Wobst: Abenteuer Kryptologie, 1997
[Abelson98]	Abelson, Anderson, Bellovin, et al.: Risiken von Key Recovery. Key Escrow und Trusted Third Party-Verschlüsselung, DuD 1998, S. 14 ff.
[Beucher/Schmoll99]	Beucher, Schmoll: Kryptotechnologie und Exportbeschränkung, CR 8/1999

18.7
Die Nutzung digitaler Funktelegramme im Rettungsdienst

Die Einrichtung digitaler Funknetze für Behörden und Organisationen mit Sicherheitsaufgaben lässt noch immer auf sich warten. Durch den Einsatz digitaler Funktelegramme auf den bestehenden Funkkanälen kann die Klartextübertragung von personenbezogenen Daten im Sprechfunk vermieden werden.

Bereits mit meinem 21. Tätigkeitsbericht (Ziff. 16.3) habe ich auf die Abhörgefahren beim Funkverkehr der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) hingewiesen und in der Folge über die technische Entwicklung und die Veränderungen der rechtlichen Randbedingungen berichtet. Leider ist trotz aller Bemühungen die Einführung digitaler, verschlüsselnder und damit abhörsicherer Funknetze in den zurückliegenden zwölf Jahren nicht zustande gekommen. Vielmehr ist sogar zu befürchten, dass es angesichts der Komplexität der Anforderungen und der schwierigen Haushaltslage bei Bund, Ländern und Kommunen noch lange dauern wird, bis es zu einer flächendeckenden Versorgung in diesem Bereich kommt.

Seit Jahren wird auf verschiedenen Ebenen in Bund und Ländern in Ad-hoc-Ausschüssen, Arbeits- und Projektgruppen um die taktisch-betrieblichen Anforderungskataloge, daraus resultierende Leistungsmerkmale und die technische Ausgestaltung der Funknetze gerungen. Bereits 1998 wurde in Berlin und Brandenburg der erste Vortestbetrieb mit digitaler Funktechnik durchgeführt und seit Juli 2001 läuft im Großraum Aachen ein Pilotprojekt. Auf Beschluss der Innenministerkonferenz wurde sogar schon eine "Zentralstelle zur Vorbereitung der Einführung eines bundeseinheitlichen digitalen Sprech- und Datenfunksystems –Digitalfunk" (ZED) eingerichtet. Diese hatte bereits ihre Arbeit aufgenommen und ein Interessenbekundungsverfahren zur Ermittlung des Finanzbedarfs durchgeführt. Doch die Finanzminister der Länder kamen auf ihrer Sitzung im Juni 2002 zu dem Ergebnis, dass eine Finanzierung der ermittelten 7,1 Mrd. Euro für den Aufbau und den Betrieb des Netzes bis zum Jahre 2015 ohne Endgerätekosten nicht machbar ist. Seit diesem Zeitpunkt geht es nun zum einen darum, einen finanzierbaren Mindeststandard zu definieren zum anderen ringen Bund und Länder bis heute um die Verteilung der Lasten.

Vor dem Hintergrund dieser Situation, dass der aus Datenschutzsicht wichtige und notwendige Betrieb eines bundeseinheitlichen Digitalfunks für BOS kurzfristig nicht zu erwarten ist, hatte ich, einer Anfrage des Hessischen Sozialministeriums nachgehend, im Laufe des Jahres 2003 zum Einsatz von digitalen Funktelegrammen auf den bestehenden analogen Funkkanälen Stellung genommen. Der Kreisausschuss des Lahn-Dill-Kreises hatte angeregt, mich in die Diskussion um den Einsatz dieser technischen Möglichkeiten einzubeziehen, da die damit verbundenen Mehrkosten bei der Beschaffung der Funkgeräte, z. B. zusammen mit neuen Fahrzeugen für den Rettungsdienst, gerechtfertigt sein müssen.

Gerade im Rettungswesen werden sehr sensitive, in der Regel medizinische Daten verbunden mit einer Adresse und ggf. einem Namen im Klartext übermittelt. Hier ist seit Jahren ein vordringlicher Handlungsbedarf gegeben, einen gegenüber der unverschlüsselten Übermittlung über einen Funkkanal höheren Sicherheitsstand zu erzielen. Da eine schnelle Übermittlung dieser Daten im vorrangigen gesundheitlichen Interesse der Betroffenen oder aber auch der Einsatzkräfte ist, erfolgte sie trotz der einfachen Abhörbarkeit auf den vorhandenen Sprechfunkkanälen.

Mittlerweile sind aber Funkgeräte am Markt verfügbar, die mit Zusatzkomponenten die digitalen Kurztelegramme, wie sie in der Technischen Richtlinie Funkmeldesystem der BOS beschrieben sind, umsetzen können. Damit wird es möglich, bestimmte Informationen über die Telegramme zu übertragen, beim Empfänger in einem Display anzuzeigen und somit aus dem einfach mitzuhörenden Sprechfunk auszuklammern. Insgesamt ergeben sich, wenn die Telegramme konsequent zur Übermittlung personenbezogener oder -beziehbarer Daten genutzt werden, mehrere Vorteile:

- Leider kommt es in Einzelfällen beim Sprechfunk immer wieder zu Übermittlungsfehlern. Wenn dann z. B. eine Adressangabe falsch verstanden wird, führt das gerade im Rettungswesen zu u. U. lebensbedrohlichen Zeitverzögerungen. Diese Gefahr ist beim Einsatz der Funktelegramme praktisch ausgeschlossen, da die Adresse im Display des Empfängers angezeigt wird. Da auch Adressen in verschiedenen Ortsteilen gleich lauten können, können zur Sicherheit die bei den BOS üblichen Zielkoordinaten mit den Telegrammen übertragen werden. Mit dieser Verbesserung wird auch einer datenschutzrechtlichen Forderung entsprochen, weil die Daten im Interesse der Betroffenen unverfälscht übermittelt werden, und ihre Integrität gewahrt bleibt.

- Im Einsatzgebiet einer Kreisverwaltung können mehrere Hundert Einsatzkräfte berechtigt am Sprechfunk teilnehmen. Da mit den Funktelegrammen auch eine Adressierung der Empfängergeräte verbunden ist, kommen die so übermittelten Daten nur noch bei den Kräften an, die am konkreten Einsatzgeschehen beteiligt sind.

- Zwar lassen die technischen Voraussetzungen der analogen Funkkanäle auch bei Funktelegrammen den Einsatz einer praktikablen Verschlüsselung nicht zu, und mit einem präparierten Empfänger, der die Adressierung ignoriert, ist es somit möglich, die Funktelegramme unbefugt auszuwerten. Der Aufwand eines Lauschers auf den Funkkanälen der BOS verschiebt sich aber insgesamt vom einfachen Mithören zum gezielten Abhören.

Auch wenn digitale Funktelegramme nicht die Eigenschaften verschlüsselnder Systeme haben, ist mit ihrem Einsatz eine deutliche qualitative Verbesserung gegenüber der bisherigen Situation verbunden. Für meine Stellungnahme war somit zu prüfen, ob die Einführung neuer digitaler Systeme zeitnah zu erwarten ist oder aber die Nutzung der Funktelegramme für einige Jahre als angemessene Übergangslösung einzusetzen ist.

Da bis Mitte 2003 in den entscheidenden Gremien keinerlei Fortschritt erkennbar war, der zu einer Ausschreibung und einem damit verbundenen Zeithorizont für die Ablösung der vorhandenen Technik führen würde, habe ich mich in meiner Stellungnahme deutlich für die Nutzung der digitalen Funktelegramme ausgesprochen.

Ende des Jahres haben sich nun Bund und Länder auf eine unterschriftsreife Dachvereinbarung einigen können. Allerdings klammert die Vereinbarung, die Grundlage für eine einheitliche Ausschreibung sein wird, die Frage der endgültigen Finanzierungsverteilung zunächst aus. Offensichtlich sind alle Beteiligten bemüht, die Voraussetzungen dafür zu schaffen, dass bis zur Fußball-Weltmeisterschaft 2006 die ersten einsatzfähigen Teilnetze zur Verfügung stehen. Kritische Stimmen gehen jedoch davon aus, dass die flächendeckende Versorgung der BOS mit digitalen Funknetzen wegen des hohen Finanzierungsvolumens erst 2012 oder danach abgeschlossen sein wird.

Da die Geräteausstattung der Rettungsdienste und des Katastrophenschutzes erfahrungsgemäß eher am Ende der Beschaffungskette stehen, sehe ich mich in meiner Stellungnahme bestätigt. Heute zu beschaffende Geräte mit der notwendigen Mehrausstattung für den Einsatz von digitalen Funktelegrammen werden voraussichtlich noch rund zehn Jahre dazu beitragen, die Offenbarung personenbezogener oder -beziehbarer Daten im Sprechfunk des Rettungswesens zu vermeiden.

19. Bilanz

19.1
Übertragung der Zuständigkeit für Untersuchungen zur Dienstfähigkeit von Beamtinnen und Beamten in der hessischen Landesverwaltung auf die Versorgungsämter (31. Tätigkeitsbericht, Ziff. 19.2)

Meine Prüfungen im Zusammenhang mit der Übertragung der Zuständigkeit für Dienstunfähigkeitsuntersuchungen von den Gesundheitsämtern auf die Versorgungsverwaltung hat dazu geführt, dass das Sozialministerium im Wege einer Erlassbereinigung den durch Zeitablauf außer Kraft getretenen Erlass vom 24. Juli 1990 (StAnz. S. 1655) erneuerte. Bei den Beratungen hierzu war meine Dienststelle eingeschaltet und brachte einige datenschutzrechtliche Klarstellungen ein.

Nach wie vor problematisch ist allerdings der von mir kritisierte Sachverhalt, dass es für die Tätigkeit der Versorgungsverwaltung keine spezifische rechtliche Grundlage gibt und es bei der Umsetzung durch die Versorgungsämter an eindeutigen Vorgaben fehlt.

Die Stellungnahme der Landesregierung zu meiner Kritik an den fehlenden rechtlichen Vorgaben für die Tätigkeit der Versorgungsverwaltung einerseits und den unzureichend konzipierten Formularvordrucken zur Datenverarbeitung andererseits bleibt Wesentliches schuldig.

Zwar wird eingeräumt, dass die bislang verwendeten Unterlagen wie Einwilligungserklärungen zur Datenanforderung bei Dritten (insbesondere den Gesundheitsämtern) sowie die Unterrichtung und Erklärung auf dem Anamnesebogen voneinander getrennt und entsprechend neu formuliert werden müssen. Die Schaffung von rechtlichen Grundlagen für die Tätigkeit der Versorgungsverwaltung hält das Ministerium jedoch weiterhin nicht für erforderlich. Dabei argumentiert man, dass keinesfalls die Funktion des Amtsarztes auf die Ärzte der hessischen Versorgungsverwaltung übertragen worden sei und es sich bei den vorzunehmenden Untersuchungen ausdrücklich nicht um amtsärztliche Untersuchungen handele. Aus diesem Grund seien weder eine Änderung der beamtenrechtlichen Vorschriften des § 51 Abs. 1 HBG noch eine dem § 18a der Zweiten Durchführungsverordnung zum Gesetz über die Vereinheitlichung des Gesundheitswesens (DO-Gesundheitsämter) entsprechende Vorschrift für die Versorgungsverwaltung zu schaffen.

Diese Einschätzung vermag ich nach wie vor nicht zu teilen. Sie ist auch in sich nicht schlüssig. Grundlage für die Datenerhebung und Verarbeitung der Gesundheitsämter ist § 18a der DO-Gesundheitsämter, in dem u. a. explizit geregelt ist, in welchem Umfang medizinische Daten an die das Gutachten in Auftrag gebende Stelle weitergeleitet werden dürfen. Diese Regelung kann zwar inhaltlich auf die Versorgungsverwaltung übertragen werden, muss jedoch formell im Verordnungswege für die Versorgungsverwaltung geregelt sein. Durch eine solche Regelung hätten sich die erheblichen Irritationen, welche bei der Anforderung von Unterlagen bei den Gesundheitsämtern entstanden sind, von vornherein vermeiden lassen. Ferner hat man in der Versorgungsverwaltung bislang Vordrucke verwendet, in denen dem Betroffenen mitgeteilt wird, dass Rechtsgrundlage für die Datenverarbeitung die §§ 18 und 18a der Zweiten Durchführungsverordnung zum Gesetz über die Vereinheitlichung des Gesundheitswesens sei. Diese Mitteilung ist offensichtlich falsch und bedarf einer Korrektur, denn in diesen Vorschriften ist lediglich die Zuständigkeit der Gesundheitsämter für Dienstunfähigkeitsuntersuchungen und deren Befugnis zur Datenverarbeitung in diesem Zusammenhang geregelt. Grundlage der Datenverarbeitung der Versorgungsämter kann jedoch nur eine für die Tätigkeit der Versorgungsverwaltung geltende Rechtsgrundlage sein. Im Übrigen haben mir die Stellen, die im Rahmen meiner Prüfungen aufgesucht wurden, diese Auffassung bestätigt.

19.2
Anonymität im Internet (29. Tätigkeitsbericht, Ziff. 11.4; 30. Tätigkeitsbericht, Ziff. 6.2)

Im November 2003 bat mich das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD), bei der Staatsanwaltschaft Frankfurt die Löschung des Datensatzes eines Internetnutzers zu überprüfen. Die Staatsanwaltschaft hatte den Datensatz bei dem Anonymisierungsdienst "AN.ON – Anonymität.Online", an dem das Landeszentrum als Partner beteiligt ist, beschlagnahmt.

Die anonyme Nutzung des Internets ist bereits in früheren Tätigkeitsberichten thematisiert worden (vgl. 29. Tätigkeitsbericht, Ziff. 11.4; 30. Tätigkeitsbericht, Ziff. 6.2). Während der Internetnutzung fallen bei den Internet-Zugangsdiensteanbietern und den Internet-Diensteanbietern zahlreiche Daten über den Nutzer an. Neben den IP-Adressen können dies Angaben über Browser, Hardware, Betriebssystem und Anwendungsprogramme, eingestellte Sprache und E-Mail-Adresse, wenn sie im Browser gespeichert ist, Kennungen von Cookies und URLs besuchter Webseiten sein. Der Nutzer des Internets zieht gleichsam eine Datenspur hinter sich her, die Interessierten Auskunft über seine Aktivitäten im Netz geben kann.

Schutz dagegen bieten Anonymisierungsdienste. Sie ermöglichen das anonyme Websurfen, indem sie die Kommunikation über anonymisierende Zwischenrechner, so genannte Mixe, leiten. Das Projekt JAVA ANON PROXY (JAP) ist eine Soft- und Hardware-Entwicklung für solche Anonymisierungsdienste. Die Kommunikation bei JAP erfolgt nicht direkt zwischen den Clients und den Webservern, sondern über eine Mix-Proxy-Kaskade. Die Anonymität entsteht durch die gleichzeitige Nutzung vieler Teilnehmer. Jeder Betreiber eines Mix-Proxy-Servers verpflichtet sich zudem, keine Log-Dateien zu speichern und keine Daten mit anderen Mix-Proxy-Betreibern auszutauschen. Die Betreiber werden von unabhängigen Prüfstellen überwacht.

Die Möglichkeit zum anonymen Surfen im Internet ist gesetzlich nicht nur erlaubt, sondern sogar geboten. § 4 Abs. 6 Teledienstedatenschutzgesetz (TDDSG) bestimmt:

§ 4 Abs. 6 TDDSG

Der Diensteanbieter hat dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren.

§ 18 Abs. 6 Mediendienste-Staatsvertrag enthält für Mediendienste eine gleichlautende Vorschrift.

Wie der nachfolgende Fall zeigt, kann anonymisiertes Internetsurfen allerdings mit den Interessen der Strafverfolgungsbehörden kollidieren.

Im Juni dieses Jahres erkundigte sich das Landeskriminalamt Hessen bei den Projektpartnern des Anonymisierungsdienstes "AN.ON – Anonymität.Online", ob eine Auskunft über die IP-Adresse eines JAP-Nutzers möglich sei, gegen den wegen Besitzes von Kinderpornographie ermittelt werde. Da sich die Projektpartner verpflichtet hatten, keine Protokolle mitzuschreiben, waren für die Vergangenheit keine Daten vorhanden. Bis zu dem Zeitpunkt der Anfrage enthielt die eingesetzte Software keine Protokollfunktion. Um nicht in den Verdacht der Strafvereitelung zu kommen, entwickelte und implementiere das Projekt eine Protokollierungs-Software, die es ermöglicht, für die Zukunft Zugriffe auf eine anzugebende IP-Adresse zu protokollieren und dabei Adressen des Anfragers, Request, Datum und Uhrzeit zu erfassen.

Die Staatsanwaltschaft erwirkte im Juli 2003 eine auf die §§ 100g, 100h Strafprozessordnung (StPO) gestützte Anordnung des Amtsgerichts Frankfurt, welche die Partner des Anonymisierungsdienstes verpflichtete, den Zugriff auf eine bestimmte IP-Nummer zu protokollieren und mitzuteilen. Dagegen legte das ULD Beschwerde ein. Das Landgericht Frankfurt hob daraufhin den Beschluss auf, nachdem es zuvor bereits die Aussetzung der Vollziehung angeordnet hatte. Nach Auffassung des Gerichts regeln die Vorschriften der §§ 100g, 100h StPO nur Fälle, in denen Daten grundsätzlich aufgezeichnet und gespeichert werden, was vorliegend jedoch nicht der Fall war, denn der Anonymisierungsdienst war gerade darauf angelegt, keine personenbezogenen Daten zu erfassen. Bis zur Aussetzung der Vollziehung war mit der eingesetzten Software ein Datensatz protokolliert worden.

Nach Aussetzung der Vollziehung des Beschlusses des Amtsgerichts Frankfurt erwirkte die Staatsanwaltschaft beim Amtsgericht Frankfurt im August 2003 einen Durchsuchungsbeschluss für die Räume des "Projekts AN.ON – Anonymität.Online" an der TU Dresden. Der Direktor des Instituts für Systemarchitektur gab daraufhin den erstellten Protokolldatensatz heraus. Auf die Beschwerde der Projektbetreiber stellte das Landgericht Frankfurt am 21. Oktober 2003 fest, dass die Durchsuchungsanordnung rechtswidrig war, da sie eine Umgehung der §§ 100g, 100h StPO darstellte.

Die Betreiber des AN.ON-Projektes verlangten nunmehr von der Staatsanwaltschaft die Löschung der vorhandenen Daten in allen Akten bzw. elektronischen Dateien. Das ULD bat mich, die Löschung zu kontrollieren.

Die Staatsanwaltschaft Frankfurt weigert sich jedoch, den Datensatz zu löschen. Sie teilte mir mit, grundsätzlich würden vor Abschluss des Verfahrens keine Daten gelöscht, da sonst die Gefahr bestünde, dass ihr Manipulation der Beweismittel vorgeworfen würde. Die Tatsache, dass das Landgericht sowohl die Auskunftseinholung als auch die Durchsuchungsanordnung für rechtswidrig erklärt habe, spiele insoweit keine Rolle, dies sei lediglich eine Frage der Beweisverwertung. Es sei auch unerheblich, dass die Datenerhebung durch die Staatsanwaltschaft von Anfang an unzulässig gewesen sei. Die Staatsanwaltschaft stützt sich dabei auf die - auch von verfassungsgerichtlicher Rechtsprechung gestützte - Auffassung, dass auch ein bei einer rechtswidrigen Durchsuchung erlangtes Beweismittel grundsätzlich verwertbar sei.

Diese Rechtsauffassung ist aus datenschutzrechtlicher Sicht nicht haltbar. Die Datenerhebung war zu keinem Zeitpunkt rechtmäßig. Die Voraussetzungen für eine Auskunftserteilung nach §§ 100g, 100h StPO haben nie vorgelegen. Die Durchsuchungsanordnung wurde eingeholt zu einem Zeitpunkt, in dem die Vollziehung des Auskunftsersuchens durch das Landgericht im Rahmen des Beschwerdeverfahrens ausdrücklich ausgesetzt war. Dabei musste auch der Staatsanwaltschaft klar sein, dass, wenn das Auskunftsverlangen unzulässig war, auch eine Durchsuchung/Beschlagnahme unzulässig wäre. Ein insoweit eindeutig rechtswidrig erhobenes Datum kann nicht auf noch unabsehbare Zeit Teil der Ermittlungsunterlagen bleiben. Da dieser Vorgang eindeutig abgrenzbar vom sonstigen Ermittlungsverfahren ist, erscheint ein erfolgversprechender Vorwurf der Manipulation der Ermittlungsakten nicht denkbar. Dies ist eine Konstellation, die eine Abweichung von der grundsätzlichen Verwertbarkeit geradezu verlangt. Personenbezogene Daten sind gemäß § 19 Abs. 4 HDSG zu löschen, wenn ihre Verarbeitung unzulässig ist. Das gilt erst recht, wenn diese Verarbeitung von Anfang an unzulässig war.

Ich verkenne nicht, dass bei einer (gebotenen) rigiden Wahrung des Datenschutzes, der Datenschutz in Kollision mit legitimen Strafverfolgungsinteressen (z. B. im Zusammenhang mit der Kinderpornographie oder der Terrorismusbekämpfung) geraten kann. Der Zugriff der Staatsanwaltschaft auf Daten in Fällen der geschilderten Art erfordert präzise beschrieben Befugnisnormen, an denen es de lega lata fehlt.

19.3
Prüfung von Datensicherheitsmaßnahmen mit Hilfe eines Portscanners (30. Tätigkeitsbericht, Ziff. 14.5)

In meinem 30. Tätigkeitsbericht habe ich von Prüfergebnissen zur Datensicherheit berichtet, die ich u. a. mit Hilfe eines Portscanners erhalten hatte. Auch im letzten Jahr habe ich weitere Prüfungen vorgenommen. Im Wesentlichen haben sich die Feststellungen aus dem 30. Tätigkeitsbericht bestätigt. An einem Beispiel möchte ich jedoch erläutern, welche Konsequenzen aus den Prüfungen für mich besonders wichtig sind.

Bei einer Daten verarbeitenden Stelle habe ich alle Server gescannt, die sich in der DMZ (demilitarisierte Zone; Bereich der gegenüber dem Internet durch eine Firewall geschützt ist und sich vor dem durch eine weitere Firewall geschützte internen Netz befindet) befanden. Es handelte sich um 23 IP-Adressen, die aber nicht alle einem physischen Rechner entsprachen. Durch die Scan-Läufe wurden ca. 20 kritische und 100 mittlere Schwachstellen gefunden. Das war ein unzureichendes Ergebnis. Bei einer genaueren Untersuchung stellte sich heraus, dass etwa die Hälfte der Einstufungen in der gegebenen Konstellation, in der sich die Server hinter einer Firewall befanden, heruntergestuft werden konnten. Trotzdem waren schnelle Reaktionen erforderlich.

Nach einem Monat erreichte mich die Stellungnahme:

- Für alle Schwachstellen waren die Verantwortlichen für deren Beseitigung bestimmt. Die zu treffenden Maßnahmen waren festgelegt und der Status der Umsetzung war erfasst. Danach waren zwei Drittel der kritisch eingestuften Schwachstellen beseitigt. Der Rest sollte in der Folgewoche behoben werden und lediglich für eine kritische Schwachstelle war noch nicht terminiert, wann sie ausgeräumt sein würde. Diese Schwachstelle war aber durch Maßnahmen an anderen Stellen abgemildert worden. Bei den mittleren Schwachstellen stellte sich die Situation ähnlich dar.

- Auf organisatorischer Ebene waren die Verantwortlichkeiten geklärt. Insbesondere hatte man den Administratoren explizit die Aufgabe zugewiesen, sich über Schwachstellen und deren Behebung zu informieren. Außerdem sollten die Systeme mit Portscannern getestet werden und die gefundenen Schwachstellen beseitigt werden. Verantwortlich für die korrekte Umsetzung der Vorgaben war der Bereichsleiter für den Betrieb.

In diesem Fall war es zwar wichtig, dass für die gefundenen Schwachstellen schnell adäquate Gegenmaßnahmen ergriffen wurden, aber für die Zukunft waren die organisatorischen Änderungen noch wichtiger.

Ich werde im nächsten Jahr prüfen, ob die organisatorischen Änderungen zu einer dauerhaften Verbesserung der Lage geführt haben.

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

20.1
Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. März 2003

20.1.1
Forderungen an Bundesgesetzgeber und Bundesregierung

Immer umfassendere Datenverarbeitungsbefugnisse, zunehmender Datenhunger sowie immer weitergehende technische Möglichkeiten zur Beobachtung und Durchleuchtung der Bürgerinnen und Bürger zeichnen den Weg zu immer mehr Registrierung und Überwachung vor. Das Grundgesetz gebietet dem Staat, dem entgegenzutreten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, das Recht auf informationelle Selbstbestimmung der Bürger und Bürgerinnen, wie in den Verfassungen zahlreicher deutscher Länder und in den Vorschlägen des Europäischen Verfassungskonvents, als eigenständiges Grundrecht im Grundgesetz zu verankern.

Die Datenschutzbeauftragten werden Bundesgesetzgeber und Bundesregierung bei der Weiterentwicklung des Datenschutzes unterstützen. Sie erwarten, dass die in der Koalitionsvereinbarung enthaltenen Absichtserklärungen zur umfassenden Reform des Datenschutzrechtes in der laufenden Legislaturperiode zügig verwirklicht werden.
Sie sehen dabei folgende essentielle Punkte:

Schwerpunkte für eine Modernisierung des Bundesdatenschutzgesetzes

- Im Vordergrund muss die Stärkung der informationellen Selbstbestimmung und des Selbstdatenschutzes stehen: Jeder Mensch muss tatsächlich selbst entscheiden können, welche Datenspuren er hinterlässt und wie diese Datenspuren verwertet werden. Ausnahmen müssen so gering wie möglich gehalten und stets in einer präzise formulierten gesetzlichen Regelung festgeschrieben werden.

- Es muss im Rahmen der gegebenen Strukturunterschiede ein weitgehend gleichmäßiges Schutzniveau für den öffentlichen und den nicht öffentlichen Bereich gelten. Die Einwilligung in die Datenverarbeitung darf nicht zur Umgehung gesetzlicher Aufgaben- und Befugnisgrenzen missbraucht werden.

- Die Freiwilligkeit der Einwilligung muss gewährleistet sein.

- Vor der Nutzung von Daten für Werbezwecke muss die informierte und freie Einwilligung der Betroffenen vorliegen ("opt in" statt "opt out").

Technischer Datenschutz

Wesentliche Ziele des technischen Datenschutzes müssen darin bestehen, ein hohes Maß an Transparenz bei der Datenverarbeitung zu erreichen und den System- und Selbstdatenschutz zu stärken. Hersteller und Anbieter müssen verpflichtet werden, den Nutzerinnen und Nutzern die geeigneten Mittel zur Geltendmachung ihrer Rechte auch auf technischem Wege zur Verfügung zu stellen.

Realisierung von Audit und Gütesiegel als marktwirtschaftliche Elemente im Datenschutz

Bislang ist das Datenschutzrecht in Deutschland in erster Linie als Ordnungsrecht ausgestaltet. Seine Einhaltung soll durch Kontrolle, Kritik und Beanstandung durchgesetzt werden. Dagegen fehlen Anreize für Firmen und Behörden, vorbildliche Datenschutzkonzepte zu verwirklichen. Mit dem Datenschutzaudit könnte Firmen und Behörden ein gutes Datenschutzkonzept bestätigt werden und es würde ihnen die Möglichkeit eröffnen, damit zu werben. Das Gütesiegel ist ein Anreiz, IT-Produkte von vornherein datenschutzgerecht zu gestalten und damit Marktvorteile zu erringen.

Eine datenschutzkonforme Technikgestaltung ist eine wichtige Voraussetzung für einen effizienten Datenschutz. Audit und Gütesiegel würden die Aufmerksamkeit auf das Thema Datenschutz lenken und so die stärkere Einbeziehung von Kundinnen und Kunden fördern. Deshalb müssen die noch ausstehenden gesetzlichen Regelungen zur Einführung des im Bundesdatenschutzgesetz vorgesehenen Datenschutzaudits umgehend geschaffen werden.

Förderung von datenschutzgerechter Technik

Die Verwirklichung des Grundrechtsschutzes hängt nicht allein von Gesetzen ab. Auch die Gestaltung der Informationstechnik hat großen Einfluss auf die Möglichkeit für alle Menschen, ihr Recht auf informationelle Selbstbestimmung auszuüben. Bislang spielt das Thema Datenschutz bei den öffentlichen IT-Entwicklungsprogrammen allenfalls eine untergeordnete Rolle. Neue IT-Produkte werden nur selten unter dem Blickwinkel entwickelt, ob sie datenschutzgerecht, datenschutzfördernd oder wenigstens nicht datenschutzgefährdend sind.

Notwendig ist, dass Datenschutz zu einem Kernpunkt im Anforderungsprofil für öffentliche IT-Entwicklungsprogramme wird.

Datenschutzgerechte Technik stellt sich nicht von alleine ein, sondern bedarf auch der Förderung durch Anreize. Neben der Entwicklung von Schutzprofilen und dem Angebot von Gütesiegeln kommt vor allem die staatliche For-

schungs- und Entwicklungsförderung in Betracht. Die Entwicklung datenschutzgerechter Informationstechnik muss zu einem Schwerpunkt staatlicher Forschungsförderung gemacht werden.

Anonyme Internetnutzung

Das Surfen im World Wide Web mit seinen immensen Informationsmöglichkeiten und das Versenden von E-Mails sind heute für viele selbstverständlich. Während aber in der realen Welt jeder Mensch zum Beispiel in einem Buchladen stöbern oder ein Einkaufszentrum durchstreifen kann, ohne dass sein Verhalten registriert wird, ist dies im Internet nicht von vornherein gewährleistet. Dort kann jeder Mausklick personenbezogene Datenspuren erzeugen, deren Summe zu einem aussagekräftigen Persönlichkeitsprofil und für vielfältige Zwecke (z. B. Marketing, Auswahl unter Stellenbewerbungen, Observation von Personen) genutzt werden kann. Das Recht auf Anonymität und der Schutz vor zwangsweiser Identifizierung sind in der realen Welt gewährleistet (in keiner Buchhandlung können Kundinnen und Kunden dazu gezwungen werden, einen Ausweis vorzulegen). Sie werden aber im Bereich des Internet durch Pläne für eine umfassende Vorratsspeicherung von Verbindungs- und Nutzungsdaten bedroht.

Das Recht jedes Menschen, das Internet grundsätzlich unbeobachtet zu nutzen, muss geschützt bleiben. Internet-Provider dürfen nicht dazu verpflichtet werden, auf Vorrat alle Verbindungs- und Nutzungsdaten über den betrieblichen Zweck hinaus für mögliche zukünftige Strafverfahren oder geheimdienstliche Observationen zu speichern.

Unabhängige Evaluierung der Eingriffsbefugnisse der Sicherheitsbehörden

Schon vor den Terroranschlägen des 11. September 2001 standen den deutschen Sicherheitsbehörden nach einer Reihe von Antiterrorgesetzen und Gesetzen gegen die Organisierte Kriminalität weit reichende Eingriffsbefugnisse zur Verfügung, die Datenschutzbeauftragten und Bürgerrechtsorganisationen Sorgen bereiteten:

Dies zeigen Videoüberwachung, Lauschangriff, Rasterfahndung, langfristige Aufbewahrung der Daten bei der Nutzung des Internet und der Telekommunikation, Zugriff auf Kundendaten und Geldbewegungen bei den Banken.

Durch die jüngsten Gesetzesverschärfungen nach den Terroranschlägen des 11. September 2001 sind die Freiräume für unbeobachtete individuelle oder gesellschaftliche Aktivitäten und Kommunikation weiter eingeschränkt worden. Bürgerliche Freiheitsrechte und Datenschutz dürfen nicht immer weiter gefährdet werden.

Nach der Konkretisierung der Befugnisse der Sicherheitsbehörden und der Schaffung neuer Befugnisse im Terrorismusbekämpfungsgesetz sowie in anderen gegen Ende der 14. Legislaturperiode verabschiedeten Bundesgesetzen ist vermehrt eine offene Diskussion darüber notwendig, wie der gebotene Ausgleich zwischen kollektiver Sicherheit und individuellen Freiheitsrechten so gewährleistet werden kann, dass unser Rechtsstaat nicht zum Überwachungsstaat wird. Dazu ist eine umfassende und systematische Evaluierung der im Zusammenhang mit der Terrorismusbekämpfung eingefügten Eingriffsbefugnisse der Sicherheitsbehörden notwendig.

Die Datenschutzbeauftragten halten darüber hinaus eine Erweiterung der im Terrorismusbekämpfungsgesetz vorgesehenen Pflicht zur Evaluierung der neuen Befugnisse der Sicherheitsbehörden auf andere vergleichbar intensive Eingriffsmaßnahmen – wie Telefonüberwachung, großer Lauschangriff und Rasterfahndung – für geboten.

Die Evaluierung muss durch unabhängige Stellen und an Hand objektiver Kriterien erfolgen und aufzeigen, wo zurückgeschnitten werden muss, wo Instrumente untauglich sind oder wo die negativen Folgewirkungen überwiegen. Wissenschaftliche Untersuchungsergebnisse zur Evaluation des Richtervorbehalts z. B. bei Telefonüberwachungen machen deutlich, dass der Bundesgesetzgeber Maßnahmen zur Stärkung des Richtervorbehalts – und zwar nicht nur im Bereich der Telefonüberwachung – als grundrechtssicherndes Verfahrenselement ergreifen muss.

Stärkung des Schutzes von Gesundheitsdaten

Zwar schützt die Jahrtausende alte ärztliche Schweigepflicht Kranke davor, dass Informationen über ihren Gesundheitszustand von denjenigen unbefugt weitergegeben werden, die sie medizinisch betreuen. Medizinische Daten werden aber zunehmend außerhalb des besonderen ärztlichen Vertrauensverhältnisses zu Patienten und Patientinnen verarbeitet. Telemedizin und High-Tech-Medizin führen zu umfangreichen automatischen Datenspeicherungen. Hinzu kommt ein zunehmender Druck, Gesundheitsdaten z. B. zur Einsparung von Kosten, zur Verhinderung von Arzneimittelnebenfolgen oder "zur Qualitätssicherung" einzusetzen. Die Informatisierung der Medizin durch elektronische Aktenführung, Einsatz von Chipkarten, Nutzung des Internets zur Konsultation bis hin zur ferngesteuerten Behandlung mit Robotern erfordern es deshalb, dass auch die Instrumente zum Schutz von Gesundheitsdaten weiterentwickelt werden.

Der Schutz des Patientengeheimnisses muss auch in einer computerisierten Medizin wirksam gewährleistet sein. Die Datenschutzbeauftragten begrüßen deshalb die Absichtserklärung in der Koalitionsvereinbarung, Patientenschutz und Patientenrechte auszubauen. Dabei ist insbesondere sicherzustellen, dass Gesundheitsdaten außerhalb der eigentlichen Behandlung soweit wie möglich und grundsätzlich nur anonymisiert oder pseudonymisiert verarbeitet werden dürfen, soweit die Verarbeitung im Einzelfall nicht durch ein informiertes Einverständnis gerechtfertigt ist. Das Prinzip des informierten und freiwilligen Einverständnisses ist insbesondere auch für eine Gesundheitskarte zu beachten, und zwar auch für deren Verwendung im Einzelfall.

Der Bundesgesetzgeber wird auch aufgefordert gesetzlich zu regeln, dass Patientendaten, die in Datenverarbeitungsanlagen außerhalb von Arztpraxen und Krankenhäusern verarbeitet werden, genauso geschützt sind wie die Daten in der ärztlichen Praxis.

Geprüft werden sollte schließlich, ob und gegebenenfalls wie der Schutz von Gesundheitsdaten durch Geheimhaltungspflicht, Zeugnisverweigerungsrecht und Beschlagnahmeverbot auch dann gewährleistet werden kann, wenn diese, z. B. in der wissenschaftlichen Forschung, mit Einwilligung oder auf gesetzlicher Grundlage von anderen Einrichtungen außerhalb des Bereichs der behandelnden Ärztinnen und Ärzte verarbeitet werden.

Datenschutz und Gentechnik

Die Entwicklung der Gentechnik ist atemberaubend. Schon ein ausgefallenes Haar, ein Speichelrest an Besteck oder Gläsern, abgeschürfte Hautpartikel oder ein Blutstropfen - dies alles eignet sich als Untersuchungsmaterial, um den genetischen Bauplan eines Menschen entschlüsseln zu können. Inzwischen werden Gentests frei verkäuflich angeboten. Je mehr Tests gemacht werden, desto größer wird das Risiko für jeden Menschen, dass seine genetischen Anlagen von anderen auch gegen seinen Willen analysiert werden. Versicherungen oder Arbeitgeber und Arbeitgeberinnen werden ebenfalls Testergebnisse erfahren wollen.

Niemand darf zur Untersuchung genetischer Anlagen gezwungen werden; die Durchführung eines gesetzlich nicht zugelassenen Tests ohne Wissen und Wollen der betroffenen Person und die Nutzung daraus gewonnener Ergebnisse muss unter Strafe gestellt werden.

In der Koalitionsvereinbarung ist der Erlass eines "Gen-Test-Gesetzes" vorgesehen. Ein solches Gesetz ist dringend erforderlich, damit der datenschutzgerechte Umgang mit genetischen Daten gewährleistet wird. Die Datenschutzbeauftragten haben dazu auf ihrer 62. Konferenz in Münster vom 24. bis 26. Oktober 2001 Vorschläge vorgelegt.

Datenschutz im Steuerrecht

Im bisherigen Steuer- und Abgabenrecht finden sich äußerst lückenhafte datenschutzrechtliche Regelungen. Insbesondere fehlen grundlegende Rechte, wie ein Akteneinsichts- und Auskunftsrecht. Eine Pflicht zur Information der Steuerpflichtigen über Datenerhebungen bei Dritten fehlt ganz.

Die jüngsten Gesetzesnovellen und Gesetzesentwürfe, die fortschreitende Vernetzung und multinationale Vereinbarungen verschärfen den Mangel: Immer mehr Steuerdaten sollen zentral durch das Bundesamt für Finanzen erfasst werden. Mit einheitlichen Personenidentifikationsnummern sollen Zusammenführungen und umfassende Auswertungen der Verbunddaten möglich werden. Eine erhebliche Ausweitung der Kontrollmitteilungen von Finanzbehörden und Kreditinstituten, die ungeachtet der Einführung einer pauschalen Abgeltungssteuer geplant ist, würde zweckungebundene und unverhältnismäßige Datenübermittlungen gestatten. Die zunehmende Vorratserhebung und -speicherung von Steuerdaten entspricht nicht dem datenschutzrechtlichen Grundsatz der Erforderlichkeit.

Die Datenschutzbeauftragten fordern deshalb, die Aufnahme datenschutzrechtlicher Grundsätze in das Steuerrecht jetzt anzugehen und den Betroffenen die datenschutzrechtlichen Informations- und Auskunftsrechte zuzuerkennen.

Arbeitnehmerdatenschutz

Persönlichkeitsrechte und Datenschutz sind im Arbeitsverhältnis vielfältig bedroht, zum Beispiel durch

- die Sammlung von Beschäftigtendaten in leistungsfähigen Personalinformationssystemen, die zur Erstellung von Persönlichkeitsprofilen genutzt werden,

- die Übermittlung von Beschäftigtendaten zwischen konzernangehörigen Unternehmen, für die nicht der Datenschutzstandard der EG-Datenschutzrichtlinie gilt,

- die Überwachung des Arbeitsverhaltens durch Videokameras, die Protokollierung der Nutzung von Internetdiensten am Arbeitsplatz,

- die Erhebung des Gesundheitszustands, Drogen-Screenings und psychologische Testverfahren bei der Einstellung.

Die hierzu von den Arbeitsgerichten entwickelten Schranken wirken unmittelbar nur im jeweils entschiedenen Einzelfall und sind auch nicht allen Betroffenen hinreichend bekannt. Das seit vielen Jahren angekündigte Arbeitnehmerdatenschutzgesetz muss hier endlich klare gesetzliche Vorgaben schaffen.

Die Datenschutzbeauftragten fordern deshalb, dass für die in der Koalitionsvereinbarung enthaltene Festlegung zur Schaffung von gesetzlichen Regelungen zum Arbeitnehmerdatenschutz nunmehr rasch ein ausformulierter Gesetzentwurf vorgelegt und anschließend zügig das Gesetzgebungsverfahren eingeleitet wird.

Stärkung einer unabhängigen, effizienten Datenschutzkontrolle

Die Datenschutzbeauftragten fordern gesetzliche Vorgaben, die die völlige Unabhängigkeit der Datenschutzkontrolle sichern und effektive Einwirkungsbefugnisse gewährleisten, wie dies der Art. 28 der EG-Datenschutzrichtlinie gebietet.

Die Datenschutzkontrollstellen im privaten Bereich haben bis heute nicht die völlige Unabhängigkeit, die die Europäische Datenschutzrichtlinie vorsieht. So ist in der Mehrzahl der deutschen Länder die Kontrolle über den Datenschutz im privaten Bereich nach wie vor bei den Innenministerien und nachgeordneten Stellen angesiedelt und unterliegt damit einer Fachaufsicht. Selbst in den Ländern, in denen die Landesbeauftragten diese Aufgabe wahrnehmen, ist ihre Unabhängigkeit nicht überall richtlinienkonform ausgestaltet.

Stellung des Bundesdatenschutzbeauftragten

Die rechtliche Stellung des Bundesdatenschutzbeauftragten als unabhängiges Kontrollorgan muss im Grundgesetz abgesichert werden.

Verbesserung der Informationsrechte

Die im Bereich der Informationsfreiheit tätigen Datenschutzbeauftragten unterstützen die Absicht in der Koalitionsvereinbarung, auf Bundesebene ein Informationsfreiheitsgesetz zu schaffen. Nach ihren Erfahrungen hat sich die gemeinsame Wahrnehmung der Aufgaben zum Datenschutz und zur Informationsfreiheit bewährt, weshalb sie auch auf Bundesebene realisiert werden sollte. Zusätzlich muss ein Verbraucherinformationsgesetz alle Produkte und Dienstleistungen erfassen und einen Informationsanspruch auch gegenüber Unternehmen einführen.

20.1.2
TCPA darf nicht zur Aushebelung des Datenschutzes missbraucht werden

Mit großer Skepsis sehen die Datenschutzbeauftragten des Bundes und der Länder die Pläne zur Entwicklung zentraler Kontrollmechanismen und -infrastrukturen auf der Basis der Spezifikationen der Industrie-Allianz „Trusted Computing Platform Alliance“ (**TCPA**).

Die TCPA hat sich zum Ziel gesetzt, vertrauenswürdige Personalcomputer zu entwickeln. Dazu bedarf es spezieller Hard- und Software. In den bisher bekannt gewordenen Szenarien soll die Vertrauenswürdigkeit dadurch gewährleistet werden, dass zunächst ein spezieller Kryptoprozessor nach dem Einschalten des PC überprüft, ob die installierte Hardware und das Betriebssystem mit den von der TCPA zertifizierten und auf zentralen Servern hinterlegten Konfigurationsangaben übereinstimmen. Danach übergibt der Prozessor die Steuerung an ein TCPA-konformes Betriebssystem. Beim Start einer beliebigen Anwendersoftware prüft das Betriebssystem dann deren TCPA-Konformität, beispielsweise durch Kontrolle der Lizenz oder der Seriennummer, und kontrolliert weiterhin, ob Dokumente in zulässiger Form genutzt werden. Sollte eine der Prüfungen Abweichungen zur hinterlegten, zertifizierten Konfiguration ergeben, lässt sich der PC nicht booten bzw. das entsprechende Programm wird gelöscht oder lässt sich nicht starten.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen alle Aktivitäten, die der Verbesserung des Datenschutzes dienen und insbesondere zu einer manipulations- und missbrauchssicheren sowie transparenten IT-Infrastruktur führen. Sie erkennen auch die berechtigten Forderungen der Softwarehersteller an, dass kostenpflichtige Software nur nach Bezahlung genutzt werden darf.

Wenn aber zentrale Server einer externen Kontrollinstanz genutzt werden, um mit entsprechend modifizierten Client-Betriebssystemen Prüf- und Kontrollfunktionen zu steuern, müssten sich Anwenderinnen und Anwender beim Schutz sensibler Daten uneingeschränkt auf die Vertrauenswürdigkeit der externen Instanz verlassen können. Die Datenschutzbeauftragten erachten es für unzumutbar, wenn

- Anwenderinnen und Anwender die alleinige Kontrolle über die Funktionen des eigenen Computers verlieren, falls eine externe Kontrollinstanz Hardware, Software und Daten kontrollieren und manipulieren kann,

- die Verfügbarkeit aller TCPA-konformen Personalcomputer und der darauf verarbeiteten Daten gefährdet wäre, da sowohl Fehler in der Kontrollinfrastruktur als auch Angriffe auf die zentralen TCPA-Server die Funktionsfähigkeit einzelner Rechner sofort massiv einschränken würden,

- andere Institutionen oder Personen sich vertrauliche Informationen von zentralen Servern beschaffen würden, ohne dass der Anwender dies bemerkt,

- die Nutzung von Servern oder PC davon abhängig gemacht würde, dass ein Zugang zum Internet geöffnet wird,

- der Zugang zum Internet und E-Mail-Verkehr durch Softwarerestriktionen behindert würde,

- der Umgang mit Dokumenten ausschließlich gemäß den Vorgaben der externen Kontrollinstanz zulässig sein würde und somit eine sehr weitgehende Zensur ermöglicht wird,

- auf diese Weise der Zugriff auf Dokumente von Konkurrenzprodukten verhindert und somit auch die Verbreitung datenschutzfreundlicher Open-Source-Software eingeschränkt werden kann und

- Programmergänzungen (Updates) ohne vorherige Einwilligung im Einzelfall aufgespielt werden könnten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb Hersteller von Informations- und Kommunikationstechnik auf, Hard- und Software so zu entwickeln und herzustellen, dass

- Anwenderinnen und Anwender die ausschließliche und vollständige Kontrolle über die von ihnen genutzte Informationstechnik haben, insbesondere dadurch, dass Zugriffe und Änderungen nur nach vorheriger Information und Einwilligung im Einzelfall erfolgen,

- alle zur Verfügung stehenden Sicherheitsfunktionen für Anwenderinnen und Anwender transparent sind und

- die Nutzung von Hard- und Software und der Zugriff auf Dokumente auch weiterhin möglich ist, ohne dass Dritte davon Kenntnis erhalten und Nutzungsprofile angelegt werden können.

Auf diese Weise können auch künftig die in den Datenschutzgesetzen des Bundes und der Länder geforderte Vertraulichkeit und Verfügbarkeit der zu verarbeitenden personenbezogenen Daten sichergestellt und die Transparenz bei der Verarbeitung dieser Daten gewährleistet werden.

20.1.3
Datenschutzbeauftragte fordern vertrauenswürdige Informationstechnik

Anwenderinnen und Anwender von komplexen IT-Produkten müssen unbedingt darauf vertrauen können, dass Sicherheitsfunktionen von Hard- und Software korrekt ausgeführt werden, damit die Vertraulichkeit, die Integrität und die Zurechenbarkeit der Daten gewährleistet sind. Dieses Vertrauen kann insbesondere durch eine datenschutzgerechte Gestaltung der Informationstechnik geschaffen werden. Ausbleibende Erfolge bei eCommerce und eGovernment werden mit fehlendem Vertrauen in einen angemessenen Schutz der personenbezogenen Daten und mangelnder Akzeptanz der Nutzerinnen und Nutzer erklärt. Anwenderinnen und Anwender sollten ihre Sicherheitsanforderungen präzise definieren und Anbieter ihre Sicherheitsleistungen schon vor der Produktentwicklung festlegen und für alle nachprüfbar dokumentieren. Die Datenschutzbeauftragten des Bundes und der Länder wollen Herstellerinnen und Hersteller und Anwenderinnen und Anwender von Informationstechnik unterstützen, indem sie entsprechende Werkzeuge und Hilfsmittel zur Verfügung stellen.

So bietet der Bundesbeauftragte für den Datenschutz seit dem 11. November 2002 mit zwei so genannten Schutzprofilen (Protection Profiles) Werkzeuge an, mit deren Hilfe Anwenderinnen und Anwender bereits vor der Produktentwicklung ihre datenschutzspezifischen Anforderungen für bestimmte Produkttypen beispielsweise im Gesundheitswesen oder im eGovernment detailliert beschreiben können. Kerngedanke der in diesen Schutzprofilen definierten Sicherheitsanforderungen ist die Kontrollierbarkeit aller Informationsflüsse eines Rechners gemäß einstellbarer Informationsflussregeln. Die Schutzprofile sind international anerkannt, da sie auf der Basis der "Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria)" entwickelt wurden. Herstellerinnen und Hersteller können datenschutzfreundliche Produkte somit nach international prüffähigen Vorgaben der Anwenderinnen und Anwender entwickeln. Unabhängige Prüfinstitutionen können diese Produkte dann nach Abschluss der Entwicklung nach international gültigen Kriterien prüfen. [1]

In Schleswig-Holstein bietet das Unabhängige Landeszentrum für Datenschutz ein Verfahren mit vergleichbarer Zielsetzung an, das ebenfalls zu überprüfbarer Sicherheit von IT-Produkten führt. Für nachweislich datenschutzgerechte IT-Produkte können Hersteller ein so genanntes Datenschutz-Gütesiegel erhalten. Das Landeszentrum hat auf der Grundlage landesspezifischer Rechtsvorschriften bereits im Jahr 2002 einen entsprechenden Anforderungskatalog veröffentlicht und zur CeBIT 2003 eine an die Common Criteria angepasste Version vorgestellt. [2]

Die Datenschutzbeauftragten des Bundes und der Länder empfehlen die Anwendung von Schutzprofilen und Auditierungsprozeduren, damit auch der Nutzer oder die Nutzerin beurteilen kann, ob IT-Systeme und -Produkte vertrauenswürdig und datenschutzfreundlich sind. Sie appellieren an die Hersteller, entsprechende Produkte zu entwickeln bzw. vorhandene Produkte anhand bereits bestehender oder gleichwertiger Schutzprofile und Anforderungskataloge zu modifizieren. Sie treten dafür ein, dass die öffentliche Verwaltung vorrangig solche Produkte einsetzt.

20.1.4
Datenschutzrechtliche Rahmenbedingungen zur Modernisierung des Systems der gesetzlichen Krankenversicherung

In der Diskussion über eine grundlegende Reform des Rechts der gesetzlichen Krankenversicherung (GKV) werden in großem Maße datenschutzrechtliche Belange berührt. Erweiterte Befugnisse zur Verarbeitung von medizinischen Leistungs- und Abrechnungsdaten sollen eine stärkere Kontrolle der Patientinnen und Patienten sowie der sonstigen beteiligten Parteien ermöglichen. Verbesserte individuelle und statistische Informationen sollen zudem die medizinische und informationelle Selbstbestimmung der Patientinnen und Patienten verbessern sowie die Transparenz für die Beteiligten und für die Öffentlichkeit erhöhen.

---

[1] Die Schutzprofile mit dem Titel „BISS – Benutzerbestimmbare Informationsflusskontrolle“ haben die Registrierungskennzeichen BSI-PP-0007-2002 und BSI-PTT-008-2002 und sind beim Bundesbeauftragten für den Datenschutz unter http://www.bfd.bund.de/technik/protection_profile.html abrufbar.

[2] Die Ergebnisse der bisherigen Auditierungen durch das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein sind unter http://www.datenschutzzentrum.de/guetesiegel veröffentlicht.

So sehen Vorschläge des Bundesministeriums für Gesundheit und Soziale Sicherung zur Modernisierung des Gesundheitswesens u. a. vor, dass bis zum Jahr 2006 schrittweise eine elektronische Gesundheitskarte eingeführt wird und Leistungs- und Abrechnungsdaten zusammengeführt werden sollen. Boni für gesundheitsbewusstes Verhalten und Ausnahmen oder Mali für gesundheitsgefährdendes Verhalten sollen medizinisch rationales Verhalten der Versicherten fördern, was eine Überprüfung dieses Verhaltens voraussetzt. Derzeit werden gesetzliche Regelungen ausgearbeitet.

Die Datenschutzbeauftragten des Bundes und der Länder weisen erneut auf die datenschutzrechtlichen Chancen und Risiken einer Modernisierung des Systems der GKV hin.

Viele Vorschläge zielen darauf ab, Gesundheitskosten dadurch zu reduzieren, dass den Krankenkassen mehr Kontrollmöglichkeiten eingeräumt werden. Solche individuellen Kontrollen können indes nur ein Hilfsmittel zu angestrebten Problemlösungen, nicht aber die Problemlösung selbst sein. Sie sind auch mit dem Recht der Patientinnen und Patienten auf Selbstbestimmung und dem Schutz der Vertrauensbeziehung zwischen ärztlichem Personal und behandelten Personen nicht problemlos in Einklang zu bringen. Eingriffe müssen nach den Grundsätzen der Datenvermeidung und der Erforderlichkeit und Verhältnismäßigkeit auf ein Minimum beschränkt bleiben. Möglichkeiten der anonymisierten oder pseudonymisierten Verarbeitung von Patientendaten müssen ausgeschöpft werden. Eine umfassendere Information der Patientinnen und Patienten, die zu mehr Transparenz führt und die Verantwortlichkeiten verdeutlicht, ist ebenfalls ein geeignetes Hilfsmittel.

Sollte im Rahmen gesetzlicher Regelungen zur Qualitätssicherung und Abrechnungskontrolle für einzelne Bereiche der Zugriff auf personenbezogene Behandlungsdaten unerlässlich sein, müssen Vorgaben entwickelt werden, die

- den Zugriff auf genau festgelegte Anwendungsfälle begrenzen,
- das Prinzip der Stichprobe zugrunde legen,
- eine strikte Einhaltung der Zweckbindung gewährleisten und
- die Auswertung der Daten einer unabhängigen Stelle übertragen.

1. Die Datenschutzbeauftragten erkennen die Notwendigkeit einer verbesserten Datenbasis zur Weiterentwicklung der gesetzlichen Krankenversicherung an. Hierzu reichen wirksam pseudonymisierte Daten grundsätzlich aus. Eine Zusammenführung von Leistungs- und Versichertendaten darf nicht dazu führen, dass über eine lückenlose zentrale Sammlung personenbeziehbarer Patientendaten mit sensiblen Diagnose- und Behandlungsangaben z. B. zur Risikoselektion geeignete medizinische Profile entstehen. Dies könnte nicht nur zur Diskriminierung einzelner Versicherter führen, sondern es würde auch die sozialstaatliche Errungenschaft des solidarischen Tragens von Krankheitsrisiken aufgegeben. Zudem wären zweckwidrige Auswertungen möglich, für die es viele Interessierte gäbe, von Privatversicherungen bis hin zu Arbeitgebern. Durch sichere technische und organisatorische Verfahren, die Pseudonymisierung der Daten und ein grundsätzliches sanktionsbewehrtes Verbot der Reidentifizierung pseudonymisierter Datenbestände kann solchen Gefahren entgegengewirkt werden.

2. Die Einführung einer Gesundheitschipkarte kann die Transparenz des Behandlungsgeschehens für die Patientinnen und Patienten erhöhen, deren schonende und erfolgreiche medizinische Behandlung effektivieren und durch Vermeidung von Medienbrüchen und Mehrfachbehandlungen Kosten senken. Eine solche Karte kann aber auch dazu genutzt werden, die Selbstbestimmungsrechte der Patientinnen und Patienten zu verschlechtern. Dieser Effekt würde durch eine Pflichtkarte eintreten, auf der – von den Betroffenen nicht beeinflussbar – Diagnosen und Medikationen zur freien Einsicht durch Ärztinnen und Ärzte sowie sonstige Leistungserbringende gespeichert wären. Zentrales Patientenrecht ist es, selbst zu entscheiden, welchem Arzt oder welcher Ärztin welche Informationen anvertraut werden.

   Die Datenschutzkonferenz fordert im Fall der Einführung einer Gesundheitschipkarte die Gewährleistung des Rechts der Patientinnen und Patienten, grundsätzlich selbst zu entscheiden,

   - ob sie überhaupt verwendet wird,
   - welche Daten darauf gespeichert werden oder über sie abgerufen werden können,
   - welche Daten zu löschen sind und wann das zu geschehen hat,
   - ob sie im Einzelfall vorgelegt wird und
   - welche Daten im Einzelfall ausgelesen werden sollen.

   Sicherzustellen ist weiterhin

   - ein Beschlagnahmeverbot und Zeugnisverweigerungsrecht, in Bezug auf die Daten, die auf der Karte gespeichert sind,
   - die Beschränkung der Nutzung auf das Patienten-Arzt/Apotheken-Verhältnis und
   - die Strafbarkeit des Datenmissbrauchs.

   Die Datenschutzkonferenz hat bereits zu den datenschutzrechtlichen Anforderungen an den "Arzneimittelpass" (Medikamentenchipkarte) ausführlich Stellung genommen (Entschließung vom 26. Oktober 2001). Die dort formulierten Anforderungen an eine elektronische Gesundheitskarte sind weiterhin gültig. Die „Gemeinsame Erklärung des Bundesministeriums für Gesundheit und der Spitzenorganisationen zum Einsatz von Telematik im Gesundheitswesen“ vom 3. Mai 2002, wonach "der Patient Herr seiner Daten" sein soll, enthält gute Ansatzpunkte, auf deren Basis die Einführung einer Gesundheitskarte betrieben werden kann.

3. Die Datenschutzbeauftragten anerkennen die Förderung wirtschaftlichen und gesundheitsbewussten Verhaltens als ein wichtiges Anliegen. Dies darf aber nicht dazu führen, dass die Krankenkassen detaillierte Daten über die private Lebensführung erhalten ("fährt Ski", "raucht", "trinkt zwei Biere pro Tag"), diese überwachen und so zur "Gesundheits-

polizei" werden. Notwendig ist deshalb die Entwicklung von Konzepten, die ohne derartige mitgliederbezogene Datensätze bei den Krankenkassen und ihre Überwachung auskommen.

4. Die Datenschutzbeauftragten begrüßen alle Pläne, die darauf hinauslaufen, das Verfahren der GKV allgemein sowie die individuelle Behandlung und Datenverarbeitung für die Betroffenen transparenter zu machen. Maßnahmen wie die Einführung der Patientenquittung, die Information über das Leistungsverfahren und über Umfang und Qualität des Leistungsangebotes sowie eine verstärkte Einbindung der Patientinnen und Patienten durch Unterrichtungen und Einwilligungserfordernisse stärken die Patientensouveränität und die Selbstbestimmung.

20.1.5
Kennzeichnung von Daten aus besonders eingriffsintensiven Erhebungen

Das Bundesverfassungsgericht hat in seinem Urteil zur strategischen Fernmeldeüberwachung des Bundesnachrichtendienstes festgestellt, dass sich die Zweckbindung der bei dieser Maßnahme erlangten personenbezogenen Daten nur gewährleisten lässt, wenn auch nach ihrer Erfassung erkennbar bleibt, dass es sich um Daten handelt, die aus Eingriffen in das Fernmeldegeheimnis stammen. Eine entsprechende Kennzeichnung ist daher von Verfassung wegen geboten. Dementsprechend wurde die Kennzeichnungspflicht in der Novellierung des G 10-Gesetzes auch allgemein für jede Datenerhebung des Bundesnachrichtendienstes und des Verfassungsschutzes im Schutzbereich des Art. 10 GG angeordnet.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die Pflicht zur Kennzeichnung auf Grund der Ausführungen des Bundesverfassungsgerichts nicht auf den Bereich der Fernmeldeüberwachung beschränkt ist. Sie gilt auch für vergleichbare Methoden der Datenerhebung, bei denen die Daten durch besonders eingriffsintensive Maßnahmen gewonnen werden und deswegen einer strikten Zweckbindung unterliegen müssen.

Deshalb müssen zumindest solche personenbezogenen Daten, die aus einer Telefon-, Wohnraum- oder Postüberwachung erlangt wurden, besonders gekennzeichnet werden.

20.1.6
Elektronische Signatur im Finanzbereich

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass mit dem Signaturgesetz und der Anpassung von mehr als 3.000 Rechtsvorschriften in Deutschland die rechtlichen Voraussetzungen geschaffen wurden, um die "qualifizierte elektronische Signatur" der eigenhändigen Unterschrift gleichzustellen. Die administrativen und technischen Voraussetzungen sind inzwischen weitgehend vorhanden. Mehr als 20 freiwillig akkreditierte Zertifizierungsdiensteanbieter nach dem Signaturgesetz sind von der Regulierungsbehörde für Telekommunikation und Post (RegTP) zugelassen. Sowohl Chipkarten, die für die qualifizierte elektronische Signatur zugelassen sind, als auch die dafür erforderlichen Lesegeräte sind verfügbar.

Für die elektronische Kommunikation zwischen der Finanzverwaltung und den Bürgerinnen und Bürgern ist die "qualifizierte elektronische Signatur" gesetzlich vorgeschrieben. Die Finanzverwaltung will eine Übergangsbestimmung in der Steuerdatenübermittlungsverordnung vom 28. Januar 2003 nutzen, nach der bis Ende 2005 eine lediglich fortgeschrittene, die so genannte "qualifizierte elektronische Signatur mit Einschränkungen" eingesetzt werden kann. Aus folgenden Gründen lehnen die Datenschutzbeauftragten dieses Vorgehen ab:

- Die "qualifizierte elektronische Signatur mit Einschränkungen" bietet im Gegensatz zur "qualifizierten elektronischen Signatur" und der "qualifizierten elektronischen Signatur mit Anbieterakkreditierung" keine umfassend nachgewiesene Sicherheit, vor allem aber keine langfristige Überprüfbarkeit. Die mit ihr unterzeichneten elektronischen Dokumente sind unerkannt manipulierbar. Die "qualifizierte elektronische Signatur mit Einschränkungen" hat geringeren Beweiswert als die eigenhändige Unterschrift.

- Die technische Infrastruktur, die die Finanzverwaltung für die "qualifizierte elektronische Signatur mit Einschränkungen" vorgesehen hat, kann sie verwenden, um elektronische, fortgeschritten oder qualifiziert signierte Dokumente von Bürgerinnen und Bürgern und Steuerberaterinnen und Steuerberatern zu prüfen und selbst fortgeschrittene Signaturen zu erzeugen. Damit die Finanzverwaltung selbst qualifiziert signieren kann, reicht eine Ergänzung mit einem qualifizierten Zertifikat aus.
- Für die elektronische Steuererklärung ELSTER sollen Zertifizierungsdienste im außereuropäischen Ausland zugelassen werden, für die weder eine freiwillige Akkreditierung noch eine Kontrolle durch deutsche Datenschutzbehörden möglich ist, anstatt Zertifizierungsdienste einzuschalten, die der Europäischen Datenschutzrichtlinie entsprechen. Damit sind erhebliche Gefahren verbunden, die vermeidbar sind.

- Die elektronische Signatur soll auch zur Authentisierung der Steuerpflichtigen und Steuerberater gegenüber ELSTER genutzt werden, obwohl die Trennung der Schlüsselpaare für Signatur und Authentisierung unerlässlich und bereits Stand der Technik ist.

Die Datenschutzbeauftragten des Bundes und der Länder befürchten, dass bei Schaffung weiterer Signaturverfahren mit geringerer Sicherheit die Transparenz für die Anwenderinnen und Anwender verloren geht und der sichere und verlässliche elektronische Rechts- und Geschäftsverkehr in Frage gestellt werden könnte.
Abweichend vom Vorgehen der Finanzverwaltung hat sich die Bundesregierung sowohl im Rahmen der Initiative "Bund Online 2005" als auch im so genannten Signaturbündnis für sichere Signaturverfahren eingesetzt. Das Verfahren ELSTER sollte genutzt werden, um sogleich qualifizierten und damit sicheren Signaturen zum Durchbruch zu verhelfen.

Vor diesem Hintergrund empfiehlt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder der Bundesregierung,

- dass die Finanzbehörden Steuerbescheide und sonstige Dokumente ausschließlich qualifiziert signiert versenden,
- den Bürgerinnen und Bürgern eine sichere, zuverlässige, leicht einsetzbare und transparente Technologie zur Verfügung zu stellen,
- unterschiedliche Ausstattungen für abgestufte Qualitäten und Anwendungsverfahren zu vermeiden,
- die Anschaffung von Signaturerstellungseinheiten mit zugehörigen Zertifikaten und ggf. Signaturanwendungskomponenten für "qualifizierte elektronische Signaturen mit Anbieterakkreditierung" staatlich zu fördern,
- die vorhandenen Angebote der deutschen und sonstigen europäischen Anbieter vornehmlich heranzuziehen, um die qualifizierte elektronische Signatur und den Einsatz entsprechender Produkte zu fördern,
- eGovernment- und eCommerce-Projekte zu fördern, die qualifizierte elektronische Signaturen unterhalb der Wurzelzertifizierungsinstanz der RegTP einsetzen und somit Multifunktionalität und Interoperabilität gewährleisten,
- die Entwicklung von technischen Standards für die umfassende Einbindung der qualifizierten elektronischen Signatur zu fördern,
- die Weiterentwicklung der entsprechenden Chipkartentechnik voranzutreiben.

20.1.7
Transparenz bei der Telefonüberwachung

Nach derzeitigem Recht haben die Betreiber von Telekommunikationsanlagen eine Jahresstatistik über die von ihnen zu Strafverfolgungszwecken durchgeführten Überwachungsmaßnahmen zu erstellen. Diese Zahlen werden von der Regulierungsbehörde für Telekommunikation und Post veröffentlicht. Auf diese Weise wird die Allgemeinheit über Ausmaß und Entwicklung der Telekommunikationsüberwachung in Deutschland informiert.

Nach aktuellen Plänen der Bundesregierung soll diese Statistik abgeschafft werden. Begründet wird dies mit einer Entlastung der Telekommunikationsunternehmen von überflüssigen Arbeiten. Zudem wird darauf verwiesen, dass das Bundesjustizministerium eine ähnliche Statistik führt, die sich auf Zahlen der Landesjustizbehörden stützt. Dabei wird verkannt, das die beiden Statistiken unterschiedliches Zahlenmaterial berücksichtigen. So zählen die Telekommunikationsunternehmen jede Überwachungsmaßnahme getrennt nach den einzelnen Anschlüssen, während von den Landesjustizverwaltungen nur die Anzahl der Strafverfahren erfasst wird.

In den vergangenen Jahren ist die Zahl der überwachten Anschlüsse um jährlich etwa 25 v.H. gestiegen. Gab es im Jahr 1998 noch 9.802 Anordnungen, waren es im Jahr 2001 bereits 19.896. Diese stetige Zunahme von Eingriffen in das Fernmeldegeheimnis sehen die Datenschutzbeauftragten des Bundes und der Länder mit großer Sorge. Eine fundierte und objektive Diskussion in Politik und Öffentlichkeit ist nur möglich, wenn die tatsächliche Anzahl von Telefonüberwachungsmaßnahmen bekannt ist. Allein eine Aussage über die Anzahl der Strafverfahren, in denen eine Überwachungsmaßnahme stattgefunden hat, reicht nicht aus. Nur die detaillierten Zahlen, die derzeit von den Telekommunikationsunternehmen erhoben werden, sind aussagekräftig genug.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine Beibehaltung der Unternehmensstatistik nach § 88 Absatz 5 Telekommunikationsgesetz sowie ihre Erstreckung auf die Zahl der Auskünfte über Telekommunikationsverbindungen, um auf diesem Wege bessere Transparenz bei der Telefonüberwachung zu schaffen.

20.2
Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 28. April 2003

20.2.1
Verbesserung statt Absenkung des Datenschutzniveaus in der Telekommunikation

Im Zuge der bevorstehenden Novellierung des Telekommunikationsgesetzes plant die Bundesregierung neben der Abschaffung der Unternehmensstatistik (vgl. dazu Entschließung der 65. Konferenz vom 28. März 2003 zur Transparenz bei der Telefonüberwachung) eine Reihe weiterer Änderungen, die zu einer Absenkung des gegenwärtigen Datenschutzniveaus führen würden.

Zum einen ist vorgesehen, die Zweckentfremdung von Bestandsdaten der Telekommunikation (z. B. Art des Anschlusses, Kontoverbindung, Befreiung vom Telefonentgelt aus sozialen oder gesundheitlichen Gründen) für Werbezwecke weitergehend als bisher schon dann zuzulassen, wenn der Betroffene dem nicht widerspricht. Dies muss – wie bisher – die informierte Einwilligung des Betroffenen voraussetzen.

Außerdem plant die Bundesregierung, Daten, die den Zugriff auf Inhalte oder Informationen über die näheren Umstände der Telekommunikation schützen (wie z. B. PINs und PUKs – Personal Unblocking Keys –), in Zukunft der Beschlagnahme für die Verfolgung beliebiger Straftaten zugänglich zu machen. Bisher kann der Zugriff auf solche Daten nur angeord-

net werden, wenn es um die Aufklärung bestimmter schwerer Straftaten geht. Diese Absenkung oder gar Aufhebung der verfassungsmäßig gebotenen Schutzschwelle für Daten, die dem Telekommunikationsgeheimnis unterliegen, wäre nicht gerechtfertigt; dies ergibt sich auch aus dem Urteil des Bundesverfassungsgerichts vom 12. März 2003.

Aus der Sicht des Datenschutzes ist auch die Versagung eines anonymen Zugangs zum Mobilfunk problematisch. Die beabsichtigte Gesetzesänderung führt dazu, dass z. B. der Erwerb eines "vertragslosen" Handys, das mit einer entsprechenden – im Prepaid-Verfahren mit Guthaben aufladbaren – SIM-Karte ausgestattet ist, einem Identifikationszwang unterliegt. Dies hat zur Folge, dass die Anbieter von Prepaid-Verfahren eine Reihe von Daten wegen eines möglichen Zugriffs der Sicherheitsbehörden auf Vorrat speichern müssen, die sie für ihre Betriebszwecke nicht benötigen. Die verdachtslose routinemäßige Speicherung zu Zwecken der Verfolgung eventueller, noch gar nicht absehbarer künftiger Straftaten würde auch zur Entstehung von selbst für die Sicherheitsbehörden sinn- und nutzlosen Datenhalden führen. So sind erfahrungsgemäß z. B. die Erwerber häufig nicht mit den tatsächlichen Nutzern der Prepaid-Angebote identisch.

Insgesamt fordern die Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber auf, das gegenwärtige Datenschutzniveau bei der Telekommunikation zu verbessern, statt es weiter abzusenken. Hierzu sollte jetzt ein eigenes Telekommunikations-Datenschutzgesetz verabschiedet werden, das den Anforderungen einer freiheitlichen Informationsgesellschaft genügt und später im Zuge der noch ausstehenden zweiten Stufe der Modernisierung des Bundesdatenschutzgesetzes mit diesem zusammengeführt werden könnte.

20.3
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 30. April 2003

20.3.1
Neuordnung der Rundfunkfinanzierung

Die Länder bereiten gegenwärtig eine Neuordnung der Rundfunkfinanzierung vor, die im neuen Rundfunkgebührenstaatsvertrag geregelt werden soll. Die dazu bekannt gewordenen Vorschläge der Rundfunkanstalten lassen befürchten, dass bei ihrer Umsetzung die bestehenden datenschutzrechtlichen Defizite nicht nur beibehalten werden, sondern dass mit zum Teil gravierenden Verschlechterungen des Datenschutzes gerechnet werden muss:

- Insbesondere ist geplant, alle Meldebehörden zu verpflichten, der GEZ zum In-Kraft-Treten des neuen Staatsvertrages die Daten aller Personen in Deutschland zu übermitteln, die älter als 16 Jahre sind. Dadurch entstünde bei der GEZ faktisch ein bundesweites zentrales Register aller über 16-jährigen Personen mit Informationen über ihre sozialen Verhältnisse (wie Partnerschaften, gesetzliche Vertretungen, Haushaltszugehörigkeit und Empfang von Sozialleistungen), obwohl ein großer Teil dieser Daten zu keinem Zeitpunkt für den Einzug der Rundfunkgebühren erforderlich ist.

- Auch wenn in Zukunft nur noch für ein Rundfunkgerät pro Wohnung Gebühren gezahlt werden, sollen alle dort gemeldeten erwachsenen Bewohner von vornherein zur Auskunft verpflichtet sein, selbst wenn keine Anhaltspunkte für eine Gebührenpflicht bestehen. Für die Auskunftspflicht reicht es demgegenüber aus, dass zunächst – wie bei den amtlichen Statistiken erfolgreich praktiziert – nur die Meldedaten für eine Person übermittelt werden, die dazu befragt wird.

- Zudem soll die regelmäßige Übermittlung aller Zu- und Wegzüge aus den Meldedaten nun um Übermittlungen aus weiteren staatlichen bzw. sonstigen öffentlichen Dateien wie den Registern von berufsständischen Kammern, den Schuldnerverzeichnissen und dem Gewerbezentralregister erweitert werden. Auf alle diese Daten will die die GEZ künftig auch online zugreifen.

- Gleichzeitig soll die von den zuständigen Landesdatenschutzbeauftragten als unzulässig bezeichnete Praxis der GEZ, ohne Wissen der Bürgerinnen und Bürger deren personenbezogene Daten bei Dritten – wie beispielsweise in der Nachbarschaft oder bei privaten Adresshändlern – zu erheben, ausdrücklich erlaubt werden.

- Schließlich sollen die bisher bestehenden Möglichkeiten der Aufsicht durch die Landesbeauftragten für den Datenschutz ausgeschlossen werden, sodass für die Rundfunkanstalten und die GEZ insoweit nur noch eine interne Datenschutzkontrolle beim Rundfunkgebühreneinzug bestünde.

Diese Vorstellungen der Rundfunkanstalten widersprechen dem Verhältnismäßigkeitsprinzip und sind daher nicht akzeptabel.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen ihre Forderung nach einer grundlegenden Neuorientierung der Rundfunkfinanzierung, bei der datenschutzfreundliche Modelle zu bevorzugen sind. Sie haben hierzu bereits praktikable Vorschläge vorgelegt.

20.4
Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 16. Juli 2003

20.4.1
Bei der Erweiterung der DNA-Analyse Augenmaß bewahren

Derzeit gibt es mehrere politische Absichtserklärungen und Gesetzesinitiativen mit dem Ziel, die rechtlichen Schranken in § 81g StPO für die Entnahme und Untersuchung von Körperzellen und für die Speicherung der dabei gewonnenen DNA-

Identifizierungsmuster (sog. genetischer Fingerabdruck) in der zentralen DNA-Analyse-Datei des BKA abzusenken. Die Vorschläge gehen dahin,

- zum einen als Anlasstat zur Anordnung einer DNA-Analyse künftig nicht mehr - wie vom geltenden Recht gefordert - in jedem Fall eine Straftat von erheblicher Bedeutung oder - wie jüngst vom Bundestag beschlossen - eine Straftat gegen die sexuelle Selbstbestimmung zu verlangen, sondern auch jede andere Straftat mit sexuellem Hintergrund oder sogar jedwede Straftat ausreichen zu lassen,

- zum anderen die auf einer eigenständigen, auf den jeweiligen Einzelfall bezogenen Gefahrenprognose beruhende Anordnung durch Richterinnen und Richter entfallen zu lassen und alle Entscheidungen der Polizei zu übertragen.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass die Anordnung der Entnahme und Untersuchung von Körperzellen zur Erstellung und Speicherung eines genetischen Fingerabdrucks einen tief greifenden und nachhaltigen Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen darstellt; dies hat auch das Bundesverfassungsgericht in seinen Beschlüssen vom Dezember 2000 und März 2001 bestätigt.

Selbst wenn bei der DNA-Analyse nach der derzeitigen Rechtslage nur die nicht-codierenden Teile untersucht werden: Schon daraus können Zusatzinformationen gewonnen werden (Geschlecht, Altersabschätzung, Zuordnung zu bestimmten Ethnien, möglicherweise einzelne Krankheiten wie Diabetes, Klinefelter-Syndrom). Auch deshalb lässt sich ein genetischer Fingerabdruck mit einem herkömmlichen Fingerabdruck nicht vergleichen. Zudem ist immerhin technisch auch eine Untersuchung des codierenden Materials denkbar, so dass zumindest die abstrakte Eignung für viel tiefer gehende Erkenntnisse gegeben ist. Dies bedingt unabhängig von den gesetzlichen Einschränkungen ein höheres abstraktes Gefährdungspotential.

Ferner ist zu bedenken, dass das Ausstreuen von Referenzmaterial (z. B. kleinste Hautpartikel oder Haare), das mit dem gespeicherten Identifizierungsmuster abgeglichen werden kann, letztlich nicht zu steuern ist, so dass in höherem Maß als bei Fingerabdrücken die Gefahr besteht, dass genetisches Material einer Nichttäterin oder eines Nichttäters an Tatorten auch zufällig, durch nicht wahrnehmbare Kontamination mit Zwischenträgern oder durch bewusste Manipulation platziert wird. Dies kann für Betroffene im Ergebnis zu einer Art Umkehr der Beweislast führen.

Angesichts dieser Wirkungen und Gefahrenpotentiale sehen die Datenschutzbeauftragten Erweiterungen des Einsatzes der DNA-Analyse kritisch und appellieren an die Regierungen und Gesetzgeber des Bundes und der Länder, die Diskussion dazu mit Augenmaß und unter Beachtung der wertsetzenden Bedeutung des Rechts auf informationelle Selbstbestimmung zu führen. Die DNA-Analyse darf nicht zum Routinewerkzeug jeder erkennungsdienstlichen Behandlung und damit zum alltäglichen polizeilichen Eingriffsinstrument im Rahmen der Aufklärung und Verhütung von Straftaten jeder Art werden. Auf das Erfordernis der Prognose erheblicher Straftaten als Voraussetzung einer DNA-Analyse darf nicht verzichtet werden.

Im Hinblick auf die Eingriffsschwere ist auch der Richtervorbehalt für die Anordnung der DNA-Analyse unverzichtbar. Es ist deshalb auch zu begrüßen, dass zur Stärkung dieser grundrechtssichernden Verfahrensvorgabe für die Anordnungsentscheidung die Anforderungen an die Begründung des Gerichts gesetzlich präzisiert wurden. Zudem sollte die weit verbreitete Praxis, DNA-Analysen ohne richterliche Entscheidung auf der Grundlage der Einwilligung der Betroffenen durchzuführen, gesetzlich ausgeschlossen werden.

20.5
Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 7. August 2003

20.5.1
Zum automatischen Software-Update

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die zunehmenden Bestrebungen von Softwareherstellern, über das Internet unbemerkt auf die Personalcomputer der Nutzerinnen und Nutzer zuzugreifen.

Zur Gewährleistung der Sicherheit und der Aktualität von System- und Anwendungssoftware ist es notwendig, regelmäßig Updates vorzunehmen. Weltweit agierende Softwarehersteller bieten in zunehmendem Maße an, im Rahmen so genannter Online-Updates komplette Softwarepakete oder einzelne Updates über das Internet auf die Rechner ihrer Kunden zu laden und automatisch zu installieren. Diese Verfahren bergen erhebliche Datenschutzrisiken in sich:

- Immer öfter werden dabei - oftmals vom Nutzer unbemerkt oder zumindest nicht transparent - Konfigurationsinformationen mit personenbeziehbaren Daten aus dem Zielrechner ausgelesen und an die Softwarehersteller übermittelt, ohne das dies im derzeit praktizierten Umfang aus technischen Gründen erforderlich ist.

- Darüber hinaus bewirken Online-Updates vielfach Änderungen an der Software der Zielrechner, die dann in der Regel ohne die erforderlichen Tests und Freigabeverfahren genutzt werden.

- Ferner ist nicht immer sichergestellt, dass andere Anwendungen problemlos weiter funktionieren. Das - unbemerkte - Update wird dann nicht als Fehlerursache erkannt.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass Änderungen an automatisierten Verfahren zur Verarbeitung personenbezogener Daten oder an den zugrunde liegenden Betriebssystemen Wartungstätigkeiten im datenschutzrechtlichen Sinn sind, und daher nur den dazu ausdrücklich ermächtigten Personen möglich sein dürfen. Sollen im

Zusammenhang mit derartigen Wartungstätigkeiten personenbezogene Daten von Nutzerinnen und Nutzern übermittelt und verarbeitet werden, ist die ausdrückliche Zustimmung der für die Daten verantwortlichen Stelle erforderlich.

Die meisten der derzeit angebotenen Verfahren zum automatischen Software-Update werden diesen aus dem deutschen Datenschutzrecht folgenden Anforderungen nicht gerecht. Insbesondere fehlt vielfach die Möglichkeit, dem Update-Vorgang ausdrücklich zuzustimmen. Die Daten verarbeitenden Stellen dürfen daher derartige Online-Updates nicht nutzen, um Softwarekomponenten ohne separate Tests und formelle Freigabe auf Produktionssysteme einzuspielen.

Auch für private Nutzerinnen und Nutzer sind die automatischen Update-Funktionen mit erheblichen Risiken für den Schutz der Privatsphäre verbunden. Den Erfordernissen des Datenschutzes kann nicht ausreichend Rechnung getragen werden, wenn unbemerkt Daten an Softwarehersteller übermittelt werden und somit die Anonymität der Nutzerinnen und Nutzer gefährdet wird.

Die Datenschutzbeauftragten des Bundes und der Länder fordern daher die Software-Hersteller auf, überprüfbare, benutzerinitiierte Update-Verfahren bereitzustellen, die nicht zwingend einen Online-Datenaustausch mit dem Zielrechner erfordern. Auch weiterhin sollten datenträgerbasierte Update-Verfahren angeboten werden, bei denen lediglich die für den Datenträgerversand erforderlichen Daten übertragen werden. Automatisierte Online-Update-Verfahren sollten nur wahlweise angeboten werden. Sie sind so zu modifizieren, dass sowohl der Update- als auch der Installationsprozess transparent und revisionssicher sind. Software-Updates dürfen in keinem Fall davon abhängig gemacht werden, dass den Anbietern ein praktisch nicht kontrollierbarer Zugriff auf den eigenen Rechner gewährt werden muss. Personenbezogene Daten dürfen nur dann übermittelt werden, wenn der Verwendungszweck vollständig bekannt ist und in die Verarbeitung ausdrücklich eingewilligt wurde. Dabei ist in jedem Fall das gesetzlich normierte Prinzip der Datensparsamkeit einzuhalten.

20.6
Entschließung der 66. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. September 2003

20.6.1
Zum Gesundheitsmodernisierungsgesetz

Die Datenschutzkonferenz begrüßt, dass mit den gesetzlichen Regelungen zur Gesundheitskarte und zu dem bei den Spitzenverbänden der Krankenkassen und der Kassenärztlichen Bundesvereinigung gebildeten zentralen Datenpool datenschutzfreundliche Lösungen erreicht werden konnten. Die Gesundheitskarte unterliegt auch künftig der Verfügungsgewalt der Patientinnen und Patienten. Für den quartals- und sektorenübergreifenden Datenpool dürfen nur pseudonymisierte Daten gespeichert werden.

Die Datenschutzkonferenz wendet sich nicht grundsätzlich gegen zusätzliche Kontrollmechanismen der Krankenkassen.
Die Datenschutzbeauftragten kritisieren, dass sie zu wesentlichen, erst in letzter Minute eingeführten und im Schnellverfahren realisierten Änderungen nicht rechtzeitig und ausreichend beteiligt wurden. Diese Änderungen bedingen erhebliche Risiken für die Versicherten:

- Für das neue Vergütungssystem werden künftig auch die Abrechnungen der ambulanten Behandlungen mit versichertenbezogener Diagnose an die Krankenkassen übermittelt. Mit der vorgesehenen Neuregelung könnten die Krankenkassen rein tatsächlich umfassende und intime Kenntnisse über 60 Millionen Versicherte erhalten. Die Gefahr gläserner Patientinnen und Patienten rückt damit näher. Diese datenschutzrechtlichen Risiken hätten durch die Verwendung moderner und datenschutzfreundlicher Technologien einschließlich der Pseudonymisierung vermieden werden können. Leider sind diese Möglichkeiten überhaupt nicht berücksichtigt worden.

- Ohne strenge Zweckbindungsregelungen könnten die Krankenkassen diese Daten nach den verschiedensten Gesichtspunkten auswerten (z. B. mit Data-Warehouse-Systemen).

Die Datenschutzkonferenz nimmt anerkennend zur Kenntnis, dass vor diesem Hintergrund durch Beschlussfassung des Ausschusses für Gesundheit und Soziale Sicherheit eine Klarstellung dahingehend erfolgt ist, dass durch technische und organisatorische Maßnahmen sicherzustellen ist, dass zur Verhinderung von Versichertenprofilen bei den Krankenkassen

- eine sektorenübergreifende Zusammenführung der Abrechnungs- und Leistungsdaten unzulässig ist und dass
- die Krankenkassen die Daten nur für Abrechnungs- und Prüfzwecke nutzen dürfen.

Darüber hinaus trägt eine Entschließung des Deutschen Bundestages der Forderung der Datenschutzkonferenz Rechnung, durch eine Evaluierung der Neuregelung in Bezug auf den Grundsatz der Datenvermeidung und Datensparsamkeit unter Einbeziehung der Möglichkeit von Pseudonymisierungsverfahren sicherzustellen, dass Fehlentwicklungen vermieden werden.

Die Datenschutzkonferenz hält eine frühestmögliche Pseudonymisierung der Abrechnungsdaten für notwendig, auch damit verhindert wird, dass eine Vielzahl von Bediensteten personenbezogene Gesundheitsdaten zur Kenntnis nehmen kann.

20.6.2
Konsequenzen aus der Untersuchung des Max-Planck-Instituts über Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation

Das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg hat im Mai dieses Jahres sein im Auftrag des Bundesministeriums der Justiz erstelltes Gutachten "Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen" vorgelegt. Darin hat es festgestellt, dass

- die Zahl der Ermittlungsverfahren, in denen TKÜ-Anordnungen erfolgten, sich im Zeitraum von 1996 bis 2001 um 80 v.H. erhöht (1996: 2149; 2001; 3868) hat,

- die Gesamtzahl der TKÜ-Anordnungen pro Jahr im Zeitraum von 1990 bis 2000 von 2.494 um das Sechsfache auf 15.741 gestiegen ist,

- sich die Zahl der jährlich davon Betroffenen im Zeitraum von 1994 bis 2001 von 3.730 auf 9.122 fast verdreifacht hat,

- in 21 v.H. der Anordnungen zwischen 1.000 und 5.000 Gespräche, in 8 v.H. der Anordnungen mehr als 5.000 Gespräche abgehört worden sind,

- der Anteil der staatsanwaltschaftlichen Eilanordnungen im Zeitraum von 1992 bis 1999 von ca. 2 v.H. auf ca. 14 v.H. angestiegen ist,

- die Beschlüsse in etwa Dreiviertel aller Fälle das gesetzliche Maximum von 3 Monaten umfassen, Dreiviertel aller Maßnahmen tatsächlich aber nur bis zu 2 Monaten andauern,

- lediglich 24 v.H. der Beschlüsse substanziell begründet werden,

- es nur in 17 v.H. der Fälle Ermittlungserfolge gegeben hat, die sich direkt auf den die Telefonüberwachung begründenden Verdacht bezogen,

- 73 v.H. der betroffenen Anschlussinhaberinnen und -inhaber nicht über die Maßnahme unterrichtet wurden.

Die Telefonüberwachung stellt wegen ihrer Heimlichkeit und wegen der Bedeutung des Rechts auf unbeobachtete Kommunikation einen gravierenden Eingriff in das Persönlichkeitsrecht der Betroffenen dar, zu denen auch unbeteiligte Dritte gehören. Dieser Eingriff kann nur durch ein legitimes höherwertiges Interesse gerechtfertigt werden. Nur die Verfolgung schwerwiegender Straftaten kann ein solches Interesse begründen. Vor diesem Hintergrund ist der Anstieg der Zahl der Verfahren, in denen Telefonüberwachungen angeordnet werden, kritisch zu bewerten. Dieser kann – entgegen häufig gegebener Deutung – nämlich nicht allein mit dem Zuwachs der Anschlüsse erklärt werden. Telefonüberwachungen müssen ultima ratio bleiben. Außerdem sind die im Gutachten des Max-Planck-Instituts zum Ausdruck kommenden strukturellen Mängel zu beseitigen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert den Gesetzgeber und die zuständigen Behörden auf, aus den Ergebnissen der Untersuchung daher folgende Konsequenzen zu ziehen:

- Der gesetzliche Richtervorbehalt darf nicht aufgelockert werden. Die Verwertung der angefertigten Aufzeichnungen sollte in Fällen staatsanwaltschaftlicher Eilanordnungen davon abhängig gemacht werden, dass ein Gericht rückwirkend deren Rechtmäßigkeit feststellt.

- Um die Qualität der Entscheidungen zu verbessern, sollte die Regelung des § 100b StPO dahin gehend ergänzt werden, dass die gesetzlichen Voraussetzungen der Anordnung einzelfallbezogen darzulegen sind. Die Rechtsfolgen für erhebliche Verstöße gegen die Begründungsanforderungen sollten gesetzlich geregelt werden (z. B. Beweisverwertungsverbote).

- Um die spezifische Sachkunde zu fördern, sollten die Aufgaben der Ermittlungsrichterinnen und -richter auf möglichst wenige Personen konzentriert werden. Die Verlagerung auf ein Kollegialgericht ist zu erwägen.

- Der Umfang des – seit Einführung der Vorschrift regelmäßig erweiterten – Straftatenkataloges des § 100a StPO muss reduziert werden.

- Um eine umfassende Kontrolle der Entwicklung von TKÜ-Maßnahmen zu ermöglichen, muss in der StPO eine Pflicht zur zeitnahen Erstellung aussagekräftiger Berichte geschaffen werden. Jedenfalls bis dahin muss auch die in § 88 Abs. 5 TKG festgelegte Berichtspflicht der Betreiber von Telekommunikationsanlagen und der Regulierungsbehörde beibehalten werden.

- Der Umfang der Benachrichtigungspflichten, insbesondere der Begriff der Beteiligten, ist im Gesetz näher zu definieren, um die Rechte, zumindest aller bekannten Geprächsteilnehmerinnen und -teilnehmer zu sichern. Für eine längerfristige Zurückstellung der Benachrichtigung ist zumindest eine richterliche Zustimmung entsprechend § 101 Abs. 1 Satz 2 StPO vorzusehen. Darüber hinaus müssen die Strafverfolgungsbehörden beispielsweise durch Berichtspflichten angehalten werden, diesen gesetzlich festgeschriebenen Pflichten nachzukommen.

- Zum Schutz persönlicher Vertrauensverhältnisse ist eine Regelung zu schaffen, nach der Gespräche zwischen den Beschuldigten und zeugnisverweigerungsberechtigten Personen grundsätzlich nicht verwertet werden dürfen.

- Zur Sicherung der Zweckbindung nach §§ 100b Abs. 5 StPO und 477 Abs. 2 Satz 2 StPO muss eine gesetzliche Verpflichtung zur Kennzeichnung der aus TKÜ-Maßnahmen erlangten Daten geschaffen werden.

- Die Höchstdauer der Maßnahmen sollte von drei auf zwei Monate reduziert werden.

- Auch auf Grund der Weiterentwicklung der Technik zur Telekommunikationsüberwachung (z. B. IMSI-Catcher, stille SMS, Überwachung des Internetverkehrs) ist eine Fortführung der wissenschaftlichen Evaluation dieser Maßnahmen unabdingbar. Die gesetzlichen Regelungen sind erforderlichenfalls deren Ergebnissen anzupassen.

20.7
Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 27. Oktober 2003

20.7.1
Verschlechterung des Datenschutzes im Entwurf des neuen Telekommunikationsgesetzes

Die Bundesregierung hat am 15. Oktober 2003 den Entwurf für ein neues Telekommunikationsgesetz beschlossen. Dieser Entwurf sieht jetzt zwar - entsprechend der Forderung der Datenschutzbeauftragten – die vorläufige Beibehaltung der Unternehmensstatistik zu Überwachungsmaßnahmen vor, im Übrigen enthält er aber gravierende Verschlechterungen des Datenschutzniveaus.

Insbesondere berechtigt der Gesetzentwurf die Diensteanbieter, grundsätzlich alle entstehenden Verkehrsdaten (also auch alle Zielrufnummern) unverkürzt bis zu sechs Monate nach Versendung der Rechnung zu speichern. Damit wird ohne Not und ohne überzeugende Begründung eine Regelung aufgegeben, die bisher die regelmäßige verkürzte Speicherung von Zielrufnummern vorsieht, wenn die Kundinnen und Kunden sich nicht für die vollständige Speicherung oder vollständige Löschung entscheiden. Die bisherige Regelung berücksichtigt in ausgewogener Weise sowohl die Datenschutz- als auch die Verbraucherschutz-Interessen der beteiligten Personen und hat sich in der Praxis bewährt.

Die Beibehaltung des bisherigen angemessenen Datenschutzstandards sollte nicht von der Initiative der Betroffenen abhängig gemacht werden, sondern allen zugute kommen, die nicht ausdrücklich eine weitergehende Speicherung wählen. Zudem sind die Rechte der angerufenen Teilnehmerinnen und Teilnehmer zu berücksichtigen, in die durch eine Speicherung der unverkürzten Verkehrsdaten zusätzlich eingegriffen wird.

Die Datenschutzbeauftragten bekräftigen in diesem Zusammenhang ihre an der geplanten Pflicht zur Zwangsidentifizierung beim Erwerb von so genannten Prepaid-Handys geübte Kritik. Auch sie würde zu einer verdachtslosen Datenspeicherung auf Vorrat führen. Da diejenigen, die solche Handys kaufen, diese häufig abgeben und nicht identisch sind mit den späteren Nutzerinnen und Nutzern, bringen diese Daten keinen nennenswerten Informationsgewinn für die Sicherheitsbehörden.

Schließlich soll der Zugriff auf Daten, mittels derer auch der Zugriff auf Inhalte oder nähere Umstände einer Telekommunikation geschützt wird (Passwörter, PINs, PUKs), voraussetzungslos, also ohne Bindung an einen Straftatenkatalog und ohne Richtervorbehalt, den Strafverfolgungsbehörden, der Polizei und den Nachrichtendiensten eröffnet werden. Auch darin läge ein unverhältnismäßiger und praktisch nicht zu kontrollierender Eingriff in das Grundrecht nach Art. 10 GG.

Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber auf, den Entwurf bei den bevorstehenden Beratungen in diesen sensiblen Daten zu korrigieren und den gebotenen Schutz des Telekommunikationsgeheimnisses sicherzustellen.

21. Materialien

Technische und IT-organisatorische Vorgaben (Mindeststandards) für die Einrichtung und für den Betrieb von Telearbeitsplätzen in der hessischen Landesverwaltung (StAnz. 2003, S. 4963 ff.)

1. Regelungsbereich

Die technischen und IT-organisatorischen Mindeststandards wurden von einer interministeriellen Arbeitsgruppe erarbeitet und verstehen sich als Ergänzung zu der Anschlussvereinbarung zur Einführung von alternierender Telearbeit in der hessischen Landesverwaltung vom 20. Juni 2003. Sie sind geeignet, notwendige technische Regelungen und Sicherheitsanforderungen zu erläutern und als Handreichungen die Umsetzung zu unterstützen. Zur schnellen Übersicht ist eine Checkliste für die Einrichtung und den Betrieb von Telearbeitsplätzen beigefügt (Anlage 1).

Die Regelungen umfassen alle IT-unterstützten Büroarbeitsplätze außerhalb von Diensträumen. Mobile Arbeitsplätze werden hiervon nicht erfasst. Je nach Ausstattung und Funktionalität greifen die fixierten Mindeststandards. Wird ein PC-Arbeitsplatz über ein öffentliches Netz an die Dienststelle angebunden, stellen sich weiter gehende Sicherheitsanforderungen als bei einem ausgelagerten Kanzlei-PC-Arbeitsplatz, für den ein Datenaustausch per Diskette geregelt wurde. Zusätzlich sind alle für die Integration der Telearbeitsplätze in das häusliche Umfeld vorgegebenen Mindeststandards verpflichtend für die Dienststellen und die Beschäftigten.
Die Anforderungen aus den Aufgabenstellungen bestimmen die IT-Ausstattung und insbesondere auch die notwendigen IT-Leistungen. Können diese Voraussetzungen über vorhandene Standardlösungen nicht geschaffen werden, so ist der Einsatz anderer Software zu prüfen. Die vorhandenen IT-Lösungen sollen sich so den technischen (Weiter-)Entwicklungen stellen. Auf Abschnitt 3 wird verwiesen.

Für bereits bestehende Telearbeitsplätze, die momentan nicht den Mindeststandards entsprechen, wird eine Übergangsfrist für die notwendige Nachrüstung bis Ende des Jahres 2004 eingeräumt. Bei Anwendungen, mit denen sensitive Daten nach § 7 Abs. 4 des Hessischen Datenschutzgesetzes (HDSG) verarbeitet werden, sind die Mindeststandards vorrangig umzusetzen. Der Einsatz chipkartenbasierter bzw. biometrischer Verfahren kommt für Telearbeitsplätze spätestens dann in Betracht, soweit solche Sicherheitslösungen in der Dienststelle zur Anwendung kommen.

2. Mindeststandards

2.1 Einrichtung von Telearbeitsplätzen

2.1.1 Vorbereitungen

Der Entscheidung über die Einrichtung eines Telearbeitsplatzes sollen in jedem Fall zunächst die nachstehenden grundsätzlichen Abwägungen auf Seiten der Dienststelle wie auch bei den Beschäftigten vorausgehen:

- sind die zu verrichtenden Tätigkeiten für den Einsatz der Telearbeit geeignet (Vertraulichkeit, Verfügbarkeit notwendiger Daten, Art der zu verarbeitenden Daten)?
- haben die Beschäftigten die Grundkompetenz, um selbstständig mit der IT-Technik umgehen zu können?
- sind die persönlichen und räumlichen Voraussetzungen im häuslichen Umfeld überhaupt für die Aufnahme weitgehend selbst bestimmter Arbeit geeignet?

2.1.2 Festlegen technischer Ausstattungsstandards

Die Dienststelle entscheidet über den Einsatz der IT-Technik, die Konfiguration und die Softwareausstattung bei der Einrichtung von Telearbeitsplätzen. Sie definiert (sofern noch nicht vorhanden) einen "Warenkorb" und stattet den jeweiligen Telearbeitsplatz nach den fachlichen Anforderungen aus. Die Einrichtung von PC-Arbeitsplätzen wird sich an den IT-Standards der Dienststelle orientieren. Das umfasst auch den Einsatz von mobilen PCs (Laptops, Notebooks u. a.).

Insbesondere gilt dabei:

- Die IT-Ausstattung (Hard- und Software) wird von der Dienststelle kostenlos zur Verfügung gestellt.
- Das Betriebssystem des Telearbeitsplatzes muss über ein vergleichbar dem in der Dienststelle geregelten Sicherheitsniveau verfügen.
- Die Art der Nutzung der Fachanwendung(en) liegt im Ermessen der Dienststelle. Diese muss eine sichere und akzeptable Nutzung der Fachanwendung sicherstellen.
- Die zur Verfügung gestellte IT-Ausstattung darf nur für dienstliche Aufgaben genutzt werden.
- Private Software darf auf dem Telearbeitsplatz nicht installiert werden.
- Über Notwendigkeit und Art der "WAN-Anbindung" (Datenübertragung) entscheidet die Dienststelle; es darf nur eine freigegebene technische Lösung gewählt werden.
- Die Dienststelle entscheidet über die notwendige elektronische Kommunikation und richtet diese auf dem Telearbeitsplatz ein.

2.2 Einrichtung, Betreuung und Wartung der Telearbeitsplätze

Der Dienststelle obliegt die Verantwortung für die ordnungsgemäße Installation, die ergonomische Arbeitsplatzausstattung und für die Funktionsfähigkeit der technischen Ausstattung. Sie kann dabei Arbeiten auf externe Dienstleister delegieren

(Vertrag nach § 4 HDSG erforderlich) oder dem Beschäftigten in vertretbarem Umfang Pflichten zum ordnungsgemäßen Betrieb übertragen, ohne sich jedoch abschließend der Verantwortung entziehen zu können.

2.2.1 Installation der Telearbeitsplätze

Die Dienststelle

- übernimmt grundsätzlich den Transport sowie die Installation des Telearbeitsplatzes vor Ort im häuslichen Umfeld; dies kann auch vom jeweiligen Beschäftigten übernommen werden;
- stellt die Betriebsbereitschaft in Zusammenarbeit mit dem Beschäftigten her;
- prüft die ergonomische Arbeitsplatzausstattung. Ggf. stellt sie entsprechendes Mobiliar oder sonstige Einrichtungsgegenstände kostenlos zur Verfügung. Eine entsprechende Checkliste ist als Arbeitshilfe Bestandteil dieses Katalogs (Anlage 2).
- [Anmerkung: Die Anlage 2 ist hier nicht abgedruckt.]
- erstattet die notwendigen und nachgewiesenen IT-Kosten (Telefongebühren, Verbrauchsmittel etc.) soweit die Materialien nicht von der Dienststelle zur Verfügung gestellt werden.

Die Beschäftigten

- übernehmen die häuslichen Betriebskosten (Miete, Strom, Heizung) und
- achten darauf, dass Änderungen im häuslichen Umfeld, die eine Veränderung der Teilnahmevereinbarung bzw. des Genehmigungsbescheides erfordern, rechtzeitig der Dienststelle mitgeteilt werden.

2.2.2 Support/Hotline

Die Dienststelle

- stellt einen angemessenen Service für den Problemfall sicher;
- sichert eine präventive Beratung zu.

2.3 Sicherheit und Datenschutz

Die Dienststelle ist auch beim Einsatz von Telearbeit die Daten verarbeitende Stelle und damit für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich. Sie muss deshalb die nach § 10 HDSG notwendigen technischen und organisatorischen Maßnahmen vorgeben. Auf die Ziff. 8.1 sowie 8.4 der Anschlussvereinbarung vom 20. Juni 2003 wird an dieser Stelle ausdrücklich verwiesen.

2.3.1 Allgemeine technisch/organisatorische Regelungen (Sicherheitskonzept)

Die Anbindung des Telearbeitsplatzes ist eine Erweiterung des Datennetzes der Dienststelle. Für den Telearbeitsplatz gelten mindestens die gleichen Sicherheitsanforderungen, wie für einen in der Dienststelle vernetzten PC-Arbeitsplatz. Die im Detail zu treffenden Regelungen sollten Bestandteil des Sicherheitskonzeptes der Dienststelle sein.

Dabei gelten folgende Grundannahmen:

- Die Vertraulichkeit dienstlicher Unterlagen am Telearbeitsplatz muss gewährleistet sein.
- Die Verwaltungsnetze (Hessen Corporate Network – HCN –, Local Area Network –LAN –) müssen gegen unbefugten Zugriff geschützt sein. Es dürfen nur von der Dienststelle berechtigte Personen vom Telearbeitsplatz auf dienstliche Daten zugreifen können.
- Die Vertraulichkeit und Integrität der zwischen dem Telearbeitsplatz und der Dienststelle übertragenen Daten muss gewahrt sein.
- Die Zugriffsrechte sind auf das unbedingt notwendige Maß zu reduzieren.
- Das gesamte Verfahren muss revisionssicher sein.
- Die Sicherheitsanforderungen des Landesdatennetzes (HCN) müssen in die Sicherheitsüberlegungen bei den Verantwortlichen der Dienststelle einbezogen sein. Technische Lösungen müssen konform zum Sicherheitskonzept des HCN sein (siehe Abschnitt 3).

2.3.2 Umsetzung der technisch/IT-organisatorischen Mindeststandards

Bei der Konfiguration der Telearbeitsplätze:

- Durch das Betriebssystem oder zusätzlicher Sicherheitshard- und -software müssen Benutzerprofile festgelegt werden, um Benutzer (Telearbeiter, Administrator) unterscheiden und (Mindest-)Zugriffrechte vergeben zu können.
- Eine Authentisierung mindestens per Password ist zwingend einzurichten. Wenn möglich, sind zusätzliche technische Einrichtungen, wie chipkartenbasierter Logon oder biometrische Verfahren zu nutzen.
- Der Zugang per Telearbeit muss über eine zusätzliche USER-ID/Password-Abfrage abgesichert sein. Wurde eine solche Kennung über einen längeren Zeitraum nicht genutzt, ist sie automatisch zu sperren.

Bei der Speicherung/Sicherung dienstlicher Daten:

- Die Speicherung dienstlicher Daten sollte grundsätzlich remote auf dem Server der Dienststelle erfolgen.
- Bei lokaler Speicherung (Ausnahme) sind die Daten zu verschlüsseln (mindestens per Password-Schutz – möglichst jedoch Verschlüsselung per Chipkarte).

- Die Verantwortlichkeiten für die Form und den Zeitintervall der notwendigen Datensicherung sind festzulegen (z. B. Sicherung der lokalen Daten durch den Beschäftigten).

Bei der Datenübertragung/-transporten:

- Die WAN-Anbindung (Wide Area Network) des Telarbeitsplatzes muss durch Einrichtung geschlossener Benutzergruppen auf Telekommunikationsebene, Virtual Private Network (VPN) oder andere Sicherheitsfunktionen (Rufnummerprüfung, Call-Back) abgesichert sein. Eine Prüfung dieser Vorgaben findet bei der Freigabe nach Ziffer 3 statt.
- Die Datenübertragung muss verschlüsselt erfolgen (anerkanntes kryptografisches Verfahren). Ein solches Verfahren sollte auch bei der Übersendung von Disketten und anderen Datenträgern zur Anwendung kommen. Die Übertragung von Akten sollte in verschlossenen Behältern erfolgen.

Bei der Nutzung des Internets:

- Ist ein dienstlich begründeter Internet-Zugang erforderlich, muss er über einen zentralen, durch eine Firewall gesicherten Punkt, der von der Dienststelle festgelegt ist, erfolgen.

3. Produkte und Freigaben für die Anbindung der Telearbeitsplätze

Die technische Anbindung der häuslichen Telearbeitsplätze an die Dienststellen unterliegt besonders strengen Sicherheitsanforderungen. Andererseits verlangt die qualifizierte Arbeit im häuslichen Umfeld nach einer umfassenden IT-Unterstützung vergleichbar der innerhalb der Dienststelle. Der notwendige Kompromiss zwischen unabdingbaren zentralen Sicherheitsvorgaben und individuellen, fachbezogenen Anforderungen kann zu unterschiedlichen IT-Lösungen führen, muss jedoch bezogen auf die Produktentscheidung kontrollierbar und nachvollziehbar sein.

Für den Produkteinsatz gelten die nachstehenden Vorgaben:

- Die WAN-Anbindung der Telearbeitsplätze muss auf Basis der vom Programmmanagement für die Landesverwaltung freigegebenen Produkte erfolgen. Eine aktuelle Produktliste ist als Anlage 3 beigefügt. Fortschreibungen der Produktliste werden im Landesintranet veröffentlicht.
- [Anmerkung: Die Anlage 3 ist hier nicht abgedruckt.]
- Gibt es für die geplante Aufgabenstellung oder auf Grund sonstiger wichtiger Umstände keine geeignete technische Lösung im "Warenkorb" der zugelassenen Produkte, so ist die Dienststelle gehalten, eine funktionierende Lösung zu suchen, die den Mindeststandards entspricht.
- Der Einsatz einer neuen IT-Lösung muss zuvor mit dem Betreiber des HCN (der HZD) sowie mit dem Hessischen Datenschutzbeauftragten abgestimmt und dem Programmmanagement zur Entscheidung über eine Freigabe zugeleitet sein.

4. Revision

Der Anschluss extern installierter IT-Arbeitsplätze erfordert eine besondere Aufmerksamkeit bei IT-Verwaltern und Verantwortlichen. Wegen des daraus entstehenden besonderen Gefährdungspotentials müssen die externen Verbindungsversuche und LogIns zum IT-System der Dienststelle protokolliert und regelmäßig ausgewertet werden. Nur so ist versteckten Gefährdungen wirkungsvoll zu begegnen.

Im Rahmen seiner Gesamtverantwortung für den ordnungsgemäßen Einsatz der Telearbeitsplätze hat die Dienststelle oder eine berechtigte bzw. von ihr beauftragte Stelle ein Zutrittsrecht zu der Wohnung der Beschäftigten (s. dazu Ziff. 6.1 der Anschlussvereinbarung vom 20. Juni 2003) bei:

- der Kontrolle der Datensicherheit des Telearbeitsplatzes durch den beauftragten behördlichen Datenschutzbeauftragten.
- Wartungsarbeiten, Kontrolle, Störungsbehebung oder einer notwendigen Veränderung der IT-Ausstattung durch die behördliche Administration.

Ferner ist dem Hessischen Datenschutzbeauftragten ein Zutrittsrecht einzuräumen.
Der Personalvertretung wird die Möglichkeit eingeräumt, an den Begehungen teilzunehmen.

Anlage 1 (Teil 1)

Checkliste für die Einrichtung und den Betrieb von Telearbeitsplätzen

Prüfpunkte	**Dienststelle**	**Beschäftigte**
Aufgabe ist grundsätzlich für Telearbeit geeignet		
Arbeit ist eigenständig durchführbar	▲	●
Ergebnis konkret und messbar	▲	●
keine wesentlichen Störungen des Dienstablaufs	▲	●
Telearbeit ist nicht durch spezialgesetzliche Regelungen ausgeschlossen	▲	
Beschäftigte(r) erfüllt die persönlichen Voraussetzungen		
benötigte Kenntnisse sind vorhanden	●	▲
Grundkompetenz für den selbstständigen Umgang mit der IT-Technik wurde erworben	●	▲
persönliche und räumliche Verhältnisse sind für Telearbeit geeignet	●	▲
Datenübertragung		
Form des Datenaustauschs ist geregelt (Datenträger, WAN usw.)	▲	
Zugriff auf Netzlaufwerke und Fachanwendungen ist geregelt	▲	
Ausstattung entspricht der Aufgabenstellung		
geeignete Hard- und Software von der Dienststelle gestellt	▲	
Sicherheitsniveau entspricht mindestens dem der Dienststelle (Virenscanner, Bildschirmschoner, Sperrung nicht benötigter Laufwerke, Sicherungssoftware usw.)	▲	●
WAN-Anbindung ist eingerichtet (wo notwendig)	▲	
elektronische Kommunikation im erforderlichen Umfang ist eingerichtet (z. B. E-Mail)	▲	
WAN-Anbindung entspricht den Vorgaben		
Anbindung auf Basis freigegebener Produkte	▲	
Einsatz eines noch nicht freigegebenen Verfahrens geplant:		
- Abstimmung mit HZD und HDSB ist erfolgt	▲	
- Freigabe durch Programmmanagement liegt vor	▲	
Internetzugang nur über von der Dienststelle bestimmte zentrale, per Firewall gesicherte Punkte	▲	●
potenzieller Arbeitsplatz ist geeignet		
notwendige Infrastruktur (Telekommunikation, adäquate Stromversorgung usw.) ist vorhanden bzw. kann zur Verfügung gestellt werden	●	▲
Arbeitsplatz kann ergonomisch korrekt eingerichtet werden bzw. ist es bereits	●	▲
Betreuung und Wartung sind geregelt		
angemessene Benutzerbetreuung ist sichergestellt	▲	
präventive Beratung wird angeboten	▲	

Symbole:

▲	verantwortlich
●	Mitwirkung

Anlage 1 (Teil 2)

Checkliste für die Einrichtung und den Betrieb von Telearbeitsplätzen

Prüfpunkte	**Dienststelle**	**Beschäftigte**
Modalitäten bzgl. Übernahme der Betriebskosten sind geklärt		
nachgewiesene IT-Kosten (Telefongebühren, Verbrauchsmittel) werden ersetzt (Verbindungs-nachweise oder Pauschalregelung)	▲	●
häusliche Betriebskosten (Strom, anteilige Miete, Heizung usw.) zu Lasten des/der Beschäftigten		▲
Datenschutz und -sicherheit sind gewährleistet		
technische und organisatorische Maßnahmen i.S.v. § 10 HDSG sind von der Dienststelle vorgegeben	▲	
Vertraulichkeit dienstlicher Unterlagen ist gesichert	▲	●
Datenzugriffe nur durch berechtigte Personen	▲	●
Verwaltungsnetze (HCN, LAN) sind vor unbefugtem Zugriff über den Telearbeitsplatz geschützt	▲	
Sicherheitsanforderungen des HCN sind erfüllt, technische Lösungen sind konform zum Sicherheitskonzept des HCN	▲	
Zugriffe sind auf das unbedingt notwendige Maß beschränkt	▲	
Vertraulichkeit und Integrität der übertragenen Daten ist sichergestellt (Verschlüsselung, elektronische Signatur, MAC)	▲	
Speicherung von Daten grundsätzlich auf Servern der Dienststelle	▲	●
andernfalls: verschlüsselt und mindestens Passwort-Schutz, möglichst jedoch per Chipkarte	▲	●
Verantwortlichkeit für Form und Zeitintervall der Datensicherung ist festgelegt	▲	●
Benutzer und -rechte sind im Betriebssystem oder durch zusätzliche Sicherheitsinstanzen differenziert eingerichtet	▲	
lokale Authentisierung durch Passwort ist eingerichtet, wo möglich werden zusätzliche Einrichtungen (Chipkarte, Biometrie) zur Zugangskontrolle genutzt	▲	
Telearbeit wird über eine weitere USER-ID/Passwort-abfrage (Telearbeits-Account) auf dem Server gesichert	▲	
Telearbeits-Account wird nach längerer Inaktivität automatisch gesperrt	▲	
Revisionssicherheit		
Externe Verbindungsversuche und LogIns auf das IT-System der Dienststelle werden protokolliert und unter dem Aspekt der Datensicherheit regelmäßig ausgewertet	▲	
Zugangsrechte zur Wohnung		
Zugangsrechte für HDSB sind vereinbart	▲	▲
Zugangsrechte für Personalvertretung und behördlichen Datenschutzbeauftragten sind vereinbart	▲	▲
Zugangsrechte für Administratoren zur Einrichtung, Wartung und Reparatur sind vereinbart	▲	▲
Ausstattung des Arbeitsplatzes entspricht den Vorgaben		
Installation ordnungsgemäß erfolgt, Funktionsfähigkeit geprüft, Betriebsbereitschaft hergestellt	▲	●
ergonomische Arbeitsplatzausstattung ist geprüft	▲	●

Symbole:

▲	verantwortlich
●	Mitwirkung