15. Wahlperiode

Drucksache **15/4790**

HESSISCHER LANDTAG

17. 03. 2003

Einunddreißigster Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

vorgelegt am 31. Dezember 2002
nach § 30 des Hessischen Datenschutzgesetzes vom 7. Januar 1999

Eingegangen am 17. März 2003 · Ausgegeben am 31. März 2003
Druck: Druckerei Chmielorz GmbH · Ostring 13 · 65205 Wiesbaden · Auslieferung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden

INHALTSVERZEICHNIS

1. Vorwort

Das Berichtsjahr 2002 war durch zahlreiche neue Eingriffsermächtigungen geprägt, die durch die Bundesgesetzgebung zur Terrorismusbekämpfung, zur Ausweitung der Überwachungsbefugnisse der Finanzbehörden und zur Gesundheitsreform geschaffen worden sind. Auch die hessische Landesgesetzgebung hatte zahlreiche Rückwirkungen auf den Datenschutz. Im Vordergrund standen die Novellen zum Verfassungsschutz, zum Hessischen Gesetz über die öffentliche Sicherheit und Ordnung und zum Pressegesetz. In allen drei Bereichen haben sich die Vorstellungen des Datenschutzes nur begrenzt durchsetzen lassen. Die Gesetzgebung zur Rasterfahndung hat neue Gerichtsverfahren ausgelöst.

Die elektronische Datenspeicherung nimmt ungeachtet aller Widerstände aus der Bevölkerung zu, wobei die Speicherungen von Gesundheits- und Steuerdaten an der Spitze stehen. Noch nicht ganz überschaubar sind die Risiken, die sich aus der zunehmenden Auftragsdatenverarbeitung ergeben, die Finanz- aber auch andere Behörden inzwischen bei privaten Unternehmen vornehmen lassen.

Willentliche Verstöße gegen die datenschutzrechtlichen Vorschriften sind in größerem Umfang nicht aufgetreten. Überwiegend liegen Fehlverhalten vor, die unbedacht entstanden sind. Nennenswerte Sicherheitslücken in der behördlichen EDV sind nicht erkennbar geworden. Vorsorgliche Sicherheitsstrategien – wie in der hessischen Justiz – vermeiden Datenschutzverletzungen, die durch Nachbesserung behoben werden müssten.

Verfahrensrechtliche Wünsche der Oppositionsparteien haben dazu geführt, dass die Stellungnahme der hessischen Landesregierung zum Bericht für das Jahr 2001 sehr viel ausführlicher ausgefallen ist als in den Vorjahren. Die ausführliche Auseinandersetzung der Landesregierung mit meinem Bericht begrüße ich sehr. Bedauerlicherweise hat dieses Bemühen dazu geführt, dass die Stellungnahme erst im Dezember dieses Jahres vorgelegt worden ist, sodass weder eine Beratung im Innenausschuss des Hessischen Landtags noch im Plenum in zeitnaher Form hat stattfinden können. Die Neuwahl des Hessischen Landtags wird weitere Verzögerungen mit sich bringen, so dass zwischen den im Jahr 2000 getroffenen Feststellungen und deren Erörterung zwei Jahre liegen werden. Außerdem wird der nunmehr vorgelegte Bericht für 2002 sich mit der parlamentarischen Erörterung des Berichts für 2001 voraussichtlich überschneiden.

Kernpunkte des 31. Tätigkeitsberichts

1. Zu den datenschutzrechtlich umstrittensten Themen des Berichtsjahres gehört die Rasterfahndung in Hessen. Nachdem der erste Anlauf gescheitert war, hat der Landesgesetzgeber § 26 Abs. 1 Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) geändert. Die verabschiedete neue Ermächtigungsnorm hat sich als überaus schwer handhabbar erwiesen, was in einem Urteil des Verwaltungsgerichts Gießen zum erneuten Stopp der angelaufenen Datensammlung für die Rasterfahndung geführt hatte. Inzwischen hat der Verwaltungsgerichtshof der Beschwerde des Landeskriminalamtes stattgegeben. Inwieweit das Hauptsacheverfahren abweichende Feststellungen zur Wirksamkeit der Anordnung der Rasterfahndung – hierüber hat der Verwaltungsgerichtshof noch nicht entschieden – hervorbringen wird, ist noch nicht absehbar. Der intensive Eingriff in die informationelle Selbstbestimmung derjenigen, die in die Rasterfahndung einbezogen werden, hätte es geboten erscheinen lassen, Verfahren und gesetzliche Anforderungen an Datenerhebungen und -abgleiche präziser und schärfer zu fassen, als das gegenwärtig in § 26 HSOG der Fall ist (Ziff. 2).

2. Die datenschutzrechtliche Neuregelung des Presserechts ist unbefriedigend. Zu kritisieren ist insbesondere, dass keine redaktionsinternen Datenschutzbeauftragten vorgesehen und keine Kontrollverfahren für Presseunternehmen eingeführt worden sind, die sich dem „Pressekodex“ nicht zu unterwerfen bereit sind (Ziff. 11.1).

3. Die neu geschaffenen Überwachungsbefugnisse des Landesamtes für Verfassungsschutz sehen keinen Schonraum vor, der den Zeugnisverweigerungsrechten der Journalisten nach § 53 Abs. 1 Strafprozessordnung entspricht. Für die Freiheit der Berichterstattung ist es unerlässlich, die journalistische Arbeit von staatlicher Überwachung der Kommunikation freizustellen, sofern keine Anhaltspunke für einen Verdacht der Mittäterschaft bestehen. Dem Landesgesetzgeber ist zu empfehlen, in die ohnehin notwendige Novelle zum Gesetz über das Landesamt für Verfassungsschutz wie in das HSOG Ausnahmeregelungen aufzunehmen, die die Kommunikation von Journalisten für redaktionelle Zwecke von Überwachungsmaßnahmen durch Staatsbehörden frei stellen (Ziff. 8.2).

4. Durch die Neufassung des Hessischen Hochschulgesetzes werden Evaluationsverfahren zum Standard hochschulrechtlicher Datenerhebung und -verarbeitung. Die Universität in Kassel hat den Entwurf einer Satzung für Evaluationen mit mir abgestimmt (Ziff. 14.1). Ich habe zudem selbst eine Mustersatzung entworfen, die sowohl die Anforderungen an aussagefähige Evaluationsverfahren wie datenschutzrechtliche Anforderungen berücksichtigt (Ziff. 25.5).

5. Die Videoüberwachung in Hessen ist im Berichtsjahr weiter ausgeweitet worden (Ziff. 3.1). Allerdings nimmt sie trotz stetiger Ausweitung in den Städten bislang nicht den Umfang an, über den aus anderen europäischen Staaten, insbesondere aus England, berichtet wird. Die Videoüberwachung wirft – wenn sie gemeinsam von Gemeinden und Polizei betrieben wird – die Frage der Anwendung des § 15 Hessisches Datenschutzgesetz auf, über die im Berichtszeitraum noch kein Einverständnis erzielt werden konnte. Die bisherigen Erfahrungen zeigen, dass die Videoüberwachung dort erfolgreich ist, wo ihr Ziel auf eine Verlagerung von Kriminalitätsschwerpunkten ausgerichtet ist. Keine ausreichenden Erfahrungen liegen zu der Frage vor, ob die Videoüberwachung die Zahl der Straftaten insgesamt eindämmen kann.

6. Unverkennbar ist, dass der Steuerstaat in den letzten Jahren weiter den Weg hin zu „gläsernen Unternehmen“ und „gläsernen Steuerbürgern“ beschreitet, was zu einer Mehrzahl kritischer Anfragen von Steuerpflichtigen geführt hat. Der Steuerstaat entwickelt sich immer weiter zum Überwachungsstaat; vorsorgliche Datenbeschaffung und Aufbau von Vorratsdatenbanken beim Bundesamt für Finanzen verdrängen anlassbezogene Ermittlungen (Ziff. 10.1 und Ziff. 10.3). Da es sich um Bundesgesetzgebung handelt, bemühe ich mich als Vorsitzender des Arbeitskreises Steuern, über die Hessische Staatskanzlei, den Hessischen Minister der Finanzen und den Bundesrat Einfluss zu gewinnen. Ausdruck dieser Bemühungen ist die Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 7. Januar 2003 (Ziff. 24.9) und die Kritik an der Pflicht zur Kontrollmitteilung der Banken (Ziff. 10.3). Die Pflicht zur Angabe der Steuernummer auf Rechnungen, die Pflichtangaben und der Umgang mit Freistellungsbescheinigungen des Baugewerbes und das Verlangen nach Gruppenauskünften über Subunternehmer geben zu datenschutzrechtlichen Bedenken Anlass (Ziff. 10.2). Auf Widerstand stößt nach wie vor auch die Pflicht der Unternehmen, den Finanzbehörden Kopien der betriebsinternen EDV zu überlassen. Diese Pflicht gewinnt höhere Tragweite, falls erweiterte Kontrollmitteilungen – wie im Entwurf des Steuervergünstigungsabbaugesetzes geplant – gestattet werden.

7. Deutliche Fortschritte sind bei der Umsetzung der datenschutzrechtlichen Anforderungen und Vorkehrungen zu verzeichnen, die der Einsatz der EDV in der Justiz gebietet. In einer gemeinsamen Arbeitsgruppe mit dem Hessischen Ministerium der Justiz konnten nahezu alle aufgeworfenen Fragen im Einvernehmen gelöst werden. Nach wie vor habe ich im Hinblick auf den Datenschutz, die Gewaltenteilung und die richterliche Unabhängigkeit Bedenken, der Hessische Zentrale für Datenverarbeitung als Verwaltungsbehörde jene weitreichenden Befugnisse zuzuerkennen, die sie mit dem nach dem Konzept beabsichtigten Betreuungsumfang hat. Verschleifungen zwischen Gerichtsbarkeit und Innenministerium sollten allein der rechtsstaatlichen Optik wegen vermieden werden (Ziff. 5.1).

8. Eine Prüfung des Projektes „Elektronische Fußfessel“ hat zu datenschutzfreundlicheren Lösungen geführt. Da die Fußfessel ein schwerwiegender Eingriff in das Recht auf informationelle Selbstbestimmung ist, der sich hinsichtlich der Eingriffsintensität der Führungsaufsicht nähert, halte ich weiterhin eine eigenständige gesetzliche Rechtsgrundlage für erforderlich (Ziff. 23.3).

9. Erstmals sind Versuche einer Dienststellenleitung aufgetreten, Informationen des Personalrats, die mir zur datenschutzrechtlichen Kontrolle übermittelt worden waren, als Verrat von Dienst- und Betriebsgeheimnissen zu qualifizieren. Nachdem dienstliche Sanktionen angekündigt worden waren, habe ich die Missachtung des § 28 Abs. 1 Satz 2 HDSG gerügt (Ziff. 19.1).

10. Soweit auf einen zentralen Datenpool wie künftig in der gesetzlichen Krankenversicherung oder auf gemeinsame Datenspeicherungen wie in den Praxis- und Kompetenznetzen zugegriffen werden soll, sind nicht nur die Zugriffsberechtigungen ein datenschutzrechtliches Problem. Eigenständige Gefahren gehen von der hohen Akkumulation von Daten aus. Deren Zweckbestimmung muss – da regelmäßig hoch sensitive Daten erfasst werden – vorab und konkret festgelegt werden. Zudem sind Schutzvorschriften gegen Zweckänderungen zu schaffen, die eine nachträgliche Umwidmung ausschließen. Soweit für die Aufgabenwahrnehmung ausreichend, sind pseudonymisierte oder anonymisierte Parallelspeicherungen vorzusehen, die durch Datentreuhänder gegen Durchgriffe auf personenbezogene Daten zu schützen sind. In der Neigung, immer größere Datenakkumulationen in Pools zusammenzuführen oder dezentrale Speicher zu vernetzen, liegen besondere datenschutzrechtliche Gefahren (Ziff. 17.2).

11. Neue Probleme schaffen mobile Datenspeicher und Chipkarten, wie sie im Gesundheitswesen geplant (Ziff. 17.1), in den Hochschulen eingesetzt (Ziff. 14.3) und für die biometrische Sicherheit der Personalausweise und Pässe vorbereitet werden. Die Datensicherheit, die auch für mobile Datenspeicher dieser Art erfüllt werden muss, zwingt zu neuen Lösungen. Datenschutzrechtliche Grundforderung ist, dass die betroffenen Personen volle Kenntnis der gespeicherten Daten erhalten können (Lesegeräte), dass sie über die Freigabe von Datensegmenten entscheiden können (Gesundheitskarten) und dass Verwendungen ausgeschlossen werden, für die die Speicherkarten nicht vorgesehen worden waren. Missbräuchliche Nutzung, etwa durch Arbeitgeber im Einstellungsverfahren oder Versicherungen vor Abschluss von Verträgen, muss ausgeschlossen werden (zu biometrischen Daten s. Ziff. 24.1).

12. Auf dem Gebiet des technischen Datenschutzes und der Datensicherheit haben die Informatiker und Informatikerinnen der Dienststelle der zunehmenden Vernetzung öffentlicher Stellen besonderes Augenmerk gewidmet. Auf Grund der begrenzten Personalausstattung bin ich nicht in der Lage, die datenschutztechnische Sicherheit öffentlicher Stellen des Landes und der Gemeinden flächendeckend zu überprüfen. Gleichwohl verfolge ich nach wie vor das Ziel, durch vorsorgliche Beratung erkennbar gewordene Sicherheitsrisiken zu vermeiden. Spezielle Probleme und Sicherheitslücken bei Software und bei der Handhabung großer Netze sind ebenfalls in meinem Bericht dargestellt (Ziff. 12.3). Über neue Tendenzen und die Bewertung der Sicherheitsaspekte bei den im Vormarsch begriffenen funkbasierten Netzen wird in einem weiteren Beitrag berichtet (Ziff. 12.1).

13. Besonderes Augenmerk wurde der zunehmenden Internetanbindung öffentlicher Stellen gewidmet. Um Angriffe auf die Behördennetze zu unterbinden, wurde in der Dienststelle ein Verfahren erprobt, das mit einem vorgelagerten Server arbeitet. Mit dieser Terminalserverlösung findet der Kontakt zum Internet nicht im eigenen (sicheren) Netz statt, sondern wird auf den Server ausgelagert (eigener Netzbereich). Als Grafik (Terminalserverfenster) verlieren aktive Elemente ihre schädigende Wirkung im eigenen Netz, da Schadenprogramme aus dem Internet nicht in das Netz gelangen. Die Untersuchung zeigt, dass Graphical Firewalls sichere und praktikable Lösungen bieten (Ziff. 12.4).

2. Terrorismusbekämpfung

Rasterfahndung

Auch nach der Novellierung des Hessischen Gesetzes über die Sicherheit und Ordnung gibt es erhebliche Probleme bei der Organisation von Rasterfahndungsmaßnahmen im Rahmen der bundesweiten Aktion zur Suche nach so genannten „Schläfern" infolge der Anschläge vom 11. September 2001.

2.1
Rasterfahndungsanordnungen im Oktober 2001

Wie in allen Bundesländern so ist auch in Hessen gestützt auf die alte Fassung des § 26 Hessisches Gesetz über die Öffentliche Sicherheit und Ordnung (HSOG) nach dem 11. September 2001 eine Rasterfahndungsmaßnahme angelaufen.

§ 26 HSOG (alte Fassung)

(1) Die Polizeibehörden können von öffentlichen Stellen oder Stellen außerhalb des öffentlichen Bereichs zur Abwehr einer gegenwärtigen Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person die Übermittlung von automatisiert gespeicherten personenbezogenen Daten bestimmter Personengruppen zum Zwecke des Abgleichs mit anderen Datenbeständen verlangen, wenn Tatsachen die Annahme rechtfertigen, dass dies zur Abwehr der Gefahr erforderlich ist. Rechtsvorschriften über ein Berufs- oder besonderes Amtsgeheimnis bleiben unberührt.

...

(4) Die Maßnahme bedarf außer bei Gefahr im Verzug der richterlichen Anordnung. Für das Verfahren gilt § 39 Abs. 1 mit der Maßgabe, dass das Amtsgericht zuständig ist, in dessen Bezirk die Polizeibehörde ihren Sitz hat. Die Anordnung muss die zur Übermittlung verpflichtete Person sowie alle benötigten Daten und Merkmale bezeichnen. ... Die oder der Datenschutzbeauftragte ist durch die Polizeibehörde zu unterrichten.

Dazu waren vom Landeskriminalamt (LKA) auf Grundlage mehrerer richterlicher Anordnungen des AG Wiesbaden, in denen eine gegenwärtige Gefahr bejaht worden war, von verschiedenen Stellen Daten angefordert worden, die einem bestimmten Profil entsprachen. Betroffen waren unter anderem Studenten technischer Fachrichtungen aus vorwiegend arabischen Heimatländern. Aufgrund der Beschwerde eines von der Maßnahme betroffenen Studenten hat das Oberlandesgericht (OLG) Frankfurt am Main mit Beschluss vom 21. Februar 2002 die erstinstanzlichen Entscheidungen aufgehoben (Az.: 20 W 55/02). Als Begründung hat das OLG u. a. ausgeführt: Sinn der richterlichen Anordnung sei, dass die zuständige Tatsacheninstanz selbst die Tatsachen feststellt, die eine richterliche Anordnung im Rahmen des § 26 HSOG rechtfertigen. Vom Vorliegen einer gegenwärtigen Gefahr im Sinne dieses Gesetzes sei nicht auszugehen. Die Anforderungen an den Gefahrenbegriff seien deshalb so hoch, weil in die Rechte einer Vielzahl von Nichtstörern eingegriffen werde. Nach der Aktenlage fehlten hinreichende Anhaltspunkte dafür, dass im maßgeblichen Zeitpunkt die Voraussetzungen des Gesetzes vorgelegen hätten. Überdies äußerte das OLG erhebliche Zweifel zur Eignung der Rasterfahndung und zur Erforderlichkeit der Datenübermittlungen. Allerdings hat es diese Frage im Ergebnis offen gelassen.

Infolge der Entscheidung sind alle in Hessen im Rahmen dieser Rasterfahndungsmaßnahme erhobenen Daten einschließlich solcher, die zum bundesweiten Abgleich schon an das Bundeskriminalamt weitergeleitet worden waren, gelöscht worden. Dessen habe ich mich vergewissert. Bis zu diesem Zeitpunkt hatten im Wesentlichen nur Vorbereitungsarbeiten stattgefunden. Zu einer Rasterung der erhobenen Daten im eigentlichen Sinne war es noch nicht gekommen.

2.2
Novellierung des HSOG

Als Reaktion auf die Entscheidung des OLG Frankfurt wurde von den Fraktionen der CDU und FDP im Hessischen Landtag am 12. Februar 2002 eine Änderungsnovelle zum HSOG vorgelegt. Ziel war, die Voraussetzungen für Rasterfahndungsmaßnahmen zu senken und die Durchführung solcher Maßnahmen durch den Wegfall des Richtervorbehaltes zu vereinfachen.

Dieser Gesetzentwurf war sehr umstritten. Er wurde nach mehreren kontroversen Debatten im August in 3. Lesung verabschiedet.

§ 26 HSOG (i. d. F. vom 11. September 2002)

(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.

...

(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. ...

Auch ich habe mehrmals im Laufe des Gesetzgebungsverfahrens zu dem Entwurf Stellung genommen. Dabei habe ich vor allem zu zwei Punkten Kritik geäußert:

Das Gesetz sieht nunmehr vor, dass tatsächliche Anhaltspunkte die Annahme rechtfertigen sollen, dass das Rasterungsverfahren für die Verhütung der bezeichneten Straftaten erforderlich ist. Diese Einfügung „tatsächlicher Anhaltspunkte“ bezieht sich nicht auf die Wahrscheinlichkeit von Straftaten von erheblicher Bedeutung – wie es sachgerecht wäre –, sondern auf die Prognose, ob das Rasterungsverfahren sinnvoll ist oder nicht.

Sachgerecht wäre eine Regelung, die tatsächliche Anhaltspunkte in der Weise in die gesetzliche Regelung einbringt, dass der Verdacht bevorstehender Straftaten durch tatsächliche Anhaltspunkte zu unterfüttern ist. Die geforderte Prognose ist ein Prozess gedanklicher Vorausschau, für den tatsächliche Anhaltspunkte allenfalls in Form von Erfahrungssätzen eine Rolle spielen, nicht aber im Sinne einer konkret zu treffenden Diagnose über das bereits vorliegende Geschehen. Insofern ist die systematische Stellung dieses Kriteriums im Gesetz nicht sachgerecht. Tatsachen können nur die Ausgangslage abstützen, von der die Vermutung bevorstehender Straftaten herrührt, nicht aber die Möglichkeit der Abwehr. Diese ist von einer wertenden Einschätzung, nicht aber von Tatsachen abhängig, die zur Anordnung führen.

Der Verzicht auf eine richterliche Anordnung hat zur Folge, dass die gegen die Betroffenen gerichteten Anordnungen als Verwaltungsakte ergehen müssen. Betroffene sind nicht die Stellen, von denen die Daten verlangt werden, sondern die Bürgerinnen und Bürger, in deren informationelle Selbstbestimmung eingegriffen und deren Daten erhoben werden sollen. Diese Verwaltungsakte müssen damit sie wirksam werden zugestellt werden. Am einfachsten kann das durch Allgemeinverfügung im Wege der öffentlichen Bekanntmachung erfolgen (§ 41 Abs. 3 HVwVfG).

2.3
September 2002 – Neue Rasterfahndung

Die Änderung des HSOG trat am 12. September in Kraft. Noch an diesem Tage wurde durch das LKA in Abstimmung mit dem Landespolizeipräsidium eine Anordnung zur erneuten Rasterfahndung in Hessen erlassen. Auf Grundlage dieser Anordnung ergingen über zwanzig Polizeiverfügungen an öffentliche und nicht-öffentliche Stellen in Hessen, wieder Daten entsprechend dem Profil aus dem letzten Jahr zu liefern. Diese Verfügungen waren als Verwaltungsakt mit der Anordnung des Sofortvollzuges ausgestaltet.

Gegen diese Verfügungen gab es eine Vielzahl von Einwendungen, und zwar von den Hochschulen und betroffenen Studenten.

Auch ich habe gegenüber den betroffenen Stellen, dem Innenministerium und dem LKA Bedenken geäußert.

2.3.1
Kein Verwaltungsakt gegen Hoheitsträger

Es gehört zu den Grundstrukturen des Verwaltungsrechts, dass Hoheitsträger einander nicht mit hoheitlichen Verfügungen traktieren dürfen. Meist wird das mit dem Schlagwort gekennzeichnet: „Keine Polizeigewalt gegenüber Hoheitsträgern“. Es besteht Einvernehmen, dass alle Hoheitsträger den polizeirechtlichen Pflichten zu genügen haben, also auch den aus § 26 Abs. 1 HSOG hervorgehenden. Es besteht aber ebenso Einvernehmen darüber, dass sie das aus eigener Pflichterfüllung heraus zu tun haben.

Das Verlangen des LKA gegenüber den Hochschulen (und den anderen betroffenen öffentlichen Stellen) ist in der Sache ein Amtshilfeersuchen: Die Hochschulen sollen dem LKA Teile ihrer Datenbestände verfügbar machen, um diesem die Erfüllung seiner Abgleichaufgabe möglich zu machen. § 26 Abs. 1 HSOG stellt insofern eine lex specialis zu § 5 Abs. 1 Nr. 3 und 4 Hessisches Verwaltungsverfahrensgesetz dar. Dort wird auf die Kenntnis von Tatsachen (Daten) abgestellt, die der ersuchenden Behörde unbekannt sind, die sie aber zur Erfüllung ihrer Aufgaben benötigt.

Die Durchführung der Amtshilfe regelt sich nach dem für die Hochschulen geltenden Recht: Sie müssen daher in eigener Zuständigkeit prüfen, inwieweit die vom LKA beanspruchte Datenübermittlung mit den Grundrechten auf informationelle Selbstbestimmung vereinbar ist, die den Studierenden zukommen. Dabei kommt der Frage entscheidende Bedeutung zu, ob die Duldungspflichten, die für die Studierenden verfügt worden sind, wirksam geworden sind. Ist dies nicht der Fall, so dürfen sie dem Amtshilfeersuchen nicht nachkommen.

2.3.2
Kenntnis der Betroffenen

Während der Gesetzesberatungen hatte ich darauf verwiesen, dass die Beseitigung des bisherigen Richtervorbehalts dazu führt, dass die zuständige Polizeibehörde selbst die Eingriffe zu verfügen hat. Wegen des in der Verfügung liegenden Grundrechtseingriffs kann das nur durch Verwaltungsakt erfolgen. Die rechtsstaatlichen Verfahrensgrundsätze und die Rechtsweggarantie des Art. 19 Abs. 4 Grundgesetz gebieten,

– dass der mit der Rasterung eintretende Eingriff in die Rechte der betroffenen Grundrechtsträger im Wege einer Allgemeinverfügung verbindlich gemacht werden muss, und

– dass die betroffenen Personen davon verlässliche Kenntnis erlangen, um ihnen effektiven Rechtsschutz zu eröffnen.

Die Personen, deren Namen und Eigenschaften erhoben und gerastert werden sollen, sind nur grundrechtlich in ihrer informationellen Selbstbestimmung betroffen und besitzen eine Klagebefugnis i. S. d. § 42 Abs. 2 Verwaltungsgerichtsordnung (VwGO). Das ist unstreitig; die angerufenen Verwaltungs- und Oberverwaltungsgerichte in allen Ländern haben die Klagebefugnis der klagenden Studenten anerkannt.

2.3.3
Rasterfahndung als erforderliches Mittel

§ 26 Abs. 1 HSOG sieht in seiner Neufassung als Voraussetzung für die Anordnung einer Rasterfahndung vor, dass tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass die Rasterfahndung das erforderliche und unentbehrliche Mittel darstellt.

In der Verfügung des LKA fand sich keine Auseinandersetzung mit der Frage, ob die bisherigen Erfahrungen, die mit der Rasterfahndung in anderen Bundesländern seit Herbst 2001 gewonnen worden sind, wirklich tatsächliche Anhaltspunkte für die Geeignetheit und Erforderlichkeit geliefert haben. Soweit meine Informationen reichen, ist trotz des hohen Personal- und Mitteleinsatzes bislang kein Terrorist aufgrund des Datenabgleichs gefasst oder entdeckt worden. Die in der Verfügung des LKA dargelegten Ermittlungsergebnisse und Strafverfolgungsmaßnahmen sind keine Frucht der Rasterfahndung, sondern beruhen auf Hinweisen fremder Geheimdienste und Strafverfolgungsorgane oder sind als Erfolge der deutschen Strafverfolgungsbehörden auszuweisen.

Die präventive Rasterfahndung ist hingegen bislang ohne vorzeigbare Erkenntnisse geblieben. Nach meiner Ansicht sind tatsächliche Anhaltspunkte für die Erforderlichkeit daher derzeit nicht nachweisbar. Deshalb sind die gesetzlichen Voraussetzungen für die Rasterfahndung nicht gegeben.

2.4
Ergebnisse der eingelegten Rechtsmittel

Einige der betroffenen Hochschulen hatten Widerspruch gegen die Verfügungen des LKA erhoben und vor den Verwaltungsgerichten beantragt, die aufschiebende Wirkung gemäß § 80 Abs. 5 VwGO wiederherzustellen.

Darauf hat das LKA reagiert und die Bescheide abgeändert. Nunmehr wurde ein Amtshilfeersuchen an die öffentlichen Stellen gerichtet. Während einige Hochschulen daraufhin Daten geliefert haben, haben andere auch weiterhin ihre Vorbehalte zum Ausdruck gebracht. Gleichzeitig haben mehrere Studenten Rechtsmittel eingelegt. Eine Klage vor dem Staatsgerichtshof blieb allerdings zunächst ohne Erfolg, da der Antragsteller den Rechtsweg nicht ausgeschöpft hatte.

Das Verwaltungsgericht (VG) Gießen hat in zwei Entscheidungen vom 8. November 2002 den Hochschulen Gießen und Marburg im Rahmen des einstweiligen Rechtsschutzes aufgegeben, die Daten der antragstellenden Studenten zunächst nicht zu übermitteln. Zur Begründung hat es ausgeführt, dass die Hochschulen nicht ausreichend – nämlich überhaupt nicht – geprüft hätten, ob im Rahmen des § 14 HDSG eine Übermittlung zulässig wäre. Das Amtshilfeersuchen sei rechtswidrig, denn es bestünden Bedenken bezüglich der Zuständigkeit des LKA. Ferner sei das Amtshilfeersuchen zu unbestimmt, da nicht klar dargelegt sei, welche Studiengänge erfasst sein sollten. Schließlich würden auch Daten verlangt, die bei den Hochschulen nicht (mehr) verarbeitet werden dürfen, weil bei exmatrikulierten Studierenden Daten wie Geburtsort und -land sowie Staatsangehörigkeit gelöscht sein müssten.

In seinen Entscheidungen setzt sich das Gericht kritisch mit den formalen Voraussetzungen der Anordnung einer Rasterfahndungsmaßnahme gem. § 26 HSOG auseinander. Nach seiner Ansicht wäre ein Verwaltungsakt die zutreffende Rechtsform. Dieser Verwaltungsakt habe Drittwirkung, so dass zum Wirksamwerden auch eine Bekanntgabe gegenüber den Studierenden notwendig sei.

Weiterhin setzt sich das Gericht mit der Verarbeitung der Daten durch die Polizei auseinander. Problematisiert wird der Abgleich der so genannten Prüffälle im BKA in einer „Verbunddatei“ mit bundesweit – auch auf freiwilliger Basis – erhobenen Daten. Das BKA habe keine eigene Befugnis zur Durchführung einer Rasterfahndungsmaßnahme. Die Übermittlung in die Verbunddatei stelle eine zweckändernde Verarbeitung dar, für die es im HSOG keine Rechtsgrundlage gebe. Die normalen Übermittlungsnormen seien im Rahmen der Anwendung des § 26 HSOG unanwendbar.

Einige Hochschulen haben nach dieser Entscheidung erklärt, keine Daten liefern zu wollen, andere Hochschulen haben das LKA aufgefordert, die Daten zurückzugeben oder zumindest nicht zu verarbeiten, bis die Entscheidung in der Hauptsache ergangen sei.

Gegen die Entscheidungen des VG Gießen hat das LKA Beschwerde eingelegt. Anfang Februar 2003 hat der Verwaltungsgerichtshof der Beschwerde stattgegeben. Entschieden wurde dabei nur über die Befugnis und Pflicht der Universitäten, die angeforderten Daten auf Ersuchen des LKA zu übermitteln. Zu der vom VG beschiedenen Frage, ob die Wirksamkeit der Anordnung der Rasterfahndung notwendige Bedingung für ein rechtmäßiges Amtshilfeersuchen ist, schweigt der Beschluss des VGH. Deswegen ist nicht vorhersehbar, wie dessen Entscheidung zur Wirksamkeit der Anordnung der Rasterfahndung im Hauptsacheverfahren ausfallen wird.

3. Querschnittsthemen

3.1
Videoüberwachung

Die Zahl der Videoüberwachungsanlagen hat auch im vergangenen Berichtsjahr weiter zugenommen. In vielen Fällen ist meine Dienststelle im Vorfeld der Installierung der Kameras eingeschaltet worden. Dies hat dazu geführt, dass manche Anlage kleiner dimensioniert wurde als ursprünglich geplant und dass Techniken eingesetzt wurden, die verhindern, dass private Wohnbereiche von der Videoüberwachung mit erfasst werden.

3.1.1
Gemeinsame Verfahren

Es hat sich herausgestellt, dass die meisten Videoüberwachungsanlagen in den hessischen Städten und Gemeinden zwar von diesen geplant und finanziert werden, die Daten aber zur Polizei übertragen und von ihr ausgewertet werden. In anderen Fällen werden die Anlagen jedoch sowohl von den Ordnungsbehörden der Gemeinden als auch von der Polizei betrieben. Bei diesen gemeinsam betriebenen Videoüberwachungsanlagen handelt es sich nach meiner Auffassung um gemeinsame Verfahren i. S. v. § 15 Hessisches Datenschutzgesetz (HDSG), die vor Inbetriebnahme die Beteiligung des Hessischen Datenschutzbeauftragten voraussetzen.

§ 15 Abs. 1 HDSG

Die Einrichtung eines automatisierten Verfahrens, das mehreren datenverarbeitenden Stellen gemeinsam die Verarbeitung personenbezogener Daten ermöglicht, ist nur zulässig, wenn dies unter Berücksichtigung der schutzwürdigen Belange der Betroffenen und der Aufgaben der beteiligten Stellen angemessen ist. Die Benutzung des Verfahrens ist im Einzelfall nur erlaubt, wenn hierfür die Zulässigkeit der Datenverarbeitung gegeben ist. Vor der Einrichtung oder Änderung eines gemeinsamen Verfahrens ist der Hessische Datenschutzbeauftragte zu hören. Ihm sind die Festlegungen nach Abs. 2 Satz 1, das Verfahrensverzeichnis nach § 6 Abs. 1 und das Ergebnis der Untersuchung nach § 7 Abs. 6 Satz 3 vorzulegen.

Die polizeirechtliche Zulässigkeit gemeinsamer Verfahren ist problematisch, weil das Hessische Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) keine Ermächtigung für solche gemeinsamen Verfahren aller Gefahrenabwehrbehörden kennt. Ein Einvernehmen mit dem Landespolizeipräsidium über die Anwendung des § 15 HDSG als datenschutzrechtliche Auffangregelung hat noch nicht erzielt werden können. Die Weigerung, § 15 HDSG anzuwenden, hat letztlich zur Konsequenz, dass der gemeinsame Betrieb derartiger Überwachungsanlagen polizei- und datenschutzrechtlich rechtswidrig ist.

3.1.2
Neue Anlagen in Kommunen

Neue größere Überwachungsanlagen sind im Berichtsjahr in Gießen, Kassel und Limburg in Betrieb genommen worden. In allen Fällen wurden die Installierungen der Anlagen damit begründet, dass es sich bei den ausgewählten Orten um Kriminalitätsschwerpunkte handele.

3.1.2.1
Videoanlage am Gießener Marktplatz

Die ersten Überlegungen zu einer Überwachung des Gießener Marktplatzes stammen schon aus dem Jahre 2000. Damals wurde im Stadtparlament beantragt, in Zusammenarbeit mit der Polizei eine solche Anlage zu errichten. Damit sollten Straftaten verhindert werden, benannt wurden in der öffentlichen Diskussion dabei zunächst vor allem Taschendiebstähle und Beschaffungskriminalität. Des Weiteren gelte dieser Platz als Treffpunkt zur Verabredung von Straftaten. Als Besonderheit war angedacht, die an diesem Platz vorhandenen Anlagen der Verkehrsüberwachung des Busbahnhofes mitzunutzen. Nach längerer Diskussion wurde dann jedoch entschieden, dass die Stadt eine zusätzliche Anlage kauft und diese (zunächst) von der Polizei eingesetzt wird.

Im Juli d. J. hat das Polizeipräsidium Mittelhessen auf Anfrage die näheren Einzelheiten zur Verwirklichung dieses Projektes mitgeteilt. Danach wird die Anlage von der Polizei in Betrieb genommen. Zu einem späteren Zeitpunkt soll auch bei der Stadt Gießen ein Monitor aufgestellt werden. Das Polizeipräsidium Westhessen geht davon aus, dass die Untersuchung der Kriminalitätslage ausreicht, sowohl die Indikation einer Anlage gemäß § 14 Abs. 3 HSOG für die Polizei als auch die gemäß Abs. 4 dieser Vorschrift für die Stadt als allgemeine Gefahrenabwehrbehörde zu begründen.

Auch für die Nutzung der Anlage durch die Polizei waren aus meiner Sicht Nachbesserungen erforderlich. So soll nach der für den Einsatz der Anlage geschaffenen Dienstanweisung ein Zugriff auf die Monitore auch durch Organisationseinheiten ermöglicht werden, die nicht mit der Kontrolle des Marktplatzes und der entsprechenden Einsatzsteuerung befasst sind. An welche Zwecke im Rahmen der gesetzlichen Regelungen dabei gedacht wird, geht aus den Unterlagen nicht hervor.

Schließlich enthält die Dienstanweisung einen Hinweis, dass die Beobachtung der Fensterfronten von Wohn- und Geschäftshäusern untersagt ist. Aus den technischen Beschreibungen der eingesetzten Anlage war zu entnehmen, dass ein technischen Ausblenden durch eine „so genannte Privatzonenschaltung *beziehungsweise* privacy-masking“ möglich ist. Ich habe gefordert, dass diese technischen Maßnahmen auch eingesetzt werden müssen.

Eine Reaktion steht noch aus.

3.1.2.2
Videoüberwachung in Limburg

Die Anlage in Limburg fällt mit 14 installierten Kameras vergleichsweise groß aus. Dies hat seinen Grund insbesondere darin, dass zahlreiche Kameras die sehr unübersichtliche Unterführung des Bahnhofs und ihrer Zugangsbereiche im Visier haben. Bei der Einstellung der Schwenkbereiche der Kameras sind Mitarbeiterinnen meiner Dienststelle beteiligt gewesen. So konnte durch den Einsatz neuerer Technik erreicht werden, dass der Blick in Wohnungen und Geschäftsräume durch Sektorabtrennungen verhindert wird. Wird beispielsweise die Kamera auf die Fenster eines Wohnhauses geschwenkt, so wird das Bild automatisch schwarz. Die kontrollierenden Beamten haben damit nicht die Möglichkeit, sich in Privaträume zu zoomen.

3.1.3
Videoüberwachung in Verkehrsmitteln

Nicht nur öffentliche Plätze werden überwacht. Auch in Bussen und Bahnen hält die Videotechnik inzwischen Einzug. So werden bei der Hanauer Straßenbahn AG die neuen Busse mit Videotechnik ausgestattet. Es sind bis zu vier Kameras pro Bus installiert. Von einer Kamera, die den hinteren Busteil aufnimmt, werden die Bilder auf einen Monitor beim Fahrer übertragen. Die Busfahrer sollen in die Lage versetzt werden „randalierende“ Fahrgäste im Blick zu behalten. Insbesondere verspricht man sich vom Einsatz dieser Technik, dass die Sachbeschädigungen, wie etwa das Aufschlitzen der Sitze, zurückgehen. Bisher hat sich diese Erwartung bestätigt. Von weiteren Kameras werden Daten auf Wechselplatten aufgezeichnet, die der Fahrer nach Schichtschluss aus dem Bus entfernt. Zugriff auf diese Platten hat nur besonders autorisiertes Personal. Die Platten dürfen nur im Falle eines Zwischenfalls zur Beweissicherung ausgewertet werden. Die Auswertung erfolgt an einem Einzelplatz-PC, der sich in einem zusätzlich abgeschotteten Raum befindet. Kommt es zu keinem Zwischenfall, der eine Auswertung erforderlich machen würde, werden die auf einem Ringspeicher gespeicherten Daten nach 24 Stunden automatisch überschrieben. Zu bemängeln war bei den geprüften Anlagen, dass die Fahrgäste nicht deutlich auf die Videoüberwachung aufmerksam gemacht wurden. Eine Nachbesserung wurde zugesichert.

3.1.4
Videoüberwachung der Sicherheitszone einer Justizvollzugsanstalt

Eine ganz andere Zielrichtung als in den vorgenannten Beispielen hat die Videoüberwachung der Außenmauern und des Sicherheitszaunes einer Justizvollzugsanstalt. Trotzdem kann auch eine solche Zielrichtung einer Videoüberwachung berechtigte Interessen von Betroffenen beeinträchtigen.

Aufgrund einer Bürgereingabe besichtigte ich in einer hessischen Justizvollzugsanstalt die Funktionsweise der dort testweise und probehalber eingesetzten Videokameras. Gemeinsam mit der Leitung der Justizvollzugsanstalt wurde

festgestellt: Mit den ferngesteuerten, um 360 Grad schwenkbaren Kameras wurden nicht nur die Außenmauern und der Sicherheitszaun des Gefängnisses überwacht, sondern auch personenbezogene Informationen, insbesondere der Bewohner der benachbarten Häuser aufgenommen. Meine Mitarbeiter stimmten mit der Vollzugsanstalt darin überein, dass diese Aufnahmen nur beiläufig und unbeabsichtigt erfolgen, aber doch häufig unvermeidbar sind und die Anwohner in ihrer Privatsphäre beeinträchtigen. So war es mit den verwendeten Hochleistungskameras beispielsweise möglich, Fenster benachbarter Gebäude derart „gut“ auf den Monitor heranzuzoomen, dass bei Beleuchtung oder bei geöffneten Gardinen in die Wohnungen gesehen werden konnte. Das war auch der Anlass für die Datenschutzbeschwerde eines Nachbarn, der sich durch den Kameraeinsatz im Garten beobachtet fühlte. Der Leiter der Justizvollzugsanstalt versprach sofort Abhilfe. Die Herstellerfirma sollte die Schwenkungsbreite der Kameras durch technische Einrichtungen an einer bestimmten Stelle blockieren oder durch Abklebungen an den Aufnahmeeinrichtungen das Sichtfeld einschränken.

Beim zweiten Prüftermin führten die Sicherheitsbeamten der Justizvollzugsanstalt die Kameras erneut vor. Sie sind nach wie vor um 360 Grad schwenkbar. Sobald die Kamera aber vom unmittelbaren Bereich des Sicherheitszaunes wegschwenkt, zeigt der Bildschirm zunächst eine schwarze Abklebung, danach nur schwarz. Erst, wenn die Kamera so weit geschwenkt wird, dass sie den Sicherheitszaun in der entgegengesetzten Blickrichtung erreicht, erscheint erneut ein Teilbild mit der Abklebung und nach und nach wieder das volle Bild. Durch Abklebungen mit einer Folie auf den Aufnahmeköpfen der Kameras wird sichergestellt, dass nur ein ganz bestimmter Bildausschnitt aufgenommen und aufbereitet wird. Der abgeklebte Bildausschnitt wird bei der Aufnahme und der Wiedergabe ausgespart. Die Wirkung der Abklebung funktioniert auch beim Zoomen des Bildes. Wird beispielsweise in einer bestimmten Kamerastellung ausschließlich der Sicherheitszaun aufgenommen, so ist die Sicht durch keine Abklebung gehindert. Wird hingegen der Sichtwinkel erweitert, so dass private Wohnbereiche ins Blickfeld „fließen“ würden, so fließt mit steigendem Winkel die abgeklebte schwarze Fläche mehr und mehr ins Bild. Diese Funktion wurde meinen Mitarbeitern bei allen eingesetzten Kameras vorgeführt. Die beiläufige und unbeabsichtigte Aufnahme personenbezogener Daten kann jetzt nur noch in unvermeidbaren Ausnahmefällen erfolgen. Regelmäßig sind die aufgenommenen Passanten oder vorbeifahrenden Fahrzeuge derart weit von der Kamera entfernt, dass sie nicht oder nur schwer identifiziert werden können. Eine personenbeziehbare, durch Nachbearbeitung identifizierende Aufnahme von Personen erfolgt nur dann, wenn diese sich so nah am Sicherheitszaun aufhalten, dass Anlass zur Überprüfung besteht.

Gegen einen dauerhaften Einsatz der gegenwärtig noch probeweise eingesetzten Kameras ist damit aus datenschutzrechtlicher Sicht prinzipiell nichts mehr einzuwenden. Es müssen noch Festlegungen darüber getroffen werden, in welchen Situationen Aufnahmen zum Speichern hergestellt werden, wie, zu welchen Zwecken und wie lange die Filmaufnahmen aufbewahrt werden. Dies ist in einer Beschreibung nach § 18 Abs. 2 Bundesdatenschutzgesetz i. V. m. § 187 Satz 1 Strafvollzugsgesetz festzuhalten.

Den Nachbarn, der mich angeschrieben hatte, habe ich informiert. Es handelt sich um ein Beispiel guter Kooperation mit der Gefängnisleitung.

3.2
Auftragsdatenverarbeitung im Raumordnungsverfahren – Ausbau des Rhein-Main-Flughafens

Das Regierungspräsidium Darmstadt hat im Rahmen des Raumordnungsverfahrens die Auswertung der Einwendungen gegen den geplanten Ausbau des Rhein-Main-Flughafens einer Privatfirma übertragen, die damit als Auftragnehmer i. S. d. Hessischen Datenschutzgesetzes tätig wurde. Ich habe die Verträge, die mit dem Auftragnehmer abgeschlossen wurden unter datenschutzrechtlichen Aspekten überprüft und die ordnungsgemäße Verarbeitung der Daten bei der beauftragten Firma kontrolliert. Mein Augenmerk war auch darauf gerichtet, dafür Sorge zu tragen, dass keine personenbezogenen Daten an die Betreiberin Fraport AG übermittelt werden.

Die Beauftragung einer Privatfirma zur Auswertung der in vielen Fällen personenbezogenen Einwenderdaten ist datenschutzrechtlich dann möglich, wenn die Rahmenbedingungen des § 4 Hessisches Datenschutzgesetz (HDSG) zur Auftragsdatenverarbeitung eingehalten werden. Zwischen dem Regierungspräsidium Darmstadt als zuständiger Behörde für die Durchführung des Raumordnungsverfahrens und einer Firma aus Nordrhein-Westfalen wurde ein Vertrag abgeschlossen, der dem von meiner Dienststelle empfohlenen Mustervertrag zur Datenverarbeitung im Auftrag entspricht. Danach hat sich die beauftragte Firma verpflichtet, die Vorschriften des Hessischen Datenschutzgesetzes einzuhalten. In dem Vertrag wurden präzise Regelungen festgeschrieben, welche Rechte und Pflichten der Auftraggeber und der Auftragnehmer haben, insbesondere welche Datensicherungsmaßnahmen im Einzelnen vom Auftragnehmer zu treffen sind. Im Übrigen hat sich die Auftragnehmerin der Kontrolle durch den Hessischen Datenschutzbeauftragten unterworfen. Von diesem Kontrollrecht habe ich zu Beginn des Jahres 2002 Gebrauch gemacht.

Die beim Regierungspräsidium eingegangenen Einwendungen wurden dort gescannt; der Datenträger wurde dann per Kurier zum beauftragten Unternehmer transportiert. Durch eine stichprobenartige Kontrolle eines Datenträgers konnte ich mich davon überzeugen, dass die Daten verschlüsselt auf dem Datenträger hinterlegt waren. Dabei konnte jeweils nur die empfangsberechtigte Stelle den für sie bestimmten Datenträger entschlüsseln.

Aus allen Einwendungen wurden von der Auftragnehmerin die vorgetragenen Argumente gegen das Vorhaben extrahiert. Die vorgetragenen Argumente wurden in einer Datenbank den jeweiligen Einwendern zugeordnet. Einmal wöchentlich wurde der aktuelle Bestand exportiert, auf eine CD gebrannt und dem Regierungspräsidium auf dem oben beschriebenen Weg wieder zur Verfügung gestellt. Die Fraport AG als Flughafenbetreiberin erhielt jeweils auch eine Auflistung der vorgetragenen Einwendungen – allerdings hinsichtlich der privaten Einwender nur in anonymisierter Form. Die Träger der öffentlichen Belange wurden der Fraport AG als Einwender bekannt gegeben. Davon haben sich meine Mitarbeiter bei der Fraport AG zusammen mit Mitarbeitern des Regierungspräsidiums Darmstadt überzeugt. Ich konnte überprüfen, dass die Fraport AG den für das Regierungspräsidium bestimmten Datenträger nicht auswerten konnte, da sie nicht in der Lage war, diese Daten zu entschlüsseln. Der Erfüllung dieser Forderung galt mein besonderes Augenmerk; anders als im Planfeststellungsverfahren ist es für die Fraport AG im Rahmen des Raumordnungsverfahrens in keiner Weise erforderlich, dass sie sich in personenbezogener Form mit den einzelnen Einwendungen auseinander setzt.

Die Ablauforganisation hinsichtlich des Auswertens, Erfassens und Zuordnens der Argumente hatte das beauftragte Unternehmen bis auf einige Kleinigkeiten zur Zufriedenheit geregelt. Das Verfahren war so transparent ausgestaltet, dass die Auftragnehmerin und das Regierungspräsidium jederzeit nachvollziehen konnten, wer wann welche Daten bearbeitet hatte. Die technischen und organisatorischen Maßnahmen ließen keine Manipulationsmöglichkeit der personenbezogenen Daten und keine zweckwidrige Verwendung unter normalen Umständen zu. Eine festgestellte Lücke bei den räumlichen Sicherheitsmaßnahmen wurde auf das Betreiben meiner Mitarbeiter hin behoben.

Für die Dauer der Auswertung der Daten wurde in den speziell für dieses Verfahren genutzten Räumlichkeiten ein abgetrenntes Netzwerk eingerichtet, das eigens verlegte Leitungen nutzte. Andere Bereiche des Unternehmens hatten keinerlei Möglichkeiten, auf den Datenbestand aus dem Raumordnungsverfahren zuzugreifen. Lediglich bei der Passwortverwaltung war Kritik zu üben. Die Passwortverwaltung entsprach in Teilen nicht dem Stand der Technik. Hier habe ich gefordert, dass die Anmeldeprozedur dem Stand der Technik angepasst wird (dazu 30. Tätigkeitsbericht, Ziff. 14.1 und IT-Grundschutzhandbuch).

Die getroffenen rechtlichen, organisatorischen und technischen Maßnahmen stellten ausreichend sicher, dass unbefugte Personen die Daten von Einwendern nicht zur Kenntnis nehmen konnten.

3.3
Datenverarbeitung im Zusammenhang mit der Verleihung von öffentlichen Auszeichnungen und Ehrungen

Die Überlegungen der Landesregierung, die fehlende gesetzliche Regelung für die Verarbeitung von Daten im Zusammenhang mit der Verleihung von öffentlichen Auszeichnungen und Ehrungen zu schaffen, sind bis heute nicht in eine Gesetzesvorlage gemündet. Dies führt zu unzulässigen Datensammlungen bei Landes- und Kommunalbehörden, die meist unbefristet aufgehoben werden. Betroffene, deren Auszeichnung abgelehnt wird, erfahren nie, dass eine Datensammlung über sie besteht.

3.3.1
Anstoß zur Auszeichnung und Rechtsnatur des Verfahrens

Öffentliche Stellen in Hessen verleihen eine Vielzahl von Auszeichnungen oder Ehrungen (z. B. Hessischer Verdienstorden, Wilhelm-Leuschner-Medaille, Ehrenbrief, Rettungsmedaille, städtische Ehrenbürgerschaften, -medaillen, -plaketten, -bezeichnungen oder Ehrenpreise) und sind auch im Verfahren der Verleihung von Bundesauszeichnungen beteiligt (z. B. beim Bundesverdienstkreuz mit seinen verschiedenen Ehrungsstufen).

Die Verleihung solcher Auszeichnungen erfolgt auf Anregung von Dritten. Anregungen können Politiker, Institutionen (z. B. Vereine, die Industrie- und Handelskammern, Organisationen politischer Parteien) oder Bürgerinnen und Bürger geben. Solche Anregungen sind von recht unterschiedlicher Qualität – auch in Bezug auf Umfang und Erheblichkeit der zu dem oder der Vorgeschlagenen mitgeteilten Daten.

Auch wenn die Praxis in Einzelfällen anders aussehen kann, sollte die vorgeschlagene Person grundsätzlich von dem Vorschlag nichts wissen; die Auszeichnung sollte eine „Überraschung“ für sie oder ihn sein.

Das Verfahren bis zur Verleihung oder Versagung ist kein Verwaltungsverfahren im Sinne des Hessischen Verwaltungsverfahrensgesetzes; die Entscheidung kein Verwaltungsakt, weshalb eine Negativentscheidung auch nicht begründet werden muss und nicht mit Rechtsmitteln überprüft werden kann.

Bei der Entscheidung über die Verleihung einer Auszeichnung wird geprüft, ob die Angaben der Person, die den Vorschlag unterbreitet hat, eine Ehrung rechtfertigen, ob sie zutreffen und ob es in der Person des Betroffenen Gründe gibt, die gegen eine Auszeichnung sprechen. Zu diesem Zweck werden ohne Wissen der betroffenen Person bei öffentlichen Stellen und bei Dritten eine Vielzahl von personenbezogenen Daten erhoben, die ein umfassendes Persönlichkeitsbild ergeben.

3.3.2
Verfahrensabläufe bis zur Entscheidung über die Verleihung

3.3.2.1
Verfahren vor Verleihung von Bundesauszeichnungen

Beim Bundesverdienstorden für hessische Bürgerinnen und Bürger hat die Hessische Staatskanzlei die Federführung. Geht die Anregung bei ihr ein, fordert sie den Landrat, bei kreisfreien Städten die Wohnsitzgemeinde, zu Auskünften und weiteren Ermittlungen auf. In dem Formschreiben wird gebeten, zunächst die Ermittlungen der Verdienste durchzuführen und erst wenn sich diese im Hinblick auf die vorgesehene Auszeichnung als ausreichend erwiesen haben, die Ermittlungen zur Ordenswürdigkeit durchzuführen. Die Ermittlungen sollten möglichst innerhalb von drei Monaten abgeschlossen sein. Geht der Vorschlag direkt beim Landrat oder der Wohnsitzgemeinde ein, wird diese von sich aus tätig und informiert die Staatskanzlei darüber, dass ihr ein Vorschlag vorliegt.

Die Verdienste werden auf Basis der Angaben aus dem Schreiben, mit dem die Auszeichnung angeregt wurde, durch schriftliche Anfragen ermittelt. Regelmäßig wird dabei eine Kopie des Schreibens mitversandt. Zur Ermittlung der Ordenswürdigkeit wird ein Auszug aus dem Bundeszentralregister (polizeiliches Führungszeugnis) und – wenn es sich um Bürger der ehemaligen Deutschen Demokratischen Republik handelt – eine Auskunft bei der Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik in Berlin sowie – bei Betroffenen, deren Geburtsdatum vor 1926 liegt – eine Auskunft beim Bundessarchiv und der zuständigen Spruchkammer zur Ermittlung einer eventuellen nationalsozialistischen Vergangenheit angefordert. Die Gemeinden gehen – um Zeit zu sparen – regelmäßig so vor, dass Verdienste und Ordenswürdigkeit parallel ermittelt werden.

Die Erkenntnisse werden in einem Bericht zusammengefasst, der mit dem Führungszeugnis und sonstigen Auskünften an die Hessische Staatskanzlei weitergegeben wird. Diese bittet die einschlägigen Ressorts um Stellungnahme zur Auszeichnung (z. B. das Hessische Sozialministerium bei Personen, die wegen ihres Engagements im sozialen Bereich geehrt werden sollen; das Hessische Ministerium für Wirtschaft, Verkehr und Landesentwicklung bei Ehrungen für wirtschaftliches Engagement) und schließt die Prüfung unter Berücksichtigung aller Ergebnisse mit einem Entscheidungsvorschlag für den Bundespräsidenten ab. Der Vorschlag beinhaltet auch einen Lebenslauf mit beruflichem Werdegang und die für die Beurteilung der Auszeichnungswürdigkeit wichtigen Daten. In der Mehrzahl der Fälle wird die Auszeichnung empfohlen, es kann aber auch eine Ablehnung der Auszeichnung vorgeschlagen werden, z. B. wenn die Verdienste eine solche Auszeichnung (noch) nicht rechtfertigen. Selbst wenn die Verleihung befürwortet wird, muss das Bundespräsidialamt dem nicht folgen. Es teilt seine Entscheidung der Hessischen Staatskanzlei mit und übersendet bei positiver Entscheidung den Orden zur Aushändigung. Die Verleihung findet regelmäßig in festlichem Rahmen mit ausführlicher Laudatio statt, für die Daten aus den Erhebungen zur Verleihungsentscheidung verwendet werden. Die betroffene Person wird mit der Einladung über die Verleihung informiert und erhält in diesem Zusammenhang auch die Information, dass personenbezogene Daten gespeichert sind. Auch die Person oder Institution, die die Verleihung angeregt hat, erhält eine Information über die Entscheidung. Über die anstehende Verleihung wird regelmäßig das zuvor beteiligte Ressort und die Presse informiert. Die Verleihung wird im Staatsanzeiger veröffentlicht. Wird sie abgelehnt, so erfährt die betroffene Person nichts; lediglich die Person oder Institution, die die Verleihung angeregt hat, wird darüber informiert; Ablehnungsgründe werden dabei grundsätzlich nicht mitgeteilt.

Die Akten, die im Zusammenhang mit der Entscheidung über die Verleihung entstehen, werden sowohl bei der Staatskanzlei als auch bei den von mir im Rahmen des Informationsbesuches befragten Gemeinden aufbewahrt und zwar unabhängig davon, ob es zu einer Verleihung kommt oder nicht. Fristen für die Aussonderung waren nicht vorgesehen.

3.3.2.2
Verfahren vor Verleihung von Landesauszeichnungen

Bei Landesauszeichnungen ist das Verfahren ähnlich. Für die Entscheidung über die Verleihung des Hessischen Verdienstordens werden die gleichen Ermittlungen angestellt wie für Bundesauszeichnungen. Bei den anderen Landesauszeichnungen wird zur Ermittlung der Ordenswürdigkeit nur ein Führungszeugnis angefordert. Die Entscheidung über die Verleihung eines Ehrenbriefes des Landes Hessens wird in den kreisfreien Städten von den Oberbürgermeistern, im Übrigen von den Landräten getroffen. Die Hessische Staatskanzlei ist hierbei nicht mehr eingeschaltet. Die Entscheidung über die Verleihung der Rettungsmedaille trifft die Staatskanzlei.

3.3.2.3
Verfahren vor Verleihung von Auszeichnungen anderer öffentlicher Stellen in Hessen (z. B. Kommunen)

Die Gemeinden in Hessen verleihen selbst eine Vielzahl von Auszeichnungen und Ehrungen. Die der Entscheidung über diese Verleihungen vorausgehenden Datenerhebungen führen die Gemeinden selbst durch. Auskünfte beim Bundeszentralregister oder dem Staatsarchiv werden nach meinen Recherchen nicht eingeholt. Die Entscheidung wird kurz begründet.

Handelt es sich um allseits bekannte Personen des öffentlichen Lebens der Kommune, werden kaum Datenerhebungen durchgeführt; der überwiegende Teil der erforderlichen Daten kann aus öffentlich zugänglichen Quellen entnommen werden. Allerdings werden Grunddaten in der Regel durch Auskunft beim Einwohnermeldeamt verifiziert. In anderen Fällen erfolgen umfangreiche Erhebungen, insbesondere, wenn es um die Ermittlung von ehrenamtlichen Tätigkeiten oder den Einsatz im Wirtschaftsleben oder für Vereine geht.

3.3.3
Rechtsgrundlagen für Auszeichnungen und Ehrungen

Rechtsgrundlagen für die Verleihung von Auszeichnungen finden sich für die Bundesauszeichnungen im Gesetz über Titel, Orden und Ehrenzeichen vom 26. Juli 1957 (BGBl. I S. 844) sowie dem Verdienstordensstatut und Ausführungsbestimmungen. Für die verschiedenen Landesauszeichnungen gibt es keine entsprechende zusammengefasste Rechtsgrundlage; sie sind in mehreren gesetzlichen (z. B. Hessische Rettungsmedaille im Gesetz über die staatliche Anerkennung von Rettungstaten, GVBl. 1953 S. 123) oder untergesetzlichen Vorschriften geregelt (z. B. Erlass über die Stiftung des Hessischen Verdienstordens sowie Richtlinie dazu, GVBl. 1989 S. 443; 1998 S. 313, 2002 S. 571 ff.; Erlass über die Stiftung des Ehrenbriefes des Landes Hessen in der Fassung vom 23. Mai 2002, GVBl. S. 575). Die Grundlagen für Verleihung der kommunalen Ehrungen sind – jedenfalls bei den beiden großen Kommunen, denen ich einen Informationsbesuch abgestattet habe – in Ehrungsordnungen niedergelegt. Datenschutzrechtliche Regelungen oder spezielle Erlaubnistatbestände finden sich in keiner dieser Regelungen.

3.3.4
Datenschutzrechtliche Bewertung des derzeitigen Verfahrens

Da für die Datenverarbeitung keine Einwilligung der Betroffenen eingeholt wird – diese sollen gerade nichts von der Absicht der Ehrung wissen – ist sie nach § 7 Hessisches Datenschutzgesetz (HDSG) nur zulässig, wenn eine spezielle Rechtsvorschrift oder das HDSG dies erlauben. Wie oben erläutert, sind datenschutzrechtliche Spezialvorschriften für die Verarbeitung personenbezogener Daten im Zusammenhang mit der Verleihung von Auszeichnungen und Ehrungen auf Bundesebene und in Hessen nicht vorhanden. Deshalb kommt als Rechtsgrundlage für die Verarbeitung von Daten durch öffentliche Stellen in Hessen in Auszeichnungsangelegenheiten allein das HDSG in Betracht. Zwar erlaubt § 11 Abs. 1 HDSG Datenverarbeitungen, soweit sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der datenverarbeitenden Stelle liegenden Aufgaben und für den jeweils damit verbundenen Zweck erforderlich sind; die weiteren Regelungen des HDSG müssen dann jedoch strikt eingehalten werden.

§ 11 HDSG erlaubt grundsätzlich nur die Verarbeitung von für die Aufgabenerledigung erforderlichen Daten.

§ 11 HDSG

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

(2) Sind personenbezogene Daten in Akten derart verbunden, dass ihre Trennung nach erforderlichen und nicht erforderlichen Daten nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist, dann sind die Kenntnisnahme, die Weitergabe innerhalb der datenverarbeitenden Stelle und die Übermittlung der Daten, die nicht zur Erfüllung der jeweiligen Aufgabe erforderlich sind, über Abs. 1 hinaus zulässig. Diese Daten unterliegen insoweit einem Verwertungsverbot.

In vielen Fällen sind in den Verleihungsakten Daten enthalten, die für die Entscheidung über die Verleihung einer Auszeichnung oder Ehrung nicht erforderlich sind. Solche Daten sind insbesondere in Anregungsschreiben und in Mitteilungen von angefragten Stellen bei der Ermittlung der Verdienste, besonders in Mitteilungen von Privatpersonen oder nicht-öffentlichen Stellen enthalten. Hier finden sich beispielsweise Daten nicht nur über die betroffene Person, sondern auch über deren Eltern (vollständige Namen und Berufsbezeichnung der Eltern), Ehegatten (Tätigkeiten, Heirats-, Geburts- und Sterbedatum), Kinder (Geburtsdaten, Ausbildung) sowie sonstige für das Verfahren völlig unerhebliche Daten (z. B. Sozialverhalten). Oft wird die Persönlichkeit charakterisiert und es werden Persönlichkeitsbewertungen abgegeben, die sich dann in den Akten befinden. Häufig werden auch Gesundheitsdaten oder andere unter die Vorschrift des § 7 Abs. 4 HDSG fallende Daten mitgeteilt, obwohl dies für die Verleihungsentscheidung unerheblich ist. Gerade bei älteren Personen wird der Gesundheitszustand oft als Begründung dafür angeführt, dass eine Auszeichnung (bald) erfolgen sollte. Die Verarbeitung solcher Daten setzt nach § 7 Abs. 4 HDSG eine spezielle Rechtsgrundlage voraus; § 11 HDSG genügt hierfür nicht.

§ 7 Abs. 4 HDSG

Soweit nicht eine Rechtsvorschrift die Verarbeitung personenbezogener Daten über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Gewerkschaftszugehörigkeit, die

Gesundheit oder das Sexualleben vorsieht oder zwingend voraussetzt, darf eine Verarbeitung nur nach §§ 33 bis 35 und 39 erfolgen. Im Übrigen ist eine Verarbeitung aufgrund dieses Gesetzes nur zulässig, wenn sie ausschließlich im Interesse des Betroffenen liegt und der Hessische Datenschutzbeauftragte vorab gehört worden ist.

Besonders problematisch sind – der Natur der Sache nach – Datenerhebungen, die nicht beim Betroffenen, sondern bei Dritten erfolgen. § 12 HDSG sieht dagegen vor, dass Datenerhebungen grundsätzlich beim Betroffenen zu erfolgen haben und lässt nur in besonders geregelten Fällen Ausnahmen zu.

§ 12 Abs. 1 bis 3 HDSG

(1) Personenbezogene Daten sind grundsätzlich bei dem Betroffenen mit seiner Kenntnis zu erheben. ...

(2) Bei öffentlichen Stellen dürfen Daten im Einzelfall ohne seine Kenntnis nur erhoben werden, wenn

1. eine Rechtsvorschrift dies vorsieht, zwingend voraussetzt oder der Betroffene eingewilligt hat,
2. die Bearbeitung eines vom Betroffenen gestellten Antrags ohne Kenntnis der Daten nicht möglich ist oder Angaben des Betroffenen überprüft werden müssen ...,
3. die Abwehr erheblicher Nachteile für das Allgemeinwohl oder von Gefahren für Leben, Gesundheit und persönliche Freiheit dies gebietet,
4. sich bei Gelegenheit der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben oder
5. die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Belange des Betroffenen beeinträchtigt werden können.

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

Keine der in § 12 Abs. 2 und 3 HDSG aufgeführten Ausnahmen trifft hier zu. Eine Rechtsgrundlage für die Datenerhebung ohne Kenntnis des Betroffenen gibt es demzufolge nicht.

Gleiches gilt für die Übermittlung von Daten von öffentlichen Stellen, die dort vorhanden sind, aber nicht für diesen Zweck erhoben wurden. § 13 Abs. 2 HDSG verweist auf die Ausnahmen in § 12 Abs. 2 und 3 HDSG, die gerade nicht einschlägig sind.

§ 13 Abs. 1 und 2 HDSG

(1) Personenbezogene Daten dürfen grundsätzlich nur für den Zweck weiterverarbeitet werden, für den sie erhoben oder gespeichert worden sind.

(2) Sollen personenbezogene Daten zu Zwecken verarbeitet werden, für die sie nicht erhoben oder gespeichert worden sind, dann ist dies nur aus den in § 12 Abs. 2 und 3 genannten Gründen zulässig. Besondere Amts- oder Berufsgeheimnisse bleiben unberührt.

Nach § 19 Abs. 3 HDSG sind personenbezogene Daten unverzüglich zu löschen, wenn sie für den ursprünglichen Verarbeitungszweck nicht mehr erforderlich sind.

§ 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 aufgrund 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.

Nach der Entscheidung über die Verleihung einer Auszeichnung oder Ehrung sind die Daten für diesen Zweck nicht mehr erforderlich. Zur Begründung der weiteren Aufbewahrung wurden meiner Mitarbeiterin beim Informationsbesuch in einer Gemeinde dargelegt, dass die Daten für Glückwünsche zu runden Geburtstagen genutzt würden. In der Staatskanzlei wurde die weitere Aufbewahrung mit der Vermeidung neuer Datenerhebung bei späteren Auszeichnungsanregungen begründet. Dass die Bereitstellung der für die Prüfung einer Auszeichnung erhobenen Daten für andere Zwecke nicht mit dem Datenschutz in Einklang zu bringen ist, liegt auf der Hand. Auch das nachvollziehbare Argument der Aufbewahrung zur Verwendung in einem späteren Verleihungsverfahren ist datenschutz-

rechtlich nicht korrekt, da Zweck der Datenverarbeitung nur das jeweilige Verfahren zur Entscheidung über die Verleihung einer Auszeichnung ist. Nachdem diese Entscheidung gefallen ist, ist die Datenspeicherung für diesen Zweck nicht mehr erforderlich.

Nach § 18 HDSG haben Betroffene das Recht auf Auskunft und Benachrichtigung über die zur ihrer Person gespeicherten Daten. Bei Akten tritt an Stelle des Auskunfts- ein Einsichtsrecht.

§ 18 HDSG

(1) Datenverarbeitende Stellen, die personenbezogene Daten automatisiert speichern, haben die Betroffenen von dieser Tatsache schriftlich zu benachrichtigen und dabei die Art der Daten sowie die Zweckbestimmung und die Rechtsgrundlage der Speicherung zu nennen. ...

(2) Eine Pflicht zur Benachrichtigung besteht nicht, wenn

1. die Daten beim Betroffenen erhoben oder von ihm mitgeteilt worden sind,
2. die Verarbeitung der personenbezogenen Daten durch Gesetz ausdrücklich vorgesehen ist,
3. der Betroffene auf andere Weise Kenntnis von der Verarbeitung seiner Daten erlangt hat,
4. die Benachrichtigung des Betroffenen unmöglich ist oder einen unverhältnismäßigen Aufwand erfordert.

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

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

...

(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. ...

Eine Benachrichtigung unterbleibt, wenn keine Auszeichnung verliehen wird. Wegen der Besonderheiten des Verfahrens der Verleihung von Auszeichnungen oder Ehrungen ist eine Benachrichtigung auch künftig nicht beabsichtigt. Bei Ablehnungen, aber auch im Fall einer Positiventscheidung, wird kein (umfassendes) Auskunfts- oder Einsichtsrecht gewährt.

Das derzeitige Verfahren im Zusammenhang mit der Verleihung von Auszeichnungen und Ehrungen ist deshalb – solange eine spezielle Rechtsgrundlage fehlt – aus mehreren Gründen datenschutzrechtlich unzulässig.

3.3.5
Regelungsbedarf

Aus den unter 3.3.4 aufgeführten fehlenden Rechtsgrundlagen ergibt sich der Umfang des Regelungsbedarfes, der als Grundlage für die Rechtmäßigkeit der Datenverarbeitung im Zusammenhang mit der Verleihung von Auszeichnungen und Ehrungen notwendig ist. Eckpunkte sind:

- Die Ermächtigung zur Erhebung personenbezogener Daten ohne Kenntnis der Betroffenen zum Zweck der Entscheidung über die Verleihung öffentlicher Auszeichnungen sowie die Ermächtigung für die Übermittlung von Daten durch öffentliche Stellen zu diesem Zweck.
- Der Erhebung bei öffentlichen Stellen sollte der Vorrang vor der Erhebung bei Dritten eingeräumt werden, da die Praxis zeigt, dass öffentliche Stellen regelmäßig nur erforderliche Daten übermitteln, während Dritte häufig nicht nach der Erforderlichkeit unterscheiden und „Überschussdaten“ liefern.
- Eine ausdrückliche Ermächtigung zur Erhebung von Daten nach § 7 Abs. 4 Satz 1 HDSG, soweit sie für die Entscheidung unabdingbar sind.
- Daten von Betroffenen, von denen bekannt ist, dass sie keine öffentliche Auszeichnung oder Ehrung möchten, dürfen nicht erhoben werden.
- Die Regelung muss konkrete Löschfristen vorgeben.
- Es muss ein Erlaubnistatbestand geschaffen werden, Daten über die Entscheidung hinaus aufzubewahren. Hier darf – dem Grundsatz der Datensparsamkeit entsprechend – nur ein reduzierter Datensatz aufbewahrt werden.
- Die Auskunfts- beziehungsweise Einsichtsrechte und die Benachrichtigungspflichten dürfen nur reduziert werden, wenn ausreichende Garantien für die Betroffenen gewährt werden, z. B. durch Einschaltung des Hessischen Datenschutzbeauftragten bei Ablehnung der Auskunft.

3.3.6
Stand der Überlegungen der Landesregierung

In einer gemeinsamen Arbeitsgruppe der Hessischen Staatskanzlei, des Hessischen Innenministeriums und meiner Beteiligung wurden zunächst aufwändig die Grundlagen und verschiedenen Erfordernisse des Verfahrens für Auszeichnungen und Ehrungen aufgearbeitet und diskutiert. Auf Basis der gewonnenen Erkenntnisse wurde ein Vorschlag für ein hessisches Gesetz zur Regelung der Datenverarbeitung im Zusammenhang mit der Verleihung von Auszeichnungen und Ehrungen erarbeitet. Nachdem die Arbeitsgruppe mehr als ein Jahr gearbeitet hatte, geriet der Fortgang ins Stocken, weil grundsätzliche Erwägungen, die bereits am Anfang geklärt waren, erneut aufgegriffen wurden. Deshalb habe ich im Juni 2002 in einem Schreiben an die Hessische Staatskanzlei die datenschutzrechtlichen Probleme dargestellt und Eckpunkte für eine gesetzliche Regelung formuliert. Wider Erwarten hat die Hessische Staatskanzlei die Einbringung eines solchen Gesetzes abgelehnt und stattdessen am Jahresende dem Hessischen Ministerium des Innern und für Sport die Einfügung einer im Wortlaut mit mir abgestimmten Sondervorschrift in das Hessische Datenschutzgesetz vorgeschlagen. Ob und inwieweit von dort der Vorschlag weiter verfolgt wird, war bei Redaktionsschluss noch nicht absehbar.

Festzuhalten bleibt, dass auch in der 15. Wahlperiode die Rechtsgrundlage für die Datenverarbeitung im Zusammenhang mit der Verleihung von Orden und Ehrenzeichen nicht geschaffen wurde. Infolgedessen finden fortgesetzt Eingriffe in den Datenschutz statt, die gesetzlich nicht legitimiert sind. Die Entwicklung muss in der nächsten Wahlperiode zu einem datenschutzgerechten Abschluss gebracht werden.

3.4
Verweigerung der Auskunft über eigene Daten

Das Recht auf Auskunft über eigene Daten wird Anfragern oft zu Unrecht vorenthalten.

Zu den elementaren Rechten der von der Verarbeitung ihrer personenbezogenen Daten Betroffenen gehört das Recht auf Auskunft über Daten, die zur eigenen Person gespeichert werden. Neben zahlreichen bereichsspezifischen Regelungen – sind § 18 Hessisches Datenschutzgesetz (HDSG) und im Bundesdatenschutzrecht § 19 Bundesdatenschutzgesetz (BDSG) maßgebend.

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

(6) Abs. 1 und 3 gelten nicht, soweit eine Abwägung ergibt, dass die dort gewährten Rechte des Betroffenen hinter dem öffentlichen Interesse an der Geheimhaltung oder einem überwiegenden Geheimhaltungsinteresse Dritter zurücktreten müssen. Die Entscheidung trifft der Leiter der speichernden Stelle oder dessen Stellvertreter. Werden Auskunft oder Einsicht nicht gewährt, ist der Betroffene unter Mitteilung der wesentlichen Gründe darauf hinzuweisen, dass er sich an den Hessischen Datenschutzbeauftragten wenden kann.

...

§ 19 BDSG

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

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

2. die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden, und
3. den Zweck der Speicherung.

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

(2) Absatz 1 gilt nicht für personenbezogene Daten, die nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen und eine Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.

(3) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

(4) Die Auskunftserteilung unterbleibt, soweit

1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben gefährden würde,
2. die Auskunft die öffentliche Sicherheit und Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder
3. die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheimgehalten werden müssen

und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.

(5) Die Ablehnung der Auskunftserteilung bedarf einer Begründung nicht, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Falle ist der Betroffene darauf hinzuweisen, dass er sich an den Bundesbeauftragten für den Datenschutz wenden kann.

(6) Wird dem Betroffenen keine Auskunft erteilt, so ist sie auf sein Verlangen dem Bundesbeauftragten für den Datenschutz zu erteilen, soweit nicht die jeweils zuständige oberste Bundesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die Mitteilung des Bundesbeauftragten an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand der verantwortlichen Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.

(7) Die Auskunft ist unentgeltlich.

Im Gegensatz zum BDSG sieht das HDSG zusätzlich zum Auskunftsrecht ein Akteneinsichtsrecht vor, sofern keine Geheimhaltung notwendig ist. Einsichtsrechte finden sich in den für den Sicherheitsbereich geltenden bereichspezifischen Vorschriften nicht. Alle Regelungen zum Auskunftsrecht sehen vor, dass die Auskunft in bestimmten Fällen verweigert werden kann. In solchen Fällen muss der Anfrager darauf hingewiesen werden, dass er sich an den Datenschutzbeauftragten wenden kann. Zum Thema existieren in großem Umfang wissenschaftliche Abhandlungen, Rechtsprechung und weiteres Material (dazu beispielsweise Nungesser, HDSG, § 18, Rdnr. 19 ff.; Gola/Schomerus, BDSG, § 19, vor Rdnr. 1 und 1 ff.).

Trotz der klaren Vorschriften kommt es im Alltag recht häufig vor, dass Betroffenen die Auskunft über die zur eigenen Person gespeicherten Daten verweigert wird – nur teilweise zu Recht. Im Berichtszeitraum wurden Einzelfälle der Auskunftsverweigerung durch öffentliche Stellen aus verschiedenen Anwendungsbereichen an mich herangetragen.

3.4.1
Justizvollzug

Ein Insasse einer hessischen Justizvollzugsanstalt bat mich u. a. um Auskunft, ob auch er Datenschutzrechte genieße und ein Recht auf Auskunft über eigene Daten habe. Ich wies ihn auf die im Jahre 1998 mit dem 4. Gesetz zur Änderung des Strafvollzugsgesetzes (StVollzG – BGBl. I S. 2462) ins Strafvollzugsrecht eingefügten Bestimmung in § 185 StVollzG hin.

§ 185 StVollzG

Der Betroffene erhält nach Maßgabe des § 19 des Bundesdatenschutzgesetzes Auskunft und, soweit eine Auskunft für die Wahrnehmung seiner rechtlichen Interessen nicht ausreicht und er hierfür auf die Einsichtnahme angewiesen ist,

Akteneinsicht. An die Stelle des Bundesbeauftragten für den Datenschutz in § 19 Abs. 5 und 6 des Bundesdatenschutzgesetzes tritt der Landesbeauftragte für den Datenschutz, an die Stelle der obersten Bundesbehörde tritt die entsprechende Landesbehörde.

Einige Zeit danach meldete sich der Gefangene erneut bei mir und führte an, die Justizvollzugsanstalt ignoriere sein Auskunftsverlangen. Die Anstalt antwortete mir auf Nachfrage, die Fragen des Verurteilten seien sämtlich beantwortet worden. Der Gefangene erwiderte, er habe Anfang Januar um Auskunft über die Speicherung personenbezogener Daten gebeten. Dabei habe er folgende Auflistung gestellt:

1. Stammdaten zu seiner Person
2. Daten aus dem Bundeszentralregister
3. personenbezogene Meldedaten
4. Sozialversicherungsdaten
5. Verkehrszentralregisterdaten
6. erkennungsdienstliche, personenbezogene Daten (ggf. digitalisierte Fotografie)
7. vermerkte Übermittlungssperren
8. Gesundheitsdaten

Er legte mir die Antwort der Anstaltsleitung vom Mai diesen Jahres vor. Sie lautete:

„Sehr geehrter Herr ....,

ich bitte die verspätete Antwort auf Ihr Schreiben vom 07.01.02 zu entschuldigen.

zu 1: Ihre Stammdaten werden gespeichert

zu 3: geben Sie bei der Aufnahme an

zu 4: verweise ich Sie an die Arbeitsverwaltung

zu 5: wird von der zuständigen Vollstreckungsbehörde an uns versandt

zu 6: diese Daten werden nach der VGO (Anmerkung: Vollstreckungsgeschäftsordnung) aufbewahrt

zu 7: erbitte ich nähere Erklärung

zu 8: wenden Sie sich an den Arzt

zu 2: siehe Punkt 4“

Ich schrieb erneut die Anstalt an, denn diese Auskunft entsprach in keiner Weise den gesetzlichen Anforderungen des § 19 BDSG, auf den § 185 StVollzG verweist. Ich kündigte eine Beanstandung nach § 27 HDSG an. Nunmehr meldete sich der Anstaltsleiter. Er reklamierte ein Versehen seines Mitarbeiters und versicherte, dass inzwischen mit dem Gefangenen gemeinsam ausführlich alle seine Fragen erörtert worden seien und dass er auszugsweise Akteneinsicht und Einsicht in Computerausdrucke erhalten habe.

3.4.2
Strafverfolgung

3.4.2.1
Amtsanwaltschaft

In einem zweiten Fall hatte ein Ermittlungsverfahren wegen Körperverletzung ergeben, dass der Beschuldigte unschuldig war. Die zuständige Amtsanwaltschaft hatte das Verfahren nach § 170 Abs. 2 Strafprozessordnung (StPO) eingestellt. Nachdem sich der ehemals Beschuldigte – mit Erfolg – vergewissert hatte, dass die Polizei zu diesem Sachverhalt keine Daten gespeichert hat, musste er zur Kenntnis nehmen, dass die Justizbehörde sehr wohl Daten zu dem Vorgang aufbewahrt. Auch wenn sich seine Unschuld ergeben hatte, durften bestimmte Grunddaten zum Ermittlungsverfahren, wenn auch nur zeitlich befristet, zur Dokumentation des Vorganges aufbewahrt werden. Um Genaues zu erfahren, wandte er sich an die Justizbehörde. Die ihm erteilte Antwort legte er mir vor und bat mich um eine Stellungnahme. Seine schriftlich gestellte Frage lautete:

„... bitte ich um Auskunft und Benachrichtigung über

1. die zu meiner Person gespeicherten Daten,

2. die Rechtsgrundlage, die Dauer und den Zweck der Speicherung,

3. die Empfänger von Datenübermittlungen, soweit dies gespeichert ist beziehungsweise war.“

Die schriftlich erteilte, unbefriedigende Antwort zu dieser Frage lautete:

„ ...(es)... findet bei Ihnen – wie bei allen anderen auch – das geltende Datenschutzrecht und die Aktenordnung seine Anwendung ....“

Ich musste die Justizbehörde auf die in § 491 StPO getroffene bereichsspezifische Regelung zum Recht auf Auskunft über eigene Daten aufmerksam machen.

§ 491 StPO

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

(2) Eine Auskunft an Nichtverfahrensbeteiligte unterbleibt auch, wenn hierdurch der Untersuchungszweck gefährdet werden könnte oder überwiegende schutzwürdige Interessen Dritter entgegenstehen. Liegen diese Voraussetzungen vor, bedarf die Ablehnung der Auskunftserteilung keiner Begründung. § 19 Abs. 5 Satz 2 und Abs. 6 des Bundesdatenschutzgesetzes gilt entsprechend.

(3) Ist der Betroffene bei einer gemeinsamen Datei nicht in der Lage, die speichernde Stelle festzustellen, so kann er sich an jede beteiligte speicherungsberechtigte Stelle wenden. Über die Erteilung einer Auskunft entscheidet diese im Einvernehmen mit der Stelle, die die Daten eingegeben hat.

Durch den Verweis in § 491 Abs. 1 StPO auf § 19 des BDSG orientiert sich der Umfang der Auskunftspflicht an den Fragen des Beschuldigten. Diese waren mit der erteilten Aussage, dass das Datenschutzrecht und die Aktenordnung Anwendung fände, keineswegs beantwortet. Die Justizbehörde sagte zu, die Auskunft nachzubessern, dem Betroffenen ein Gespräch anzubieten, in dem ihm auch Einsicht in einen Computerausdruck angeboten wurde. Tatsächlich umfasste die Datenspeicherung folgende Informationen: Familienname, Vorname, Geburtsdatum, Geburtsort, Anschrift, Aktenzeichen, Eingangsdatum, Organisationskennziffer der bearbeitenden Stelle, Angabe des Delikts wegen dem ermittelt wurde, Tatzeit, Erledigungsart und Erledigungsdatum. Diese Datenspeicherung ist gem. § 484 StPO zulässig. Außerdem wurde dem (ehemals) Beschuldigten substanziiert Antwort auf seine weiteren Fragen erteilt.

3.4.2.2
Staatsanwaltschaft

In einem dritten Fall erfuhr eine Versicherung, die eine Anwaltskanzlei mit der Interessenwahrnehmung ihres Versicherten in einer Strafsache beauftragt hatte, dass gegen ihn noch in einer anderen Sache ermittelt wurde. Sie erteilte ihre Deckungszusage nur unter Vorbehalt und bat den Antragsteller um nähere Aufklärung. Daraufhin fragte er bei der Staatsanwaltschaft nach, ob und wenn ja, was gegen ihn vorliege. Auf Erinnerung entschuldigte sich die Staatsanwaltschaft vier Monate nach seiner Anfrage unter Hinweis auf ein Büroversehen für die verspätete Antwort. Die Antwort auf seine Frage lautete lapidar:

„Zu Ihren Anfragen verweise ich auf § 491 StPO und § 19 BDSG. Es steht Ihnen frei, sich an den Bundesbeauftragten für den Datenschutz zu wenden.“

Daraufhin wandte er sich an den Bundesbeauftragten für den Datenschutz und bat um Mitteilung, ob eine Strafanzeige gegen ihn vorliege und ggf. um Übersendung einer Kopie. Zwar verweist für den Fall der Auskunftsverweigerung § 491 Abs. 2 StPO auf § 19 Abs. 5 und 6 BDSG. Dort ist vom Bundesdatenschutzbeauftragten die Rede, doch tritt an dessen Stelle, wenn datenverarbeitende Stelle eine Landesbehörde ist, der Landesdatenschutzbeauftragte. Die Staatsanwaltschaft hätte daher nicht auf den Bundesdatenschutzbeauftragten, sondern auf mich verweisen müssen. Davon abgesehen wäre es angebracht gewesen, zu erläutern, dass die Auskunft verweigert wird. Denn so konnte der Betroffene allenfalls ahnen, weshalb er sich an den Bundesdatenschutzbeauftragten wenden soll.

Nachdem der Bundesdatenschutzbeauftragte den Vorgang mit der Bitte um Übernahme der Bearbeitung übersandt hatte, informierte ich den Betroffenen, dass der Datenschutzbeauftragte nicht an Stelle der Staatsanwaltschaft die gewünschte Auskunft erteilen oder Kopien zur Verfügung stellen könne. Nur die Rechtmäßigkeit einer Auskunftsverweigerung ist zu prüfen. Ggf. ist auf Auskunftserteilung durch die speichernde Stelle zu drängen. Anlässlich eines mit der Staatsanwaltschaft vereinbarten Termins zur Akteneinsicht wurde mir die Akte unvollständig vorgelegt. Nur in den Verwaltungsvorgang, in dem auf den Bundesdatenschutzbeauftragten verwiesen worden war, konnte ich Einsicht nehmen. Es handele sich um eine laufende Strafsache von großer Bedeutung – so die Staatsanwaltschaft. Es sei ein Beschluss nach § 102 StPO (Durchsuchung beim Verdächtigen) ergangen. Der Beschluss sei aber noch nicht vollstreckt. Deshalb dürfe der Betroffene nicht informiert werden. Sonst werde der Erfolg, der mit der Durchsuchung erreicht werden soll, vereitelt (vgl. § 19 Abs. 4 Nr. 1 BDSG). Die Auskunftsverweigerung zu begründen, sei nicht angetan, denn schon mit der Begründung werde der beabsichtigte Zweck der Maßnahme gefährdet (vgl. § 19 Abs. 5 BDSG).

Natürlich sind Verfahren, in denen Auskunft nebst Begründung unterbleiben müssen, realistisch. Auch die Datenschutzgesetze treffen dafür Vorsorge. Trotzdem erschien es mir notwendig, die Fallgestaltung konkret nachzuvollziehen. Ich wies auf die zeitliche Distanz hin. Mittlerweile bemühte sich der Betroffene bereits seit zehn Monaten vergeblich zu erfahren, ob und wegen welchen Vorwurfes gegen ihn ermittelt wird. Der zuständige Staatsanwalt schlug vor, dass mich der Abteilungsleiter in den nächsten Tagen anrufen werde, um nähere Informationen zu übermitteln. Während des Anrufs erklärte der Abteilungsleiter, der zuständige Staatsanwalt sei gerade in Urlaub. Er selbst kenne den Verfahrensstand nicht genau. Wir vereinbarten ein weiteres Gespräch in der nächsten Monatshälfte. Nunmehr teilte die Staatsanwaltschaft mit, der Durchsuchungsbeschluss sei jetzt vollstreckt. Bei der Durchsuchung sei dem Betroffenen auch eröffnet und erläutert worden was genau gegen ihn vorliege. Mein Verlangen, die Rechtmäßigkeit der Auskunftsverweigerung substanziiert zu prüfen, habe sich erledigt. Auch der Betroffene erklärte sein Verlangen für erledigt.

3.4.3
Ausländer

In einem vierten Fall versuchte ein im Jahre 1993 nach Ablehnung seines Asylantrages abgeschobener rumänischer Staatsangehöriger vergeblich, wieder nach Deutschland einreisen zu dürfen. Sämtliche Anträge wurden, ohne sie zu begründen, abgelehnt. Eine von ihm beauftragte deutsche Anwaltskanzlei bat beim Bundesverwaltungsamt in seinem Namen um Selbstauskunft über Daten, die im Ausländerzentralregister (AZR) gespeichert sind. Das AZR erteilte Auskunft nach § 34 des Gesetzes über das Ausländerzentralregister (AZRG).

§ 34 AZRG

(1) Die Registerbehörde erteilt dem Betroffenen auf Antrag über die zu seiner Person gespeicherten Daten, auch soweit sie sich auf Herkunft oder Empfänger dieser Daten beziehen, unentgeltlich Auskunft. Der Antrag muss die Grundpersonalien enthalten. Die Registerbehörde bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.

(2) Die Auskunftserteilung unterbleibt, soweit

1. die Auskunft die ordnungsgemäße Erfüllung der Aufgaben gefährden würde, die in der Zuständigkeit der öffentlichen Stelle liegen, die die Daten an das Register übermittelt hat,
2. die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde oder
3. die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheimgehalten werden müssen

und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.

(3) Sind die Daten des Betroffenen von einer der in § 20 Abs. 1 bezeichneten öffentlichen Stellen (Anmerkung: Verfassungsschutzbehörden, Militärischer Abschirmdienst und Bundesnachrichtendienst), den Polizeivollzugsbehörden oder den Staatsanwaltschaften an das Register übermittelt worden, ist die Auskunft über die Herkunft der Daten nur mit deren Einwilligung zulässig. Dasselbe gilt für die Auskunft über den Empfänger der Daten, soweit sie an die in Satz 1 bezeichneten Stellen oder an Gerichte übermittelt worden sind. Die Einwilligung darf nur unter den in Absatz 2 bezeichneten Voraussetzungen versagt werden. Die in § 20 Abs. 1 bezeichneten öffentlichen Stellen können ihre Einwilligung darüber hinaus unter den in § 15 Abs. 2 Nr. 2 des Bundesverfassungsschutzgesetzes, auch in Verbindung mit § 7 des BND-Gesetzes und § 9 des MAD-Gesetzes, bezeichneten Voraussetzungen versagen.

(4) Gegenüber dem Betroffenen bedarf die Ablehnung der Auskunftserteilung keiner Begründung, wenn dadurch der mit der Ablehnung verfolgte Zweck gefährdet würde. Die Begründung ist in diesem Fall zum Zweck einer datenschutzrechtlichen Kontrolle schriftlich niederzulegen und fünf Jahre aufzubewahren. Sie ist durch geeignete Maßnahmen gegen unberechtigten Zugriff zu sichern. Der Betroffene ist darauf hinzuweisen, dass er sich an den Bundesbeauftragten für den Datenschutz wenden kann.

(5) Wird dem Betroffenen keine Auskunft erteilt, ist sie auf sein Verlangen dem Bundesbeauftragten für den Datenschutz zu erteilen, soweit nicht die jeweils zuständige oberste Bundesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die Mitteilung des Bundesbeauftragten an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand der speichernden Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.

Es informierte korrekt, welche Personalien und ausländerrechtlichen Informationen vorliegen und bei welcher Behörde die nachträgliche Befristung des aufgrund der Abschiebung verfügten unbefristeten Wiedereinreiseverbotes beantragt werden kann. Es informierte darüber hinaus:

„Weiterhin bestehen im Ausländerzentralregister Speicherungen, die Ihnen gemäß § 34 Abs. 3 in Verbindung mit Abs. 2 AZRG nicht mitgeteilt werden können. Ihnen steht jedoch die Möglichkeit offen, sich gemäß § 34 Abs. 4 AZRG an den Bundesbeauftragten für den Datenschutz zu wenden.“

Das AZR hatte damit unter Hinweis auf § 34 Abs. 3 AZRG die Auskunft verweigert. Dem von dem Anwalt eingeschalteten Bundesdatenschutzbeauftragten hatte das AZR mitgeteilt, hessische Behörden hätten eine Fahndung veranlasst. Allerdings dürfe dem Anfrager keine Auskunft erteilt werden, die Rückschlüsse auf die Fahndung zuließen, weil ansonsten die Vollstreckung eines Haftbefehls beeinträchtigt werden könnte. Der Bundesdatenschutzbeauftragte gab die weitere Bearbeitung der Angelegenheit an mich ab.

Ich stellte fest, dass die Fahndung durch das Landeskriminalamt auf einem Haftbefehl des Amtsgerichts Dieburg beruhte. Dem Haftbefehl lag folgender Sachverhalt zu Grunde: Vor ca. neun Jahren, wenige Tage nach der Abschiebung des Rumänen, wurde gegen ihn wegen eines Ladendiebstahls von mehreren Flaschen Weinbrand Anklage beim Amtsgericht Dieburg erhoben. Dass der Angeschuldigte kurz vorher von einer anderen Behörde abgeschoben worden war, hatte – warum auch immer – niemand festgestellt. Deswegen wurde das Verfahren wegen unbekannten Aufenthaltes des Angeschuldigten vorläufig eingestellt. In dem danach ergangenen Haftbefehl ist als Haftgrund „Fluchtgefahr“ eingetragen.

Damit schien der Anfrager chancenlos. Seine Einreiseanträge waren abgelehnt worden, sein Auskunftsverlangen ebenfalls. Als Datenschutzbeauftragter durfte ich ihn nicht informieren. Richtig wäre es gewesen, wenn das Bundesverwaltungsamt – wie es § 34 Abs. 3 AZRG vorsieht – versucht hätte, die Einwilligung der speichernden Stelle in die Information des Betroffenen einzuholen.

Zugunsten einer pragmatischen Lösung habe ich mit dem zuständigen Amtsrichter in Dieburg ein Gespräch geführt. Er ermächtigte mich, den Anwalt gemäß § 34 Abs. 5 letzter Halbsatz AZRG über den Sachverhalt, das Aktenzeichen und die zuständige Behörde zu informieren, damit sich der Angeschuldigte den strafrechtlichen Vorwürfen stellen kann.

3.4.4
Verfassungsschutz

Auch aus dem Bereich des Verfassungsschutzes erreichen mich regelmäßig Anfragen Betroffener, die Auskunft über die eigene Person betreffende Datenspeicherungen wünschen.

Die bereichsspezifische Rechtsgrundlage ist § 18 des Gesetzes über das Landesamt für Verfassungsschutz (VerfSchG).

§ 18 VerfSchG

(1) Der betroffenen Person ist vom Landesamt für Verfassungsschutz auf Antrag gebührenfrei Auskunft über die zu ihrer Person gespeicherten Daten sowie den Zweck und die Rechtsgrundlage der Verarbeitung zu erteilen.

(2) Abs. 1 gilt nicht, soweit eine Abwägung ergibt, dass das Auskunftsinteresse der betroffenen Person gegenüber dem öffentlichen Interesse an der Geheimhaltung der Tätigkeit des Landesamtes für Verfassungsschutz oder einem überwiegenden Geheimhaltungsinteresse Dritter zurücktreten muss. Ein Geheimhaltungsinteresse liegt dann vor, wenn

1. eine Gefährdung der Aufgabenerfüllung durch die Auskunftserteilung zu besorgen ist,
2. durch die Auskunftserteilung Quellen gefährdet sein können oder die Ausforschung des Erkenntnisstandes oder der Arbeitsweise des Landesamtes für Verfassungsschutz zu befürchten ist,
3. die Auskunft die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde oder
4. die Daten oder die Tatsache der Speicherung nach einer Rechtsvorschrift oder wegen der überwiegenden berechtigten Interessen eines Dritten geheimgehalten werden müssen.

Die Entscheidung trifft der Behördenleiter oder ein von ihm besonders beauftragter Mitarbeiter.

(3) Die Auskunftsverpflichtung erstreckt sich nicht auf die Herkunft der Daten und die Empfänger von Übermittlungen.

(4) Die Ablehnung der Auskunftserteilung bedarf keiner Begründung, soweit dadurch der Zweck der Auskunftsverweigerung gefährdet würde. Die Gründe der Auskunftsverweigerung sind aktenkundig zu machen. Wird die Auskunftserteilung abgelehnt, ist die betroffene Person auf die Rechtsgrundlage für das Fehlen der Begründung und darauf hinzuweisen, dass sie sich an den Hessischen Datenschutzbeauftragten wenden kann. Mitteilungen des Hessischen Datenschutzbeauftragten dürfen keine Rückschlüsse auf den Erkenntnisstand des Landesamtes für Verfassungsschutz zulassen, sofern es nicht einer weitergehenden Auskunft zustimmt.

Aus Gründen der Geheimhaltung ist es nicht angebracht, die an mich herangetragenen Einzelfälle in tatsächlicher Hinsicht näher darzustellen. Festzuhalten ist, dass das Hessische Landesamt für Verfassungsschutz (LfV) die gesetzliche Regelung in allen an mich herangetragenen Fällen korrekt angewandt hatte.

Wiederholt hatten Anfragende ein besonders stark ausgeprägtes Auskunftsinteresse, z. B. weil sie aufgrund einer Datenübermittlung des LfV ihren Arbeitsplatz verloren hatten. Trotzdem war das von der Verfassungsschutzbehörde geltend gemachte Geheimhaltungsinteresse so stark, dass dem Betroffenen nur eine Teilauskunft erteilt werden konnte. Die (teilweise) Auskunftsverweigerung wurde von mir als rechtmäßig anerkannt. Umgekehrt wurde in Fällen Auskunft erteilt, obwohl kein besonderes Auskunftsinteresse geltend gemacht worden war.

Das LfV zog sich in keinem Fall auf pauschale Auskunftsverweigerungen zurück, sondern nahm eine korrekte Abwägung zwischen im Einzelfall vorliegenden Geheimhaltungsinteressen einerseits und den ggf. geltend gemachten Auskunftsinteressen andererseits vor. Auch die Nebenbestimmungen des § 18 Abs. 2 bis 4 VerfSchG wurden eingehalten: Die Entscheidung über die Auskunftsverweigerung wird jeweils vom Behördenleiter oder einem von ihm besonders beauftragten Mitarbeiter getroffen. Die Begründung wird – wenn sie dem Anfrager nicht eröffnet wird – aktenkundig gemacht. Der Betroffene wird darauf hingewiesen, dass er sich an mich wenden könne.

3.4.5
Polizei

3.4.5.1
Unfallaufnahme

Ein Fahrradfahrer, der an einem Unfall beteiligt war, wollte seinen Schaden nebst Schmerzensgeld bei der Versicherung des Unfallgegners geltend machen. Es gab Streit zwischen den Parteien, wer und zu welchem Anteil an dem Unfall Schuld war. Der Fahrradfahrer bat um Einsicht in das Unfallaufnahmeprotokoll der Polizei.

Die bereichsspezifische Auskunftsvorschrift für die Datenverarbeitung der Polizei ist § 29 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG).

§ 29 HSOG

(1) Der betroffenen Person ist auf Antrag gebührenfrei Auskunft zu erteilen über

1. die zu ihrer Person gespeicherten Daten,
2. die Herkunft der Daten und die Empfängerinnen oder die Empfänger von Übermittlungen, soweit dies festgehalten ist,
3. den Zweck und die Rechtsgrundlage der Speicherung und sonstigen Verwendung.

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

(2) Abs. 1 gilt nicht für Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden.

(3) Abs. 1 gilt außerdem nicht, soweit eine Abwägung ergibt, dass die dort gewährten Rechte der betroffenen Person hinter dem öffentlichen Interesse an der Geheimhaltung oder einem überwiegenden Geheimhaltungsinteresse Dritter zurücktreten müssen. Die Entscheidung trifft die Behördenleitung oder eine von dieser beauftragte Bedienstete oder ein von dieser beauftragter Bediensteter.

(4) Die Ablehnung der Auskunftserteilung bedarf einer Begründung insoweit nicht, als durch die Mitteilung der Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde.

(5) Wird Auskunft nicht gewährt, ist die betroffene Person darauf hinzuweisen, dass sie sich an die Datenschutzbeauftragte oder den Datenschutzbeauftragten wenden kann. Dies gilt nicht in den Fällen des Abs. 1 Satz 4. Die Mitteilung der Datenschutzbeauftragten oder des Datenschutzbeauftragten an die betroffene Person darf keine Rückschlüsse auf den Erkenntnisstand der speichernden Stelle zulassen, sofern sie nicht einer weitergehenden Auskunft zustimmt.

(6) Sind die personenbezogenen Daten in ein anhängiges Strafverfahren eingeführt, so ist vor Erteilung der Auskunft die Zustimmung der Staatsanwaltschaft herbeizuführen.

(7) Statt einer Auskunft über Daten können die Gefahrenabwehr- und die Polizeibehörden unbeschadet des Abs. 3 Satz 1 der betroffenen Person Akteneinsicht gewähren.

Weiterhin regelt eine „Richtlinie über die Aufgaben der Polizeibehörden bei Straßenverkehrsunfällen (Unfallaufnahmerichtlinien)“ des Hessischen Ministeriums des Innern und für Landwirtschaft, Forsten und Naturschutz vom 28. Dezember 1995 (StAnz. 1996 S. 211 ff.) unter Ziffer 8.1:

Ziffer 8.1 Unfallaufnahmerichtlinien

Anderen Behörden, öffentlichen Körperschaften und Personen, die ein berechtigtes Interesse (z. B. für die Prüfung bürgerlich-rechtlicher Ansprüche oder für die Vorbereitung eines Verwaltungsverfahrens) darlegen können, wie z. B. Unfallbeteiligten oder deren Rechtsanwälten, Haftpflichtversicherern oder Krankenkassen, kann, sofern keine begründeten Bedenken bestehen, auf entsprechende Ersuchen Auskunft erteilt werden über

– Ort und Zeitpunkt des Unfalls,
– die amtlichen Kennzeichen der Kraftfahrzeuge,
– die Personalien der Kfz-Halterin oder des Kfz-Halters sowie von Unbeteiligten und Geschädigten,
– die sachbearbeitende Polizeibehörde und das Aktenzeichen des Vorgangs,
– die zuständige Verfolgungsbehörde.

Weitergehende Auskünfte sind nur mit Zustimmung der Verfolgungsbehörde zu erteilen, Verbleiben Ermittlungsvorgänge auf der Dienststelle (s. Nr. 4.1.1) ist Auskunft zu erteilen, soweit dies auf Grund der Vorgänge möglich ist. Ersuchen um Akteneinsicht ist grundsätzlich zu entsprechen.

Auskünfte können auch durch Überlassung von Durchschriften oder Kopien erteilt werden.

Dem Radfahrer wurde eröffnet, dass ihm aus Datenschutzgründen keine Auskunft erteilt werden könne. Er möge sich bitte an einen Rechtsanwalt wenden. Ihm werde Akteneinsicht gewährt.

Diese Auskunft war mit den maßgebenden Regelungen nicht vereinbar. Zwar gilt das Auskunftsrecht nicht absolut. Soweit jedoch Auskunft und Akteneinsicht gewährt werden kann, muss sie dem Betroffenen selbst ebenso gegeben werden wie einem Bevollmächtigten. Mit meiner Unterstützung hakte der Unfallbeteiligte bei der zuständigen Polizeibehörde nach. Vier Monate nach dem Unfall erhielt er eine Kopie des Unfallprotokolls. Wegen weitergehender Informationswünsche – er wollte den Wortlaut der späteren Einlassungen von Unfallzeugen zur Kenntnis bekommen – wurde er unter Angabe von Aktenzeichen und der Anschrift an die Strafverfolgungsbehörde verwiesen, die mittlerweile mit dem Vorgang befasst war. Das war nicht zu beanstanden.

3.4.5.2
Noch ein Haftbefehl

Ein Frankfurter Rechtsanwalt erhielt davon Kenntnis, dass über seinen ausländischen Mandanten im polizeilichen Informationssystem eine Fahndung gespeichert ist. Der Anwalt stellte Auskunftsanträge bei der Polizei und beim Ausländerzentralregister. Das Ausländerzentralregister erteilte Auskunft gemäß § 34 AZRG (Zitat s. Ziff. 3.4.3) und teilte u. a. unter Angabe des Aktenzeichens und der Anschrift der Strafverfolgungsbehörde mit, dass über den Betroffenen eine Fahndung gespeichert ist.

Anders verfuhr das Hessische Landeskriminalamt: Es ließ sich auch durch meine Intervention nicht dazu bewegen, dem Betroffenen Auskunft zu erteilen oder – wie in § 29 Abs. 6 HSOG vorgesehen – die Zustimmung der Strafverfolgungsbehörde einzuholen. Es lehnte die Auskunft ab. Da nicht definitiv erkennbar sei, woher der Anwalt Kenntnis von der Fahndung gehabt habe, sei davon auszugehen, dass es sich bei der Anfrage um einen Ausforschungsversuch handele. Somit sei gemäß § 29 Abs. 3 HSOG zu verfahren. Immerhin wurde der in § 29 Abs. 5 HSOG vorgesehene Hinweis auf meine Kontrollmöglichkeit erteilt.

Ich habe dem Anwalt und auch dem Landeskriminalamt mitgeteilt, dass die Auskunftsverweigerung nicht rechtmäßig war. Eine Auskunftsverweigerung nach § 29 Abs. 3 HSOG erfordert, sofern kein Geheimhaltungsinteresse eines Dritten vorrangig ist, ein vorrangiges öffentliches Geheimhaltungsinteresse. Die Ausschreibung zur Fahndung beruhte im vorliegenden Fall auf einem richterlichen Untersuchungshaftbefehl. Dieser ist gemäß §§ 35, 114a StPO dem Betroffenen spätestens mit der Verhaftung bekannt zu geben. Es war deswegen kein Grund ersichtlich, den Verfahrensbevollmächtigten nicht in Kenntnis zu setzen. Da der Betroffene gegen einen Haftbefehl das Beschwerderecht hat, muss ihm die Möglichkeit gegeben werden, die im Strafprozessrecht zugelassenen Rechtsmittel auch tatsächlich zu ergreifen. Dazu gehört die Mitteilung des Aktenzeichens, unter dem der Haftbefehl erlassen worden ist. Zwar liegt es auf der Hand, dass in bestimmten Einzelfällen kriminaltaktische Überlegungen vorrangig sein können, den Betroffenen über eine Ausschreibung zur Fahndung nicht in Kenntnis zu setzen. Dass aber hier ein solcher Fall vorlag, war nicht dargetan. Eine inhaltliche Information an den Betroffenen nachzuholen, war freilich nicht mehr erforderlich, da er in der Zwischenzeit vom Ausländerzentralregister alle gewünschten Informationen erhalten hatte.

3.4.6
Finanzämter

Ein Steuerpflichtiger führte einen umfangreichen Schriftwechsel mit einem Finanzamt, in dessen Verlauf es zu verschiedenen Fehlern durch Bedienstete des Finanzamtes gekommen war: falsche Adressierung, falscher Inhalt, falsche

Bezugsschreiben und nicht verschlossene Briefe. Der Steuerpflichtige hatte nach allem Zweifel, dass seine Schreiben vollständig in die Finanzamtsakte gelangt waren und bearbeitet werden konnten.

Auf seine wiederholte Bitte, ihm mitzuteilen, ob bestimmte, genauer bezeichnete Schreiben in der Akte vorhanden sind, erhielt er keine Antwort. Er wandte sich daher an mich, um durch Einsichtnahme in die Akte die Angelegenheit zu klären.

In der Tat sieht das Steuerverfahrensrecht, im Wesentlichen in der Abgabenordnung (AO) geregelt, ein Recht auf Akteneinsicht nicht vor. Zur Auskunft sind die Finanzbehörden hingegen im Rahmen eines Anhörungsverfahrens nach § 91 Abs. 1 AO verpflichtet; außerdem erteilen sie Auskunft über die Rechte und Pflichten der Steuerpflichtigen (§ 89 S. 2 AO). Da die Abgabenordnung seitens der Finanzverwaltung als eigene bereichsspezifische Lösung datenschutzrechtlicher Probleme angesehen wird, wird derzeit eine ergänzende Anwendung der allgemeinen Datenschutzgesetze abgelehnt.

Im Anwendungserlass (zu §§ 89, 91 AO) zur Abgabenordnung wird festgehalten, dass den Beteiligten ein allgemeines Recht auf Akteneinsicht im Steuerfestsetzungsverfahren nicht eingeräumt wird. Im Einzelfall kann allerdings nach Ermessen Akteneinsicht gewährt werden. Aktenauskunft ist den Finanzbehörden zwar gestattet, es besteht jedoch ebenfalls kein Anspruch. Im vorliegenden Fall wurde das Ermessen gegenüber dem Beteiligten nicht ausgeübt.

Die Akteneinsicht durch meine Mitarbeiter erfolgte reibungslos und vollständig. Im Ergebnis konnte festgestellt werden, dass sämtliche Schreiben des Steuerpflichtigen in der Akte abgeheftet waren.

Der Fall zeigt, dass eine gesetzliche Regelung zu einem bereichsspezifischen Akteneinsichts- und -auskunftsrecht dringend notwendig ist. Nur so kann eine Gleichbehandlung auch jener Steuerpflichtigen im Steuerfestsetzungsverfahren gewährleistet werden, die sich keines Steuerberaters bedienen (können).

3.5
Elektronisches Fahrgeldmanagement

In immer mehr Verkehrsgesellschaften und Verkehrsverbünden werden inzwischen statt herkömmlicher elektronische Fahrscheine ausgegeben, die mit einem Chip ausgestattet sind. Der Einsatz derartiger Systeme kann je nach Ausgestaltung dazu führen, dass Bewegungsprofile der Kartenbesitzer erzeugt werden können. Um einen möglichst datenschutzfreundlichen Einsatz dieser neuen Systeme zu gewährleisten, hat eine Arbeitsgruppe aus Vertretern verschiedener Datenschutzbeauftragter – darunter auch Hessen – und Vertretern von Verkehrsunternehmen unter Vorsitz des Verbandes Deutscher Verkehrsunternehmen im vergangenen Jahr versucht, generelle datenschutzrechtliche Grundanforderungen an ein elektronisches Fahrgeldmanagement zu formulieren.

Die gemeinsame Arbeitsgruppe hat Vorschläge erarbeitet, die den Gremien des Verbandes Deutscher Verkehrsunternehmen vorgelegt wurden. Im Einzelnen wurden die folgenden Punkte als wünschenswerte Grundelemente eines elektronischen Fahrgeldmanagements herausgearbeitet:

- Die Datenverarbeitung muss für die Kunden transparent sein, indem die Zwecke der Datenverarbeitung festgelegt und die einzelnen daraus resultierenden Datenverarbeitungsvorgänge beschrieben werden – differenziert nach Nutzungsart.
- Den Fahrgästen muss die Möglichkeit eingeräumt werden, der Nutzung ihrer Kundendaten zu Werbezwecken zu widersprechen.
- Die Fahrgäste müssen eine freie Entscheidungsmöglichkeit haben zwischen anonymer Fahrt und besonderen Leistungsangeboten, die die Verarbeitung personenbezogener Daten voraussetzen.
- Daten für Planungszwecke und zur Optimierung des Angebotes sind anonym zu erheben oder zu anonymisieren.
- Kunden- oder kartenbezogene Auswertungen dürfen nur zu den festgelegten Zwecken erfolgen. Zur Abrechnung innerhalb eines Verbundes dürfen allenfalls kartenbezogene Daten übermittelt werden.
- Der Zugriff des Kontrollpersonals in den Verkehrsmitteln muss auf die zur Kontrolle notwendigen Daten beschränkt sein.
- Die Systemkomponenten sind so auszugestalten, dass
  - keine Möglichkeit für Unbefugte besteht, an Terminals für bargeldlose Zahlung die Eingabedaten, insbesondere Authentifikationsdaten zur Kenntnis zu nehmen,
  - Fehlermeldungen der Zugangs-Erfassungssysteme die Betroffenen nicht öffentlich diskriminieren und
  - die Fahrgäste in angemessenen Umfang die Möglichkeit haben, den Inhalt der Chipkarte auszulesen.
- Es müssen Vorkehrungen gegen missbräuchliche Verwendung der Daten bei Verlust des Speichermediums getroffen werden (beispielsweise Verschlüsselung).
- Es sind Regelfristen für die Löschung der Daten festzulegen. Die Speicherung der Daten muss so kurz wie möglich sein.

4. Europa

Schengener Durchführungsübereinkommen

Auch im Berichtszeitraum 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.

4.1
Gemeinsame Geschäftsstelle

Die nunmehr einjährigen Erfahrungen der Gemeinsamen Kontrollinstanz mit der eigenen Geschäftsstelle für Schengen, Europol und das Zollinformationssystem sind positiv. Die Sitzungen sind besser vorbereitet, Stellungnahmen zu verschiedenen Problemen werden entworfen, Kontakte zu anderen Ratsgruppen oder auch dem Europäischen Parlament werden hergestellt. Seit kurzem erhält der Leiter der Geschäftsstelle Unterstützung durch einen juristischen Mitarbeiter aus Großbritannien.

Die Gemeinsame Kontrollinstanz hat beschlossen, den Tätigkeitsbericht nunmehr nur alle zwei Jahre zu verfassen, sodass der nächste erst im Dezember 2003 erscheinen wird.

4.2
Erneuerung des Schengener Informationssystems

Wichtigstes Thema im Berichtszeitraum waren die Pläne für ein erweitertes Schengener Informationssystem (SIS), das so genannte SIS II. Zunächst wurden Anfang des Jahres in der Gruppe SIS des Rats verschiedene Vorschläge für eine Erweiterung des SIS erarbeitet. Die Gemeinsame Kontrollinstanz hat sich in einer Stellungnahme vom 2. Mai 2002, an der die deutsche Delegation maßgeblich beteiligt war, dazu geäußert. Dabei ging es insbesondere um Folgendes:

– **Zugriff der nationalen staatlichen Kraftfahrzeugregisterstellen auf bestimmte SIS-Daten**

  Die Gemeinsame Kontrollinstanz hat darauf hingewiesen, dass es für eine nationale Kraftfahrzeugregisterstelle sinnvoll sein kann, beispielsweise vor der Anmeldung des KFZ zu prüfen, ob es in anderen Ländern als gestohlen ausgeschrieben ist. Allerdings ist hierfür eine Änderung der entsprechenden Artikel im Schengener Durchführungsübereinkommen (SDÜ) erforderlich.

– **Zugriff von EUROJUST auf das SIS**

  Bei EUROJUST handelt es sich um eine Stelle auf europäischer Ebene, in der von den Mitgliedstaaten entsandte Staatsanwälte, Richter und Polizeibeamte in bestimmten justiziellen Angelegenheiten zusammenarbeiten. Für die Realisierung eines Zugriffs von Eurojust auf das SIS müsste auf jeden Fall das SDÜ geändert werden, insbesondere müsste festgelegt werden, zu welchen Zwecken auf welchen Datenbestand zugegriffen werden darf.

– **Hinzufügung bestimmter Einzelangaben einer gesuchten Person oder Sache**

  Diskutiert wird, ob der Datensatz zu einer im SIS ausgeschriebenen Person um Angaben wie beispielsweise „Art der Straftat“, „flüchtige Person“, „psychisch gefährdete Person“, „Sexualstraftäter“, „des Drogenhandels verdächtige Person“ erweitert werden soll. Die Gemeinsame Kontrollinstanz hat sich gegen die Verarbeitung mehr oder weniger „subjektiver“ Angaben ausgesprochen, die von der jeweiligen Wertung des eingebenden Sachbearbeiters abhängen. Sie hat auch darauf hingewiesen, dass sich das SIS durch die Aufnahme von weiteren Angaben zu der ausgeschriebenen Person immer mehr von einem Treffer-/Kein-Treffer-System zu einem System mit neuer Funktion – nämlich einer Textdatei – entwickelt.

– **Konventionelle Unterlagen in den SIRENE-Büros**

  Die Vorschläge sehen erstmals eine Regelung der Tätigkeit der SIRENE-Büros und der Verarbeitung der dort anfallenden Unterlagen vor. 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 BKA), die das Nationale Schengener Informationssystem (NSIS) betreibt, aber auch andere damit zusammenhängende Aufgaben – wie die Verarbeitung entsprechender Informationen in Papierform – wahrnimmt. Die Gemeinsame Kontrollinstanz hat darauf hingewiesen, dass sie eine derartige Verrechtlichung begrüßt. Insbesondere sollte in diesem Zusammenhang eine Regelung für den Umgang mit den konventionellen Unterlagen in der SIRENE nach Löschung des SIS-Datensatzes gefunden werden. Die Gemeinsame Kontrollinstanz war hier immer der Auffassung, dass diese Unterlagen nach Löschung des Datensatzes im SIS vernichtet werden müssen.

– **Aufnahme von Lichtbildern und Fingerabdrücken**

  Anders als von mir im 30. Tätigkeitsbericht (Ziff. 20.2) berichtet, ist nicht mehr die Einstellung von DNA-Profilen vorgesehen, sondern es geht ausschließlich um Lichtbilder und Fingerabdrücke. Die Gemeinsame Kontrollinstanz hat klargestellt, dass sie gegen die Aufnahme anderer biometrischer Daten grundlegende Einwände hat. Bei den Lichtbildern und Fingerabdrücken muss die Erforderlichkeit für die Aufnahme in das SIS dargelegt werden.

– **Vollprotokollierung aller Abrufe aus dem SIS**

  Vorgesehen ist, dass nunmehr jeder Abruf (früher war es nur jeder zehnte Abruf) aus dem SIS zu protokollieren ist und die Speicherfrist der Protokolldaten auf ein Jahr verlängert wird. Die Gemeinsame Kontrollinstanz hat dagegen keine Einwände. Sie weist in diesem Zusammenhang darauf hin, dass die Protokolldaten um weitere wichtige Bestandteile, die für eine effektive Kontrolle erforderlich sind, erweitert werden sollten. Dabei geht es beispielsweise um die Angabe des Ortes, des Datums und der Uhrzeit der Abfrage, deren Gründe, Identifizierung des Endgeräts oder der Stelle, welche die Abfrage vorgenommen hat.

– **Verlängerung der Speicherfrist für die Ausschreibungen im SIS**

  Die Gemeinsame Kontrollinstanz wendet sich gegen jede Verlängerung der Speicherfrist. Sie ist entschieden dagegen, dass so genannte Höchstfristen durch so genannte Prüffristen ersetzt werden. Prüffrist bezeichnet in diesem Zusammenhang eine solche Frist, nach der die Behörde angehalten ist zu prüfen, ob die weitere Speicherung erforderlich ist. Nach den Erfahrungen in einzelnen Mitgliedsstaaten werden so genannte Prüffristen oft verzögert und teilweise auch gar nicht wahrgenommen. Deshalb sollte es bei Höchstfristen bleiben, bei deren Ablauf ein Datensatz automatisch gelöscht wird.

Unter der spanischen Ratspräsidentschaft wurden am 11. Juni 2002 sowohl ein Entwurf für eine Verordnung und als auch für einen Beschluss des Rats zur Änderung des Schengener Durchführungsübereinkommens vorgelegt. Die Parallelität von Verordnung und Beschluss zur Änderung des Schengener Durchführungsübereinkommens beruht darauf, dass bei der Integration von Schengen in die Europäische Union durch den Amsterdamer Vertrag Regelungen des SDÜ sowohl dem Vertrag über die Europäische Union als auch dem Vertrag über die Europäische Gemeinschaft zugeordnet wurden.

Der größte Teil der früheren Vorschläge findet sich in den jüngsten Entwürfen wieder. Änderungen bestehen zum einen darin, dass auf die Aufnahme von Fingerabdrücken und Lichtbildern in das SIS verzichtet wurde, andererseits aber der Kreis der Zugriffsberechtigten auf Europol, Gerichte und Staatsanwaltschaften ausgeweitet wurde.

Die Gemeinsame Kontrollinstanz hat in ihrer Stellungnahme zu den Verordnungs- und Beschlussentwürfen festgestellt, dass der geplante Zugriff von Europol derzeit nicht abschließend beurteilt werden kann. Europol könnte durch einen Zugriff auf das SIS nur feststellen, ob eine Ausschreibung zu einer bestimmten Person vorliegt, aber keine Daten über die Einzelheiten des betreffenden Falls erhalten. Für einen Europol-Zugriff beispielsweise auf die Daten nach Art. 96 SDÜ, also die Ausschreibungen zur Einreiseverweigerung für Drittausländer, liegen keine in die Zuständigkeit der zugriffsbefugten Behörden fallenden Gründe auf der Hand. Es sollte daher die Erforderlichkeit eines Zugriffs von Europol näher begründet werden.

Die Schaffung der entsprechenden Rechtsakte zur Änderung des SDÜ wird voraussichtlich noch einige Zeit in Anspruch nehmen. Die Gemeinsame Kontrollinstanz wird sich daran aktiv beteiligen.

5. Justiz

5.1
Rahmenbedingungen für den IT-Einsatz in der Justiz

Richterliche Unabhängigkeit und Gewaltenteilung bedingen beim Einsatz von moderner Informationstechnik und Netzen in der Justiz hohe Anforderungen an die Ausgestaltung für Administration und Wartung dieser Technik, insbesondere auch beim Einsatz justizfremder Personen und Institutionen.

5.1.1
Das Konzept der Landesregierung

Die hessische Landesregierung beabsichtigt im Rahmen eines großen Modernisierungsprojekts der hessischen Justiz alle Gerichte und Justizbehörden mit moderner Informationstechnik (IT) auszustatten. Damit sollen im Ergebnis alle dort Tätigen über sämtliche zukunftsfähigen Justiz-Fachanwendungen sowie E-Mail-Kommunikation verfügen. Schließlich sollen Zugriffsmöglichkeiten der Richter, Staatsanwälte und Rechtspfleger auf das juristische Informationssystem Juris eingerichtet werden.

Verwirklicht wird dieses Vorhaben in Zusammenarbeit mit der Hessischen Zentrale für Datenverarbeitung (HZD), die die Netze entwickelt, strukturiert und aufbaut. Im laufenden Betrieb liegt ein Großteil der Administratorenaufgaben bei der HZD.

Um die komplexe System-Umgebung wirtschaftlich betreiben zu können, wurde dazu von der HZD in Zusammenarbeit mit der Justiz ein zentraler Systembetrieb aufgebaut. Dabei werden drei strukturelle und organisatorische Maßnahmen angewendet:

– eine mehrstufige Betreuungsstruktur für die problemorientierte Steuerung,

– standardisierte Serviceprozesse und -verfahren in Betrieb und Administration,

– Überwachungssysteme für die präventive Problembeseitigung und Systemfortschreibung.

Die Einführung dieser Technik ist in vielen Bereichen auch erstmals mit einem Angebot an die Richterschaft verbunden, PCs an jedem Arbeitsplatz einzusetzen und gleichzeitig auf die in den Serviceeinheiten (zum Teil schon länger) eingesetzten Anwendungsprogramme zuzugreifen. Das Vorhaben führte in der Richterschaft zum Teil zu erheblicher Unruhe. Verstärkt hat sich diese zu Beginn des Jahres artikuliert – auch anknüpfend an mein Thesenpapier „Datenschutz in der Justiz“ (s. 30. Tätigkeitsbericht, Ziff. 28.2) und die daraus entstandene Diskussion, in die sich das Justizministerium und verschiedene Gerichtspräsidenten eingeschaltet haben.

Die Diskussion konzentrierte sich – ausgehend von den Anforderungen der richterlichen Unabhängigkeit – auf zwei Schwerpunkte. Zum einen wurden Bedenken artikuliert, ob die HZD als justizfremde, dem Hessischen Innenministerium unterstellte Institution so weitreichende Aufgaben bei der Entwicklung und im täglichen Betrieb der IT in den Gerichten wahrnehmen darf. Außerdem wurden Befürchtungen geäußert, dass durch die (neuen) Verwaltungsprogramme unzulässige Kontrollen über die Tätigkeiten und den Schriftverkehr der Richterschaft ausgeübt werden könnten. Befürchtet wurde dabei vor allem auch, dass Statistiken und andere Überblicke zu Erledigungszahlen erstellt werden und die Dauer der Bearbeitung einzelner Gerichtsverfahren und Ähnliches erfasst werden könnten.

Gegen den umfassenden Einsatz der HZD habe ich Einwendungen erhoben, weil eine Verwaltungsbehörde auf richterliche Daten zugreifen kann. Das gefährdet die Gewaltenteilung, die richterliche Unabhängigkeit, das Beratungsgeheimnis und den Datenschutz.

5.1.2
Anforderungen der Gewaltenteilung und der richterlichen Unabhängigkeit

Die unterschiedlichen Auffassungen zu den sich aus der Gewaltenteilung sowie der richterlichen Unabhängigkeit ergebenden Anforderungen an den Einsatz externen Sachverstandes wurden in einer Arbeitsgruppe von Mitarbeitern des Hessischen Justizministeriums und aus meiner Behörde ausführlich diskutiert. In einem längeren Papier wurde eine Bewertung des im Bereich der Justiz geplanten Projektes unter den Aspekten der Gewaltenteilung und der richterlichen Unabhängigkeit vorgenommen.

Weithin konnte Einvernehmen erzielt werden; meine Vorbehalte gegen die weitreichenden Administrationsbefugnisse der HZD habe ich aufrechterhalten. Die Verquickung richterlicher und exekutiver Zuständigkeiten widerspricht der tradierten Gewaltenteilung und der richterlichen Unabhängigkeit.

5.1.2.1
Gewaltenteilung

Das in Art. 20 Abs. 2 Satz 2 Grundgesetz (GG) wurzelnde Prinzip der Gewaltenteilung weist jeder Gewalt einen Kernbereich zu.

Art. 20 Abs. 2 GG

Alle Staatsgewalt geht vom Volke aus. Sie wird vom Volke in Wahlen und Abstimmungen und durch besondere Organe der Gesetzgebung, der vollziehenden Gewalt und der Rechtsprechung ausgeübt.

Der jeweilige Kernbereich ist unantastbar. Art. 20 Abs. 2 schützt gegen Durchbrechungen zu Lasten einzelner Gewalten. Die Gewaltenteilung verlangt eine grundsätzliche organisatorische Trennung von Legislative, Exekutive und Judikative. Eine absolute Trennung in allen Bereichen ist allerdings nicht verwirklichbar. Notwendigerweise muss sich die Justizverwaltung in vielen Bereichen bei der Aufgabenerfüllung der Spezialkenntnisse justizfremder Dritter bedienen. Entscheidend ist, dass die Justizverwaltung jederzeit die inhaltliche Steuerung und fachliche Aufsicht besitzt. Dabei müssen die Kernaufgaben im Bereich der Rechtsprechung von den Gerichten selbst, begrenzte Kontrolltätigkeiten vom Justizressort, nicht von der allgemeinen Verwaltung, geleistet werden.

Gleichzeitig begründet das Rechtsstaatsprinzip die verfassungsrechtliche Pflicht des Staates, für eine funktionstüchtige Rechtspflege zu sorgen. Der Staat muss Gerichte zur Verfügung stellen, die alle auf sie zukommenden Aufgaben in gerichtsverfassungsmäßiger Besetzung, in angemessener Zeit und mit der gebotenen Sorgfalt bewältigen können. Den Rahmen dazu geben die parlamentarisch zugewiesenen Haushaltsmittel.

5.1.2.2
Richterliche Unabhängigkeit

Die Unabhängigkeit der Richter steht in unmittelbarem Zusammenhang mit der Gewaltenteilung.

Art. 97 Abs. 1 GG

Die Richter sind unabhängig und nur dem Gesetz unterworfen.

Unabhängigkeit ist der Oberbegriff für die sachliche Unabhängigkeit (Freiheit von Weisungen) und die persönliche Unabhängigkeit (Unabsetzbarkeit) der Richter. Beide Elemente der Unabhängigkeit stehen in einer Wechselwirkung zueinander. Sachliche richterliche Unabhängigkeit bedeutet, dass der Richter keine Weisungen für seine richterliche Tätigkeit erhalten darf und nur dem Gesetz verpflichtet nach eigener richterlicher Überzeugung zu entscheiden hat. Weisung ist dabei im weitesten Sinne auch als Empfehlung oder Nahelegung zu verstehen. Jegliche Einflussnahme auf die Entscheidung des Richters ist rechtswidrig. Weisungsfreiheit besteht nur für die richterliche Tätigkeit. Unabhängigkeit ist kein Privileg und kein Selbstzweck, sondern sie wird dem Richter gewährt, um eine gerechte, von sachfremden Einflüssen freie Rechtsprechung zu ermöglichen. Das meint die Spruchpraxis und alle Tätigkeiten, die mit der Rechtsfindung in unmittelbarem Zusammenhang stehen. Dazu gehören Tätigkeiten, die der Vorbereitung einer Entscheidung dienen, wie die Terminbestimmung, Ladung, Sitzung, Abkürzung oder Verlängerung von Fristen und solche, die der Verhandlung vorausgehen, die während der Verhandlung ausgeübt werden oder die ihr nachfolgen.

Für die Auswahl technischer Gerätschaften, EDV-Programme und deren Administration bedeutet dies, dass darauf zu achten ist, dass keine Kontrolle über die richterliche Tätigkeit eröffnet wird, die als Folge ein Beeinflussen durch unzulässigen Druck ermöglichen könnte. Andererseits hat die Rechtsprechung anerkannt, dass technische Maßnahmen, die potenziell geeignet sind, die richterliche Unabhängigkeit zu beeinträchtigen, dann keinen Eingriff darstellen, wenn es dem Willen des Richters freisteht, von ihnen Gebrauch zu machen oder nicht.

5.1.2.3
Ergebnisse der Arbeitsgruppe

Unter Beachtung dieser Prämissen hat die Arbeitsgruppe zwei Lösungsmöglichkeiten entwickelt. Zum einen geht sie davon aus, dass durch die Verteilung der Aufgaben zwischen dem technischen Dienstleister HZD als Landesbetrieb, den justizeigenen Dienstleistern bei den Mittelbehörden und den örtlichen Systembetreuern in den Justizbehörden die Rechtsprechung im Kernbereich ihrer Tätigkeit vor Zugriffen Externer auf Daten der dritten Gewalt geschützt werden kann. Dagegen habe ich Vorbehalte geäußert.

Zugleich soll sichergestellt werden, dass die Systembetreuung im unmittelbaren Umfeld des Kernbereichs der Rechtsprechung von Kräften der Justizverwaltung erledigt wird. Eine Verletzung des Gewaltenteilungsprinzips soll so vermieden werden. Zu diesem Zweck sollte nach meiner Auffassung die zuständige Abteilung der HZD der ausschließlichen Aufsicht des Justizministeriums unterstellt werden.

Die Ausgestaltung der Zugriffsrechte, die Einführung einer Verschlüsselungssoftware für Verzeichnisse und Dokumente sowie die Schaffung der Möglichkeit des „Offline-Betriebes“ der richterlichen Netz-PC soll sicherstellen, dass richterliche Daten „nach den Regeln der Kunst“ bestmöglich gegen rechtswidrige Einflussnahme und Einsicht geschützt sind. Auch die Abschottung des Netzes gegen das Internet dient diesem Zweck.

Ich selbst halte eine von den Gerichtsbarkeiten selbst betriebene Administration für sachgerechter und wegen der richterlichen Unabhängigkeit für erforderlich.

Nach Ansicht der Arbeitsgruppe würden die Belange der Gewaltenteilung und der richterlichen Unabhängigkeit am weitestgehenden gewahrt, wenn die für die Systembetreuung der Justiz zuständigen Betriebsteile der HZD organisatorisch der Justiz eingegliedert würden.

Sollte dieser Vorschlag nicht umgesetzt werden können, hält es die Arbeitsgruppe für die „zweitbeste“ Lösung, die Befugnisse der HZD und die Aufsichtsrechte der Justiz in einem Fernwartungsvertrag zu regeln, für dessen Ausgestaltung sie in Anlehnung an den Mustervertrag des Hessischen Datenschutzbeauftragten (s. 29. Tätigkeitsbericht, Ziff. 11.3) Vorgaben formuliert hat.

5.1.2.4
Konsequenzen für die Gestaltung der Systeme

Für die Strukturen und Zugriffsrechte in den so betriebenen Systemen – auch für die einzelnen in diesen Netzen eingesetzten Verwaltungsprogramme – sind letztlich die folgenden Grundsätze zu beachten:

– Soweit es keine besonderen Regelungen in den Verfahrensordnungen gibt, muss die automatisierte Vorgangsbearbeitung den derzeitigen Bearbeitungsgang der Papierakten nachbilden.

– Die Festlegung von Zugriffsrechten innerhalb der einzelnen DV-Verfahren muss den Zuständigkeiten des Geschäftsverteilungsplanes folgen und liegt insoweit in der Hand des Präsidiums.

– In den Systemen kann es nur dienstliche Verzeichnisse zur Ablage von Dokumenten geben.
– Für Dokumente, die der richterlichen Unabhängigkeit unterliegen und noch nicht Teil der Akte in Papierform sind, sollten besondere Verzeichnisse zugelassen werden. Für diese sind zusätzliche Zugriffsrestriktionen und gesonderte Verschlüsselungen zu gestatten.
– Der Einsatz von Dritten zur Betreuung der Anlagen oder für die Administration darf nur in der Weise erfolgen, dass eine begleitende Kontrolle durch gerichtseigenes Personal jederzeit erfolgen kann. Das Weisungsrecht auch für Mitarbeiter von Rechenzentren etc. muss im Bereich der Gerichte liegen, soweit deren Netze administriert werden.

5.1.3
Das Netzkonzept

5.1.3.1
Support

Um die Vorgaben technisch und organisatorisch umzusetzen, hat das Justizministerium zusammen mit der HZD in einer Netzbeschreibung seine Überlegungen präzisiert. Die folgenden Beschreibungen gelten soweit das Konzept schon bei Gerichten umgesetzt ist. Es wurde zuerst im Bereich der Zivilgerichtsbarkeit eingeführt. Die Umsetzung in allen Gerichten soll kontinuierlich erfolgen.

Eine wesentliche Komponente betrifft die Installation von Software und den Support von Benutzern und Behörden. Hierzu wurde eine automatische Installation und Softwareverteilung implementiert.

Der First-Level-Support, d. h. die Behebung von einfacheren Problemen, wird durch die Vor-Ort-Betreuer vorgenommen.

Der Second-Level-Support, d. h. die Bearbeitung von Problemen, die durch die Vor-Ort-Betreuer nicht mehr behoben werden können, wird zweigeteilt. Soweit es sich um Probleme der Fachanwendungen handelt, unterstützen Mitarbeiter von Fachgruppen aus der Justiz die Behörden. So gibt es beim „elektronischen Grundbuch“ eine Projektgruppe beim Oberlandesgericht und beim Verfahren MESTA eine Projektgruppe bei der Generalstaatsanwaltschaft. Soweit jedoch eine Unterstützung bei schwierigen technischen Problemen nötig ist, wird diese durch die HZD mit ihrer Außenstelle in Hünfeld gegeben. Die HZD dokumentiert ihre Tätigkeiten mit einem speziellen Tool, in dem alle Fehlermeldungen und die vorgenommenen Schritte der HZD-Mitarbeiter festgehalten werden müssen.

Der Third-Level-Support erfolgt durch die Hersteller. Er kommt zum Tragen, wenn ein Problem durch den Second-Level-Support nicht beseitigt werden konnte.

Weiterhin werden in der Netzbeschreibung auch Vorgaben zu grundsätzlichen Sicherheitseinstellungen des Betriebssystems gemacht.

5.1.3.2
Technische Umsetzung

Generell ist zunächst zu beachten, dass die besonderen Anforderungen an die eingesetzten IT-Systeme in Bezug auf den einzelnen Richter und andere Mitarbeiter im Gegensatz zu den Anforderungen an ein zentrales Installations-, Aktualisierungs- und Betreuungskonzept stehen. Die große Zahl der im Justizbereich zu betreuenden Rechner erfordert gewisse Kompromisse. Das gilt auch bei einer Administration durch gerichtseigene Bedienstete.

Wesentlicher Bereich der Anforderungen ist der Komplex „Nachvollziehbarkeit“ der Administration. In der Judikative bedeutet das „Nicht-Nachvollziehbarkeit“ der richterlichen Arbeit am Einzelplatzrechner.

Dies wird durch eine „anonyme“ Standardkonfiguration gelöst, die erst bei der jeweiligen Anmeldung des Nutzers mit dessen Arbeitsumgebung ausgestattet wird. Dieser Zuschnitt umfasst

– die zusätzlichen Programme, die z. B. dem Richter verfügbar gemacht werden (JUDOG, Juris, Asyldatenbank etc.)
– Verzeichnisse, auf die der Nutzer zugreifen muss
– die Daten des Benutzerprofils, also insbesondere die persönlichen Einstellungen und das Verzeichnis „Eigene Dateien“

5.1.3.2.1
Standardarbeitsplatz

Die große Zahl der durch die HZD zu installierenden und zu betreuenden Arbeitsplätze bedingt eine Standardinstallation, die in einem zweiten Schritt den individuellen Aufgaben und Arbeitstechniken des Benutzers angepasst werden muss.

Zu den vereinbarten Standards zählt neben der einheitlichen Betriebssystem- und Basissoftwareausstattung auch die Sicherstellung der Einhaltung dieser Standards. Um dies zu gewährleisten, sind

– die Dateiablagen ins Netzwerk verlagert
– Zugriffe auf die lokalen Laufwerke (Betriebssystem und Anwendungen) für den Benutzer ausgeschlossen (Ausnahme: Diskettenlaufwerk für den Datenaustausch)
– Zugriffe auf einige Systemfunktionen eingeschränkt (z. B. Systemsteuerung, Befehl „Ausführen“)
– die nutzbaren Anwendungen durch eine Positivliste restriktiv eingeschränkt.

5.1.3.2.2
Individueller Arbeitsplatzrechner

Um dem Einzelnutzer die benötigten Daten zur Verfügung zu stellen, ist für den Standardarbeitsplatz ein vierstufiges Gruppenkonzept entwickelt worden.

– Die erforderlichen Programme und Verzeichnisse werden im Rahmen des Anmeldeskriptes anhand dieser Gruppenzuordnung ermittelt und dementsprechend installiert (neue Programme) beziehungsweise bereitgestellt (Verzeichnisse). Diese Gruppen umfassen in der ersten Stufe die allgemeine Zuordnung „Benutzer beziehungsweise Administrator“.
– Die zweite Stufe umfasst den Bereich „Abteilungen“ (= Verzeichnisse).
– Die dritte Stufe enthält die arbeitstechnisch notwendigen „Funktionen“ (= Programme).
– Die vierte Stufe regelt die Arbeitsmöglichkeiten ohne Verbindung zum lokalen Netz (Offline-Betrieb).

Da ein Nutzer in der Regel nur unter besonderen Umständen (Versetzung, Umsetzung, Rechnerstörung) den Arbeitsplatz wechselt oder sein Rechner ausgetauscht wird, hält sich der zeitliche Rahmen, den eine Voll-Installation benötigt, im überschaubaren Bereich. Die Zuordnung der Verzeichnisse ist jeweils schnell erfolgt, so dass auch unter diesen besonderen Umständen die Anmeldeprozedur keine spürbare Zeitverzögerung darstellt.

5.1.3.2.3
Persönliche Verzeichnisse

Das persönliche Verzeichnis (auch als „Profil“ bezeichnet) enthält nicht nur die Konfiguration der Arbeitsumgebung, sondern ist (in der Standardkonfiguration) auch Speicherort aller Benutzerdaten, insbesondere für Dokumente („Eigene Dateien“) und temporäre Objekte (Zwischenspeicher des Browsers, Cookies usw.). Solche Daten können auch zur Überwachung und Kontrolle des Benutzers herangezogen werden.

Daher kommt diesem Verzeichnis im Rahmen des Konzepte eine besondere Bedeutung zu: Das Benutzerprofil wird grundsätzlich auf einem Domänencontroller gespeichert („server-basiertes Profil“).

Bei der **ersten Anmeldung** eines Benutzers werden alle auf dem Rechner vorhandenen Profildaten im Rahmen der Anmeldeprozedur gelöscht. Danach wird ein neues Profilverzeichnis erstellt und die Dateien des Benutzers werden in das Verzeichnis kopiert. Damit ist sichergestellt, dass der Benutzer „Besitzer“ im Sinne des Windows-Konzeptes ist. Die Berechtigungen des Verzeichnisses werden anschließend mit dem Befehl „cacls“ („change acls“ – „acl“ = access control list, Zugriffskontrollliste) auf den Benutzer beschränkt. Damit haben auch Administratoren keinen Zugriff auf dieses Verzeichnis.

Bei einer **erneuten Anmeldung** am Rechner, greift ein anderer Mechanismus der Anmeldeprozedur: Nun wird geprüft, ob der Benutzer noch Besitzer seines Verzeichnisses ist. Ist dies nicht der Fall, d. h. ein Administrator hat sich Zugang zum Verzeichnis verschafft, wird der Benutzer über ein Dialogfeld informiert und aufgefordert, sich mit seinem Systembetreuer in Verbindung zu setzen.

Änderungen an den Rechten kann nur ein Administrator oder der Besitzer des Objekts vornehmen. Da Administratoren im Rahmen des Konzepts keinerlei Rechte am Verzeichnis haben, müssen sie sich selbst zum Besitzer des Objekts machen (Besitzübernahme) und können dann die Rechte modifizieren. Anschließend wäre es möglich, dem vorherigen Besitzer wieder alle Zugriffsrechte zu übertragen, so dass dieser nichts von der Manipulation bemerkt. Da aber die Rückgabe des Besitzrechts im Rahmen des Windows-Konzeptes nicht möglich ist, lässt sich über den oben beschriebenen Mechanismus eindeutig eine Manipulation nachweisen.

5.1.3.3
Kontrolle der Administration

Neben den vorher beschriebenen Methoden greifen weitere Systemeinstellungen, um unberechtigte Zugriffe auf sensitive Daten zu erschweren beziehungsweise Manipulationsversuche nachzuvollziehen. Dies umfasst im Wesentlichen die restriktive Vergabe von besonderen Systemprivilegien (insbesondere „Besitzübernahme“) und die Überwachung sicherheitsrelevanter Systemvorgänge. Zum einen wird den Vor-Ort-Betreuern ein Zugriff auf die Systemprotokolle gestattet, um Zugriffe der HZD überprüfen zu können. Des Weiteren wurde in jedem Gericht die Rolle des

„Systemrevisors“ eingerichtet. Diesem Benutzer ist – unabhängig von der Unterstützung durch HZD-Mitarbeiter und Vor-Ort-Betreuer – der kontrollierende Zugriff auf die Protokolle möglich. Damit besteht eine dritte, unabhängige Instanz zur Kontrolle der Administration.

Darüber hinaus ist es nach meiner Einschätzung erforderlich, dass Zugriffe der HZD im Rahmen der Fernwartung den Nutzern der Bildschirme unmittelbar angezeigt werden.

5.1.3.4
Zugriffsrechte für HZD-Mitarbeiter

Besonderen Rang hat in diesem Zusammenhang die Nachvollziehbarkeit der Zugriffe der HZD-Mitarbeiter im Rahmen ihrer Betreuungsaufgaben. Die Eingriffe ins Betriebssystem auf Serverebene werden im Rahmen der Protokollierung erfasst und sind durch Vor-Ort-Betreuer und Systemrevisor überprüfbar. Dies gilt insbesondere für Zugriffe auf das Dateisystem der Arbeitsplatzrechner (über administrative Freigaben), Änderungen an Datei- oder Benutzerberechtigungen, Änderung an Systemrechten und -richtlinien und ganz besonders für die Fernwartung.

5.1.3.5
Fernwartung

Im Rahmen des Second-Level-Support haben die Betreuer auch über das Netzwerk Zugang zu den Arbeitsoberflächen der Benutzer, auf deren Anforderung hin sie Remote-Support leisten sollen (die gleiche Problemstellung stellt sich eingeschränkt auch für die Vor-Ort-Betreuer). Hier besteht die Gefahr, das sich an sich berechtigte Betreuer ohne Anforderung und ohne Wissen des Arbeitsplatznutzers auf den Rechner aufschalten und sich so die Möglichkeit verschaffen, den eigentlichen Nutzer zu überwachen und auszuspionieren.

Zur Veränderung derartiger Überwachungsschritte kommt der eingesetzten Software besondere Bedeutung zu. Zwar gibt es eine große Zahl kommerzieller Software, die aber unter Kostenaspekten bei großer Nutzeranzahl nicht oder nur eingeschränkt in Betracht kommt. Im Rahmen der zur Verfügung stehenden Mittel und der Konfigurations- und Leistungsmöglichkeiten der Softwareprodukte wurde „TridiaVNC“, eine erweiterte Version der Freeware „VNC“ der AT&T-Laboratories ausgewählt. Im Gegensatz zum Originalprodukt, das eine „stille“ Aufschaltung auf einen Client-Rechner ermöglicht, sind hier verschiedene Mechanismen vorgeschaltet, die dies verhindern. Neben der Implementierung als zwei voneinander unabhängige Dienste, die standardmäßig nicht aktiv sind, steht vor der eigentlichen Sitzung ein Betreuer-Nutzer-Dialog, in dem wechselseitig die Aufschaltung angefordert und bestätigt werden muss. Erst danach werden die für die Sitzung erforderlichen Dienste gestartet und die Remote-Verbindung geöffnet.

Im Rahmen der Sitzung hat der Arbeitsplatzbenutzer jederzeit die Möglichkeit, die Fern-Sitzung zu beenden.

Nähere Informationen zu den eingesetzten Verfahren sind bei Interesse im Internet zugänglich:

VNC	http://www.uk.research.att.com/vnc
TridiaVNC	http://www.tridiavnc.com

5.1.4
Fazit

Unter diesen Rahmenbedingungen ist nach meiner Einschätzung zunächst die Verwirklichung dieses Projektes möglich. Die konkrete Umsetzung werde ich weiter beobachten. In diesem Kontext sind dann auch einzelne im Bereich der Justiz eingesetzte Verfahren zu bewerten.

5.2
Unzulässige Auskunftsersuchen an Pflichtverteidiger nach Steuerdaten

Vor der Anweisung ihrer Vergütung dürfen Gerichte den Pflichtverteidigern keine Auskunft über deren Steuernummer und das zuständige Finanzamt abverlangen, um eventuelle Steuerrückstände zu erfragen, gegen die aufgerechnet werden könnte.

Die Rechtsanwaltskammer Kassel machte mich auf folgenden Sachverhalt aufmerksam: Rechtsanwälte aus dem Kammerbezirk, die als Pflichtverteidiger in Strafsachen tätig waren, beschwerten sich, dass das Landgericht Kassel vor der Anweisung von Vergütungen über 5.000,– DM eine Steueranfrage an das zuständige Finanzamt richtet. Zu diesem Zweck wurden die betroffenen Rechtsanwälte unter Bezugnahme auf einen Erlass des Hessischen Ministeriums der Justiz vom 14. März 1983 (beruhend auf einem Erlass vom Hessischen Ministerium der Finanzen vom 18. Februar 1981) aufgefordert, ihr zuständiges Finanzamt und ihre Steuernummer mitzuteilen.

Eine Überprüfung der Sach- und Rechtslage ergab, dass die Abfragen unzulässig waren. Nicht nur waren beide Erlasse zwischenzeitlich außer Kraft getreten, wurden aber dennoch weiter angewendet. Hinzu kam, dass sie bereits im

Zeitpunkt des Erlasses auf keiner ausreichenden Ermächtigungsgrundlage beruhten. Als reine Verwaltungsvorschriften konnten sie keinen datenschutzrechtlichen Eingriff der Gerichtskasse – wie die Abfrage der Steuerdaten der Pflichtverteidiger – rechtfertigen.

Das Hessische Ministerium der Justiz sah die Vorgehensweise des Gerichts ebenfalls als unzulässig an. Es gab aber zu bedenken, dass die Aufforderung nicht von der Gerichtskasse, sondern durch Richter/Rechtspfleger veranlasst wurde und somit weitgehend der Dienstaufsicht des Ministeriums entzogen sei.

Das Ministerium hat gleichwohl mit einem Schreiben an alle hessischen Gerichte auf die Rechtslage hingewiesen und mitgeteilt, dass eine entsprechende Abfrage der Steuerdaten bei Pflichtverteidigern vor Anweisung ihrer Gebühren nicht zulässig ist. Daran ändert auch die mit Wirkung zum 1. Juli 2002 eingeführte Bestimmung des § 14 Abs. 1a Umsatzsteuergesetz nichts. Danach hat ein leistender Unternehmer in der Rechnung die ihm vom Finanzamt erteilte Steuernummer anzugeben. Diese Verpflichtung hat die Steuerverwaltung dem Unternehmer auferlegt, um die finanzamtsinterne Bearbeitung zu erleichtern. Sie entfaltet keine Wirkung gegenüber einem Rechnungsempfänger. Wenn der Leistende die Steuernummer – berechtigt oder unberechtigt – in der Rechnung nicht angibt, kann der Rechnungsempfänger ihre Bekanntgabe trotz § 14 Abs. 1a UStG nicht verlangen.

Ich gehe deshalb davon aus, dass die Verfahrensweise nicht fortgesetzt wird.

6. Polizei- und Strafverfolgungsbehörden

„Vorbeugende“ Fahndung nach einem Zechpreller

Ungewöhnliche Sachverhalte rechtfertigen ungewöhnliche Maßnahmen. In bestimmten Fällen ist es auch bei eher geringfügigen Delikten nicht unzulässig, die potenziell Geschädigten von Straftaten vor dem Täter zu warnen.

Eine Polizeibehörde brachte mir zur Kenntnis, dass ein im Umland einer Großstadt lebender Mann in den vergangenen Jahren gelegentlich als Zechpreller aufgefallen ist, und zwar in zwei Fällen im Jahre 2001. Seit einigen Monaten lebe diese Person ihre Neigung zur „Zechprellerei“ exzessiv aus. So habe er sich im Januar 2002 nach einer Zeche von über 200 € für ein gutes Essen und mehrere Flaschen Champagner an der Bar in einem Grand-Hotel „aus dem Staub“ gemacht. Mitte Februar war er erneut an der gleichen Theke, fiel auf und wurde gefasst, weil ein Kellner sich an ihn erinnerte. An einem Abend im März 2002 befand er sich gleich zweimal in der Wache des Polizeireviers, nachdem er jeweils von Gastwirten renommierter Restaurants angezeigt worden war. Noch in der gleichen Nacht wurde er ein drittes Mal in der Wache eingeliefert, musste aber nach Aufnahme der Anzeige jeweils „laufen gelassen“ werden. Er hat zwar kein Einkommen und zivilrechtlich sei bei ihm „nichts zu holen“. Da er einen festen Wohnsitz hat, bekommt die Polizei wegen der begangenen Delikte vom Haftrichter trotz der Wiederholungsgefahr keinen Haftbefehl. Der nächste Fall fand zwei Tage später im Theaterrestaurant statt. Nach weiteren zwei Tagen beging er im Opernrestaurant (180 €) zum vorläufig letzten Mal Zechprellerei.

Die Polizei bat mich um Stellungnahme, ob sie in den einschlägigen Restaurants der gehobenen Klasse ein Bild des Täters hinterlegen dürfe. Die Maßnahme verfolge dreierlei Zielrichtungen:

1. Verhütung von Straftaten
2. Verhütung der Beeinträchtigung der Rechte der Opfer
3. Fürsorgeüberlegungen gegenüber dem Täter

Als Rechtsgrundlage der Datenübermittlung käme § 23 Abs. 1 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) in Frage.

§ 23 Abs. 1 bis 3 HSOG

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

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

erforderlich ist.

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

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

Die Summe der Schäden und die Häufigkeit der Vergehen rechtfertigte nach meiner Einschätzung die Datenübermittlung an die potenziellen Opfer zur Verhütung bevorstehender Straftaten und zu erwartender weiterer Schäden. Ich habe der Polizeibehörde mitgeteilt, dass ich gegen das Vorhaben, den Restaurantinhabern ein Lichtbild des Täters zur Verfügung zu stellen, keine Einwände habe. Aufmerksam machte ich noch auf die Nebenbestimmung, dass die Datenempfänger – also die Restaurantinhaber – darauf hinzuweisen sind, dass die übermittelten Informationen nur zu dem Zweck verwendet werden dürfen, zu dem sie ihnen gegeben wurden (Abs. 3). Außerdem war aufgrund des Verweises in § 23 Abs. 2 der Täter über die Maßnahme zu unterrichten. Beides wurde zugesagt.

7. Ordnungswidrigkeiten

Zeugenangabe im Bußgeldbescheid

Das landesweit bei der Bearbeitung von Ordnungswidrigkeitenverfahren angewendete Datenverarbeitungsverfahren lässt die Auswahlmöglichkeit zu, Angaben über einen Zeugenbeweis entweder unter Nennung des Namens und Wohnortes des Zeugen oder nur unter der Angabe „Zeuge/Zeugin“ im Anhörungsschreiben zu nennen. In der Praxis wird dies nicht hinreichend beachtet. Aufgrund mehrerer Eingaben von Zeugen, die sich über die Bekanntgabe ihres Namens und Wohnortes im Anhörungsschreiben an den Beschuldigten beschwerten, musste ich feststellen, dass die Beachtung dieser Auswahlmöglichkeit zur Vermeidung von Repressalien gegenüber den anzeigeerstattenden Personen dringend geboten ist.

Bereits in meinem 28. Tätigkeitsbericht hatte ich darauf hingewiesen, dass das Datenverarbeitungsverfahren und die für die manuelle Vorgangsbearbeitung zu verwendenden landeseinheitlichen Vordrucke, bereits für das Vorverfahren die Auswahlmöglichkeit vorsehen, dass entweder Name und Wohnort der Person, die einen ordnungswidrigen Sachverhalt zur Anzeige gebracht hat, genannt werden oder aber lediglich die Angabe: Beweismittel „Zeuge/Zeugin“ im Verwarnungsgeldangebot und im Anhörungsbogen aufgenommen wird.

Die Verfolgungsbehörde hat einen Ermessensspielraum, welche der beiden Varianten sie wählt. Bei ihrer Ermessensentscheidung hat sie das Datenschutzinteresse des Zeugen gegen das Informationsinteresse des Betroffenen abzuwägen.

Eingaben an meine Behörde zeigen, dass bei der Bearbeitung von Ordnungswidrigkeiten die Verfolgungsbehörden jedoch häufig keinen Gebrauch von der bestehenden Auswahlmöglichkeit bezüglich der Zeugenangaben machen. Auch in Fällen, in denen eine Zeugenangabe nicht erforderlich ist, wird der Name z. B. des Anzeigeerstatters angegeben. Bei sachgerechter Ausübung des Ermessens sollte in Ordnungswidrigkeitenverfahren, die nur mit einem Verwarnungsgeld geahndet werden, regelmäßig der datenschutzfreundlichen Variante ohne Namens- und Adressangabe der Vorzug gegeben werden. Das gilt insbesondere für Zeugen, die keine amtliche Funktion wahrgenommen haben. Damit könnten auch die in den mir bekannten Fällen anonym erfolgten Belästigungen der Anzeigeerstatter weitgehend vermieden werden.

Zwar kann auch im Ordnungswidrigkeitenverfahren der Adressat eines Verwarnungsgeldangebotes durch Akteneinsichtnahme oder Auskunft den Namen des Zeugen beziehungsweise der Zeugin erfahren. Hierauf sind Zeugen auf jeden Fall hinzuweisen. Dennoch sollte bei solchen Verfahren auf dem Verwarnungsgeldangebot und in dem Anhörungsbogen grundsätzlich auf die Zeugenangaben verzichtet werden. Die Angabe ist in diesem Verfahrensstadium entbehrlich und nicht angemessen. Wird das Verwarnungsgeld bezahlt oder kann der Betroffene den Vorwurf schlüssig zurückweisen, kommt es zu keinem Bußgeldbescheid, in dem dann die Zeugenangaben anzugeben wären.

Ein zu erwartendes Bußgeld setzt hingegen die Kenntnis der Zeugen voraus. Im Bußgeldverfahren ist es deshalb erforderlich, dass im Anhörungsschreiben der Name und der Wohnort des Zeugen benannt wird. Auf die Angabe der vollständigen Anschrift des Zeugen kann allerdings verzichtet werden. Auf Anfrage oder durch Akteneinsichtnahme steht sie jedoch dem Betroffenen zur Verfügung.

Die Abwägung zwischen den datenschutzrechtlichen Interessen der Zeugen und dem Informationsinteresse der Betroffenen führt in diesem Fall zur Zurückstellung der Zeugenbelange. Zeugen müssen hinnehmen, dass der angezeigten Person ihre Identifikationsdaten (Name und Wohnort) sowie der Gegenstand der Zeugenaussage bekannt werden. Ausnahmen hiervon sind nach meiner Auffassung nur bei besonderer Schutzbedürftigkeit der Zeugen zu machen.

Im Interesse der Bürgerinnen und Bürger ist zu beachten, dass die vorgesehene Ermessensentscheidung getroffen werden muss. Im Regelfall wird die Abwägung zum Ergebnis haben, dass bei zu erwartendem Verwarnungsgeld auf die namentliche Nennung der Zeugen im Anhörungsschreiben verzichtet werden kann.

8. Verfassungsschutz

8.1
Neues Verfassungsschutzgesetz

Das neue Landesverfassungsschutzgesetz ist im Mai 2002 verkündet worden. Es sieht die Zuständigkeit des Verfassungsschutzes für die Bekämpfung der organisierten Kriminalität vor. Die Befugnisse zum Abhören und zur Anfertigung von Bildaufzeichnungen in Wohnungen wurden deutlich erweitert. Auch in den neuen Auskunftspflichten unter anderem für Geldinstitute, Postdienstleistungs- und Luftverkehrsunternehmen, geht das Hessische Gesetz über das novellierte Bundesverfassungsschutzgesetz hinaus.

Im letzten Tätigkeitsbericht (Ziff. 9.1) habe ich über einen Entwurf zur Änderung des hessischen Gesetzes über das Landesamt für Verfassungsschutz (VerfSchG) berichtet. Trotz meiner wiederholt vorgetragenen Kritik ist es in wichtigen Teilen dabei geblieben; zudem sind nachträgliche Befrachtungen des Entwurfs vorgenommen worden:

– Das Gesetz sieht die Einbeziehung der organisierten Kriminalität in den Aufgabenbereich des Verfassungsschutzes vor. Erfolge mit dieser neuen Kompetenz kann ich noch nicht bewerten, da nach Aussage des Verfassungsschutzes noch keine Erfahrungen vorliegen.

– Die Befugnisse zum Abhören und zur Anfertigung von Bildaufnahmen (§ 5 Abs. 2 VerfSchG) sind im Vergleich zum früheren Gesetz stark erweitert worden. Sie gehen auch weit über die Regelungen in der Novellierung des Bundesverfassungsschutzgesetzes (BVerfSchG) durch das Terrorismusbekämpfungsgesetz vom 9. Januar 2002 (BGBl. I S. 361) hinaus. Anders als das Bundesgesetz, das eine gegenwärtige gemeine Gefahr oder gegenwärtige Lebensgefahr für eine Person voraussetzt (§ 9 Abs. 2 Satz 1 BVerfSchG), reicht in Hessen schon der Verdacht, dass bestimmte Straftaten begangen wurden. Leider ist der Gesetzgeber meiner Anregung nicht gefolgt, dass die aufgrund derartiger Abhörmaßnahmen beziehungsweise heimlicher Bildaufnahmen erhobenen Informationen besonders gekennzeichnet werden. Ich hatte darauf hingewiesen, dass entsprechende Vorkehrungen, die für den Bundesnachrichtendienst bei Eingriffen in das Fernmeldegeheimnis vorgeschrieben sind, auch für Fallgestaltungen gelten müssen, bei denen personenbezogene Daten durch Maßnahmen erlangt werden, die in ihrer Art und Schwere einer Beschränkung des Fernmeldegeheimnisses gleichkommen. Auf diese Weise wäre die besondere Sensibilität für das Landesamt für Verfassungsschutz selbst, vor allem aber für alle weiteren Empfänger sofort erkennbar geworden.

– Die im Entwurf vorgesehenen Auskunftsersuchen für das Landesamt für Verfassungsschutz gegenüber Postdienstleistern, Tele- und Telekommunikationsdienstleistern, Kreditinstituten, Finanzunternehmen und Luftverkehrsunternehmen (§ 4 Abs. 7 bis Abs. 11 VerfSchG) sind beibehalten worden. Auch hier geht man weit über das neue Bundesverfassungsschutzgesetz und andere novellierte Landesverfassungsschutzgesetze hinaus, denn in Hessen gelten diese Auskunftsersuchen für das gesamte Aufgabenspektrum des Verfassungsschutzes. Auf Bundesebene dürfen beispielsweise bei der Extremismusbeobachtung derartige Auskunftsersuchen nicht gestellt werden.

– Lediglich das Vorhaben, bereits über zwölfjährige Kinder einschlägige Daten speichern zu dürfen, wurde im Gesetzgebungsverfahren ein Stück zurückgenommen. Das Alter wurde auf 14 Jahre heraufgesetzt (§ 6 Abs. 2 VerfSchG). Nach der alten Rechtslage war allerdings ein Alter von 16 Jahren vorgesehen.

– Im Verhältnis zum Entwurf blieb es auch bei der Verlängerung der Lösch- und Prüffristen, die nunmehr statt fünf beziehungsweise zehn Jahre, zehn beziehungsweise 15 Jahre betragen.

8.2
Keine Abhörbefugnis gegenüber Journalisten und anderen besonders geschützten Berufsgruppen

Bei der nächsten Novellierung des Gesetzes über das Landesamt für Verfassungsschutz sollte ein Verbot des Abhörens von Personen, die aus beruflichen Gründen ein Zeugnisverweigerungsrecht besitzen, in das Gesetz aufgenommen werden.

Im Zusammenhang mit der Novellierung des Hamburgischen Verfassungsschutzgesetzes im Herbst letzten Jahres tauchte die Frage auf, ob die in § 5 Abs. 2 des Gesetzes über das Landesamt für Verfassungsschutz (VerfSchG) stark erweiterten Befugnisse zum Abhören und Anfertigen von Bildaufnahmen in Wohnungen auch für besonders geschützte Berufsgruppen gelten. Konkret ging es darum, ob beispielsweise Gespräche eines Journalisten mit einer Person, bei der Anhaltspunkte für bestimmte Tätigkeiten im Sinn des Verfassungsschutzgesetzes vorliegen, im Büro des Journalisten abgehört werden dürfen.

Eine derartige Maßnahme würde einen Eingriff in die in Art. 5 Abs. 1 Grundgesetz garantierte Pressefreiheit darstellen.

Während nach der Strafprozessordnung derartige Maßnahmen gegenüber bestimmten Personen, die aus beruflichen Gründen ein Zeugnisverweigerungsrecht besitzen, ausgeschlossen sind (§ 100d Abs. 3 Strafprozessordnung; StPO), existiert im Verfassungsschutzgesetz ein derartiges Verbot nicht. Ich habe deshalb im Gespräch mit Vertretern des

Hessischen Ministeriums des Innern angeregt, dass bei der nächsten Novellierung des Verfassungsschutzgesetzes auch eine dem § 100d Abs. 3 StPO entsprechende Formulierung aufgenommen wird. Das Hessische Ministerium des Innern hat Bereitschaft gezeigt, eine entsprechende Regelung aufzunehmen.

8.3
Personenbezogene Daten in Sachakten des Verfassungsschutzes

Der Hessische Datenschutzbeauftragte hat sich dafür eingesetzt, dass personenbezogene Daten in so genannten Sachakten des Landesamtes für Verfassungsschutz nicht mehr verwandt werden dürfen, wenn die Akte und entsprechende Datensätze zur Person des Betroffenen gelöscht wurden.

Im Berichtsraum hatte ich mich im Rahmen eines konkreten Falles mit der Frage zu befassen, wie mit personenbezogenen Daten in so genannten Sachakten des Verfassungsschutzes zu verfahren ist, wenn die Akte zur Person des Betroffenen und entsprechende Datensätze im Nachrichtendienstlichen Informationssystem des Verfassungsschutzes (NADIS) längst gelöscht worden waren.

Bei Sachakten handelt es sich um Informationssammlungen beispielsweise zu einer extremistischen Bestrebung, in der neben allgemeinen Informationen in der Regel auch Daten zu einzelnen Personen enthalten sind. Überschreiten die Informationen zu dieser Person einen gewissen Umfang, werden die Daten in NADIS gespeichert und eine Personenakte angelegt. Wird die NADIS-Speicherung und die Personenakte nach Ablauf der vorgesehenen Fristen gelöscht, so muss dies auch Konsequenzen für die entsprechenden personenbezogenen Daten in der Sachakte haben: Bisher bestand Einvernehmen zwischen dem Landesamt für Verfassungsschutz und mir, dass diese Daten „gesperrt“ sind und nicht mehr verwandt werden dürfen.

Im erwähnten Fall argumentierte das Hessische Ministerium des Innern, dass diese Daten zwar gesperrt, eine Durchbrechung allerdings beispielsweise zur Behebung einer bestehenden Beweisnot nötig sei.

§ 19 Abs. 2 Satz 3 HDSG

(2) ... Gesperrte Daten dürfen über die Speicherung hinaus nicht mehr verarbeitet werden, es sei denn, dass die Verarbeitung zur Behebung einer bestehenden Beweisnot oder aus sonstigen im rechtlichen Interesse eines Dritten liegenden Gründen unerlässlich ist oder der Betroffene in die Verarbeitung eingewilligt hat. ...

Leider konnte keine Übereinstimmung erzielt werden, wie generell mit den personenbezogenen Daten in Sachakten zu verfahren ist.

Deshalb halte ich es für nötig, für künftige Fälle eine klare gesetzliche Regelung zu finden. An sich handelt es sich bei den Verwertungshindernissen personenbezogener Daten in Sachakten nicht um eine „Sperrung“ i. S. v. § 19 Abs. 2 HDSG. Es geht vielmehr darum, dass man aus praktischen Gründen von einer Löschung oder Unkenntlichmachung der Daten in der Sachakte absieht und stattdessen ein Verwertungsverbot statuiert. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat meine Auffassung durch einen dazu gefassten Beschluss bestätigt. Sie fordert eine gesetzliche Regelung, die primär die Löschung, auf jeden Fall aber die Sperrung der personenbezogenen Daten vorsieht.

Im Rahmen des Novellierungsverfahrens für das Hessische Verfassungsschutzgesetz habe ich eine Formulierung vorgeschlagen, die ausdrücklich ein Verwertungsverbot für die entsprechenden personenbezogenen Daten in Sachakten vorsieht. Sie lässt eine Durchbrechung nur in sehr engen Grenzen zu, nämlich wenn sie im Interesse des Betroffenen oder zur Abwehr einer Gefahr für Leib und Leben unerlässlich ist. Leider hat das Hessische Ministerium des Innern meine Vorschläge nicht aufgegriffen.

8.4
Informationsbesuch beim Landesamt für Verfassungsschutz

Die Arbeitsdatei „Auswertung“ (LARGO) im Landesamt für Verfassungsschutz Hessen ist für alle Tätigkeitsbereiche im Einsatz. Bei der Durchsicht von 36 Personen- und Sachakten wurden keine Mängel festgestellt.

8.4.1
Arbeitsdatei LARGO

Im 26. Tätigkeitsbericht (Ziff. 14.3) und im 27. Tätigkeitsbericht (Ziff. 16.2) hatte ich berichtet, dass das Landesamt für Verfassungsschutz (LfV) ein neues Datenverarbeitungssystem entwickelt. Im Unterschied zum Nachrichtendienstlichen Informationssystem (NADIS) der Verfassungsschutzämter, das in erster Linie zum Auffinden der zu einer Person angelegten Akte dient, können in LARGO alle zu einer Person oder zu einem Objekt gehörenden Texte und Informationen direkt eingespeichert werden.

Wie im 27. Tätigkeitsbericht (Ziff. 16.2) beschrieben, war seinerzeit vorgesehen, dass LARGO das Führen von Personenakten ersetzen sollte, was damals schon im Bereich Linksextremismus erfolgt war. Nunmehr hat sich der Einsatz von LARGO geändert: Es geht nicht mehr um den Ersatz der Papierakte durch ein elektronisches Medium. LARGO wird vielmehr dergestalt genutzt, dass beim LfV eingehende oder von ihm erhobene Informationen zu einer Person in aufgearbeiteter und konzentrierter Weise eingespeichert werden, um auf diese Weise schneller und einfacher abrufbar zu sein als durch das Studium einer Akte. Konventionelle Personenakten in Papierform werden parallel dazu geführt.

Bisher galt der Grundsatz, dass eine Speicherung in LARGO nur dann in Betracht kommt, wenn auch eine Speicherung in NADIS erfolgt. Davon muss jetzt abgewichen werden, denn nach dem novellierten hessischen Verfassungsschutzgesetz dürfen Informationen auch schon zu Kindern ab 14 Jahren in Dateien gespeichert werden. Bisher war die Grenze bei 16 Jahren.

§ 6 Abs. 2 VerfSchG

Das Landesamt für Verfassungsschutz darf Daten über Minderjährige, die das 14. Lebensjahr nicht vollendet haben, in zu ihrer Person geführten Akten nur speichern, wenn tatsächliche Anhaltspunkte dafür bestehen, dass der Minderjährige eine der in § 3 des Art. 10 des Gesetzes genannten Straftaten plant, begeht oder begangen hat. In Dateien ist eine Speicherung von Daten Minderjähriger, die das 14. Lebensjahr nicht vollendet haben, nicht zulässig.

Da in den entsprechenden Vorschriften für NADIS Minderjährige erst ab 16 Jahren gespeichert werden dürfen, besteht insoweit eine Diskrepanz. Die Vertreter des LfV berichteten jedoch, dass die NADIS-Vorschriften entsprechend geändert werden sollen.

8.4.2
Andere Arbeitsdateien

Bei einer datenschutzrechtlichen Überprüfung wurde festgestellt, dass der größte Teil der vom LfV betriebenen Arbeitsdateien in LARGO integriert wurde. Die uns vorgelegte Aufstellung der derzeit noch bestehenden Arbeitsdateien betrifft vor allem den Organisations- und Verwaltungsbereich.

8.4.3
Prüfung von Akten

Die durchgeführte Stichprobenprüfung von Akten ergab keine zu beanstandenden Mängel. Der Prüfung waren 36 nach verschiedenen Kriterien ausgesuchte Personen- und Sachakten unterzogen worden. Sie bezog sich auf formale Kriterien, wie die erforderliche Kontrolle von Prüf- und Löschfristen durch das LfV. Ziel der Überprüfung war gleichzeitig die Frage, ob die Sammlung von Informationen in den Akten mit den Voraussetzungen des Verfassungsschutzgesetzes vereinbar ist.

9. Ausländerrecht

9.1
Prüfung des Einbürgerungsverfahrens

Nach einer Prüfung des Einbürgerungsverfahrens im Jahre 1994 wurden Verfahrensveränderungen vorgenommen, die zu einer deutlich verbesserten Berücksichtigung der datenschutzrechtlichen Belange der Einbürgerungsbewerberinnen und -bewerber führten. Bei einer neuerlichen Prüfung wurde weiteres Vereinfachungs- und Verbesserungspotential festgestellt.

Acht Jahre nach einer Datenschutzprüfung des Einbürgerungsverfahrens beim Regierungspräsidium Darmstadt (23. Tätigkeitsbericht, Ziff. 16.1) habe ich durch eine erneute Kontrolle den Erkenntnisstand aktualisiert. Gesetzliche Grundlagen des Einbürgerungsverfahrens sind Vorschriften im Ausländergesetz (§§ 85 ff.), im Staatsangehörigkeitsgesetz (§§ 8, 9, 13) und im Gesetz zur Regelung von Fragen der Staatsangehörigkeit (§ 9).

Änderungen im Verwaltungsablauf hat das Hessische Ministerium des Innern und für Sport mit zwei neuen Vorschriften geregelt. Mit Erlass vom 25. Juni 2001 (StAnz. S. 2479) hat es Verwaltungsvorschriften über das Verfahren bei Anspruchs- und Ermessenseinbürgerungen (VfVEbg) aufgestellt und in einem weiteren Erlass vom 25. September 2001 (nicht veröffentlicht) die so genannte Regelanfrage beim Landesamt für Verfassungsschutz in Hessen eingeführt.

Bei meinem Kontrollbesuch konnte ich feststellen, dass die bei meiner Prüfung im Jahre 1994 im zuständigen Dezernat des Regierungspräsidiums festgestellten gravierenden Mängel bei technischen und organisatorischen Maßnahmen zur Datensicherung abgestellt waren.

Außerdem wurden mit der VfVEbg u. a. eine Reihe von datenschutzrechtlichen Forderungen umgesetzt, die ich schon im Anschluss an meine damalige Prüfung aufgestellt hatte und die in der Verwaltungspraxis zum Teil bereits seit einiger Zeit berücksichtigt worden sind. Nunmehr werden die Einbürgerungsbewerberinnen und -bewerber mit einem Formblatt ausführlich über die Verarbeitung ihrer personenbezogenen Daten in Kenntnis gesetzt. Es werden – im Gegensatz zu früher – keine pauschalen Einwilligungserklärungen der Antragstellerinnen und Antragsteller eingeholt, wonach in die Abfrage von Daten bei „allen am Einbürgerungsverfahren beteiligten Stellen“ eingewilligt wird. Stattdessen sieht der Erlass mehrere Fassungen von Einverständniserklärungen vor:

– eine für Abfragen, die bei allen Antragstellern getätigt werden müssen, wie z. B. beim Ausländeramt, dem Bundeszentralregister oder der Polizei,

– optional und nur bei Bedarf eine weitere Einverständniserklärung, wenn im Einzelfall Daten z. B. beim Sozialamt oder bei einer Finanzbehörde erfragt werden müssen.

Die Ergebnisse der Prüfung waren in anderen Bereichen nicht durchgängig zufriedenstellend. So werden nach wie vor überflüssige Datenerhebungen vorgenommen und nicht erforderliche Dokumente in den Akten aufbewahrt:

Voraussetzung für die Einbürgerung von Jugendlichen ist der Nachweis ausreichender Deutschkenntnisse. Nicht nur in Einzelfällen befanden sich zum Nachweis über Jahre hinweg gesammelte Schulzeugnisse von jugendlichen Einbürgerungsbewerberinnen oder -bewerbern in den Akten, obwohl bereits mit einem einzigen Dokument, nämlich z. B. dem Abiturzeugnis einer deutschen Schule, ausreichende Deutschkenntnisse nachgewiesen waren. Ich habe das Regierungspräsidium Darmstadt gebeten, bei den unteren Verwaltungsbehörden darauf hinzuwirken, keine überflüssigen Dokumente von Einbürgerungsbewerberinnen oder -bewerbern entgegenzunehmen.

Umgekehrt stieß ich auf einige Einzelfälle, bei denen aufgrund mangelnder Deutschkenntnisse oder nur sehr kurzem Aufenthalt in Deutschland vollkommen klar war, dass der Einbürgerungsantrag bereits aus diesem Grund abzulehnen war. Dennoch wurden noch weitere Datenübermittlungen z. B. von der Polizei oder dem Bundeszentralregister erbeten. Es wurde mit dem Regierungspräsidium Einvernehmen erzielt, dass solche Datenerhebungen künftig unterbleiben.

Probleme wirft die Prüfung der gesetzlichen Vorgabe auf, ob Einbürgerungsbewerberinnen beziehungsweise -bewerber straffrei sind. Nach Ziff. 24.1 VfVEbg hat die Einbürgerungsbehörde dazu eine unbeschränkte Auskunft aus dem Bundeszentralregister einzuholen, die ihr gemäß § 42 Abs. 6 Bundeszentralregistergesetz vom Generalbundesanwalt erteilt wird. Zusätzlich holen die unteren Verwaltungsbehörden nach Ziff. 19.2 VfVEbg über die örtliche Polizeidienststelle eine Stellungnahme des Landeskriminalamtes ein, ob ein Ermittlungsverfahren anhängig ist oder ob sonstige strafrechtliche Erkenntnisse vorliegen. Diese Datenerhebungen sind gesetzlich begründet durch die Regelung in § 85 Abs. 1 Nr. 5 Ausländergesetz (AuslG).

§ 85 Abs. 1 AuslG

Ein Ausländer, der seit acht Jahren rechtmäßig seinen gemütlichen Aufenthalt im Inland hat, ist auf Antrag einzubürgern, wenn er

.....

5. nicht wegen einer Straftat verurteilt worden ist.

...

Aus den von mir eingesehenen Stellungnahmen ist ersichtlich, dass die Polizeidienststellen zur Beantwortung der Anfragen ganz unterschiedliche Informationsquellen heranziehen. Einige der örtlichen Polizeibehörden erteilen Auskunft über alle im polizeilichen Informationssystem gespeicherten Erkenntnisse, einschließlich der abgeurteilten und eingestellten Ermittlungsverfahren. Andere örtliche Polizeidienststellen erteilen Auskunft aus ihrer Zentralkartei; dort sind auch Daten von Opfern und Zeugen gespeichert. Daten über Opfer und Zeugen dürfen nicht übermittelt werden. In einigen anderen Polizeibehörden wird die Anfrage vom Staatsschutzkommissariat selektiv bearbeitet.

Oft ist es schwierig und aufwändig – so das Einbürgerungsdezernat beim Regierungspräsidenten – den Informationen aus den Stellungnahmen der Polizei nachzugehen. Nicht selten wird dabei festgestellt, dass die mitgeteilten Verfahren bereits vor Jahren eingestellt worden waren. Abgesehen von dem überflüssigen Verwaltungsaufwand bei der Polizei und der Einbürgerungsbehörde sind Datenübermittlungen vorprogrammiert, die weder sachgerecht noch erforderlich sind. So sind z. B. Datenübermittlungen über abgeurteilte Fälle überflüssig, denn über sie erlangt die Einbürgerungsbehörde Kenntnis durch den Bundeszentralregisterauszug. Mitteilungen über eingestellte Verfahren sind ebenfalls überflüssig, denn sie können der Einbürgerung nicht entgegenstehen.

Unklar ist, inwieweit Doppelübermittlungen – einmal durch die Staatsschutzkommissariate, ein weiteres Mal durch die Regelanfrage beim Landesamt für Verfassungsschutz – erfolgen. Die im weiteren Verlauf des Einbürgerungsverfahrens einzuholende Stellungnahme des Landeskriminalamtes ist überflüssig, wenn dazu auf dieselbe Informationsquelle zurückgegriffen wird, wie für die Stellungsnahme der örtlichen Polizeibehörde. Ich habe das Hessische Innen-

ministerium gebeten, eine Koordination zwischen den dort ressortierten Stellen für das Einbürgerungsverfahren und die Polizei herbeizuführen. Es muss eine Lösung gefunden werden, die den datenschutzrechtlichen Belangen der Betroffenen Rechnung trägt.

Weiteres Ziel der Prüfung war, Klarheit darüber zu gewinnen, welche datenschutzrechtliche Auswirkungen die eingeführte Regelanfrage beim Hessischen Landesamt für Verfassungsschutz über Einbürgerungsbewerberinnen und -bewerber hat. Danach ist vor jeder Einbürgerung das Landesamt für Verfassungsschutz zu fragen, ob Erkenntnisse vorliegen, die der beantragten Einbürgerung entgegenstehen könnten. Bislang war eine Anfrage nur dann erforderlich, wenn konkrete Anhaltspunkte für Betätigungen bestanden, die der Einbürgerung entgegenstanden. Die Prüfung hat ergeben, dass seit Anwendung des Erlasses im September 2001 bis zum Zeitpunkt meiner Prüfung im April 2002 keine Einbürgerung wegen einer von der Verfassungsschutzbehörde übermittelten Information abgelehnt wurde.

9.2
Datenübermittlung aus dem Erziehungsregister

Die durch § 76 Abs. 4 Ausländergesetz begründete Datenübermittlungspflicht der Staatsanwaltschaften ist von der Verwendungseinschränkung des § 61 Abs. 1 Bundeszentralregistergesetz nicht tangiert.

Ein Rechtsanwalt hat mich mit folgendem Sachverhalt befasst: Seiner Mandantin, einer 22-jährigen äthiopischen Staatsangehörigen, wurden in einer Auseinandersetzung mit der Ausländerbehörde zwei Einträge im Erziehungsregister vorgehalten, die der Ausländerbehörde durch Mittlungen nach § 76 Abs. 4 Ausländergesetz (AuslG) bekannt geworden waren.

§ 76 Abs. 4 AuslG

Die für die Einleitung und Durchführung eines Straf- und eines Bußgeldverfahrens zuständigen Stellen haben die zuständige Ausländerbehörde unverzüglich über die Einleitung des Verfahrens sowie die Verfahrenserledigungen bei der Staatsanwaltschaft, bei Gericht oder bei der für die Verfolgung und Ahndung der Ordnungswidrigkeit zuständigen Verwaltungsbehörde unter Angabe der gesetzlichen Vorschriften zu unterrichten. ...

In dem einen Fall war der damals 16-Jährigen eine Ermahnung erteilt und ansonsten gemäß § 45 Abs. 2 Jugendgerichtsgesetz von einer Anklageerhebung abgesehen worden. In dem anderen Fall kam es nach der Anklageerhebung zu einer Verwarnung durch den Jugendrichter mit der Auflage, eine Geldbuße zu zahlen sowie unentgeltliche gemeinnützige Arbeit zu leisten. Der Anwalt argumentierte, diese Informationen hätten für die ausländerrechtliche Entscheidung nicht herangezogen werden dürfen, weil die Entscheidungen auch im Erziehungsregister eingetragen sind und die einschränkenden Verwendungsregelungen des § 61 Abs. 1 Bundeszentralregistergesetz (BZRG) eine Verwendung zu ausländerrechtlichen Zwecken nicht vorsehen. Das Gericht teilte die Ansicht, dass § 61 Abs. 1 BZRG der Regelung des § 76 Abs. 4 AuslG vorgehe und machte der Ausländerbehörde einen Vergleichsvorschlag, für den im konkreten Fall auch noch andere Gründe sprachen.

§ 61 Abs. 1 BZRG

Eintragungen im Erziehungsregister dürfen – unbeschadet der §§ 42a, 42c – nur mitgeteilt werden

1. den Strafgerichten und Staatsanwaltschaften für Zwecke der Rechtspflege sowie den Justizvollzugsbehörden für Zwecke des Strafvollzugs einschließlich der Überprüfung aller im Strafverfahren tätigen Personen,
2. den Vormundschaftsgerichten und Familiengerichten für Verfahren, welche die Sorge für die Person des im Register Geführten betreffen,
3. den Jugendämtern und den Landesjugendämtern für die Wahrnehmung von Erziehungsaufgaben der Jugendhilfe,
4. den Gnadenbehörden für Gnadensachen.

Da ich die Rechtsansicht des Gerichts nach Einsicht in die Akte und genauer rechtlicher Beurteilung nicht teile, habe ich keine Veranlassung gesehen, allgemeine Vorkehrungen zu fordern, damit bei künftigen ausländerrechtlichen Entscheidungen keine Informationen herangezogen werden, die auch im Erziehungsregister gespeichert sind.

Nur wenn Informationen vom Generalbundesanwalt als der registerführenden Stelle aus dem Erziehungsregister übermittelt werden sollen, gilt § 61 Abs. 1 BZRG. Will die Ausländerbehörde dagegen eine Information verwenden, die ihr von der Staatsanwaltschaft gemäß § 76 Abs. 4 AuslG übermittelt wurde, steht dem § 61 Abs. 1 BZRG – „nur“ weil die Information auch im Erziehungsregister gespeichert ist – nicht entgegen. Gegenstand der Information ist die Abschlussmitteilung der Staatsanwaltschaft. Diese ist nicht mit einer Auskunft aus dem Erziehungsregister gleichzusetzen. Auch begründet § 61 Abs. 1 BZRG kein selbständiges Verwertungsverbot.

10. Finanzwesen

10.1
Ausweitung der Überwachung, Speicherung und Online-Abrufe der Finanzverwaltung

Der Bundesgesetzgeber hat im Verlauf der letzten zwei Jahre eine Vielzahl von Überwachungsmöglichkeiten geschaffen, die von den Landesfinanzbehörden umzusetzen sind. Die teilweise zu weit reichenden oder unvollständigen Vorschriften haben zu häufigen Interventionen gegen die Gesetzes- und Ausführungsvorschriften sowie zu Anwendungsproblemen geführt. Die nachfolgende Analyse und Kritik zeigt, wie weit die Zugriffsmöglichkeiten der Finanzverwaltung auf Unternehmen und andere Steuerpflichtige inzwischen reichen und wie kurz die Distanz zum „gläsernen Unternehmen“ und „gläsernen Steuerbürger“ geworden ist.

10.1.1
Zugriff auf Firmen-EDV

Mit Einführung des § 147 Abs. 6 Abgabenordnung (AO) durch das Steuersenkungsgesetz vom 23. Oktober 2000 (BGBl. I S. 1433) haben Außenprüfer ab Januar 2002 die Möglichkeit erhalten, direkt auf die Buchhaltung des zu prüfenden Betriebes zuzugreifen und die gespeicherten Unterlagen und Aufzeichnungen auf maschinell verwertbaren Datenträgern in die Behörde mitzunehmen. Die Datenträger werden im Finanzamt mit speziellen Bearbeitungsprogrammen ausgewertet und dabei auf Lücken und andere steuerrechtlich relevante Unregelmäßigkeiten geprüft. Die Mitnahme zur Dienststelle eröffnet die Möglichkeit, Parallelbuchhaltungen aufzubauen und in Abgleichläufen steuerlich zu überprüfen. Aufgrund meiner Intervention wurden die nachgeordneten Finanzbehörden in Hessen angewiesen, dass ein möglicher routinemäßiger Abgleich mit anderen Betrieben nicht erfolgt. Außerdem dürfen die Daten nur für die fallbezogene Auswertung verwendet und nicht länger aufbewahrt werden, als für das Veranlagungsverfahren notwendig ist (s. a. 29. Tätigkeitsbericht, Ziff. 8.2).

10.1.2
Umsatzsteuer-Nachschau

Mit § 27b Umsatzsteuergesetz (UStG), eingeführt durch das Steuerverkürzungsbekämpfungsgesetz vom 19. Dezember 2001 (BGBl. I S. 3922), erhielten die Finanzbehörden die Befugnis, außerhalb einer Außenprüfung und ohne vorherige Ankündigung während der Geschäfts- und Arbeitszeiten eines Betriebes diesen zu betreten und dort steuererhebliche Feststellungen zu treffen. Noch während einer derartigen Nachschau kann diese in eine formgebundene Außenprüfung überführt werden. Die Ausführungsanweisung an die nachgeordneten Behörden wird derzeit erstellt. Die Datenschutzbehörden sind bislang nicht involviert. Der Bundesbeauftragte für den Datenschutz und ich haben sich scharf dagegen ausgesprochen, dass eine allgemeine „Nachschau“ bei allen Steuern eingeführt wird; das war ursprünglich vorgesehen (s. a. 30. Tätigkeitsbericht, Ziff. 10.1).

10.1.3
Steuernummern auf Rechnungen

Mit § 14a Abs. 1a UStG, eingeführt durch das Steuerverkürzungsbekämpfungsgesetz vom 20. Dezember 2001 (BGBl. I S. 3922), ist ein leistender Unternehmer verpflichtet, auf seinen Rechnungen seine Steuernummer anzugeben. Datenschutzrechtlich besteht die Besorgnis, dass es zu Missbrauchsmöglichkeiten kommt. Da Umsatz- und Einkommensveranlagungen meist unter derselben Steuernummer stattfinden, sind alle steuerlichen Verhältnisse der Steuerpflichtigen gefährdet. Aufgrund der auch von mir erhobenen Bedenken haben die Finanzministerien ihre Finanzämter angewiesen, allein aufgrund der Angabe der Steuernummer keine telefonischen Auskünfte mehr zu erteilen (s. a. Ziff. 10.2).

Bislang nicht geklärt ist die Problematik bei zusammenveranlagten Eheleuten, wenn der Ehepartner des Unternehmers der Angabe der gemeinsamen Steuernummer widersprochen hat.

10.1.4
Freistellungsbescheinigungen im Internet

§§ 48 bis 48d Einkommensteuergesetz (EStG), eingeführt durch Gesetz vom 30. August 2001 (BGBl. I S. 2267), verpflichten Unternehmen, die Bauleistungen vergeben, bei der Bezahlung des Werkes einen Steuerabzug von 15 v. H. des Rechnungsbetrags vorzunehmen und diese an das für den Leistenden zuständige Finanzamt abzuführen. Diese Pflicht entfällt nur, wenn der Bauunternehmer dem Bauleistungsempfänger eine Freistellungsbescheinigung vorlegt. Deren Richtigkeit kann der Auftraggeber im Internet unter bestimmten Sicherheitskriterien überprüfen. Die Zustimmung zu der Einstellung seiner Daten in das Internet wird dem Unternehmer faktisch abgenötigt, denn ohne Zustimmung kann er den Steuerabzug von 15 v. H. nicht vermeiden (s. auch Ziff. 10.2.2).

Freistellungsbescheinigungen werden nicht erteilt, wenn eine Gefährdung des zu sichernden Steueranspruches vorliegt, der Leistende seine Steuererklärung wiederholt nicht oder nicht rechtzeitig abgibt, nachhaltige Steuerrückstände

bestehen oder der Leistende seiner Mitwirkungspflicht nach § 90 AO nicht nachkommt. Die Vorlage einer Bescheinigung in einer Rechnung lässt mithin Rückschlüsse auf den Leistenden zu. Dies hat in der Praxis dazu geführt, dass bei Auftragsvergabe Firmen ohne Freistellungsbescheinigung in einem Vergabeverfahren nicht berücksichtigt werden. Nachdem die Datenschutzbeauftragten des Bundes und der Länder rechtsstaatliche Bedenken gegen die Einstellung der Freistellungsbescheinigungen in das Internetangebot des Bundesamtes für Finanzen erhoben hatten, ist eine gesonderte gesetzliche Ermächtigung dafür geschaffen worden. Die Erforderlichkeit dieser Veröffentlichung im Abrufverfahren erschließt sich nicht, da Freistellungsbescheinigungen ohnehin nur an verlässliche Steuerpflichtige vergeben werden.

10.1.5
Kontenevidenz

Mit § 24c Gesetz über das Kreditwesen (KWG), eingeführt durch das Vierte Finanzmarktförderungsgesetz vom 21. Juni 2002 (BGBl. I S. 2010), ist ein Zugriff durch die Bundesanstalt für Finanzdienstleistungsaufsicht auf alle Konten und Depots, die von Kreditinstituten für deutsche Staatsbürger oder Ausländer geführt werden, eröffnet worden. Die Auskünfte werden zur Erfüllung aufsichtlicher Aufgaben, für die Verfolgung von Straftaten und zu Zwecken nach dem Außenwirtschaftsgesetz erteilt. Die Zugriffe sind auf die Grunddaten beschränkt, Kontenstände und -bewegungen dürfen – anders als durch Staatsanwaltschaften und Verfassungsschutzämter – nicht abgerufen werden.

Der Bundesbeauftragte für den Datenschutz und ich haben gegen die Verwendung der so erlangten Daten durch die Finanzbehörden Stellung genommen. Das Zugriffsrecht der Finanzbehörden ist vom Bundesgesetzgeber nicht zugelassen worden.

Mit dem im November 2002 vorgelegten Entwurf eines Steuervergünstigungsabbaugesetzes werden nicht nur zahlreiche bislang steuerfreie Erwerbsgeschäfte der Einkommenssteuer unterworfen. Zugleich wird das Bankgeheimnis gemäß § 30a Abgabenordnung beseitigt.

Den Kreditinstituten soll aufgegeben werden, jährlich die Daten ihrer Kunden mitzuteilen, soweit diese Einkünfte aus privaten Veräußerungen von Wertpapieren oder Erträge aus Termingeschäften erlangen (Entwurf zu § 23a EStG). Außerdem sollen Gesellschaften, die Gewinne ausschütten, verpflichtet werden, diese an das Bundesamt für Finanzen mitzuteilen. Die gleiche Pflicht soll die Schuldner von Zinsforderungen treffen (Entwurf zu § 45d Abs. 1 Satz 1 EStG). Schließlich soll die bisherige Steuernummer als festes Ordnungsmerkmal durch eine eindeutige, unveränderbare Identifikationskennzeichnung ersetzt werden. Mit Hilfe dieser Identifikationskennzeichnung sollen alle Informationen über einen Steuerpflichtigen elektronisch zusammengeführt, gespeichert und für Abrufe bereitgestellt werden.

10.1.6
Steuerdatenabrufverordnung

Mit dem neuesten Entwurf der Steuerdatenabrufverordnung (Stand 30. August 2002) und dem Verfahren zur Bekämpfung des Umsatzsteuerbetruges ZAUBER (**Z**entrale Datenbank zur Speicherung und **A**uswertung von **U**msatzsteuer-**B**etrugsfällen und **E**ntwicklung von **R**isikoprofilen) werden Datenbanken mit Steuerdaten und vermeintlichen Steuerdaten als bundesweite gemeinsame Online-Verfahren geschaffen, die untereinander verbunden sind und ausgewertet werden können. Zum Abruf können alle Steuerbeamten ermächtigt werden, die die Daten zur Veranlagung, Prüfung oder Fahndung benötigen. Wer die Verantwortung für die eingebrachten Daten trägt und wie die Nachvollziehbarkeit der Zugriffsberechtigungen gesichert werden kann, regelt der Entwurf nicht. Die Einrichtung bundesweiter Datenbanken entspricht dem Trend, durch Datensammlungen Checklisten und Kriterienkataloge zu erstellen, damit gezielt Risikogruppen für Steuerhinterziehungen ausfindig gemacht und dann besonders intensiv geprüft werden können. Die Verfahrensordnung enthält derzeit eine Vielzahl datenschutzrechtlicher Mängel, die der Bundesbeauftragte und ich gegenüber dem Bundesministerium der Finanzen gerügt haben. Die Zugriffsrechte sind viel zu weit gespannt; außerdem ist der Kreis derjenigen, die Daten verändern können, nicht sachgerecht eingegrenzt.

10.1.7
Finanzrechtsprechung und Kontrollmitteilungen

Die Finanzrechtsprechung hat in jüngerer Zeit die Befugnis zur Versendung von Kontrollmitteilungen stark ausgeweitet. Nicht nur in den Fällen des § 194 Abs. 3 AO, für die der Gesetzgeber ausdrücklich Kontrollmitteilungen vorgesehen hat, sondern in weiteren Steuerfällen sind Kontrollmitteilungen zugelassen worden. Dies ist insbesondere für Kontrollmitteilungen gegen Bankkunden entschieden worden (Beschluss des Bundesfinanzhofes vom 2. August 2001 zu § 30a AO). Danach können anlässlich der Außenprüfung bei Banken festgestellte Tatbestände zu Kontrollmitteilungen an Wohnsitzfinanzämter von Bankkunden verwendet werden. Mit den geplanten Änderungen (Steuervergünstigungsabbaugesetz, s. Ziff. 5) wird diese Rechtsprechung Gesetz. § 30a AO soll aufgehoben und § 194 Abs. 3 AO erweitert werden: Erkenntnisse, die bei Außenprüfungen gewonnen werden, können steuerlich uneingeschränkt ausgewertet werden.

Es fehlt an einer gesetzlichen Ermächtigung, die den Verdachtstatbestand konkret umschreibt. Das Bundesministerium der Finanzen ist vom Bundesbeauftragten für den Datenschutz und mir aufgefordert worden, eine normenklare Vorschrift zu schaffen, die die Zulässigkeit von Kontrollmitteilungen auf erforderliche Ermittlungen beschränkt und die Tatbestände genau umschreibt, die zu Kontrollmitteilungen führen können.

10.2
Steuernummern von Unternehmern – ein ungeschütztes Datum?

Die neuen gesetzlichen Verpflichtungen an Unternehmer, ihre Steuernummer auf Rechnungen anzugeben, dadurch nachzuweisen, dass der Steueranspruch nicht gefährdet ist, haben zu erheblichen Irritationen bei den betroffenen Steuerpflichtigen geführt. Dieselben Widerstände hatte die kurz zuvor eingeführte Steuerabzugspflicht bei Bauleistungen ausgelöst.

10.2.1
Steuernummer auf der Rechnung

Aufgrund des neuen § 14 Abs. 1a Umsatzsteuergesetz (UStG), eingefügt durch das Steuerverkürzungsbekämpfungsgesetz (StVBG) vom 19. Dezember 2001 (BGBl. I S. 3922), ist der leistende Unternehmer seit dem 1. Juli 2002 verpflichtet, in der Rechnung die ihm vom Finanzamt erteilte Steuernummer anzugeben.

§ 14 Abs. 1a UStG

Der leistende Unternehmer hat in der Rechnung die ihm vom Finanzamt erteilte Steuernummer anzugeben.

In den zahlreichen Beschwerden wurden insbesondere zwei Themen problematisiert:

– Die Steuernummer eines Unternehmers wird mit der Rechnung einem nicht mehr überschaubarem Personenkreis zugänglich.

  Es besteht zu Recht die Sorge, dass mit der Steuernummer rechtsmissbräuchlich verfahren werden kann, z. B. wenn aufgrund telefonischer Nachfragen eines Unberechtigten das zuständige Finanzamt Auskünfte zur Steuernummer erteilt. Diese Gefahr besteht nicht nur für umsatzsteuerliche Ausforschungen, denn Einkommen- und Umsatzsteuer können unter derselben Steuernummer geführt werden. Die Oberfinanzdirektion (OFD) Frankfurt am Main hat auf meine entsprechende Intervention reagiert und die hessischen Finanzämter angewiesen, telefonische Auskünfte in der Regel nicht nur aufgrund der Nennung des Namens beziehungsweise der Firma und der entsprechenden Steuernummer zu erteilen. Vielmehr hat der Anrufer durch weitere Auskünfte glaubhaft zu machen, dass er befugt ist, die telefonischen Auskünfte zu erhalten, wenn sich nicht bereits aus der Fragestellung des Anrufers ergibt, dass es sich bei ihm um den Steuerpflichtigen selbst oder seinen steuerlichen Vertreter handelt. Ggf. muss durch Rückruf die Auskunftsberechtigung geklärt werden oder der Anrufer auf den Schriftweg verwiesen werden.

  Gleichwohl kann die OFD-Verfügung die datenschutzrechtlichen Bedenken nicht restlos beseitigen. Ich halte es für sinnvoll, auf die vollständige Angabe der Steuernummer zu verzichten: Zur beabsichtigten Vereinfachung der finanzamtsinternen Bearbeitung reicht der Nummernteil für das zuständige Finanzamt und der Name des Unternehmers. Des Weiteren könnte die Auskunft z. B. an eine PIN geknüpft werden, die nur dem Berechtigten (Steuerpflichtiger/Steuerberater) bekannt ist.

– Weiterhin wurde bemängelt, dass bei gemeinsam veranlagten Ehepartnern der verpflichtete Unternehmer auch zwangsläufig die Steuernummer des nicht verpflichteten Ehepartners offenbaren muss. In den mir vorliegenden Fällen hatten die Ehepartner der Offenbarung auch widersprochen. Ich halte die Offenbarung der Steuernummer aus diesem Grund für bedenklich und habe das hessische Finanzministerium um Stellungnahme gebeten. Eine Reaktion steht noch aus.

10.2.2
Steuerabzug bei Bauleistungen

Mit dem Gesetz zur Eindämmung der illegalen Betätigung im Baugewerbe vom 30. August 2001 (BGBl. I S. 2267) wurde zur Sicherung von Steueransprüchen bei Bauleistungen ein Steuerabzug eingeführt [§§ 48 bis 48d Einkommenssteuergesetz (EStG)]. Danach haben unternehmerisch tätige Auftraggeber von Bauleistungen einen Steuerabzug von 15 v. H. der Gegenleistung für Rechnung des leistenden Unternehmers vorzunehmen. Der Steuerabzug kann unterbleiben, wenn der Leistende eine gültige Freistellungserklärung vorlegt (§ 48 EStG).

§ 48 Abs. 1 und 2 EStG

(1) Erbringt jemand im Inland eine Bauleistung (Leistender) an einen Unternehmer im Sinne des § 2 des Umsatzsteuergesetzes oder an eine juristische Person des öffentlichen Rechts (Leistungsempfänger), ist der Leistungsempfänger verpflichtet, von der Gegenleistung einen Steuerabzug in Höhe von 15 vom Hundert für Rechnung des Leistenden

vorzunehmen. Ver-mietet der Leistungsempfänger Wohnungen, so ist Satz 1 nicht auf Bauleistungen für diese Wohnungen anzuwenden, wenn er nicht mehr als zwei Wohnungen vermietet. Bauleistungen sind alle Leistungen, die der Herstellung, Instandsetzung, Instandhaltung, Änderung oder Beseitigung von Bauwerken dienen. Als Leistender gilt auch derjenige, der über eine Leistung abrechnet, ohne sie erbracht zu haben.

(2) Der Steuerabzug muss nicht vorgenommen werden, wenn der Leistende dem Leistungsempfänger eine im Zeitpunkt der Gegenleistung gültige Freistellungsbescheinigung nach § 48b Abs. 1 Satz 1 vorlegt oder die Gegenleistung im laufenden Kalenderjahr den folgenden Betrag voraussichtlich nicht übersteigen wird:

1. 15.000 Euro, wenn der Leistungsempfänger ausschließlich steuerfreie Umsätze nach § 4 Nr. 12 Satz 1 des Umsatzsteuergesetzes ausführt,

2. 5.000 Euro in den übrigen Fällen.

...

Um Haftungsrisiken zu vermeiden, kann der Auftraggeber seit März 2002 durch eine elektronische Abfrage beim Bundesamt für Finanzen die Gültigkeit der Bescheinigung überprüfen (§ 48b Abs. 6 EStG). Die für diese Kontrolle notwendigen Daten hat der Leistende dem Auftraggeber mitzuteilen: u. a. Name, Anschrift, Steuernummer und ausstellendes Finanzamt (§ 48b Abs. 3 EStG). Auf die Angabe des ursprünglich auch vorgesehenen Geburtsdatums hat das hessische Finanzministerium nach meinen datenschutzrechtlichen Einwänden verzichtet. Dennoch kommt es auch hier zu einer Offenbarung der Steuernummer an einen unüberschaubaren Personenkreis mit den bereits oben dargestellten Gefahren. Jeder, der im Besitz einer Freistellungserklärung ist, kann die elektronische Abfrage beim Bundesamt der Finanzen durchführen. Der Anfragende muss dabei (s)eine Steuernummer, die Steuernummer des Leistenden und die auf dem Freistellungsbescheid vermerkte Sicherheitsnummer angeben. Als Auskunft enthält er Name und Anschrift des Leistenden sowie die Zeitspanne der Gültigkeit der Freistellungsbescheinigung.

§ 48b Abs. 3 und 6 EStG

(3) In der Bescheinigung sind anzugeben:

1. Name, Anschrift und Steuernummer des Leistenden,

2. Geltungsdauer der Bescheinigung,

3. Umfang der Freistellung sowie der Leistungsempfänger, wenn sie nur für bestimmte Bauleistungen gilt,

4. das ausstellende Finanzamt.

(6) Das Bundesamt für Finanzen erteilt dem Leistungsempfänger im Sinne des § 48 Abs. 1 Satz 1 im Wege einer elektronischen Abfrage Auskunft über die beim Bundesamt für Finanzen gespeicherten Freistellungsbescheinigungen. Mit dem Antrag auf die Erteilung einer Freistellungsbescheinigung stimmt der Antragsteller zu, dass seine Daten nach § 48b Abs. 3 beim Bundesamt für Finanzen gespeichert werden und dass über die gespeicherten Daten an die Leistungsempfänger Auskunft gegeben wird.

Die betroffenen Bauleistenden stimmen automatisch mit dem Antrag auf Erteilung einer Freistellungsbescheinigung auch der Speicherung beim Bundesamt für Finanzen und der Auskunftserteilung an den Leistungsempfänger zu. Auf einen entsprechenden Antrag oder auf die Beifügung der Bescheinigung zur Rechnung können die Bauleistenden aber nicht verzichten, da – wie Beschwerdeführer berichten – bereits in Ausschreibungsverfahren Angebote ohne Freistellungsbescheinigung nicht mehr berücksichtigt werden und daher Wettbewerbsnachteile entstehen.

Auch hiergegen bestehen Bedenken, da hier ein Rechtsvorteil (Gewährung der Freistellungsbescheinigung) unmittelbar mit einem datenschutzrechtlichen Nachteil (Bekanntgabe von persönlichen Daten und der Steuernummer, Zustimmung zur Datenspeicherung und Auskunftserteilung) verknüpft ist.

10.3
Keine zusätzlichen Kontrollmitteilungen zur geplanten Abgeltungssteuer

Die von der Bundesregierung geplanten umfangreichen Kontrollmitteilungen der Banken über Erträgnisse und Veräußerungsgewinne werden bei der Einführung einer pauschalen Abgeltungssteuer obsolet. Sie widersprechen der Idee der Abgeltungssteuer, sind unverhältnismäßig und nicht erforderlich.

Im Rahmen des Entwurfes eines Steuervergünstigungsabbaugesetzes (Stand 20. November 2002) sollen zu einer vollständigeren steuerlichen Erfassung von Erträgen und Veräußerungsgewinnen umfangreiche Kontrollmitteilungen von Banken an das Bundesamt für Finanzen eingeführt werden. Mitgeteilt werden sollen alle Kapitalerträge, Veräußerungsgewinne und sonstigen Einkünfte aus Wertpapier- und Geldgeschäften. Das Bundesamt für Finanzen soll alle Kontrollmitteilungen unter einem einheitlichen Personenkennzeichen zusammenführen und den Wohnsitz-Finanzämtern übermitteln.

Eine zeitlich nachfolgende gesetzgeberische Absicht plant die Einführung einer Abgeltungssteuer, mit der eine pauschale Besteuerung aller Kapitalerträge vorgenommen werden soll. Gleichwohl sollen die ausgeweiteten Kontrollmitteilungen nicht entfallen. Vielmehr hat das Bundesministerium der Finanzen (BMF) in einer ausführlichen Begründung an den Finanzausschuss des Deutschen Bundestages dargelegt, dass es die Kontrollmitteilungen zusätzlich zu einer Abgeltungssteuer für erforderlich erachtet. Mit einem Schreiben an den Hessischen Staatsminister für Bundes- und Europaangelegenheiten und an den Hessischen Minister der Finanzen habe ich dieser Darstellung mit folgender Argumentation widersprochen:

- Die vom BMF genannte Begründung, dass die Erträge aus Kapitalvermögen für den Fiskus sichtbar sein sollten, widerspricht der Idee der Abgeltungssteuer. Sie ist von den Ländern, die sie schon bisher erheben, gerade erfunden worden, um eine steuerliche Veranlagung ad personam nicht vornehmen zu müssen. Die anonyme Abführung ist daher ein wesentliches Kennzeichen jeder Konstruktion, die als Abgeltungssteuer bezeichnet werden kann.
- Die weitere Begründung, dass geprüft werden müsse, ob ein Kreditinstitut sich rechtmäßig bei der Abführung der Abgeltungssteuer verhalte, ist fadenscheinig. Eine derartige Kontrolle kann nur im Wege der Außenprüfung durch ungezielte Stichproben erfolgen. Sollte ein Kreditinstitut bewusst rechtswidrig nicht abführen, wird es auch keine Kontrollmitteilungen gegenteiliger Art verschicken. Es liegt schlichtweg ein Denkfehler in der Annahme, Kontrollmitteilungen könnten die vollständige Abführung der Abgeltungssteuer sicherstellen.
- Die Annahme, dass die Kenntnis der genauen Kapitalerträge auch für andere Besteuerungsgrundlagen erforderlich sei, weil sie erlaube „z. B. verschleierte Einkünfte aus dem Gewerbebetrieb oder aus selbständiger Tätigkeit“ aufzudecken, ist fernliegend. Wer Einkünfte aus Gewerbetrieb oder aus selbständiger Tätigkeit verschleiert, dürfte diese entweder sogleich verausgaben oder um der Verschleierung willen exportieren. Es ist daher nicht damit zu rechnen, dass Geschäfte ohne Rechnung und Schwarzarbeit zu legaler Kontenführung veranlassen, die sich im Wege der Kontrollmitteilung erschließen lässt.
- Als Argument des BMF verbleibt sonach lediglich die Prüfung der Kindergeldberechtigung von Eltern, deren Kinder Einkünfte aus Kapitalvermögen haben. Insofern sind heute bereits in der Steuererklärung Angaben über die Einkünfte der Kinder notwendig. Eine Überprüfung, ob diese Angaben richtig sind, muss im Zuge herkömmlicher Ermittlungen vorgenommen werden. Eine umfassende Vorratsspeicherung, die die Kapitalerträge aller deutschen Bürger erfasst, lässt sich durch die wenigen Fälle der Kindergeldberechtigung nicht legitimieren.
- Dasselbe gilt für Einkommensgrenzen, die auf die Summe der positiven Einkünfte oder den gesamten Betrag der Einkünfte bezogen sind. Auch hier werden in Einzelfällen Ermittlungen notwendig werden. Für derartige Ermittlungen mögen die entsprechenden Angaben mit den traditionellen Methoden der Abgabenordnung beschafft werden. Auch insofern ist nicht legitimierbar, dass die gesamte Bevölkerung einem Kontrollmitteilungsverfahren unterworfen wird.

Zusammenfassend erachte ich die für die Kontrollmitteilungen gegebenen Gründe für insgesamt nicht überzeugend. Sie widersprechen der Idee einer Abgeltungssteuer und sollten deswegen im weiteren Gesetzgebungsverfahren nicht verfolgt werden.

11. Recht der Presse, Medien- und Teledienste

11.1
Datenschutzvorschriften für die hessische Presse

Die im Sechsten Gesetz zur Änderung des Hessischen Pressegesetzes vom 26. November 2002 enthaltenen Vorschriften zum Datenschutz in Presseunternehmen sind nicht ausreichend.

11.1.1
Ausgangslage

Bis zum Frühjahr 2001 regelte das Bundesdatenschutzgesetz (BDSG) den Datenschutz in Presseunternehmen abschließend – oder besser gesagt – es regelte ihn nicht, denn die Verarbeitung personenbezogener Daten zu journalistisch-redaktionellen Zwecken blieb weitgehend von der Anwendung des Gesetzes ausgenommen. Das im Mai 2001 novellierte BDSG hat die Regelungskompetenz für den Datenschutz in Presseunternehmen vom Bund auf die Länder verlagert. Statt einer eigenständigen Vollregelung enthält § 41 Abs. 1 BDSG nunmehr eine von den Ländern in eigene Gesetzgebung umzusetzende Rahmenvorschrift.

§ 41 Abs. 1 BDSG

Die Länder haben in ihrer Gesetzgebung vorzusehen, dass für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Unternehmen und Hilfsunternehmen der Presse ausschließlich zu eigenen journalistisch-redaktio-

nellen oder literarischen Zwecken den Vorschriften der §§ 5, 9 und 38a entsprechende Regelungen einschließlich einer hierauf bezogenen Haftungsregelung entsprechend § 7 zur Anwendung kommen.

§ 5 BDSG regelt das Datengeheimnis, § 9 die Datensicherheit, § 38a enthält eine Bestimmung zur verbandsrechtlichen Selbstregulierung.

Zur Umsetzung hat der Hessische Landtag das Sechste Gesetz zur Änderung des Hessischen Pressegesetzes vom 26. November 2002 (GVBl. I S. 701) beschlossen. Das Gesetz (Art. 1) verweist lediglich auf die in § 41 Abs. 1 BDSG genannten Vorschriften in der jeweils geltenden Fassung. Der in das Hessische Pressegesetz neu eingefügte § 10a nutzt weder den Regelungsspielraum, den der Bundesgesetzgeber den Landesgesetzgebern eingeräumt hat, noch erfüllt er die Anforderungen der EG-Datenschutzrichtlinie.

§ 10a HPresseG

Soweit Unternehmen oder Hilfsunternehmen der Presse personenbezogene Daten ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken erheben, verarbeiten oder nutzen, gelten von den Vorschriften des Bundesdatenschutzgesetzes in der jeweils geltenden Fassung nur die §§ 5, 9 und 38a sowie § 7 mit der Maßgabe, dass nur für Schäden gehaftet wird, die durch eine Verletzung des Datengeheimnisses nach § 5 des Bundesdatenschutzgesetzes oder durch unzureichende technische oder organisatorische Maßnahmen im Sinne des § 9 des Bundesdatenschutzgesetzes eingetreten sind.

Meine Regelungsvorschläge, die ich zunächst der Landesregierung und später im Gesetzgebungsverfahren dem Landtag unterbreitet habe, sind leider unberücksichtigt geblieben. Zu den wichtigsten zählen:

- eine Auffangregelung für Unternehmen, die sich nicht dem Pressekodex des Deutschen Presserats unterwerfen,
- die Verpflichtung zur Bestellung eines redaktionsinternen Datenschutzbeauftragten,
- die datenschutzrechtliche Gleichstellung der Presse mit Rundfunk und Mediendiensten.

11.1.2
Auffangregelung

Der Deutsche Presserat hat am 28. November 2001 dem Bundespräsidenten den durch besondere Regelungen zum Redaktionsdatenschutz erweiterten „Pressekodex“ und die Beschwerdeordnung überreicht. Diese Verhaltensgrundsätze enthalten zwar materielle Selbstbeschränkungen, die typische Verstöße der Presse gegen ethische und datenschutzrechtliche Grundnormen benennen. Dennoch genügen sie den europarechtlichen Anforderungen nicht. Die Beschwerdeordnung sieht bei Verstößen weder zwingende verbandsinterne Sanktionen vor, noch schafft sie ein Instrumentarium, das den Betroffenen materiellen Ausgleich sichert.

Selbst wenn man der Ansicht ist, dass der Pressekodex und die Beschwerdeordnung des Deutschen Presserats eine angemessene Selbstregulierung bieten, bleibt das Problem, dass nur für jene Unternehmen ausreichende datenschutzrechtliche Regelungen existieren, die sich gegenüber dem Presserat zur Einhaltung des Kodex verpflichtet haben. Das werden sicherlich niemals alle Unternehmen sein. Um ein gleiches Datenschutzniveau für die gesamte Presse sicherzustellen, müsste die Datenverarbeitung dieser Unternehmen uneingeschränkt den allgemeinen Datenschutzbestimmungen unterworfen werden.

11.1.3
Redaktionsinterner Datenschutzbeauftragter

Sowohl öffentlich-rechtliche Rundfunkanstalten als auch private Rundfunkunternehmen und elektronische Mediendienste sind schon seit Jahren verpflichtet, einen internen Datenschutzbeauftragten zu bestellen, der die Einhaltung von Vorschriften über den Datenschutz im journalistisch-redaktionellen Bereich frei von Weisungen überwacht. Auch der zwischen Bund und Ländern abgestimmte Entwurf zur Novellierung des BDSG sah die Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten für den journalistisch-redaktionellen Bereich vor. Auf Druck der Presseverbände wurde die Vorschrift jedoch nicht in das novellierte Gesetz aufgenommen. Das ist umso unverständlicher, als es beim Rundfunk und den Mediendiensten zu keiner Zeit irgendwelche Anzeichen gab, dass durch die internen Datenschutzbeauftragten die journalistisch-redaktionelle Tätigkeit beeinträchtigt worden wäre.

Am Beispiel der elektronischen Mediendienste zeigt sich besonders deutlich die Widersprüchlichkeit einer Ausnahmeregelung für die Presse: Viele Presseunternehmen bieten im Internet eine Version ihrer Zeitschrift oder Tageszeitung an (elektronische Presse). Der Verlag muss für die journalistisch-redaktionelle Datenverarbeitung für die Online-Ausgabe einen internen Datenschutzbeauftragten bestellen, nicht dagegen für die journalistisch-redaktionelle Datenverarbeitung für die gedruckte Ausgabe, obwohl nicht selten dieselben Informationen in beiden Bereichen verwendet werden.

11.1.4
Zusätzliche Privilegierung

Die Presse ist nicht nur von der Verpflichtung zur Bestellung eines internen Datenschutzbeauftragten befreit, sondern genießt im Unterschied zum Rundfunk und den Mediendiensten eine ganze Reihe von datenschutzrechtlichen Privilegien: Anders als für den Rundfunk und die Mediendienste gilt für sie nicht subsidiär das allgemeine Datenschutzrecht. Sie muss Gegendarstellungen der Betroffenen nicht zusammen mit den eigenen Daten speichern. Von Rundfunk und Mediendiensten können die Betroffenen – wenn auch eingeschränkt – Auskunft über Daten verlangen, die zu ihrer Person gespeichert sind und der Berichterstattung zugrunde liegen; gegenüber der Presse existiert ein solcher Auskunftsanspruch nicht.

11.2
Novelliertes Datenschutzrecht für Tele- und Mediendienste

Unter Mitwirkung der Datenschutzbeauftragten des Bundes und der Länder sind das Teledienstegesetz, das Teledienstedatenschutzgesetz und der Mediendienste-Staatsvertrag überarbeitet worden.

11.2.1
Änderungen

Der Bundesgesetzgeber und die Landesgesetzgeber haben einen neuen rechtlichen Rahmen für den Datenschutz im Internet geschaffen. Mit Art. 1 und 3 des Gesetzes über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr vom 14. Dezember 2001 (BGBl. I S. 3721) wurden das Teledienstegesetz (TDG) und Teledienstedatenschutzgesetz (TDDSG) novelliert. Art. 3 des Sechsten Staatsvertrages zur Änderung des Rundfunkstaatsvertrages und des Mediendienste-Staatsvertrages vom 20. bis 21. Dezember 2001 (GVBl. 2002 I S. 38), der am 1. Juli 2002 in Kraft getreten ist, wurde ebenfalls angepasst.

Bund und Länder haben sich, wie schon 1997 bei der erstmaligen Regelung des Datenschutzes für Tele- und Mediendienste, auf weitgehend gleichlautende Vorschriften verständigt. Neben einer Konkretisierung des Geltungsbereichs von Teledienstegesetz, Teledienstedatenschutzgesetz und Mediendienste-Staatsvertrag sehen die Neuregelungen eine Ausweitung der Unterrichtungspflichten der Diensteanbieter vor, erleichtern die elektronische Einwilligung und präzisieren die Bedingungen für die Erstellung von Nutzungsprofilen. In das Teledienstedatenschutzgesetz sind Bußgeldvorschriften aufgenommen und im Mediendienste-Staatsvertrag ist der Bußgeldrahmen erhöht worden.

11.2.2
Geltungsbereich

Im Teledienstedatenschutzgesetz (TDDSG) und Mediendienste-Staatsvertrag (MDStV) 1997 war der Geltungsbereich nicht eindeutig definiert. Sowohl im TDDSG (§ 1 Abs. 1) als auch im MDStV (§ 16 Abs. 1) wird nunmehr ausdrücklich klar gestellt, dass das Gesetz nicht gilt, soweit die Internetnutzung im Dienst- oder Arbeitsverhältnis zu ausschließlich beruflichen oder dienstlichen Zwecken erfolgt, oder die Informations- und Kommunikationssysteme ausschließlich zur Steuerung von Arbeits- oder Geschäftsprozessen in oder zwischen Unternehmen oder öffentlichen Stellen zur Verfügung gestellt werden. In diesen Fällen bestehen zwischen den Beteiligten besondere Interessen. Die Anwendung der über die Regelungen der allgemeinen Datenschutzgesetze hinaus gehenden speziellen Verarbeitungsgrundsätze des TDDSG und des MDStV wären hier nicht sachgerecht. Das betrifft z. B. Informations- und Kommunikationssysteme, die als Arbeitsmittel dienen, Vertriebs- und Führungsinformationssysteme und Kommunikationssysteme, die der unternehmens- oder behördeninternen und übergreifenden Verknüpfung von Produktions- beziehungsweise Verwaltungsprozessen dienen.

11.2.3
Informationspflichten

Damit die Nutzer der Tele- und Mediendienste ihre Rechte einfacher geltend machen können, aber auch zur Erleichterung der staatlichen Kontrolltätigkeit erweitern das neue Teledienstegesetz (§§ 6 und 7) und der neue MDStV (§ 10) die Informationspflichten der Diensteanbieter: Werden die Dienste geschäftsmäßig angeboten, sind die Anbieter verpflichtet, u. a. Name und Anschrift, unter der sie niedergelassen sind, E-Mail-Adresse, bei zulassungspflichtiger Tätigkeit die zuständige Aufsichtsbehörde, Registereintragungen und die Umsatzsteueridentifikationsnummer anzugeben. Die Informationen müssen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sein. Sie müssen daher online an gut wahrnehmbarer Stelle stehen und ohne langes Suchen und jederzeit auffindbar sein. Eine besondere Informationspflicht hat der Diensteanbieter, wenn die Verarbeitung der Nutzerdaten in Staaten außerhalb des Anwendungsbereichs der EG-Datenschutzrichtlinie erfolgen soll (§ 4 Abs. 1 Satz 1 TDDSG, § 18 Abs. 1 Satz 1 MDStV). Da bei diesen Staaten nicht ohne weiteres von einem vergleichbaren Datenschutzniveau ausgegangen werden kann, haben die Nutzer in diesen Fällen ein besonderes Transparenzbedürfnis.

11.2.4
Elektronische Einwilligung

Durch das TDDSG und den MDStV wurde 1997 die elektronische Einwilligung in das Datenschutzrecht eingeführt. Mit den Novellierungen werden die bisherigen Anforderungen an eine wirksame elektronische Einwilligung (§ 4 Abs. 2 TDDSG, § 18 Abs. 2 MDStV) reduziert. Der Diensteanbieter muss nicht mehr sicherstellen, dass die Einwilligung nicht unerkennbar verändert werden kann. Diese Anforderung war faktisch nur bei Verwendung einer qualifizierten elektronischen Signatur zu erfüllen und deshalb auf Kritik gestoßen, da sie einer breiten Verwendung der elektronischen Einwilligung entgegenstand.

11.2.5
Nutzungsprofile

Das neue TDDSG (§ 6 Abs. 3) und der novellierte MDStV (§ 19 Abs. 4) präzisieren die Bedingungen für die Erstellung von Nutzungsprofilen. Beide Gesetze erkennen das legitime Interesse der Diensteanbieter an, sich ein Bild vom Nutzungsverhalten ihrer Kunden zu verschaffen, nicht zuletzt um das Angebot besser auf das Kundeninteresse abstimmen zu können. Nutzungsprofile können außerdem durchaus im Interesse des Nutzers liegen. Solche Profile durften und dürfen jedoch nur unter Verwendung von Pseudonymen erstellt werden. Die Neuregelungen sehen eine strikte Verarbeitungsbeschränkung auf Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Dienste vor. Die Betroffenen haben das Recht, der Erstellung von Nutzungsprofilen zu widersprechen; darauf muss der Diensteanbieter sie hinweisen.

11.2.6
Bußgeldvorschriften

Um dem Schutzanspruch des TDDSG in der Praxis stärkere Geltung zu verschaffen, hat der Gesetzgeber Bußgeldvorschriften in das Gesetz aufgenommen (§ 9). Beim Bußgeldrahmen hat er sich am Bundesdatenschutzgesetz orientiert, ihn für den Bereich der Teledienste allerdings verdoppelt. Damit soll der erhöhten Gefährdung, die für personenbezogene Daten der Nutzer in offenen Netzen besteht, Rechnung getragen werden, und es soll die teilweise sehr hohe Wirtschaftskraft der Teleddiensteanbieter berücksichtigt werden. Der MDStV enthielt von Anfang an Bußgeldvorschriften (§ 24), deshalb ist hier nur der Bußgeldrahmen verdoppelt worden.

12. Entwicklung und Empfehlungen im Bereich der Technik

12.1
Mobile Computing

Ein aktueller Überblick über Mobile Computing zeigt sowohl die Chancen als auch die Risiken.

Mobilität gehört wie Flexibilität zu den Grundbedürfnissen der modernen Gesellschaft. Heute ist der Zugang zu Sachthemen, Literatur, zeitkritischen Daten, gewerblichen und staatlichen Angeboten und Informationen jederzeit über Mobilfunknetze, drahtlose Netze oder Internettechnologien möglich. An öffentlichen Plätzen, wie Flughäfen, Bahnhöfen oder Messen, ist ein Internetzugang oder das Abrufen von E-Mail über die entsprechende Technik mittlerweile zum Standard geworden.

12.1.1
Überblick über die Technologien

	GSM	GPRS	UMTS	Bluetooth	WirelessLAN
Kosten für Endgeräte: PCMCIA, PDA, Handy	200 € bis 300 €	400 € bis 1.500 €	500 € bis 1.500 €	100 € bis 250 €	200 € bis 300 €
Technologie-Chips	50 € bis 100 €	70 € bis 150 €	> 200 €	5 € bis 40 €	30 € bis 60 €
Kosten für Infrastruktur: Basisstation	15.000 € bis 3 Mio. €	100.000 € bis 5 Mio. €	300.000 € bis 7 Mio. €	400 € bis 3.000 €	400 € bis 2.000 €
Theoretische Übertragungsrate	9,6 kbit/s	14,4 kbit/s bis 115 kbit/s	14,4 kbit/s bis 2 Mbit/s	1 Mbit/s	1 Mbit/s bis 11 Mbit/s
Sendeleistung	1 bis 2 W 8 bis 24 W	1 bis 2 W 8 bis 24 W	1 bis 2 W 8 bis 50 W	1 bis 2,5 - 100 mW	100 mW
Reichweite	bis 2 km	bis 1,5 km	bis 1 km	bis 100 m	bis 100 m
Verfügbarkeit	1983	2001	2004	2001	1987

Abbildung 1 zeigt eine Übersicht über die wichtigsten drahtlosen Technologien. Hier unterscheidet man zwischen

– öffentlichen europäischen Mobilfunk-Netzen: GSM, GPRS, UMTS

und

– den Nahbereichsnetzen: Bluetooth, WirelessLAN.

Von besonderem Interesse sind zur Zeit die WirelessLANs, die allerdings aufgrund von

Sicherheitslücken stark ins Gerede gekommen sind. Auch der Newcomer Bluetooth gewinnt immer mehr an Bedeutung. Die Attraktivität liegt sowohl in den geringen Investitionskosten als auch in den guten Übertragungsraten.

Die Kapitel 12.1.1.2.1 und 12.1.1.2.2 beschäftigen sich mit den beiden Themen, und zeigen neben den Chancen auch die Risiken auf.

GSM

Abkürzung für **G**lobal **S**ystem for **M**obile Communications.

Eine digitale Mobilfunktechnologie, die von Bedeutung ist in Europa, Australien, Indien, Afrika, Asien und dem Mittleren Osten.

GPRS

Abkürzung für **G**eneral **P**acket **R**adio **S**ervices. GPRS ist ein digitaler Datenpaketstandard für drahtlose Kommunikation oder Mobilfunk, der Datentransferraten von bis zu 150 Kbit/s ermöglicht. Im Vergleich dazu erlaubt der gängige GSM-Standard nur Datentransferraten von 9,6 Kbit/s. GPRS unterstützt einen großen Bereich an Bandbreiten und erlaubt die effiziente Nutzung eingeschränkter Bandbreiten. Insbesondere ist er auf das Senden und Empfangen von Datenpaketen unterschiedlicher Größe, beispielsweise E-Mail-Nachrichten oder Web-Browsing bis hin zu großen Datenvolumen, ausgerichtet.

UMTS

Abkürzung für **U**niversal **M**obile **T**elecommunications **S**ystem. Bezeichnet den Standard der dritten Mobilfunkgeneration. Die Übertragungsgeschwindigkeit ist bis zu 2 Mbit/s definiert. Diese hohen Datenraten ermöglichen neue Anwendungen, wie E-Commerce, E-Government und mobile Multimedia bis hin zu mobilen Videoübertragungen und Internetzugang.

Bluetooth

Eine Spezifikation für Hochgeschwindigkeitsdatenübertragung über kurze Distanzen mittels Funk zwischen Mobiltelefonen, Notebookcomputern und anderen tragbaren Geräten.

WirelessLAN (WLAN)

WLAN ist ein lokales Netzwerk, das Daten über Radiowellen, infrarotes Licht oder eine andere, nicht drahtgebundene Technik überträgt.

PCMCIA

PC Card, ein Warenzeichen der **P**ersonal **C**omputer **M**emory **I**nternational **A**ssociation, mit dem man Zusatzkarten bezeichnet, die der PCMCIA-Spezifikation entsprechen. Es gibt drei Versionen, die vom Einsatz externer Speicher über Geräte wie Modem, Fax und Netzkarten hin bis zu Geräten für drahtlose Kommunikationseinrichtungen reichen.

PDA

Abkürzung für **P**ersonal **D**igital **A**ssistant. Ein leichter Handheld-Computer mit speziellem Funktionsumfang, der sowohl der persönlichen Organisation als auch der Kommunikation dient. Fortgeschrittene Modelle bieten Multimediamerkmale und volle Online-Kompatibilität. Viele PDA-Geräte verwenden für die Eingabe einen Stift oder ein anderes Zeigegerät anstelle einer Tastatur oder Maus. Zur Datenspeicherung setzt man auf Flashspeicher und verzichtet auf verbrauchintensive Diskettenlaufwerke. Die wichtigsten Betriebssysteme sind Windows CE, PalmOS und Epoc.

12.1.1.1
Öffentliche Mobilfunknetze

Zu den modernen mobilen Datennetzen gehören die aus dem GSM-Mobilfunk entstandene GPRS-Technik sowie deren Nachfolger UMTS. Beide Techniken fußen auf dem Sicherheitssystem der GSM-Mobilfunk-Technik. Jeder Teilnehmer ist durch eine weltweit eindeutige Identifizierungsnummer, die IMSI (**I**nternational **M**obile **S**ubscriber **I**dentity) gekennzeichnet. Im Rahmen einer festgelegten Netzzugangsprozedur werden neben der IMSI auch so genannte Authentifikationsparameter zwischen den mobilen Endgeräten und dem Kommunikationsnetz ausgetauscht, um die Rechtmäßigkeit des Zugangs und die Sicherheit der Datenübertragung zu gewährleisten. Wichtig ist darüber hinaus die durch detaillierte internationale Protokolle festgelegte Verwaltung der verwendeten Verschlüsselung zwi-

schen dem Netzbetreiber und den mobilen Endgeräten. Man kann davon ausgehen, dass ein Internetzugang über ein öffentliches GPRS- oder UMTS-Datennetz den Sicherheitsanforderungen der Festnetztechnik gleichkommt.

12.1.1.2
Nahbereichsnetze

Die Nahbereichsnetze gewinnen neben den öffentlichen Mobilfunknetzen beim Transport von unterschiedlichen Telekommunikationsdiensten über die „Luftschnittstelle“ zunehmend an Bedeutung. Bluetooth und WirelessLAN rücken die Sicherheit in den Vordergrund. Im Bereich der Zugangskontrolle und der Datensicherheit bieten die unterschiedlichen Techniken verschiedene Methoden an.

12.1.1.2.1
WirelessLAN

12.1.1.2.1.1
Technik

FunkLANs beziehungsweise WirelessLANs basieren auf dem Standard IEEE 802.11.

IEEE 802.11

Allgemeiner Standard des Institute of Electrical and Electronic Engineers, der den Aufbau und die Mechanismen drahtloser Netze beschreibt.

IEEE 802.11 ist eine übergreifende Bezeichnung für eine Gruppe von IEEE-Standards, die sich mit der drahtlosen Vernetzung von kleinen LANs beschäftigen. 802.11 postuliert Schnittstellen zwischen einem drahtlosen Client und einer Basisstation oder zwei drahtlosen Clients. Die 802.11-Familie spezifiziert Übertragungsgeschwindigkeiten zwischen 1 Mbit/s und 54 Mbit/s.

Mit geringem technischen und materiellen Aufwand kann man drahtlose lokale Netze aufbauen beziehungsweise drahtgebundene Netze erweitern. Die Kommunikation erfolgt über einen sog. Access-Point.

Access Point

Zentraler Funkknoten, der für ein bestimmtes Gebiet die Versorgung der Nutzer (Clients) mit der drahtlosen Netzanbindung übernimmt.

Die meisten Staaten Europas nutzen für ihre Systeme das ISM-Frequenzband zwischen 2,4 und 2,48 GHz., das gebührenfrei und ohne zusätzliche Genehmigung betrieben werden kann. Die Sendeleistung ist auf 100 mW begrenzt. Die Systeme des Standards 802.11 übertragen Daten mit einer Rate von 1 beziehungsweise 2 Mbit/s mittels Bandspreizung, entweder mittels FHSS oder DSSS-Verfahren. Die aktuellen Systeme nach IEEE 802.11b verwenden nur das DSSS-Verfahren. Die Übertragungsrate beträgt hierbei maximal 11 Mbit/s.

FHSS

Die Abkürzung für **F**requency **H**opping **S**pread **S**pectrum. Beschreibt eine von zwei Möglichkeiten der Datenübertragung im FunkLAN. Dabei wird die Sendefrequenz innerhalb des verfügbaren Frequenzbandes permanent gewechselt. Die damit erhöhte Sicherheit wirkt sich allerdings negativ auf die Datenübertragungsrate aus.

DSSS

Direct **S**equence **S**pread **S**pectrum bezeichnet eine von zwei Möglichkeiten der Datenübertragung in FunkLANs. Dabei wird die zur Verfügung stehende Sendeenergie auf ein breites Frequenzband aufgeteilt, um die Störanfälligkeit der übertragenden Daten gegenüber Interferenzen zu verringern.

12.1.1.2.1.2
Sicherheitsmechanismen

Im Standard sind folgende Sicherheitsmechanismen definiert:

Netzwerkname
Im Standard ist verankert, dass jedem FunkLAN ein eigener Netzwerkname (ESSID, SSID) zu gewiesen werden kann.

Ist dies der Fall, dann können sich nur Teilnehmer mit der gleichen ESSID am Netzwerk anmelden. Leider wird in den meisten Fällen die ESSID in Klartext übertragen. Daten können so von Angreifern leicht in Erfahrung gebracht werden.

ESSID, SSID

Extended **S**ervice **S**et **I**dentity

MAC-Adresse
Jeder Funk-Client besitzt eine Netzwerkkarte mit eindeutiger MAC-Adresse.

MAC-Adresse

Der **M**edia **A**ccess **C**ode bezeichnet die sechsstellige, weltweit eindeutige Hardware-Adresse, die jeder Hersteller seinen Netzwerkgeräten zuteilt.

Mit Hilfe von MAC-Adress-Listen kann festgelegt werden, welcher Client mit dem Access-Point des FunkLANs kommunizieren darf. Das Pflegen dieser Listen ist mit Aufwand verbunden und nicht für alle Einsatzvarianten möglich.

Die MAC-Adressfilter in den Access-Points zum Zwecke des Zugriffschutzes sind überwindbar, da auch die MAC-Adressen der Funk-Clients abgehört und und manipuliert werden können.

WEP-Verschlüsselung
Im FunkLAN soll die Vertraulichkeit, Integrität und Authentizität durch das Wired Equivalent Privacy-Protokoll gesichert werden, das standardmäßig eine Verschlüsselung des Funkverkehrs mit einem 64-Bit-Schlüssel vorsieht. Einige Hersteller bieten optional auch Verschlüsselungstiefen bis 128 Bit an. Mittlerweile sind hier mehrere Schwächen bekannt geworden. Weitergehende Informationen hierzu erhält man in der Broschüre des Bundesamtes für Sicherheit in der Informationstechnik „Sicherheit in FunkLAN“, die im Internet (www.BSI.de/fachthem/funk-lan/index.htm) abgerufen werden kann.

WEP-Verschlüsselung

Abkürzung für **W**ired **E**quivalent **P**rivacy Protokoll

12.1.1.2.1.3
Datenschutzrechtliche Bewertung

Beim Einsatz von WirelessLAN müssen alle standardmäßig vorgegebenen Sicherheitsmechanismen genutzt werden. Sie sind durchgängig schwach ausgelegt und bieten nur einen Minimal-Schutz. Daher ist in jedem Einzelfall zu entscheiden, welche weiteren Sicherheitsoptionen gewählt werden müssen. Zur Zeit empfiehlt man für die Übertragung von sensiblen Daten den Einsatz von IPSec-Lösungen.

IPSec

Abkürzung für **I**nternet **P**rotocol **Sec**urity Protocol, eine Gruppe aus Sicherheitsprotokollen, ESP (**E**ncapsulating **S**ecurity **P**ayload) und AH (**A**uthentification **H**eader), die erhöhte Sicherheit, eine Identifikationsprüfung, eine Authentifizierung und den Wiedergabeschutz bei Daten gewährleisten, die über die IP-Komponente (Internet Protokoll) vom TCP/IP im Internet übertragen werden.

Der Markt ist aber stark im Wandel und wird voraussichtlich in der nächsten Zeit geeignete Sicherheitslösungen anbieten können.

12.1.1.2.2
Bluetooth

12.1.1.2.2.1
Technik

Der Bluetooth-Standard ist für den Aufbau drahtloser Ad-hoc-Verbindungen über kurze Distanzen zwischen Geräten unterschiedlichster Art gedacht. Er wurde 1998 von einer Firmengruppe aus Ericssen, IBM, Intel, Nokia und Toshiba begründet und mittlerweile von mehr als 2.500 Herstellern unterstützt. In diesem Zusammenhang fallen oft auch die Begriffe Piconet und Scatternet.

Piconet

Der aus Pico und Net zusammengesetzte Begriff beschreibt ein Ad-hoc-Netzwerk, bei dem mindestens zwei portable Geräte miteinander verbunden sind. Ein Gerät dient als Master und ein Gerät als Slave.

Scatternet

Eine Gruppe von unabhängigen und nicht miteinander synchronisierter Piconets, die gemeinsam auf mindestens ein Bluetoothfähiges Endgerät zugreift.

Es ist zu erwarten, dass Bluetooth zukünftig auch für die Übertragung sensibler Daten genutzt werden soll. Bluetooth unterteilt das ISM-Band bei 2,4 GHz in 79 Kanäle mit jeweils 1 MHz Bandbreite. Damit ist eine Datenrate von theoretisch 1 Mbit/s möglich.

12.1.1.2.2.2
Sicherheitsmechanismen

Für Bluetooth gibt es drei Sicherheitsmodi, in denen die Geräte betrieben werden können:

Im Sicherheitsmodus 1 **(Non-Secure Mode)** gibt es keine Authentifikation oder Verschlüsselung. Die Geräte befinden sich im Entdeckungsmodus und reagieren nur auf die Authentifizierungsanforderungen anderer Bluetooth-Geräte.

Im Sicherheitsmodus 2 **(Service-Level Enforced Security)** ist die Authentifikation abhängig von der jeweiligen Anwendung. Geräte dieser Stufe verfügen über Übertragungs-Protokolle und Anwendungen, die die Verschlüsselung selbst durchführen, nachdem der Verbindungskanal aufgebaut wurde.

Im Sicherheitsmodus 3 **(Link-Level Enforced Security)** werden Authentifikation und Verschlüsselung beim Verbindungsaufbau durchgeführt. Erfasst werden alle Anwendungen, die auf diese Verbindung kommunizieren. Ein so genannter Security-Manager – eine Komponente innerhalb der Bluetooth-Software – verwaltet und setzt die Sicherheitsregeln durch.

Mit dieser Sicherheitsarchitektur ist es allein möglich, die angewählten Geräte zu identifizieren. Die Datenherkunft und Identität des Nutzers wird nicht überprüft. Verschlüsselungsalgorithmen zwischen 8 und 128 Bit werden als Basisausstattung mitgeliefert. Bei der ersten Kontaktaufnahme zwischen zwei Bluetooth-Geräten (Pairing) kann es vorkommen, dass nicht involvierte Bluetooth-Geräte in der Nähe den Initialisierungsprozess abhören können. Dies ist dann möglich, wenn Geräte mit geringem Speicherplatz als Verbindungsschlüssel den eigenen Geräteschlüssel verwenden.

12.1.1.2.2.3
Datenschutzrechtliche Bewertung

Beim Einsatz von Bluetooth sollten alle standardmäßig vorgegebenen Sicherheitsmechanismen genutzt werden. Dies bedeutet, dass stets der Sicherheitsmodus 3 aktiviert sein sollte. Überdies ist im Einzelfall – in Abhängigkeit der Sensibilität der Daten – zu entscheiden, welche weiteren Sicherheitsoptionen gewählt werden müssen. Zur Zeit empfiehlt sich für die Übertragung von sensiblen Daten der Einsatz von IPSec-Lösungen. Der Markt ist stark in Bewegung und wird voraussichtlich in der nächsten Zeit neue Sicherheitslösungen anbieten können.

12.2
Einsatz des Active Direcotry und von Windows 2000 in der Landesverwaltung

Das Betriebssystem Windows 2000 der Firma Microsoft ist das Nachfolgeprodukt von Windows NT. Wesentliche Komponente eines Netzwerks mit Windows 2000-Servern ist das Active Directory, das auch für zukünftige Betriebssysteme von Microsoft eine zentrale Bedeutung hat. Windows 2000 und das Active Directory werden in der Hessischen Landesverwaltung und bei Hessischen Kommunen eingesetzt. Neben den Neuerungen gegenüber Windows NT fällt besonders die höhere Komplexität ins Gewicht, die eine sorgfältige Planung des Einsatzes nötig macht. Dabei geht man davon aus, dass bei großen Netzen eine Planungsphase von mehr als einem Jahr zu erwarten ist.

12.2.1
Wichtige neue Funktionen

Windows 2000 ist das Nachfolgeprodukt von Windows NT. Während es für Arbeitsplatz-Rechner mit Windows XP bereits ein weiteres Nachfolgeprodukt gibt, ist Windows 2000 für Server das aktuelle Betriebssystem von Microsoft. Mit der Einführung von Windows 2000 in einem Netzwerk müssen auch Entscheidungen zur Struktur des Netzwerks getroffen werden, die unabhängig vom Betriebssystem sind. Sie fließen insbesondere in die Planung des Active Directory (AD) ein. Die Entscheidungen sind Vorgaben, die auch bei einem Wechsel auf neue Betriebssysteme eingehalten werden müssen.

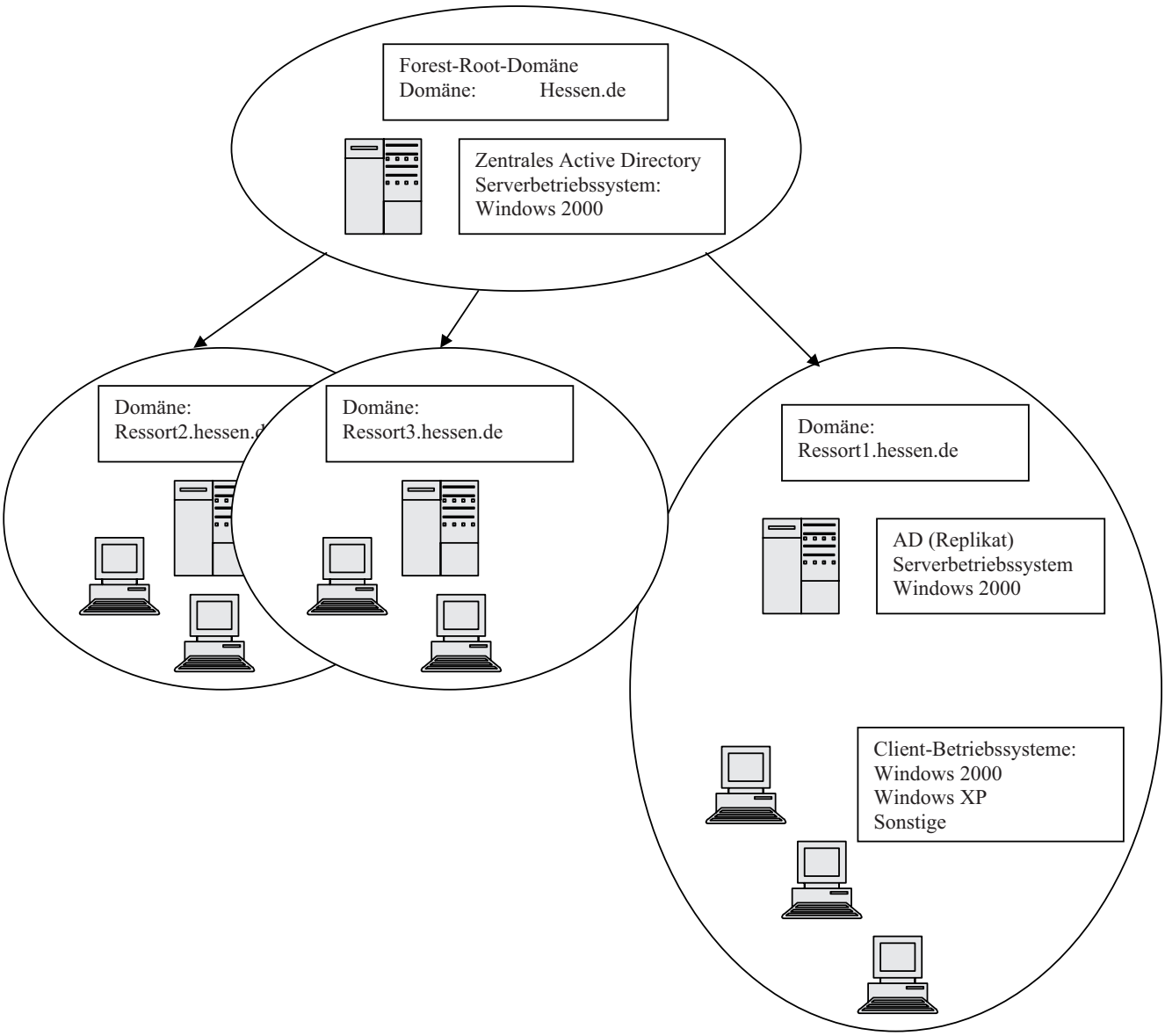
Windows 2000 besitzt im Vergleich zu Windows NT einige neue Funktionen und Komponenten.

Von den Neuerungen hat das AD die größte Bedeutung. Es wird auch von zukünftigen Betriebssystemen der Firma Microsoft genutzt, z. B. dem derzeit aktuellen Windows XP beim Einsatz in einem Netzwerk. Beim AD handelt es sich

um eine verteilte Datenbank, die alle Informationen über Domänen, Benutzer und Computer speichert. Diese Daten können auf mehrere Domänen-Controller verteilt werden und Änderungen können an jedem Domänen-Controller vorgenommen werden. Die Domänen-Controller replizieren diese Änderungen untereinander, soweit sie zum Global Catalog gehören (schematische Darstellung eines Netzwerks mit AD siehe Abbildung rechts). Durch die Verwendung des AD werden größere Domänen möglich als bei Windows NT, da das AD wesentlich mehr Einträge fassen kann als die SAM-Benutzerdatenbank eines Windows NT Domänen-Controllers.

Unter Sicherheitsaspekten spielt das AD eine wichtige Rolle, da es

– viele sicherheitsrelevante Daten enthält,



Schematische Darstellung eines Windows 2000-Netzwerkes mit Active Directory

– über eigene, dem Dateisystem sehr ähnliche Zugriffskontrollmechanismen verfügt, sowie

– die Basis für Gruppenrichtlinien ist, die das wichtigste Konfigurationswerkzeug für Zugriffsrechte und Privilegien sind.

Weitere neue Funktionen und Komponenten sind:

– Kerberos

  Die Authentisierung erfolgt in Windows 2000-Netzen mit Kerberos, einem Protokoll, das das Abhören und Entschlüsseln von Kennwörtern wesentlich erschwert.

– Verschlüsselung von Dateien

  Es gibt die Möglichkeit Dateien zu verschlüsseln. Die Verschlüsselung ist – derzeit – benutzerbezogen und muss sorgfältig geplant werden, damit im Fall einer Vertretung die Daten verfügbar sind.

– Verschlüsselte Datenübertragung

  Mit dem integrierten Protokoll IPsec können auch Datenübertragungen verschlüsselt werden.

– Terminalserver

  Ein Terminalserver ist im Betriebssystem integriert und muss nicht als Zusatzprodukt integriert werden. Es können daher mit weniger Aufwand Terminalserver-Lösungen eingeführt werden. Diese haben den Vorteil, dass nur die Ergebnisse von Verarbeitungsläufen zum Arbeitsplatzrechner als Bildschirmanzeigen übertragen werden und nicht komplette Dateien, die dann vom Arbeitsplatzrechner verarbeitet werden. (s. Ziff. 12.4)

12.2.2
Einige Problempunkte

Mit den neuen technischen Gegebenheiten sind auch Schwachstellen verbunden, die bei dem Einsatz des AD berücksichtigt werden müssen. Hier sind insbesondere zu nennen:

– Im AD werden viele personenbezogene Daten gespeichert. Es gibt dabei Muss-Felder und optionale Felder. Welche Daten gespeichert werden sollen, muss vor einem Einsatz datenschutzrechtlich geprüft werden. Dabei ist zu beachten, dass bestimmte Benutzerdaten aus dem AD, die des Global Catalog, in jeder Domäne zur Verfügung stehen.

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

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

– Alle Domänen in einem AD müssen das gleiche Schema verwenden. Soll auch nur in einer Domäne eine Software installiert werden, die eine Schemaänderung benötigt, müssen alle anderen Domänen diese Änderung mit tragen. Inkompatible Schemaänderungen durch verschiedene Softwareprodukte können dann dazu führen, dass Software nicht installiert werden kann oder fehlerhaft abläuft.

– Ist eine Domäne auf mehrere Standorte verteilt, die nur unzureichend miteinander vernetzt sind, kann die Übertragung der umfangreichen Replikationsdaten zu lange dauern, bis eine Kontosperrung in allen Standorten wirksam wird. Daher kann sich ein Benutzer, dessen Konto gesperrt worden ist, u. U. noch an anderen Standorten am System unberechtigt anmelden.

Vor dem Einsatz sind daher eine Reihe von Überlegungen anzustellen, wie sie vom Hersteller Microsoft oder, mit dem Schwerpunkt möglicher Sicherheitsprobleme, im Grundschutzhandbuch des Bundesamts für Sicherheit in der Informationstechnik (BSI) dargelegt sind. Auch mein Hamburger Kollege hat einen Leitfaden zum Datenschutz bei Windows 2000 veröffentlicht.

12.2.3
Aktivitäten der Hessischen Landesverwaltung

Um den Einsatz des AD für die Hessische Landesverwaltung vorzubereiten, wurde eine Arbeitsgruppe „Active Directory“ gebildet. Mitte 2001 hat der Landesautomationsausschuss (LAA) der Arbeitsgruppe den Auftrag erteilt, technische Grundlagen, Probleme und Lösungsmöglichkeiten für die Einführung einer landesweiten AD-Gesamtstruktur zu erörtern. Die Teilnahme an der Arbeitsgruppe stand jeder Behörde offen. Im November 2001 wurden die „Vorschläge für die Einführung einer landesweiten AD-Gesamtstruktur für die Behörden des Landes Hessen“ dem LAA vorgelegt. Der LAA befürwortete die Einrichtung einer ständigen Facharbeitsgruppe „Active Directory“ zur Pflege und Anpassung des AD an zukünftige Entwicklungen und der Erstellung eines Sicherheitskonzeptes. Die Geschäftsführung hierzu wurde dem Hessischen Ministerium des Innern übertragen.

Seit Anfang 2002 tagte die Projektgruppe „Active Directory“, in der Konzepte erarbeitet werden, um diese dem Entscheidungsgremium zuzuleiten. Wenn erforderlich, nehmen meine Informatiker als beratende Mitglieder an den Sitzungen teil. Mittlerweile wurden wesentliche Weichenstellungen vorgenommen und wichtige Konzepte erstellt und verabschiedet.

Wenn Microsoft-Betriebssysteme, wie in der Hessischen Landesverwaltung, in einem Verbund weitgehend unabhängiger Stellen eingesetzt werden sollen, muss die Netz- und Domänenstruktur den Erfordernissen genügen. In Hessen hat man sich entschieden, die „Forest-Root-Domäne“ nur als Klammer für die darunter liegenden Domänen zu nutzen. Sie wird nur insoweit genutzt, wie es für die Funktionsfähigkeit des Netzes erforderlich ist. Als Konsequenz können gerade die sicherheitsrelevanten Aktionen der Organisations-Administratoren und Schema-Administratoren auf ein Minimum reduziert werden.

Weiterhin wurden Konzepte für die IT-Struktur erstellt. Beispiele sind:

– Ein Sicherheits-Konzept für die landesweite AD-Gesamtstruktur

  Das Konzept besteht aus einzelnen Dokumenten:

  a) Sicherheitsaspekte bei Benutzerkonten und Benutzergruppen

  b) Sicherheitsaspekte für den Betrieb der AD-Domänencontroller der Domäne hessen.de und der Subdomänen

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

– Namenskonventionen für die Objekte der landesweiten AD-Gesamtstruktur

– Migrationspfade und -aufgaben

Es sind weitere Dokumente in Planung. Für das Sicherheitskonzept sollen noch zu den Bereichen Netzwerksicherheit und Virensicherheit ergänzende Dokumente erstellt werden.

In den Sicherheitskonzepten wird die Sicherheitspolicy festgelegt. Die Vorgaben sind so detailliert, dass die relevanten Parameter mit den Werten aufgeführt sind. Am Beispiel der Kennwortrichtlinien soll das deutlich werden.

KENNWORTRICHTLINIEN:

- Kennwörter müssen den Komplexitätsanforderungen entsprechen: deaktiviert
- Kennwortchronik erzwingen: Kennwortchronik von mindestens 13 Kennwörtern
- Kennwörter für alle Domänenbenutzer mit umkehrbarer Verschlüsselung speichern: deaktiviert
- Maximales Kennwortalter: 30 Tage
- Minimales Kennwortalter: 0 Tage
- Minimale Kennwortlänge: 8 Zeichen

KONTOSPERRUNGSRICHTLINIE:

- Kontosperrungsschwelle: 5 Anmeldungen
- Kontosperrdauer: 30 Minuten
- Zurücksetzungsdauer des Kontosperrungszählers: 30 Minuten

Derartige Festlegungen sind für alle sicherheitsrelevanten Systemparameter getroffen. Wenn sich ein Ressort der AD-Gesamtstruktur anschließt, muss es sich verpflichten die vorgegebenen Werte zu akzeptieren, d. h. in der Domäne einzustellen. Eine Verschärfung ist ohne Einschaltung des Entscheidungsgremiums möglich, während schwächere Werte nur nach Abstimmung mit den anderen Teilnehmern gewählt werden können.

In dem Dokument zur Einsatzkontrolle von Organisations-Administratoren und Schema-Administratoren werden die Maßnahmen beschrieben, mit denen der Gebrauch der Kennungen kontrolliert wird. So sollen die Maßnahmen u. a. erreichen, dass mindestens drei befugte Personen anwesend sein müssen, um mit den Kennungen arbeiten zu können.

Wie an diesen Beispielen deutlich wird, ist die Einführung eines Windows 2000-Netzwerkes und des dort verfügbaren AD mit einem hohen Aufwand verbunden. Da Fehler bei der Planung nur mit erheblichem personellen, technischen und finanziellen Einsatz zu korrigieren sind, halte ich die sorgfältig abgestimmte Vorgehensweise für unerlässlich und den entstehenden Aufwand für angemessen.

12.3
Software-Sicherheitslücken

Heute verfügbare Betriebssysteme, Anwendungsprogramme und Netzkomponenten haben in vielen Fällen Sicherheitslücken, die unbefugte Zugriffe erlauben oder die Einbringung von Schadfunktionen zulassen. Nur durch rechtzeitige und ausreichende Information und geeignete Vorkehrungen können sich Betreiber vor den Folgen schützen.

12.3.1
Entstehung von Sicherheitslücken

Betriebssysteme wie Windows, UNIX und auch Anwendungsprogramme wie die Office-Produkte von Microsoft sind Programme, deren Quelltext aus Hunderttausenden von Zeilen besteht. Aus dem Quelltext werden die Programme durch Compiler erstellt. Die so entstandenen Programme können unerwünschte Funktionen haben, die ausgenutzt werden können, um weitreichende Zugriffsrechte einzurichten oder Schadfunktionen einzufügen. Die unerwünschten Funktionen können aus Designfehlern, Fehlern bei der Programmierung oder einer unzulänglichen Umsetzung in den ausführbaren Code resultieren. Daneben gibt es auch Standards, die Sicherheitslücken beinhalten. Ein Beispiel ist der Standard IEEE 802.11, mit dem u. a. die Verschlüsselung für Funk-LAN beschrieben ist (siehe Ziff. 12.1). Es kann aber

auch ein Standard fehlerhaft implementiert sein. Dies galt z. B. für SSL (Secure Socket Layer)/TLS (Transport Layer Security), von dem in diesem Jahr mehrfach über Schwachstellen berichtet wurde. Sie betrafen aber immer die Implementierung.

Das SSL-Protokoll wurde ursprünglich von der Firma Netscape entwickelt. In der Version 2 fanden sich noch kleinere Sicherheitslücken, die in der Folgeversion 3.0 beseitigt wurden. Es handelte sich aber um proprietäre Produkte. Auf Basis von SSL 3.0 hat die IETF (Internet Engineering Task Force) den Internetstandard TLS entwickelt. Dabei entspricht TLS 1.0 dem SSL 3.1. TLS soll in Zukunft den SSL ersetzen.

12.3.2
Umgang mit Sicherheitslücken

Wenn Schwachstellen in Programmen bekannt werden, die auch von öffentlichen Stellen verwendet werden, stellt sich die Frage, wie damit umgegangen werden soll.

12.3.2.1
Soll im Internet auf die Lücke hingewiesen werden, auch wenn keine Lösung bekannt ist?

Diese Auffassung vertreten zum Beispiel die Betreiber von kostenlosen Informationsdiensten wie SecurityFocus mit der Mailingliste Bugtrac oder paketstorm. Sobald die Hersteller informiert wurden und Möglichkeiten zur Beseitigung gegeben waren, wird der Hinweis gemeinhin in das Internet gestellt. Die Hinweise sind aber in der Regel nicht so detailliert, dass ein Außenstehender einen Angriff darauf aufbauen kann. Nach einer Frist von etwa 30 Tagen folgen meist weitergehende Informationen, die es erlauben könnten, die Schwachstelle ausnutzen. Zum Teil werden sogar Programme bereitgestellt, um die Lücke auszunutzen (Exploits) oder, wie es die Anbieter begründen, um den eigenen Rechner auf die Lücke testen zu können. Der Nachteil dieses Vorgehens besteht darin, dass zum Teil sogar die Werkzeuge bereit gestellt werden, um Schwachstellen auszunutzen, obwohl noch keine Lösung bekannt ist, wie Angriffen begegnet werden kann.

Einige Informations-Anbieter haben eine Informationspolitik, die weniger weit geht. Im Jahr 2000 hat das CERT/CC (**C**omputer **E**mergency **R**esponse **T**eams/**C**oordination **C**enter; Carnegie-Mellon University) den bisherigen Ansatz geändert. Wenn bislang neue Sicherheitslücken bekannt wurden, wurde zusammen mit dem Hersteller und anderen Notfall-Teams versucht, die Lücken möglichst schnell und umfassend zu schließen. Sobald eine Lösung verfügbar war oder die Gesamtsituation ein Warten auf die Lösung verbot, wurden die notwendigen Informationen verteilt. Neuerdings veröffentlichen das CERT/CC und das DFN-CERT, das sich in seiner Informationspolitik an das CERT/CC anlehnt, bekannt gewordene Sicherheitslücken nach 45 Tagen, unabhängig davon, ob es Lösungen gibt. Allerdings werden keine Programme bereitgestellt, um die verwendete Software auf Lücken zu testen. Der Zeitraum kann unter Umständen verlängert werden, wenn komplexe Änderungen nötig sind (umfangreiche Untersuchung, Änderung an Kommunikationsprotokollen oder Kernkomponenten). Er kann auch verkürzt werden, wenn bereits Exploits existieren oder Angriffe bekannt werden.

Es gibt erste Hersteller, die gegen die Veröffentlichung von Sicherheitslücken ihrer Produkte vorgehen. Außerdem ist das Wissen um Sicherheitslücken eine Ware, die vermarktet werden kann. Befürchtungen, dass bisher kostenlose Informationsdienste eingestellt oder kostenpflichtig werden könnten, wurden laut, als ein Informationsdienst von einem großen Anbieter von Sicherheitssoftware aufgekauft worden war.

12.3.2.2
Soll auf die Schwachstelle erst hingewiesen werden, wenn eine Lösung angeboten wird?

Diesen Ansatz favorisieren die meisten Hersteller. Es vergeht aber oft viel Zeit zwischen dem Zeitpunkt, zu dem in „interessierten Kreisen“ eine Sicherheitslücke bekannt wird, und dem Zeitpunkt, zu dem der Hersteller eine Lösung anbietet. So wurden beispielsweise zum Internet Explorer der Fa. Microsoft am 2. Oktober 2002 zwanzig noch nicht beseitigte Lücken genannt, deren erste Veröffentlichung teilweise aus dem ersten Halbjahr 2002 und in einem Fall aus 2001 stammt. Wenn nach diesem Modell vorgegangen wird, profitieren davon besonders Personen, denen eine Schwachstelle bekannt ist. Gerade im Internet gibt es Gruppen, die auch ohne allgemein zugängliche Informationsdienste über die Existenz von Schwachstellen kommunizieren. Der Betreiber eines IT-Systems kann sich dagegen nur unvollständig oder mit viel Aufwand wappnen. Die Informationspolitik wiegt die Anwender in trügerischer Sicherheit, obwohl Angreifer eventuell mit wenig Aufwand Schaden verursachen können.

12.3.2.3
Empfehlenswerte Vorgehensweise

Aus meiner Sicht sind unabhängige Informationsanbieter unverzichtbar, die über Sicherheitslücken zeitnah informieren. Der Service sollte kostenlos sein, damit möglichst viele Interessenten erreicht werden. Die grundsätzliche Vorgehensweise der CERT, die keine Exploits veröffentlichen, halte ich für richtig.

12.3.3
Beispiel SSL

Eine Übersicht von Mängeln in Betriebssystemen und Standardprogrammen lässt sich nicht geben, da eine solche Übersicht nie umfassend und aktuell wäre. Da SSL/TLS als Standard für eine Kommunikation im Internet genutzt wird – z. B. durch die KIV Hessen –, möchte ich auf Mitteilungen der letzten Monate eingehen, nach denen SSL unsicher sei.

Im Internet gab es in den bekannten Informationsbörsen Nachrichten über Probleme mit Implementierungen des SSL-Protokolls in einigen Programmen.

– **Fehler in OPEN-SSL**

  Open-SSL hatte einen Fehler bei der Implementierung in einem bestimmten Server-Programm. Dazu gab es nach kurzer Zeit ein Patch (Programmupdate zur Fehlerbehebung).

– **Browser-Sicherheitslücke bei SSL-Zertifikaten**

  Es gab unter bestimmten Rahmenbedingungen – eine ausführliche Beschreibung ist auf der Homepage von Microsoft zu finden – die Möglichkeit, dem Browser ein SSL-Zertifikat so zu präsentieren, dass es automatisch als vertrauenswürdig akzeptiert wurde. Nur eine genaue Kontrolle der Zertifikate hätte gezeigt, dass das Zertifikat nicht authentisch ist. Dieser Fehler trat beispielsweise beim Internet-Explorer von Microsoft und bei dem im Linux-Umfeld benutzten Browser Konqueror auf. Für den Linux-Browser existierte bereits nach kurzer Zeit ein Patch. Für den Internet Explorer und andere Microsoft-Produkte, die denselben Design-Fehler hatten, lagen erst Wochen später die Patchs vor.

– **Löschen von Zertifikaten**

  Für alle Windows-Versionen gab es das Problem, dass SSL-Zertifikate wegen eines Fehlers in einem ActiveX-Steuerelement von außen gelöscht werden konnten. Auch hierzu gibt es inzwischen ein Patch.

Die genannten Probleme betreffen jeweils einzelne Implementierungen und nicht alle Produkte, die SSL unterstützen oder das Protokoll SSL selbst. Auch sind weder einzelne Schlüssel – ausreichend lange Schlüssel vorausgesetzt (mittlerweile sind 128 Bit für den symmetrischen und 1024 Bit für den RSA-Algorithmus Stand der Technik) – noch das Verfahren insgesamt gebrochen worden. Selbstverständlich müssen Patchs immer unverzüglich eingespielt werden, um die gefundenen Lücken zu schließen. Zusammenfassend ist festzuhalten, dass SSL als Standard keineswegs zu unsicher ist und nicht mehr benutzt werden sollte.

12.3.4
Vorgehensweise für Betreiber

Jeder Administrator in Behörden oder Unternehmen muss sich über mögliche Lücken der von ihm betreuten Systeme informieren. Diese Aufgabe darf nicht nur im Geschäftsverteilungsplan genannt sein. Es muss auch die Zeit für Recherchen und Abhilfemaßnahmen zur Verfügung stehen. Um einen Überblick zu bekommen, reicht es nicht, die Informationsseiten der Hersteller zu durchsuchen. Die unabhängigen Informationsanbieter, Anbieter von Sicherheitslösungen und die CERT mit ihren Mailinglisten sind unverzichtbare Quellen. Hinweise, wie eine Lücke notdürftig geschlossen werden kann, gibt es eventuell bei verschiedenen Informationsanbietern, aber Programmupdates kann man in aller Regel nur vom Hersteller erhalten.

Als technischer Laie erhält man bei vielen Informationsanbietern keine brauchbare Hilfe, da die Beschreibungen Hintergrundwissen voraussetzen. Hier bleibt in aller Regel nur die Möglichkeit, sich über Zeitschriften oder den Hersteller zu informieren. Man sollte Programmupdates der Hersteller möglichst umgehend einspielen, wenn die Lücken im eigenen Umfeld eine Rolle spielen.

12.4
Sicherere Internetanbindung über eine Terminalserverlösung (Graphical Firewall – GFW)

Terminalserverlösungen stellen eine gute, deutlich sicherere und praktikable Lösung zur Direktanbindung eines lokalen Netzes an das Internet dar.

Die Anbindung an das Internet ist in der heutigen Zeit für viele Menschen zum unverzichtbaren Teil der täglichen Arbeit, der Kommunikation und der Freizeitgestaltung geworden. Nicht nur der Umfang der verfügbaren Informationen hat zugenommen, auch die Kosten für eine permanente Anbindung (Flatrate oder Standleitung) sind ständig gesunken. Für Behörden- oder Firmennetze stellt diese Anbindung ein erhöhtes Risiko dar, das nicht zu unterschätzen ist.

Durch Zwischenschaltung eines Terminalservers kann dieses Risiko erheblich reduziert werden, da dadurch die Internetsitzung logisch vom lokalen Rechner getrennt wird. Der Terminalserver nimmt Eingaben entgegen und leitet sie weiter; Anwendungen werden in einer eigenen Umgebung ausgeführt und dem Benutzer nur die Ergebnisse in einem Anwendungsfenster angezeigt, das von lokalen Prozessen isoliert ist. Im Rahmen seiner Diplomarbeit hat ein

Student in meinem Hause die Möglichkeiten, die eine solche Terminalserver-Lösung unter Sicherheits- und Performance-Aspekten bietet, untersucht. Diese Lösung trennt logisch – ähnlich einer Firewall – Netze und Anwendungen. Deswegen wird sie auch als „graphische Firewall“ (engl. „graphical firewall“ oder GFW) bezeichnet.

12.4.1
Problemstellung

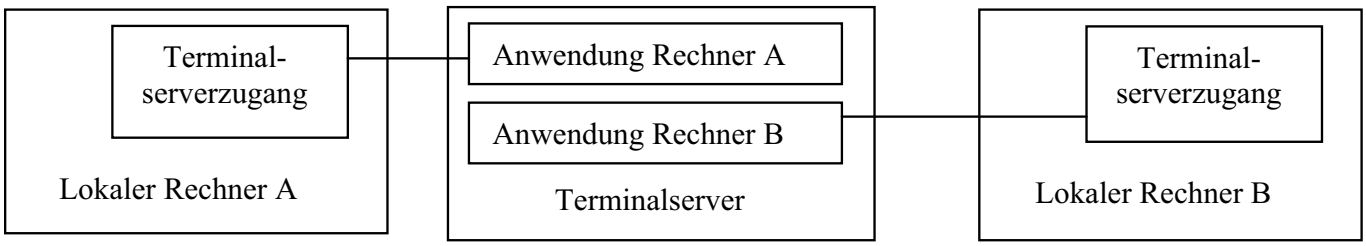
Firmen- oder Behördennetze sind für potenzielle Eindringlinge von größerem Interesse als Privat-PCs. Schon deshalb kommt einer „sicheren“ Internetanbindung hohe Bedeutung zu. Bei einer direkten Anbindung eines lokalen Netzes an das Internet können sogenannte trojanische Pferde (z. B. SubSeven), die Verbindungen aus dem lokalen Netz ins Internet öffnen, oder ActiveX-Komponenten großen Schaden anrichten, insbesondere bei Benutzern mit weitergehenden Rechten im LAN (Administratoren).

Die Einrichtung von Internetarbeitsplätzen als abgetrennte „Einzelplatzlösung“ wäre zwar grundsätzlich eine Möglichkeit, diese Risiken zu minimieren. Jedoch stellt sich dabei die Frage, wie benötigte Daten zur Weiterverarbeitung ins LAN transferiert werden. Publikationen, Präsentationen, Updates und Patches im Internet bereitzustellen, anstatt sie auf CD zu verbreiten, ist heute zur Selbstverständlichkeit geworden und der Umfang dieser Dateien sprengt in der Regel das Volumen der guten, alten Diskette. Speicherkarten und CD-Brenner in den Surf-Stationen bringen nicht nur erhöhte Kosten, sondern erfordern auch Schulungs- und Betreuungsaufwand.

Sofern ein hohes Schutzbedürfnis lokaler Netze besteht, stellt die Terminalserverlösung eine geeignete Technik dar.

12.4.2
Das Terminalserverkonzept

Das Prinzip des Terminalservers ist es, Anwendungen nicht unmittelbar auf dem lokalen Rechner auszuführen, sondern die Bearbeitung auf einem separaten Rechner vorzunehmen. Der lokale Rechner hat damit die Funktion eines Clients, der die (Server-)Prozesse auf dem Terminalserver über eine Zugangssoftware steuert.

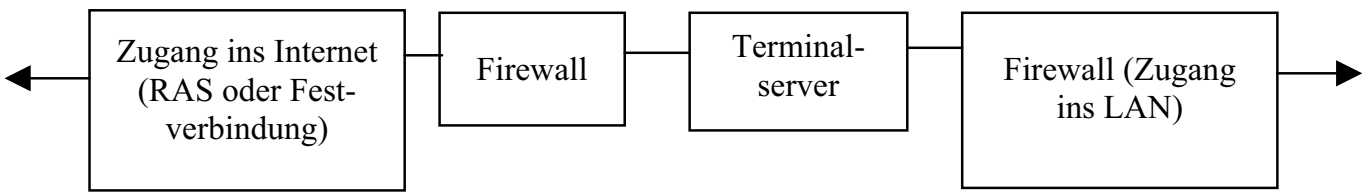


Neben der Absicherung des lokalen Netzes bietet der Terminalserver auch den Vorteil, dass die dort vorhandene Software nur einmal installiert, konfiguriert und gewartet werden muss.

12.4.3
Die Teststellung

Aufgabe der Diplomarbeit war, den Themenbereich „Internetzugang“ (ohne E-Mail) als Terminalserverlösung unter Realisierungs-, Sicherheits- und Performanceaspekten zu untersuchen. Die vollständige Konfiguration der Testumgebung würde den Rahmen dieses Beitrages sprengen, deshalb wird nur auf die wichtigsten Aspekte kurz eingegangen.

Die Testumgebung:



12.4.3.1
Zugangsserver

Für den Test wurde als Internetzugang ein aktueller Linux-Server mit ISDN-Karte und Proxyserver (Squid) verwendet. Als Alternative steht eine zweite Netzwerkkarte für eine Festverbindung zur Verfügung. Als zusätzliche Komponenten auf dem Rechner wurden realisiert:

– Einwahl nur während der Arbeitszeit

– Firewallfunktionalitäten

– URL-Filterung

Die Bereiche „Einwahl“ und „Firewall“ lassen sich unter Linux bereits mit „Bordmitteln“ realisieren:

Für die Einwahl wurden zeitgesteuert (Cron-Daemon) Befehle abgesetzt, die die ISDN-Karte in den Selbstwahlmodus schalten beziehungsweise diesen deaktivieren („isdnctrl ippp0 dialmode auto“ beziehungsweise „isdnctrl ippp0 dialmode off“).

Für die Firewall (iptables) wurden Skripte erstellt, die die Zugänge für die benötigten Dienste (HTTP, FTP, DNS) während der Arbeitszeit freigeben und in den übrigen Zeiten die Zugänge IP-seitig vollständig schließen. Auf dem Einwahlserver wurde zusätzlich ein Proxydienst installiert. Damit war bereits hier die direkte Verbindung aus dem Internet über den http-Port 80 in das Testnetz unterbrochen.

12.4.3.2
Erste Firewall

Als optionale Komponente wurde zur Sicherung des Terminalservers gegen das Internet eine Linux-Firewall zwischengeschaltet, die ebenfalls über das Regelwerk die Zugänge zwischen Einwahl- und Terminalserver überwachte.

12.4.3.3
Der Terminalserver

Die zentrale Komponente des Versuchs – der Terminalserver – sollte dem Nutzer die Möglichkeit bieten, für Recherchen und zur Beschaffung von Software (z. B. Virensignaturen) Zugang zum Internet zu erhalten. Aus Sicherheits- und Kostenaspekten wurde hier ebenfalls ein Linux-Betriebssystem eingesetzt. Als eigentliche Terminalserver-Software wurde „Virtual Network Computing“ (VNC) der Firma AT&T eingesetzt. Die graphische Oberfläche wurde mit „GNU Window Maker“ (GWM) als einfache Oberfläche realisiert. Über das Startskript wurde ferner sichergestellt, dass der verwendete Browser (Opera) nach der Anmeldung automatisch gestartet und so positioniert wurde, dass der Benutzer ihn nicht verschieben kann. Wird der Browser geschlossen, endet damit automatisch auch die Terminalserversitzung. Dadurch war sichergestellt, dass der Benutzer keinen Zugang zur Arbeitsoberfläche hatte.

Die Konfiguration von VNC umfasst in der Datei „/etc/services“ den Eintrag

„vnc 5950/tcp #VNC-Server“.

Als Port kann anstelle des Standardwerts „5950“ auch ein beliebiger, freier Port verwendet werden. In „/etc/xinetd.conf“ ist der VNC-Dienst wie folgt konfiguriert:

```
service vnc
{
socket_type  = stream
protocol     = tcp
wait         = no
user         = nobody
access_times = 6:30–18:30
server       = /usr/X11/bin/Xvnc
server_args  = –inetd –broadcast –once –geometry 800x600 –depth 24
               –fp /usr/lib/X11/fonts/misc/,/usr/lib/X11/fonst/75dpi/
}
```

Der Parameter „access_times” legt den Zeitrahmen fest, in dem der Start einer Sitzung möglich ist. Aktive Sitzungen werden nach Erreichen des Endzeitpunkts nicht beendet. Das muss über ein zeitgesteuertes Skript erfolgen, falls aktive Sitzungen zwingend geschlossen werden sollen.

Der zusätzliche Eintrag „per_source = 1” in der „defaults”-Sektion der Datei stellt sicher, dass nur eine VNC-Sitzung pro Client-Rechner gestartet werden kann.

Der Zugang der Benutzer zur Arbeitsoberfläche wird durch einen einfachen Trick realisiert: Das Fenster des Browsers ist etwas größer als der sichtbare Bildschirm, wird aber um einige Pixel nach oben verschoben, so dass die Titelleiste nicht zugänglich ist. Damit hat der Benutzer keine Möglichkeit, den aktiven Browser zu minimieren. Die für den Start der Benutzersitzung erforderliche Datei „.xinitrc“ wird hierfür wie folgt ergänzt:

```
exec /usr/X11/bin/windowmaker &
exec /usr/X11/bin/opera –geometry
800x605-2-20
```

Die Konfiguration des Browsers und der Windowmaker-Sitzung erfolgt zentral mit einem so genannten Standardbenutzer, auf dessen Konfigurationsdateien die entsprechenden Benutzerdateien verlinkt werden. Damit kann ein Be-

nutzer zwar temporär die Browsereinstellungen modifizieren, beim nächsten Start einer Sitzung werden die Standardwerte aber wiederhergestellt.

Um dem Benutzer die Möglichkeit zu bieten, heruntergeladene Dateien im lokalen Netz weiterzuverarbeiten, wurde auf dem Terminalserver ein FTP-Dienst (proFTP) installiert.

Dafür wird dem Benutzer innerhalb seines Benutzerverzeichnisses ein Ordner „Download“ zur Verfügung gestellt, in dem er Daten aus dem Internet ablegen kann. Dieses Verzeichnis stellt für den jeweiligen Benutzer über die Konfiguration des FTP-Dienstes das Wurzelverzeichnis (oberste erreichbare Dateiebene) dar, so dass er über den FTP-Client mit seiner Benutzerkennung direkt auf dieses (und nur dieses!) Verzeichnis zugreifen kann, um die dort abgelegten Daten auf seinen PC zu transferieren. Damit wird verhindert, dass der Benutzer Zugang zu den sonstigen Dateien erhält (insbesondere Konfigurationsdaten), die zum Benutzerprofil gehören. Dies würde nämlich die Maßnahmen aushebeln, die getroffen wurden, um Änderungen am Betriebssystem und den Einstellungen zu verhindern (s. vorherige Maßnahmen, um den Zugang zur Arbeitsoberfläche zu verhindern).

Ferner ist am Terminalserver ein Drucker angeschlossen, so dass Daten auch direkt am Terminalserver ausgedruckt werden können.

12.4.3.4
Client-Software

Für den Zugang zum VNC-Terminalserver wurde der „VNCviewer“, ebenfalls von AT&T verwendet. Der Zugang zum FTP-Server erfolgte über die Software „WS-FTP 95 LE“. Beide Programme sind ohne Installation lauffähig, die Benutzer müssen nur über den Aufruf (IP-Adresse und Port des VNC-Servers, Benutzer und Passwort für den Zugang) informiert werden. Die Basiseinstellungen für „WS-FTP“ lassen sich ebenfalls zentral über eine Konfigurationsdatei vornehmen, die mit der Software verteilt wird. Nach der ersten Anmeldung des Benutzers mit seinen persönlichen Daten werden diese Daten automatisch in die Konfiguration übernommen.

12.4.3.5
Filterung

Eine Regelung des möglichen Herunterladens von Dateien aus dem Internet ist nicht nur unter dienstrechtlichen Aspekten (Nutzungsordnung), sondern auch unter Sicherheitsaspekten (Viren, ActiveX, illegale Software) von Bedeutung. Daher wurde eine Filtersoftware in die Teststellung integriert. Aus den für Linux zur Verfügung stehenden Anwendungen wurden SquidGuard und DansGuardian untersucht.

SquidGuard

ist ein Zusatzprogramm zum Proxyserver Squid, das die im Browser angeforderte URL anhand von Listen auf Zulässigkeit prüft. Diese Listen („blacklists“) werden vom SquidGuard-Projekt einmal wöchentlich mit Suchrobotern automatisiert erstellt und für die Aktualisierung der Software bereitgestellt. Wird eine gesperrte URL gefunden, wird die Anforderung auf eine lokale (Fehler-) Seite umgelenkt und so der Zugang für den Benutzer gesperrt.

DansGuardian

arbeitet als eigenständige Software, die dem Proxyserver vorgeschaltet ist. Die Filtermechanismen basieren auf Schlagworten (Seiteninhalte), MIME-Typen (Download-Objekte) und optional auf den SquidGuard-Filterlisten. Hiermit wird zwar auch kein vollständiger Schutz erreicht, die Zugangs- und Downloadmöglichkeiten lassen sich aber wirkungsvoll einschränken und überwachen.

Squidguard und DansGuardian arbeiten intern mit einer Datenbank (BerkeleyDB), die installiert werden muss. Sie benötigen für die Umlenkung der gesperrten Seiten lokal einen Webserver (z. B. Apache).

12.4.4
Gegenüberstellung der möglichen Anbindungen

Die wesentlichen Aspekte der Anbindung eines Netzes an das Internet sind hier nochmals kurz als Übersicht dargestellt.

Es bedeuten:

Einzelplatz	Anbindung mit Einzelplatz-PC
GFW	Anbindung mit Terminalserver (konfiguriert als Graphical Firewall)
Direktverbindung	Anbindung des LAN direkt ans Internet
TS	Terminalserver
LAN	lokales Netz (Local Area Network)

		GFW	Einzelplatz	Direktverbindung
1	Betriebssystem	Linux	i.d.R. Windows	i.d.R. Windows
2	Sicherheit Betriebssystem	statischer Kernel, Konfiguration nicht änderbar	Windows-Sicherheitseinstellungen	Windows-Sicherheitseinstellungen, Domänensicherheitsrichtlinien
3	Verfügbare Applikation/en	nur Browser	Browser, vollständiges Betriebssystem	Browser, vollständiges Betriebssystem, verfügbare Netzressourcen
4	Pflege/Wartung der Serveranwendungen	nur TS	an jedem Rechner	zentrale Installation
5	Pflege/Wartung der Clientanwendungen	je Arbeitsplatz nur TS-Zugangssoftware (ohne Installation lauffähig)	an jedem Rechner	Software an jedem Rechner, Konfiguration teilweise zentral
6	LAN-Integration	Verbindung zum TS	keine	vollständig
7	Zugriff auf Anwendungsdaten von außen	nur Daten der Browsersitzung verfügbar	nur Daten der Browsersitzungen auf dem Rechner	alle dem Benutzer lokal und im LAN zugängliche Daten
8	Installation von Software	in den Benutzerverzeichnissen können keine ausführbaren Dateien gestartet werden	soweit mit den Rechten des Benutzers möglich auf der Arbeitsstation	soweit mit den Rechten des Benutzers möglich auf der Arbeitsstation und im LAN
9	Download von Objekten	aus dem Internet zum TS, vom TS ins LAN	über Disketten ins LAN	direkt
10	Drucken (soweit Drucker verfügbar)	am TS	am Arbeitsplatz	am Arbeitsplatz
11	Filter	zentrale Installation auf dem TS	Einzelplatzinstallation	zentrale Installation
12	Lücken	nur Linux-Schwachstellen des Browsers, betrifft lediglich die Benutzerumgebung auf dem TS	Windows-Schwachstellen, nur der lokale Rechner	Windows-Schwachstellen, lokaler Rechner und verfügbare Netzressourcen
13	Aktive Inhalte (ActiveX, Java, JavaScript)	ActiveX nur unter Windows, Java/JavaScript soweit zugelassen auf die Benutzerdaten	soweit über Browser zulässig nur lokale Daten	soweit über Browser zulässig, lokale Daten und Netzressourcen
14	Viren	soweit für Linux vorhanden, nur in der Benutzerumgebung auf dem TS, EXE-Dateien sind nicht ausführbar	auf dem lokalen Rechner, soweit vom Virenscanner nicht erkannt	auf dem lokalen Rechner und im Netz, soweit vom Virenscanner nicht erkannt

Erläuterungen:

Zu 1:
Betriebssystem

Als Betriebssystemalternativen sind im Wesentlichen nur Windows (2000 oder NT) und Linux denkbar. Der Windows 2000-Server beinhaltet einen (zusätzlich kostenpflichtigen) Terminalserver. Unter Windows NT muss auf ein externes Programm ausgewichen werden. Unter Linux kann VNC als kostenfreie Terminalserverlösung eingesetzt werden, auf die eine graphische Benutzeroberfläche (hier: Windowmaker) aufgesetzt wird.

Zu 2:
Sicherheit des Betriebssystems

Unter Windows kann der Zugang zu wichtigen Systemkomponenten über Benutzerrechte eingeschränkt werden. Große Teile des Betriebssystems sind allerdings auch dem Benutzer zugänglich. Hinzu kommt die starke Vermischung von Betriebssystem-, Anwendungs- und Benutzerdateien und die starke Verzahnung der Betriebssystemkomponenten (ActiveX, COM, OLE), die Anwendern (zumindest im Rahmen ihrer Rechte) Zugang zu Betriebssystemobjekten verschafft (ActiveX-Objekte). Damit ist nicht immer nachvollziehbar, ob Objekte im Systemverzeichnis auch wirklich zum Betriebssystem gehören oder ob sie von außen eingeschleust worden sind.

Unter Linux ist die Datenhaltung sauber und strikt getrennt. Ein Linux-System kann im Extremfall auch im Nur-Lese-Modus betrieben werden, was allerdings einigen Konfigurationsaufwand erfordert. Unter Linux basiert die GFW-Lösung auf einem an die Hardware angepassten statischen Kernel, der zusätzlich über bereits im Betriebssystem verankerte Methoden (so genannte „capabilities“) gesichert ist. Dies erlaubt, Dateien mit zusätzlichen Attributen zu versehen und die Änderung dieser Attribute auch dem Administrator (root) zu versagen. Insbesondere sind dies das Immutable-Flag, das jegliche Änderung einer Datei verbietet (z. B. Konfigurationsdateien) und das Append-Flag, das nur Anfügungen an eine Datei zulässt (z. B. Protokolle). Näheres hierzu findet sich unter 12.4.5 „Überlegungen zur Installation“. Zusätzlich wird hierfür das Programm „lcap“ (limit capabilities) benötigt, das über die Datei „boot.local“ in der frühen Startphase des Systems die eingestellten Sperren (z. B. „CAP_SYS_IMMUTABLE“, das Änderungen der erweiterten Attribute verhindert), aktiviert. Änderungen an diesem System sind damit nur im SingleUser-Modus (d. h. mit dem Root-User ohne Netzverbindung, also nur an der Systemkonsole) möglich.

Unter diesen Aspekten und der Vielzahl von Gefahren und Schwachstellen, die für Windows bekannt sind, stellt die Linux-Variante die sicherere Lösung dar.

Zu 3:
Applikationen

Die Windows-Lösungen bieten mit der Standardinstallation eine Umgebung, die die Mehrheit der Nutzer von ihrer täglichen Arbeit gewohnt ist, dafür aber unter Sicherheitsaspekten (s.o.) weniger zu empfehlen ist.

Die GFW-Lösung bietet eine reine Surf-Umgebung, in der der Benutzer einige wenige Bedienungskomponenten des verwendeten Browsers kennen muss. Die Linux-Varianten von Opera, Netscape und Mozilla unterscheiden sich nur wenig von den Windows-Versionen. Opera wurde für die Teststellung ausgewählt, da er der ressourcenschonendste Browser ist, der zur Verfügung steht.

Zu 4:
Pflege/Wartung der Serveranwendungen

Programmpflege, Wartung und Updates müssen bei Einzelplatzlösungen auf den einzelnen Rechnern durchgeführt werden. Bei der Terminalserverlösung erfolgen Installation und Konfiguration der Software hingegen einmalig auf dem Terminalserver. Updates sind damit auch leichter ausführbar und der Softwarestand bleibt überschaubar.

Zu 5:
Pflege/Wartung der Clientanwendungen

Gleiches gilt für die Konfiguration der Software für die Clients. Zwar lässt sich der MS Internet Explorer zentral über die Systemrichtlinien der Domäne beziehungsweise das Internet Explorer Administration Kit konfigurieren und sichern, jedoch sollte aus grundsätzlichen Erwägungen ein Browser verwendet werden, der nicht so eng in dem Betriebssystem verzahnt ist (vgl. aktuelle Diskussion über Sicherheitslücken des Internet Explorers, ActiveX-Problematik u. Ä.). Die in der Terminalserverumgebung eingesetzte Clientsoftware ist durchgängig ohne zusätzliche Installation lauffähig. Die für die FTP-Anbindung erforderliche Konfigurationsdatei kann ebenfalls zentral erstellt und ohne weitere Maßnahmen benutzt werden. Eine Softwareaktualisierung beschränkt sich damit auf die Verteilung der neuen Programmversionen (z. B. per E-Mail).

Zu 6:
LAN-Integration

Eine Voll-Integration in das LAN ist zwar unter dem Komfort-Aspekt am vorteilhaftesten, birgt aber auch das größte Risiko. Die Einzelplatzlösung verringert dieses Risiko, bringt dafür aber große Komfort-Einbußen. Immer mehr Daten werden im Internet zum Download angeboten und müssen zur Weiterverwendung ins LAN transferiert werden. Da diese auch zunehmend nicht mehr auf eine Diskette passen, müssen hierfür andere Lösungen angedacht werden. Möglichkeiten bieten Speicherkarten oder ein CD-Brenner im Rechner, was aber wiederum mit Kosten und Aufwand (Schulung, Betreuung usw.) verbunden ist. Die GFW bietet mit dem logisch getrennten FTP-Zugang eine einfache Möglichkeit, Daten über den Terminalserver (zweistufig) und jeweils von der inneren, sicheren Seite initiiert aus dem Internet auf den lokalen Rechner zu transferieren.

Zu 7:
Zugriff auf Anwendungsdaten von außen

Die Direktanbindung an das Internet ist dadurch besonders problematisch, dass Lücken in der Absicherung einem Eindringling von außen alle verfügbaren Daten zugänglich machen. Diese Gefahr besteht weder bei der Einzelplatz- noch bei der Terminalserverlösung.

Der Datenbestand der Einzelplatzlösung ist jeweils auf die Internetzugangs- und Sitzungsdaten des lokalen PCs beschränkt. In der GFW-Lösung bestehen ebenfalls nur solche Datenbestände.

Zu 8:
Installation von Software

Installation von Software ist in den Windows-Lösungen auf die Möglichkeiten im Rahmen der Rechte des Benutzers beschränkt. In der GFW-Lösung ist dem Benutzer die Möglichkeit genommen, im Rahmen der ihm zur Verfügung stehenden Verzeichnisse (= nur sein Benutzerverzeichnis), ausführbare Dateien (die zudem Linux-Anwendungen sein müssten) zur Ausführung zu bringen (die Konfiguration des Datenträgers verbietet die Ausführung von Programmen mit dem „noexec“-Flag).

Zu 9:
Download

Wie vorher bereits angesprochen, ist der Download-Aspekt von großer Bedeutung. Um solche Abrufe unter Beachtung damit verbundener potenzieller Sicherheitsrisiken zu ermöglichen, wurde in der überprüften GFW-Lösung ein FTP-Server integriert. Damit ist es möglich, Daten zunächst aus dem Internet in ein (und nur ein!!) Verzeichnis herunterzuladen und dann in einem zweiten, separat anzustoßenden Prozess via FTP (File Transfer Protocol) ggf. nach Virenprüfung in die LAN-Umgebung zu transferieren.

Zu 10:
Drucken

Gleiches gilt für Ausdrucke. Eine Direktanbindung erlaubt den direkten Ausdruck auf dem Arbeitsplatzdrucker, ebenso wie bei einer Einzelplatzlösung. Bei den Terminalservern kann der Ausdruck nur als Grafik, nämlich als Bildschirm-Hardcopy des Terminalserverfensters oder am Server direkt erfolgen. Alternativ können die gewünschten Seiten auch gespeichert und zum Drucken ins LAN übertragen werden.

Zu 11:
Filter

Filterlösungen müssen bei Einzelplatzlösungen und bei Direktanbindungen zusätzlich installiert werden. Hierfür entstehen wiederum Kosten und erheblicher Aufwand (Beschaffung der Software, Installation, Konfiguration, Wartung, Aktualisierung).

Die GFW-Lösung bietet mit dem Programm **„DansGuardian“** einen dreistufigen Filtermechanismus (3 Beispiele sind dem Dokument angehängt):

– URL-Filter

  Mit der Linux-Software „SquidGuard“ wird ein URL-Filter für den Proxyserver SQUID angeboten. „DansGuardian“ ist in der Lage, diese URL-Filterlisten (Kategorien u.a. Werbung, Gewalt, Pornografie, illegale Software) zu verarbeiten. Der Zugriff auf die hier eingetragenen Seiten wird von der Software blockiert. Diese bieten einen Grundstock zur Filterung. Zu beachten ist dabei aber, dass diese Listen automatisiert von Suchrobotern erstellt werden und damit notwendigerweise unvollständig sind.

– Inhalte

  „DansGuardian“ bietet ebenfalls einen Inhaltsfilter, der den Text der Webseiten analysiert und bei bestimmten Schlüsselwörtern den Zugang blockiert.

– MIME-Typen

  Als dritte Komponente – wichtig für den Download – prüft „DansGuardian“ den MIME-Typ (z. B. EXE-, ZIP oder PDF-Datei) der zum Herunterladen anstehenden Software. Ein Download wird nur für erlaubte Objekttypen freigegeben.

Zu 12 bis 14:
Lücken, Aktive Inhalte, Viren

Hier ist nur auf die grundsätzliche Anfälligkeit der Windows-Betriebssysteme hinzuweisen. Schadenprogramme (Viren, Würmer, trojanische Pferde usw.) werden zwar zunehmend auch für Linux entworfen, jedoch ist deren Schadwirkung aufgrund der wesentlich restriktiveren Sicherheitsmechanismen von Linux geringer. Denkbar wären bei diesem Betriebssystem z. B. so genannte „rootkits“ (um Administratorrechte zu erlangen). Das ist bei der GFW-Lösung so gut wie ausgeschlossen, da das für rootkits erforderliche Element des dynamischen Kernels (rootkits sind als zusätzliche Kernelmodule implementiert) fehlt.

Zu beachten ist bei Einzelplatzlösungen außerdem, dass diese i. d. R. direkt mit dem Internet verbunden sind, während bei allen anderen Lösungen vorgelagerte Sicherheitselemente (Paketfilter, Firewalls) überwunden werden müssen.

12.4.5
Überlegungen zur Installation

Abschließend sollen noch einige Empfehlungen zum Thema „Installation von Linux“ gegeben werden:

Grundsätzlich bieten alle aktuell am Markt verfügbaren Distributionen eine brauchbare Basis als Server. In Sicherheitsüberlegungen sollten aber folgende Aspekte einbezogen werden:

– Als Basis sollten zunächst nur die zum Betrieb des Servers erforderlichen Komponenten installiert werden. Die benötigten Anwendungen werden dann in einem zweiten Installationsschritt hinzugefügt und konfiguriert. Nur so lässt sich der Überblick behalten, welche Software auf dem Rechner verfügbar ist.

– Internetzugänge lassen sich auch mit „Fli4l“ realisieren. „Fli4l“ ist eine Linux-Variante, mit der ein Ethernet-, ISDN- oder DSL-Router auch ohne Festplatte mit nur einer Diskette betrieben werden kann.

– Soweit möglich, sollte für den Server auf die graphische Benutzeroberfläche (X-Server) verzichtet werden. Linux-Serveranwendungen lassen sich auch über die Konsole gut administrieren.

– Soll eine Administration über das Netz erfolgen, bietet sich das ssh-Paket („secure shell“) an. Hierbei ist zu beachten, das die (ungesicherte) Anmeldung über einen nicht privilegierten Benutzer erfolgt. Sofern Superuser-Rechte erforderlich sind, kann der Benutzerwechsel in der aktiven Sitzung über den „su“-Befehl („switch user“) erfolgen.

– Rechner, die mit dem Internet verbunden sind, sollten generell nicht über das Netz administrierbar sein, auf Anwendungen wie „ssh“ oder „webmin“ also verzichten.

– Gleiches gilt für die nicht benötigten Netzwerkdienste, die bei den Standardinstallationen i. d. R. aktiviert werden (z. B. Telnet, Maildienste). Alle nicht erforderlichen Einträge in der Datei „/etc/inetd.conf“ sollten deaktiviert werden. Sofern erforderlich, sollte der wesentlich sicherere „xinetd“-Dienst für Netzwerkdienste verwendet werden.

– Der mit den Distributionen gelieferte Kernel ist meist nicht mehr aktuell. Da in jedem Fall der Linux-Kern als statischer Kernel neu erstellt werden muss, sollte hierbei auch gleich eine aktuelle Version verwendet werden.

– Aktualitätsprobleme ergeben sich auch für die einzusetzende Software, die in den Distributionen ebenfalls oft nicht mehr aktuell ist. Die Installation über RPM-Dateien (RedHat Package-Manager) ist zwar einfach, bindet aber an die entsprechende Distribution, da die Hersteller teilweise eigene Pfadkonzepte verfolgen, die von anderen Distributionen abweichen. Außerdem ist man auf das Erscheinen neuer RPM-Dateien angewiesen, wenn Software aktualisiert werden muss.

  Das beschaffen des Quellcodes der eingesetzten Programme aus dem Internet und das anschließende manuelle Kompilieren der Software ist zwar etwas aufwendiger, stellt aber die zeitnahe Aktualisierung bei auftretenden Sicherheitslücken sicher.

– Als Dateisystem sollte EXT2, besser EXT3 verwendet werden. Neben den Journalkomponenten bieten die EXT-Dateisysteme den Zugriff auf erweiterte Attribute (über CHATTR – CHangeATTRibute beziehungsweise LSATTR – LiSt ATTRibute).

  Das Dateisystem kann damit – was Konfigurations- und Programmdateien betrifft – weitestgehend mit dem Immutable-Attribut (keine Änderungen möglich) beziehungsweise dem Appendable-Attribut (nur Anhängen möglich, z. B. für Logdateien) in Verbindung mit dem LCAP-Befehl vor Veränderungen im laufenden Betrieb geschützt werden. Wird der LCAP-Befehl in die Datei „boot.local“ eingebunden, sind Änderungen nur im SingleUser-Modus (Neustart des Systems mit dem Attribut „single“) direkt an der Systemkonsole möglich.

– Verzeichnisse sollten so weit als möglich mit restriktiven Attributen ins Dateisystem eingehängt werden. Als Beispiel sind „read-only“ für „/boot“ oder „noexec,nosuid“ für „/home“ zu nennen.

– Die Rechte der Befehle in den sbin-Verzeichnissen (/sbin, /usr/sbin und ggf. /usr/local/sbin) sollten restriktiv gehandhabt werden. Nur der Eigner „root“ darf mit vollen Zugriffsrechten ausgestattet sein, die Rechte für „Gruppe“ und „Andere“ werden entfernt, soweit es der Betrieb der installierten Anwendung zulässt.

– Der Start des Systems über den Bootlader LILO sollte nur in der Standardkonfiguration ohne zusätzliches Passwort möglich sein. In der Datei „/etc/lilo.conf“ wird zunächst im globalen Teil der Eintrag „password= <Passwort>“ eingefügt. Der Standard-Eintrag wird mit dem Zusatz „restricted“ versehen. Dies bewirkt, dass nur noch dieser ohne zusätzliche Startparameter unbeaufsichtigt gestartet werden kann. Sobald ein Parameter angehängt wird (z. B. „init=/bin/bash rw“, um eine root-Shell ohne Passworteingabe zu öffnen) wird das Boot-Passwort angefordert, ebenso bei allen anderen Einträgen, z. B. „failsafe“. Zu beachten ist, dass die Datei „lilo.conf“ mit restriktiven Rechten versehen werden muss, da das Passwort im Klartext vorliegt.

12.4.6
Anhang 1 – Internetadressen zu der beschriebenen Software

Linux-Kernel	http://www.kernel.org
LCAP	http://www.megaloman.com/~hany/RPM/lcap.html
NetFilter/Iptables	http://www.iptables.org
VNC	http://www.uk.research.att.com/vnc
Squid	http://www.squid-cache.org
ProFTP	http://www.proftpd.org
Apache	http://www.apache.org
DansGuardian	http://www.dansguardian.org
BerkeleyDB	http://www.sleepycat.com
FLi4l	http:// www.fli4l.org

12.4.7
Anhang 2 – Bildschirmmasken einer Terminalserversitzung

Abb. 1 Terminalserver-Zugang

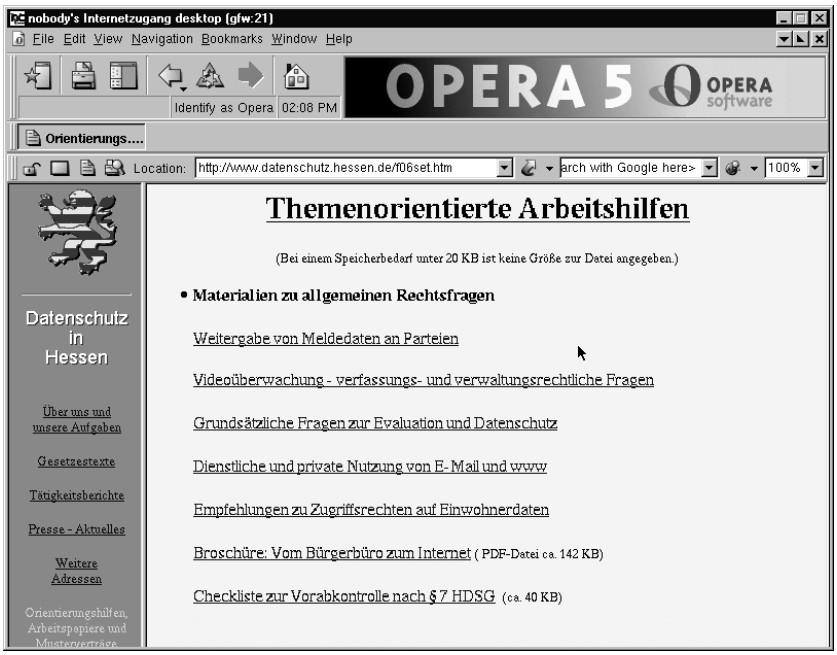


Abb. 2 Gestartete Sitzung

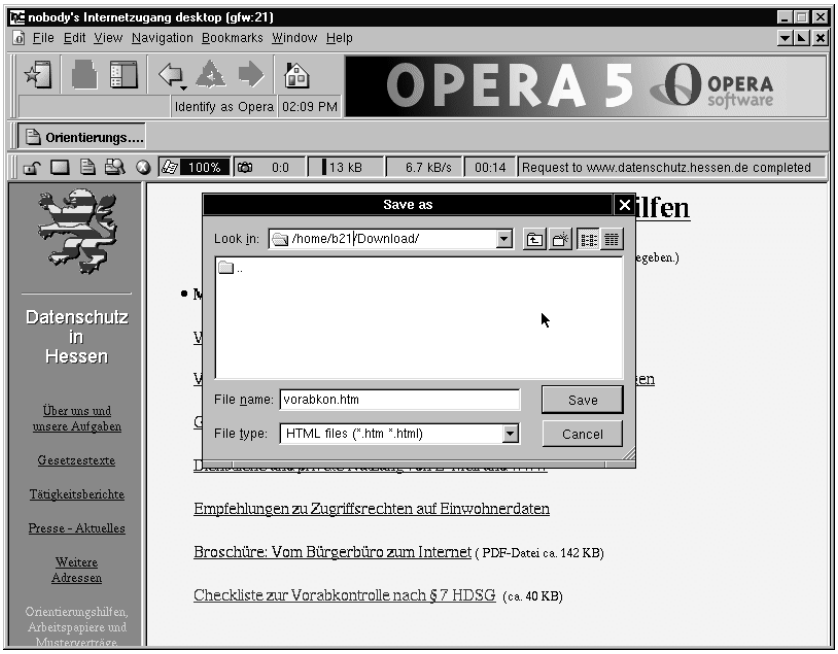


Abb. 3 Download einer Datei ins Benutzerverzeichnis

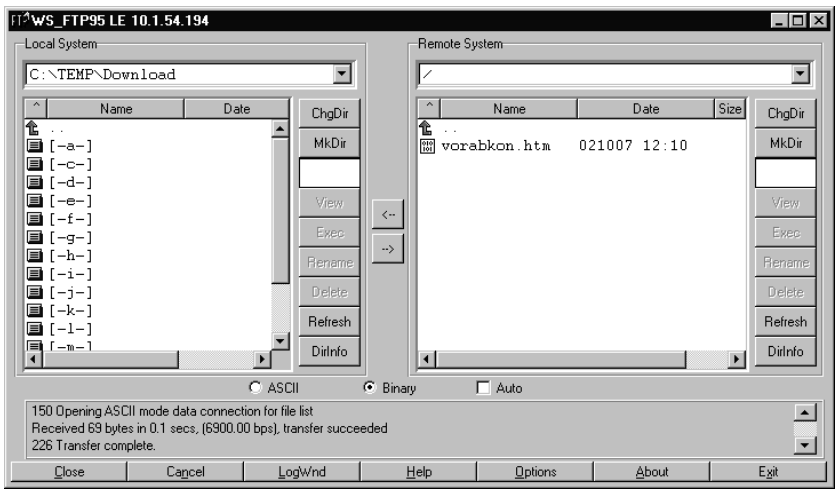


Abb. 4 Download der Datei auf den lokalen PC

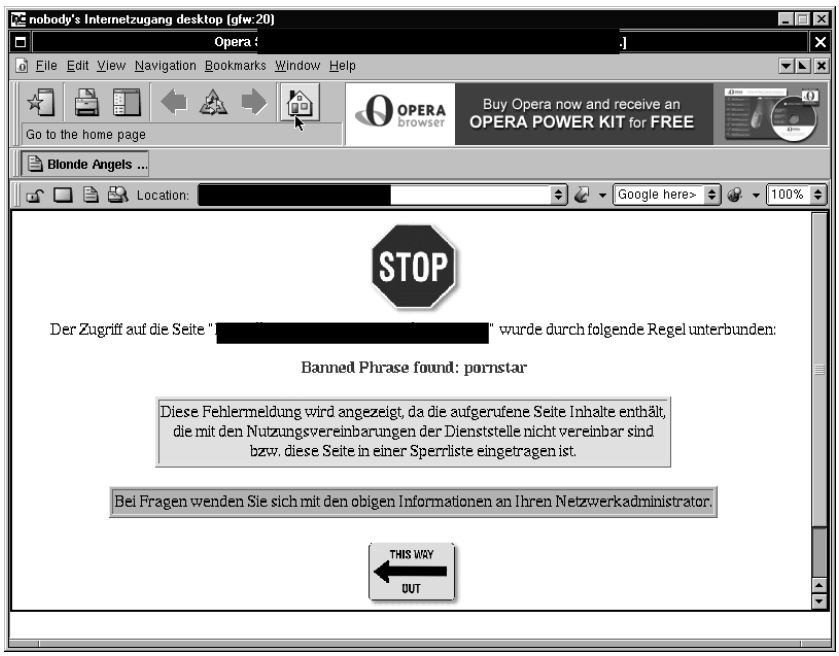


Abb. 5 Gefilterte URL

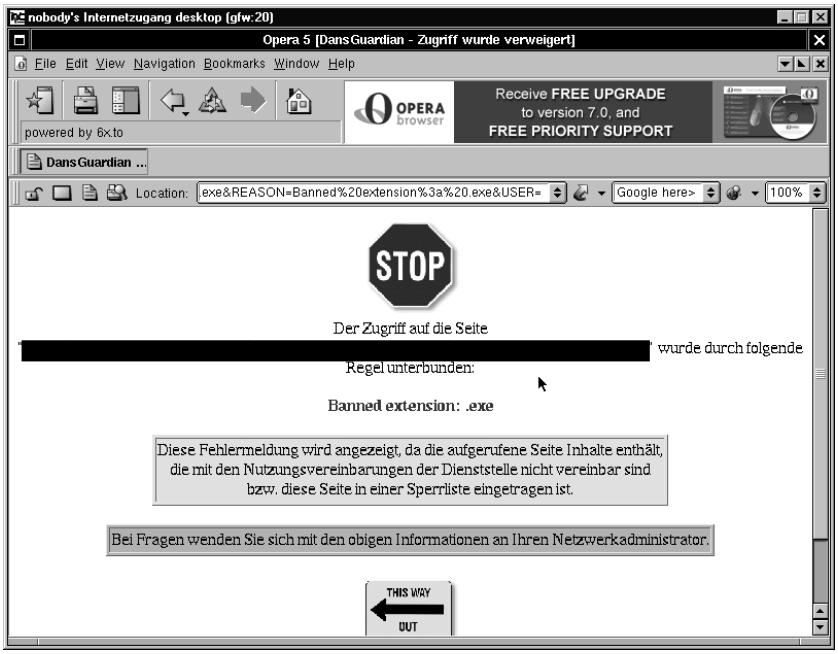


Abb. 6 Gesperrter Dateityp (hier .EXE)

12.5
Prüfung von Softwareprodukten, die mit Dateiservern eingesetzt werden

Beim Einsatz von Anwendungssoftware auf herkömmlichen Dateiservern treten immer noch Risiken und Sicherheitslücken auf. Wenn solche Programme nicht durch eine modernere Produktvariante ersetzt werden können, sind die Risiken nur durch zusätzliche technisch-organisatorische Maßnahmen auf der Betriebsystem- beziehungsweise der Netzwerkebene einzugrenzen.

In den vergangenen Jahren habe ich bei den Prüfungen lokaler Netze und darauf zugeschnittener Anwendungsprogramme verstärkt feststellen müssen, dass eine bereits länger bekannte Problemstellung in der Landes- und Kommunalverwaltung immer noch auftritt. Stellvertretend für viele andere Produkte können hier bestimmte Varianten von Prosoz und MPS-Kommunal genannt werden. Das Problem entsteht aber auch bei diesen Produkten nur unter bestimmten Randbedingungen.

Alle gängigen Dateimanager (beispielsweise Windows-Explorer) greifen auf die zu den Anwendungsprogrammen erstellten Verzeichnisbäume zu. Werden derartige Verzeichnisbäume auf dem Dateiserver eingerichtet, haben nicht nur die berechtigten Anwender Zugriff, sofern keine Zugriffssperren auf der Ebene des Betriebssystems installiert sind. Nur dann werden die unberechtigten Nutzer des Dateiservers bei Zugriffen auf diesen Verzeichnisbaum vom Betriebssystem abgewiesen. So wird erreicht, dass nicht nur innerhalb des Verfahrens durch eine integrierte Benutzerverwaltung sichergestellt ist, dass nur die Anwender auf die Daten zugreifen können, die sie im Rahmen ihrer Aufgabenstellung benötigen.

Auf der Betriebssystemebene lassen sich die Rechte der Anwender in den Verzeichnisbäumen nicht so differenzieren, dass sie den Zugriffsmöglichkeiten innerhalb der Anwendung entsprechen. Ist die Benutzerumgebung aus technischen oder organisatorischen Gründen nicht hinreichend eingeschränkt, sind den Anwendern auf der Betriebssystemebene (Explorer, Editor, usw.) ggf. alle Daten der verzeichneten Verfahren zugänglich. Diese Konstellation eröffnet das ganze Spektrum denkbarer Risiken vom Verlust der Vertraulichkeit und der Integrität bis zum Totalverlust der Daten.

Mit einer gezielten Querschnittsprüfung bei verschiedenen Kommunen habe ich mir einen Überblick verschafft, inwieweit Anwendungen noch auf Betriebssystemen ohne Zugriffssperren beziehungsweise -einschränkungen auf bestimmte Verzeichnisse und Verzeichnisbäume eingesetzt werden. Geprüft worden ist auch, ob das für die verschiedenen Verwaltungen zur Auswahl stehende Produktangebot künftig den überwiegenden Einsatz anderer technischer Lösungen erwarten lässt. Dabei ergibt sich gegenwärtig folgender Eindruck:

– Grundsätzlich sind Administratoren im Rahmen ihrer Aufgabenstellung bemüht, durch eine genaue Definition und Einschränkung der Benutzerumgebung ein hohes Maß an Sicherheit in ihren Netzwerken einzurichten. Leider entstehen bei einer konsequenten Umsetzung dieses Ansatzes so viele neue praktische Schwierigkeiten, dass dieser Lösungsweg äußerst selten umfassend realisiert wird. Die verbleibenden Restrisiken müssen dann mit erhöhtem Aufwand an Protokollierung und organisatorischen Maßnahmen kompensiert werden. Das Ergebnis bleibt insgesamt unbefriedigend und ist in Bereichen mit sensitiven Daten angesichts der möglichen Alternativen untragbar.

– Sind Betriebssysteme in der Lage, nicht nur Anwender oder Anwendergruppen mit Zugriffsrechten auszustatten, sondern lassen sich Rechte auf das ausführbare Programm übertragen, ergibt sich ein eleganter Administrations-

ansatz. In solchen Fällen lässt sich eine Berechtigungskette bilden, bei der ein Anwender nur das Programm starten kann. Dabei stellt das Betriebssystem sicher, dass nur dieses auf die Daten zugreifen kann. Gleichzeitig wird ein Zugriff auf Inhalte außerhalb des Verfahrens wirksam ausgeschlossen. Im Verfahren selbst greifen die rollenspezifischen Rechtezuweisungen. Bedauerlicherweise war diese sehr effiziente Lösung bei den Prüfungen nur in Zusammenhang mit bestimmten Versionen des Netzwerkbetriebssystems Novell Netware anzutreffen. Bietet ein Betriebssystem diese Möglichkeit nicht, so sind alle Maßnahmen zu ergreifen, die Zugriffe auf dieser Ebene wirkungsvoll abwehren.

– Zunehmend findet sich bei Anwendungen, die dafür geeignet sind, die so genannte Terminalserverlösung (s. Ziff. 12.4.2). Dabei kann der Zugriff auf die Verfahrensdaten – eine entsprechende Konfiguration vorausgesetzt – nur über eine Clientsoftware erfolgen, die den Ablauf des Programms auf einem speziellen Server steuert. Diese Variante ist mit zusätzlichen Kosten verbunden und erfordert entsprechendes Know-how. Leider wird sie deshalb nicht überall realisierbar sein.

– Bei neueren Produktentwicklungen, die zur Ablösung von Altverfahren oder als komplette Neuentwicklung am Markt angeboten werden, wird immer häufiger ein Datenbankserver als Basis für die Anwendung verwendet. Wird bei der Administration darauf geachtet, dass die Datenbankschnittstelle nur von der zugelassenen Anwendung angesprochen werden kann, sind die Daten auch bei diesen Implementierungen vor unberechtigten Zugriffen geschützt.

Fazit: Die Querschnittsprüfung hat erfreulicherweise ergeben, dass die Zahl der kritischen Installationen durch die Ablösung von Altverfahren und den Einsatz neuer Techniken stetig abnimmt.

Ich werde künftig noch stärker darauf drängen, dass Verwaltungen von den Möglichkeiten des sich verändernden Produktangebots Gebrauch machen und die jeweils sicherste, dem Stand der Technik entsprechende Variante einsetzen, wie es § 10 Abs. 2 Hessisches Datenschutzgesetz fordert.

13. Kommunen

13.1
Briefwahlunterlagen per E-Mail beantragen

Durch die Änderung der Bundeswahlordnung im Februar 2002 war es bei der Bundestagswahl im September erstmals möglich, die Briefwahlunterlagen per E-Mail zu beantragen. Um mögliche missbräuchliche Bestellungen von Briefwahlunterlagen zu verhindern, habe ich in Gesprächen mit dem Landeswahlleiter erreicht, dass dieser eine Empfehlung an die Kommunen herausgegeben hat, wie ein sowohl datenschutzgerechtes als auch wahlrechtlich sinnvolles Verfahren der Beantragung per E-Mail aussehen kann.

Die Erteilung eines Wahlscheins kann nach den geänderten bundes- und landesrechtlichen Bestimmungen auch per E-Mail oder durch eine sonstige dokumentierbare Übermittlung in elektronischer Form beantragt werden, § 27 Abs. 1 Satz 2 Bundeswahlordnung (BWO), § 13 Abs. 1 Satz 2 Landeswahlordnung (LWO).

§ 27 Abs. 1 Satz 1 und 2 BWO

Die Erteilung eines Wahlscheins kann schriftlich oder mündlich bei der Gemeindebehörde beantragt werden. Die Schriftform gilt auch durch Telegramm, Fernschreiben, Telefax, E-Mail oder durch sonstige dokumentierbare Übermittlung in elektronischer Form als gewahrt.

Die Vorschrift enthält keine Regelung darüber, wie sicherzustellen ist, dass der Wahlschein tatsächlich von der berechtigten Person beantragt wird (Authentizitätsprüfung). Zudem sind keine Anforderungen an die Sicherheit der Datenübertragung formuliert. Nach meiner Auffassung müssen die Gemeinden Verfahren anbieten, die sicherstellen, dass nur berechtigte Personen den Wahlschein beantragen sowie dafür sorgen, dass eine sichere Kommunikation zwischen Bürger und Verwaltung erfolgen kann.

Im Vorfeld der Bundestagswahl habe ich deshalb mit dem Landeswahlleiter Kontakt aufgenommen, damit von ihm zu diesen Fragen Empfehlungen an die Gemeinden formuliert werden. Der Landeswahlleiter ist dieser Anregung gefolgt und hat in einem Wahlerlass (B 19) die von mir thematisierten Punkte wie unten zitiert aufgegriffen:

Für Gemeinden, die für die Antragstellung eine Eingabemaske ins Internet stellen wollen, füge ich ein vom Bundeswahlleiter entwickeltes virtuelles Formular bei, das der Anlage 4 zur BWO nachgebildet ist; ...

Sofern die Formulare im Dialogverfahren ausgefüllt werden sollen, ist es aus der Perspektive des Datenschutzes wünschenswert, dass die Übertragung durch eine SSL-Verschlüsselung oder Verfahren mit einem vergleichbaren Schutzniveau geschützt werden.

Soll lediglich die Möglichkeit eingeräumt werden, das Antragsformular aus dem Internet herunterzuladen und es dann ausgefüllt per E-Mail zurückzusenden, oder ist ein Dialogverfahren ohne Verschlüsselung realisiert, sollte datenschutzrechtlich ein Hinweis erfolgen, dass bei einer unverschlüsselten Versendung der Daten das Risiko besteht, dass unbeteiligte Dritte die Angaben mitlesen können. Der Hessische Datenschutzbeauftragte hat in seinem 28. Tätigkeitsbericht vom 28. März 2000 im Zusammenhang mit der Bereitstellung von Online-Formularen die Verwendung des folgenden Musterhinweises empfohlen:

„Wir wollen Ihnen mit diesem Angebot einen Weg zu uns ersparen – weisen Sie aber darauf hin, dass die Daten im Internet/über E-Mail unverschlüsselt übermittelt werden, insofern also dem Datenschutz keine Rechnung getragen ist. Sie können das Formular aber ausgefüllt ausdrucken und mit normaler Post an uns schicken."

Bei der Verwendung virtueller Formulare wird regelmäßig davon auszugehen sein, dass die in dem Musterformular abgefragten Angaben übermittelt werden, so dass die Identifikation des Antragstellers ohne Rückfragen möglich ist.

Bei Wahlscheinanträgen per E-Mail, die eine zuverlässige Identifikation des Antragstellers nicht erlauben, muss die Gemeindebehörde den Betroffenen durch Rückfrage um zusätzliche Angaben – wie z. B. das Geburtsdatum – bitten.

Es gibt mittlerweile Dienstleister, die die oben formulierten Vorgaben zur Beantragung des Wahlscheins umsetzen und dies den Kommunen anbieten. Zur eindeutigen Identifizierung des Antragstellers muss der Antragsteller sowohl die Nummer des Wahlbezirks als auch die laufende Nummer der Eintragung im Wählerverzeichnis angeben. Die Übertragung erfolgt im Dialogverfahren mittels SSL-Verschlüsselung, eine im Internet etablierte Technik zur verschlüsselten Übertragung von Daten, damit Unbefugte die Daten nicht lesen können.

Eine stichprobenartige Überprüfung der Internetseiten verschiedener hessischer Städte und Gemeinden hat ergeben, dass viele der Empfehlung des Landeswahlleiters nicht gefolgt sind. In mehreren Fällen wurden keine zusätzlichen Identifikationsmerkmale verlangt und es fehlte sowohl ein Verschlüsselungsangebot als auch der Hinweis darauf, dass die Daten unverschlüsselt übertragen werden. Andere Kommunen haben Verschlüsselung angeboten, aber keine zusätzlichen Identifikationsmerkmale abgefragt beziehungsweise umgekehrt.

Werden keine zusätzlichen Identifizierungsmerkmale verlangt, so kann es Wahlrechtsprobleme geben, weil die kommunalen Wahlbehörden nicht feststellen können, ob es tatsächlich die berechtigte Person ist, die die Unterlagen beantragt hat. Sollte es Anträge Unbefugter auf Wahlscheine gegeben haben, so sind – wie bei anderen Problemen, die bei der Durchführung der Bundestagswahl auftreten – Bundes- und Landeswahlleiter gefordert, die Situation zu bewerten und erforderlichenfalls Abhilfe zu schaffen.

Die unverschlüsselte Beantragung eines Wahlscheins per E-Mail kann durch die Kommune kaum beeinflusst werden, außer durch einen Hinweis auf die damit verbundenen Risiken in ihrem Internetangebot, der von dem Bürger aber nicht zwangsläufig gelesen werden muss. Anders ist die Situation, wenn das Formular online ausgefüllt wird. In diesem Fall sollte die Kommune eine verschlüsselte Übertragung der Daten technisch sicherstellen (SSL; siehe oben). Anderenfalls muss sie die Antragsteller deutlich auf die Risiken hinweisen.

Die Internetangebote der Kommunen, die nach meiner Feststellung diese Anforderungen nicht erfüllen, werde ich dahingehend untersuchen, ob sie auch bei Formularen, die die Eingabe von sensibleren Daten voraussetzen, ähnlich sorglos verfahren.

13.2
Unzulässige Datenübermittlung durch ein städtisches Frauenbüro

Kommunale Frauenbüros verfügen über keine ihnen gesetzlich zugewiesene Aufgabe, die sie zur Übermittlung personenbezogener Daten Dritter ermächtigt. Die wohlmeinende Wahrnehmung von Interessen geschiedener Frauen gestattet keinen Eingriff in die datenschutzrechtlichen Belange anderer Personen.

Ein seit vielen Jahren in Deutschland lebender griechischer Staatsangehöriger war verwundert, als er von seiner Ausländerbehörde unter der Betreffangabe „Erlöschen Ihrer Aufenthaltserlaubnis" angeschrieben wurde. EU-Bürger genießen zwar Freizügigkeit und Privilegien zu denen auch der Anspruch auf Erteilung einer unbefristeten Aufenthaltserlaubnis gehört. Diese erlischt aber z. B. grundsätzlich, wenn sich der Inhaber mehr als sechs Monate im Ausland aufhält. Die Ausländerbehörde teilte dem Griechen mit, er habe in einem Verfahren vor einem griechischen Gericht eine eidesstattliche Versicherung abgegeben, wonach er sich in Griechenland aufhalte und dort mit seiner Tochter und seinen Eltern zusammenlebe. Sie gehe deshalb davon aus, dass seine Aufenthaltserlaubnis erloschen sei. Sollte die Annahme nicht zutreffen, möge er seine Anwesenheit im Bundesgebiet belegen – so die Ausländerbehörde.

Er erklärte bei der Ausländerbehörde, seit mehreren Jahren an seinem Wohnort selbstständig tätig zu sein und legte der Ausländerbehörde alle in Frage kommenden Unterlagen vor. Zu der angeblichen eidesstattlichen Versicherung erläuterte er, tatsächlich sei vor einem griechischen Zivilgericht eine Erklärung abgegeben worden, dass er mit seinem Kind in Griechenland lebe. Allerdings habe nicht er, sondern ein Zeuge diese Angabe gemacht. Sie habe dessen Wahrnehmung entsprochen und habe sich auf einen mehrere Jahre zurückliegenden Zeitraum bezogen, in dem er

seine Wehrdienstzeit in Griechenland ableistete und sich so oft wie möglich in seinem Elternhaus aufhielt. Seine damals fünfjährige Tochter lebte dort bei den Großeltern. Zu diesen Angaben legte er beglaubigte Übersetzungen von Gerichtsverhandlungsprotokollen vor. Die Ausländerbehörde nahm daraufhin die Annahme, seine Aufenthaltserlaubnis sei erloschen, zurück. Sie informierte ihn zugleich darüber, dass dem Anschreiben eine Datenübermittlung vorausgegangen sei, die von dem Frauenbüro der Stadtverwaltung stamme, in der seine geschiedene Ehefrau lebe. Dort hatte auch er früher mit seiner damaligen Ehefrau gewohnt.

Seine an die Stadtverwaltung gerichtete Beschwerde wurde zurückgewiesen. Zur Begründung führte die Behörde an, er selbst habe eine eidesstattliche Versicherung über einen Wohnsitz in Griechenland abgegeben. Die Einwohnermeldebehörde der Stadtverwaltung sei nach der Ausländerdatenübermittlungsverordnung verpflichtet gewesen, die Ausländerbehörde über diesen Sachverhalt zu informieren.

Daraufhin wandte er sich an mich. Er bat mich um eine datenschutzrechtliche Beurteilung, denn zum einen sei die Angabe falsch gewesen, dass er eine eidesstattliche Versicherung abgegeben habe. Zum anderen könne er nicht einsehen, was die nicht mehr zuständige Einwohnermeldebehörde mit der falschen Information zu tun habe, wie sie dazu gekommen sei und wieso diese sie an die Ausländerbehörde habe übermitteln müssen.

Auf Nachfrage erklärte mir die Stadtverwaltung, die geschiedene Ehefrau des Griechen habe dem Frauenbüro Urteile und Protokolle griechischer Gerichte vorgelegt, wonach dem Mann zunächst vorläufig, dann endgültig das Sorgerecht über die Tochter zugesprochen wurde. Sie bat um Unterstützung, da sie ein Verfahren wegen Kindesentführung gegen ihren früheren Ehemann anzustrengen beabsichtigte. Das Frauenbüro hielt sich für befugt festzustellen, ob der Betroffene noch in der Stadt wohne. Es habe dazu die Sorgerechtsbeschlüsse und Verhandlungsprotokolle an die Einwohnermeldebehörde weitergeleitet. Die Prüfung ergab, dass er seit einigen Jahren umgemeldet ist. Da die Gerichtsbeschlüsse Aussagen über einen Wohnsitz des Betroffenen in Griechenland enthielten, glaubte die Meldebehörde trotz Unzuständigkeit, sie müsse die Ausländerbehörde über diesen Sachverhalt informieren. Bei genauem Hinsehen hätte offenbar werden müssen, dass nach den beglaubigten Übersetzungen nur die Erklärung eines Zeugen Aussagen über den Wohnsitz enthielt.

Die Weitergabe der Sorgerechtsbeschlüsse an die Meldebehörde durch das Frauenbüro der Stadtverwaltung entbehrte einer Rechtsgrundlage. Es durfte diese Unterlagen nicht an die Meldebehörde weitergeben. Beschlüsse und Protokolle über Sorgerechtsverhandlungen enthalten regelmäßig zahlreiche private und familiäre Angaben zu den betroffenen Personen. Darüber hätte sich das Frauenbüro durchaus bewusst sein müssen. Sollte es – was bei dem gegebenen Verfahrensstand in Griechenland bereits sehr zweifelhaft ist – tatsächlich erforderlich gewesen sein, den Wohnsitz des Betroffenen festzustellen, hätte bei der zuständigen Meldebehörde am jetzigen Wohnort danach gefragt werden können, ohne irgendwelche Unterlagen beizufügen. Die in den Unterlagen enthaltene Aussage eines Zeugen (nicht – wie behauptet – eidesstattliche Erklärung des Betroffenen selbst) war eine Information, die die frühere Meldebehörde nicht speichert oder speichern darf, nachdem der Betroffene ordnungsgemäß am neuen Wohnsitz angemeldet war. Für die Weitergabe der Gerichtsurteile war weder eine vom Frauenbüro noch von der Meldebehörde zu erfüllende Aufgabe ersichtlich. Die Datenübermittlung war unzulässig, denn sie war zur rechtmäßigen Aufgabenerfüllung einer der beteiligten Stellen im Sinne des § 11 Abs. 1 Hessisches Datenschutzgesetz nicht erforderlich. Der Betroffene wurde in seinen datenschutzrechtlichen Belangen verletzt. Ich habe die Stadtverwaltung gebeten, die in Frage kommenden Mitarbeiterinnen des Frauenbüros zu informieren und auf die künftige Einhaltung datenschutzrechtlicher Bestimmungen hinzuweisen.

13.3
Erfassung von Auskunftssperren im Einwohnermelderegister

Jede beantragte Auskunftssperre muss sofort in das Einwohnermelderegister eingetragen werden, auch wenn sie ihre Wirksamkeit manchmal erst Jahre später entfalten soll.

Im Zusammenhang mit der Prüfung eines Einwohnermeldeamtes habe ich Folgendes festgestellt:

Bürgerinnen und Bürger, die eine Auskunftssperre wegen drohender Gefahr für Leben, Gesundheit oder persönliche Freiheit nach § 34 Abs. 5 Hessisches Meldegesetz (HMG) beantragen, widersprechen auch häufig Melderegisterauskünften in besonderen Fällen, wie z. B. gegenüber Adressbuchverlagen oder Parteien. Da eine Auskunftssperre nach § 34 Abs. 5 HMG jede Übermittlung der Daten an Dritte (ausgenommen Behörden) ausschließt, hatte das Einwohnermeldeamt darauf verzichtet, in solchen Fällen zusätzlich Widersprüche gegen Melderegisterauskünfte in besonderen Fällen nach § 35 Abs. 1 bis 4 in die Meldekartei aufzunehmen.

§ 34 Abs. 5 und 6 HMG

(5) Jede Melderegisterauskunft ist unzulässig, wenn Betroffene der Meldebehörde gegenüber das Vorliegen von Tatsachen glaubhaft gemacht haben, die die Annahme rechtfertigen, dass ihnen oder einer anderen Person hieraus eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange erwachsen kann.

(6) Die Auskunftssperre nach Abs. 5 endet mit Ablauf des dritten auf die Eintragung folgenden Kalenderjahres. Sie kann auf Antrag verlängert werden. Hierauf sind Betroffene hinzuweisen. Sie kann im Einzelfall widerrufen werden, wenn ein glaubhaft gemachtes rechtliches Interesse an der Melderegisterauskunft offensichtlich das Interesse Betroffener an der Auskunftssperre überwiegt. Sie kann auch widerrufen werden, wenn die Meldebehörde aufgrund nachträglich eingetretener oder nachträglich bekannt gewordener Tatsachen berechtigt wäre, die Eintragung der Auskunftssperre abzulehnen.

§ 35 HMG

(1) 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 Empfängerin oder der Empfänger hat die Daten spätestens einen Monat nach der Wahl zu löschen.

(2) Für Auskünfte an Träger für Abstimmungen, Bürger- und Volksbegehren gilt Abs. 1 entsprechend.

(3) Begehren Mitglieder gewählter staatlicher oder kommunaler Vertretungskörperschaften, Presse und Rundfunk eine Melderegisterauskunft über Alters- oder Ehejubiläen von Einwohnerinnen oder Einwohnern, so darf die Auskunft nur die in § 34 Abs. 1 Satz 1 genannten Daten Betroffener sowie Tag und Art des Jubiläums umfassen.

(4) Adressbuchverlagen darf Auskunft über

1. Vor- und Familiennamen
2. Doktorgrad und
3. Anschriften

sämtlicher Einwohnerinnen und Einwohner, die das achtzehnte Lebensjahr vollendet haben, erteilt werden.

(5) Betroffene haben das Recht, der Weitergabe ihrer Daten nach Abs. 1 bis 4 zu widersprechen. Sie sind bei der Anmeldung hierauf hinzuweisen.

...

Die lückenhafte Eintragung hatte zunächst keine Auswirkungen; es wurde jedoch nicht bedacht, dass Auskunftssperren wegen einer Bedrohung für Leben oder persönliche Freiheit nach § 34 Abs. 5 HMG zeitlich befristet sind (§ 34 Abs. 6 HMG). Diese Auskunftssperren enden mit Ablauf des dritten auf die Eintragung folgenden Kalenderjahres beziehungsweise nach einer beantragten Verlängerung. Zu diesem Zeitpunkt hat die Meldebehörde jedoch nur schwer beziehungsweise nicht mehr die Möglichkeit, festzustellen, ob und ggf. welche weiteren unbefristeten Auskunftssperren für Melderegisterauskünfte in besonderen Fällen seinerzeit beantragt wurden. Die entsprechenden Anträge befinden sich zwar in den Meldesachakten (sortiert nach Eingangsjahr und Anfangsbuchstabe des Namens), sind aber im Melderegister nicht vermerkt. Es besteht die Gefahr, dass sie nach Ablauf der Sperre nach § 34 Abs. 5 HMG nicht mehr berücksichtigt werden, da ein entsprechender Bezug nicht hergestellt werden kann.

Ich habe die Kommune darauf hingewiesen, dass beim Zusammentreffen von Auskunftssperren nach § 34 Abs. 5 HMG und Auskunftssperren nach § 35 Abs. 5 HMG alle Sperren in die elektronische Meldekartei eingetragen werden müssen. Für die Bereinigung der in der Vergangenheit nicht erfolgten Eintragungen habe ich der Kommune vorgeschlagen, die betroffenen Bürger nach Ablauf der Auskunftssperre nach § 34 Abs. 5 HMG darauf hinzuweisen, dass der Widerspruch nach § 35 Abs. 5 HMG versehentlich nicht berücksichtigt wurde und ggf. erneut zu beantragen ist.

14. Hochschulen

14.1
Evaluation der Lehre an hessischen Hochschulen

Für die Durchführung der Evaluation der Lehre an hessischen Hochschulen ist eine Hochschulsatzung notwendig.

14.1.1
Verwaltungsprogramm der Universität Kassel

Eine Anfrage der Verwaltung der Universität Kassel veranlasste mich, mir ein Verwaltungsprogramm näher anzuschauen, das zukunftsweisenden Charakter haben könnte. Das Dekanat der wirtschaftswissenschaftlichen Fakultät hatte ein multifunktionales Programm (Fachbereichs-Planungs-Systems, FPS) entwickelt und bereits zum Einsatz gebracht, das folgende Anwendungen vorsieht:

Erfassung aller dem Dekanat zugeordneten Studenten (Name, Matrikelnummer, Mail-Adresse), Erfassung der Anmeldungen zu Vorlesungen (wegen der Raumplanung) und der Anmeldung zu Prüfungsleistungen (Scheine usw.) sowie der Ergebnisse der Prüfungsleistung selbst.

Die letztgenannten Daten haben insoweit eine besondere Bedeutung, als die Prüfungsleistungen ab dem ersten Semester für die Abschlussprüfung erheblich sind und in manchen Studiengängen darauf angerechnet werden. Insoweit ist das Programm als papierlose Prüfungsdokumentation zu bewerten.

Die einzelnen Zugriffsrechte sind stark differenziert ausgestaltet, so haben z. B. auf die Prüfungsdaten nur der betroffene Student und die im Prüfungsverfahren beteiligten Hochschulmitarbeiterinnen und -mitarbeiter Zugriff.

Technisch war als Besonderheit u. a. vorgesehen, dass die Anmeldung von Studierenden zu Prüfungsleistungen automatisch mit der Teilnahme an einer Evaluation der Lehre an dieser Hochschule verbunden war. Zu diesem Zweck soll der Studierende sich zu einer Reihe von Beurteilungskriterien äußern, um die Qualifizierung der Vorlesungen der einzelnen Dozenten ermitteln zu können sollen. Gefragt wird u. a. nach der Verständlichkeit des Vorlesungsinhalts und der Verwendungseignung von verteilten Unterlagen. Die Antworten der Studierenden werden elektronisch zusammengeführt erfasst und für jeden Dozenten automatisiert ausgewertet. Dieser kann wiederum elektronisch freigeben, ob – neben ihm selbst – auch die Studierenden oder/und die übrigen Dozenten Zugriff auf die Auswertungen bekommen sollen. Nach verschiedenen Beschwerden veranlasste die Hochschulverwaltung das Dekanat, als technische Option einzurichten, dass der Student sich zu Prüfungsleistungen anmelden kann, auch wenn er an der Evaluation nicht teilnimmt.

Offen blieb die Frage, ob die Durchführung der Evaluation überhaupt zulässig war. Maßgebend ist § 3 Abs. 8 Hessisches Hochschulgesetz (HHG).

§ 3 Abs. 8 HHG

Die Leistungen der Hochschule in Forschung und Lehre, bei der Förderung des wissenschaftlichen Nachwuchses sowie bei der Durchführung der Gleichberechtigung von Frauen und Männern sollen regelmäßig bewertet und die Ergebnisse veröffentlicht werden. Das Präsidium regelt durch Satzung, welche personenbezogenen Daten zu diesem Zwecke erhoben, verarbeitet und in welcher Form veröffentlicht werden können.

Demnach setzt eine Befragung der Studenten zur Qualität der Lehre eine Satzung voraus, die Details zu den zu erhebenden Daten, zum Verfahren, zur Nutzung der Daten, zur Pseudonymisierung und zur Veröffentlichung festlegt. Eine solche Satzung lag zunächst nicht einmal als Entwurf vor. Das Dekanat musste das Modul zur Evaluation aus dem System solange herausnehmen, bis eine rechtsgültige und genehmigte Satzung vorliegt. Inzwischen hat das zuständige Hochschulgremium mit meiner datenschutzrechtlichen Begleitung eine Satzung beschlossen, die jedoch vom Hessischen Ministerium für Wissenschaft und Kunst noch nicht genehmigt worden ist.

14.1.2
Mustersatzung

Ich habe zudem unter zusätzlicher Beteiligung der Universität in Gießen selbst unter Ziff. 25.5 dieses Berichts eine Mustersatzung entworfen, die sowohl die Anforderungen an aussagefähige Evaluationsverfahren wie datenschutzrechtliche Anforderungen berücksichtigt. Das Ministerium hat ebenfalls einen Musterentwurf entwickelt. Die beiden Entwürfe unterscheiden sich vor allem darin, dass das Ministerium begrifflich offene Aussagen zu den Daten macht, die zur Evaluation erhoben und weiterverarbeitet werden dürfen. Der von mir verfasste Entwurf geht hingegen enumerativ vor, um normenklar festzustellen, „welche personenbezogenen Daten zu diesem Zweck erhoben, verarbeitet und in welcher Form veröffentlicht werden“ dürfen (so der Wortlaut des § 3 Abs. 8 Satz 2 HHG).

Da bis zum Redaktionsschluss für den 31. Tätigkeitsbericht kein Einvernehmen über eine gemeinsame Mustersatzung erzielt werden konnte, halte ich den eigenen Entwurf für die Hochschulen bereit.

14.2
Information der Hochschule durch Prüfungsämter

Das Hessische Justizprüfungsamt informiert regelmäßig die Studentensekretariate der Hochschule darüber, welche Jurastudentinnen und -studenten das erste Staatsexamen bestanden haben.

Die Eingabe eines Jurastudenten hatte die Frage zum Gegenstand, ob es datenschutzrechtlich zulässig ist, dass das Hessische Justizprüfungsamt, zuständig für die Durchführung des ersten juristischen Examens, den Studentensekretariaten in Listenform regelmäßig die Namen mit Matrikelnummer jener Kandidaten mitteilt, die das Examen bestanden beziehungsweise nicht bestanden haben. Die Annahme des Studenten, dass auch das Studentenwerk die Liste erhalte, stellte sich als Irrtum heraus. Der Planungs- und Organisationsauftrag der Hochschulen für das rechtswissenschaftliche Studium rechtfertigt die Übermittlung dieser Daten und deren weitere Verwendung in der Hoch-

schule. Die Kenntnis über das Bestehen beziehungsweise Nichtbestehen einer Abschlussprüfung ist zudem für die Entscheidung über die Exmatrikulation nach § 68 Hessisches Hochschulgesetz (HHG) von Bedeutung.

§ 68 HHG

(1) Mit Ablauf des Semesters, in dem das Zeugnis über die den Studiengang beendende Abschlussprüfung ausgehändigt wurde, erfolgt die Exmatrikulation, es sei denn, die Studierenden sind noch für einen anderen Studiengang immatrikuliert oder zur Promotion zugelassen. Mit der Exmatrikulation endet die Mitgliedschaft der Studierenden in der Hochschule.

(2) Studierende sind zu exmatrikulieren, wenn sie

1. dies beantragen,
2. sich nicht ordnungsgemäß zurückgemeldet haben ohne beurlaubt zu sein,
3. aufgrund eines fehlerhaften Zulassungsbescheids immatrikuliert worden sind und die Rücknahme des Zulassungsbescheids unanfechtbar geworden oder sofort vollziehbar ist,
4. bei der Rückmeldung den Nachweis über die bezahlten Beiträge für das Studentenwerk und die Studentenschaft nicht erbringen oder die Zahlung fälliger Gebühren nicht nachweisen,
5. bei der Rückmeldung die Erfüllung der Verpflichtungen nach dem Sozialgesetzbuch gegenüber der zuständigen Krankenkasse nicht nachweisen,
6. eine Vor-, Zwischen- oder Abschlussprüfung endgültig nicht bestanden haben.

(3) Wer innerhalb von zwei Jahren keinen in einer Prüfungs- oder Studienordnung vorgesehenen Leistungsnachweis erbringt, kann exmatrikuliert werden.

Hat eine Studentin oder ein Student das erste juristische Examen bestanden, ist sie beziehungsweise er von der Hochschule zu exmatrikulieren. Gleiches gilt, wenn die Prüfung endgültig nicht bestanden wurde. Würde die Hochschule den Prüfungsausgang nicht kennen, könnte mancher Studierende den auch mit Vorteilen versehenen Studentenstatus über die Prüfung hinaus nutzen. Dies soll verhindert werden.

14.3
Multifunktionale Chipkarte für Studierende an der Universität Gießen

Die Einführung der multifunktionalen Chipkarte an der Universität Gießen ist weitgehend abgeschlossen. Datenschutzrechtlich unzumutbare Risiken bestehen für den betroffenen Personenkreis nicht.

14.3.1
Sachstandsbericht

Die Justus-Liebig-Universität (JLU) ist die erste hessische Universität, die eine multifunktionale Chipkarte mit elektronischer Signatur einsetzt. Ich habe dieses Pilotprojekt datenschutzrechtlich begleitet. Bereits in meinem 30. Tätigkeitsbericht hatte ich über die geplante Einführung sowie die rechtlichen Voraussetzungen berichtet (30. Tätigkeitsbericht, Ziff. 2.3.1).

Bis zum Jahresende 2002 wurde jedem Studierenden ein Studienausweis in Form einer multifunktionalen Chipkarte ausgehändigt. Dieser ersetzt den bisher verwendeten Papierausweis. Neben einem Lichtbild und dem Namen, Vornamen und der Immatrikulationsnummer enthält der Ausweis zwei Mikroprozessoren, einen kontaktbehafteten mit Kryptoprozessor und den kontaktlos arbeitenden mit Mifare-Chip. Darüber hinaus ist auf der Karte ein Barcode angebracht. Im Gegensatz zu bisherigen Chipkartenprojekten wird an der JLU der Kryptoprozessor-Chip für die elektronische Signatur benutzt und gestattet dem Karteninhaber, sich im Internet zu authentisieren.

Durch das Land und den Bund wurde die Einführung der Chipkartenausweise mit einer finanziellen Unterstützung nach dem Hochschulbauförderungsgesetz (HBFG) im Umfang von 180.000 € gefördert. Nach Vorarbeiten wurde von der JLU im Dezember 2000 der Beschluss zur Einführung der Chipkarten gefasst. Die Auftragserteilung erfolgte nach der Begutachtung im HBFG-Verfahren und der Ausschreibung im Dezember 2001. Das Projekt wurde gefördert, weil die Karte elektronische Signaturen (mit höheren Kosten, aber auch erheblich erweitertem Anwendungsfeld) erlaubt. Die Chipkarten selbst (Erstausstattung 300.000 €) und Umrüstung des Kassensystems des Studentenwerks für die elektronische Geldbörse werden nicht bezuschusst. Die Studierenden müssen für die Chipkarte einen Pfandbetrag von 15 € hinterlegen.

Im Juni 2002 liefen erste Tests für die Kartenherstellung, weil die beteiligten Firmen und die Universität in größerem Umfang Neuland betraten. Insbesondere musste die Software im organisatorisch-betrieblichen Umfeld angepasst werden. So mussten im Studentensekretariat die Abläufe an die Programme der HIS GmbH angepasst und die Aufnahme

neuer Daten vorgesehen werden. Im Hochschulrechenzentrum musste die Software in die Benutzerverwaltung und den vorhandenen Verzeichnisdienst nach X.500/LDAP-Norm (Global Directory der Fa. Syntegra) eingebunden werden.

Um die geplanten Funktionen im Bereich der elektronischen Signatur sicherzustellen, war es nötig, für alle Studierenden zum Zeitpunkt der Chipkarten-Personalisierung eine E-Mail-Adresse festzulegen. Diese Adresse steht im so genannten Zertifikat (d. h. dem öffentlichen Teil des bei den elektronischen Signaturen verwendeten Schlüsselpaares) und muss durch eine Freischaltung des Chipkarten-Inhabers aktiviert werden.

Ab Juli 2002 wurden Chipkarten-Ausweise im Testbetrieb hergestellt, Ende August wurde mit der Produktion der Studienausweise aller Studierender begonnen. Die Ausgabe der Chipkartenausweise erfolgte bei der Rückmeldung zum Wintersemester ab 23. September 2002, soweit Ausweise schon abholbereit waren. Die Herstellung der mehr als 20.000 Ausweise wurde Mitte Dezember im Wesentlichen abgeschlossen. Zum Jahresende 2002 hatten 14.000 Studierende ihre Chipkarte abgeholt.

Das Jahr 2002 war geprägt durch den Termindruck, zum Wintersemester 2002/2003 den Chipkartenausweis in Betrieb zu nehmen. Die Personalisierung der Karten mit äußerem Aufdruck und die Bearbeitung der beiden Mikrochips erwies sich als aufwendiger als erwartet; sie erfordert eine DV-geschulte Fachkraft. Bei ca. 3 % der verwendeten Karten wird bei der Personalisierung ein Defekt festgestellt, solche Karten müssen ausgesondert werden. Für die Bearbeitung einer Chipkarte werden technisch insgesamt ca. sechs Minuten benötigt (Bild einscannen, Druckvorgang 1, Druckvorgang 2, PIN-Brief/Empfangsquittung erstellen); realistisch ist, im Mittel eher die doppelte Zeit pro Karte anzusetzen.

Mit Beginn der Kartenausgabe musste der wesentliche Teil der neuen Organisation bereitstehen. Nachdem 1.000 Karten ausgeben waren, wurden die ersten Verluste gemeldet und die Ausstellung von Ersatzkarten verlangt. An der JLU konnten die Studierenden über Webseiten im Internet Informationen über ihre Chipkarte erhalten, z. B. ob ihre Karte hergestellt werden kann oder noch etwas fehlt, abschließend wurde die Abholbereitschaft angezeigt. Die Sperre eines abhanden gekommenen Chipkartenausweises kann über das Internet veranlasst werden.

Ab 2003 werden den Studierenden die für die Chipkarte vorgesehenen Anwendungen zur Verfügung gestellt:

– Einrichtung einer E-Mail-Adresse ohne Hochschul-Account-Anmeldung (de facto wird die hochschul-externe private Mailadresse benutzt).
– Zugang zu universitäts-internen Daten und Nutzung von universitäts-lizenzierter Software,
– Datenbankzugriffe über das Internet, auch vom häuslichen Arbeitsplatz mit Authentisierung im Webserver beziehungsweise VPN-Server über die Chipkarte, gesichert durch PIN,
– sicherer Zugriff auf die eigenen Prüfungsergebnisse, soweit die Fachbereiche sich dem zentralen Prüfungsorganisationssystem angeschlossen haben,
– Rückmeldung über das Internet,
– bargeldloses Bezahlen von Kleinbeträgen im Hochschulumfeld (Mensen, Cafeterien, Bibliotheken, Hochschulrechenzentrum),
– Gebäude- beziehungsweise Raumzugang mittels Chipkarte in oder außerhalb der normalen Öffnungszeiten.

Für die Zukunft ist ein sukzessiver Abbau der Serverzugänge mit Kennung und Passwort zugunsten der Verwendung einer Chipkarte vorgesehen. Die Chipkartenverwendung ist an eine PIN gebunden.

Die E-Mail-Weiterleitung über eine persönliche (aber fiktive) Uni-Mailadresse zu der privaten Mailbox des Studierenden kann schon seit Dezember 2002 mittels Chipkarte von einem PC mit Chipkartenleser (in der Universität oder aus dem Internet) beantragt werden. Dazu muss der Studierende nichts weiter als seine private Mailadresse angeben. Die elektronische Signatur auf der Chipkarte gestattet die sichere Authentisierung. Es wird erwartet, dass mit dieser Funktion der Prozentsatz der Studierenden, der per E-Mail erreichbar ist, von derzeit 40 % auf 80 % ansteigen wird.

Für die Nutzung der Chipkarte im Internet wird erwartet, dass die Studierenden bereit sind, sich für den erhaltenen Service einen Chipkartenleser privat zu kaufen. Das Hochschulrechenzentrum verkauft dazu in seinem Shop Lesegeräte vom einfachen Modell bis zum (von den Banken für die Geldkarte) zugelassenen Spitzenmodell. Die Geräte werden zusammen mit der passenden PKI/Chipkarten-Software nur an Studierende und Mitarbeiter der Hochschule ausgegeben. Der Preis beträgt weniger als 50 % des Listenpreises (26 € für den Leser ohne eigene Tastatur). In der Universität werden alle PCs in den öffentlichen Pool-Räumen mit einem Chipkartenleser ausgestattet. Das verwendete mittlere Modell gestattet eine sichere PIN-Eingabe außerhalb des PCs über die Chipkartenleser-Nummerntastatur.

Im organisatorischen Bereich wird ab März 2003 sichergestellt, dass bei der Rückmeldung mittels PC und Chipkarte das auf der Chipkarte gespeicherte, nur ein Semester gültige Zertifikat ausgetauscht wird. Ohne gültiges Zertifikat weisen Webserver und die bekannten Programme Outlook, Outlook Express, Netscape und Mozilla die Authentisierung

mittels Chipkarte zurück. Um das Zertifikat für das nächste Semester zu übernehmen, benötigt der Studierende nur den Chipkartenleser. Er muss die Hochschule nicht mehr persönlich aufsuchen. Die Chipkarten werden ohne den bei der Rückmeldung vorgenommenen Zertifikatswechsel elektronisch ungültig. Aus praktisch-betrieblichen Gründen kann der Zertifikatsaustausch auch zu jedem späteren Zeitpunkt nachgeholt werden.

Die Universität betreibt für die Chipkarten aus Kostengründen eine eigene Zertifizierungsinstanz. Sie ist von der Zertifizierungsinstanz des Deutschen Forschungsnetzes zertifiziert. Die von der eigenen Certification Authority (CA) hergestellten Zertifikate sind nicht signaturgesetz-konform. Die Chipkarte kann aber technisch weltweit eingesetzt werden und verwendet Hard- und Software, wie sie auch bei signaturgesetz-konformen Lösungen verwendet wird. In der Universitätssatzung zur Chipkarte ist geregelt, dass die elektronische Signatur innerhalb der Hochschule (insbesondere zwischen Studierenden und der Verwaltung) verbindlich anerkannt wird.

Organisatorisch müssen neben dem halbjährlichen Zertifikatswechsel bei etwa 15.000 Chipkarten noch die Herstellung von jährlich ca. 5.000 neuen Chipkarten für Ersteinschreiber und ca. 500 Ersatzkarten wegen Kartenverlustes oder technischer Defekte bewältigt werden. Dabei müssen die 5.000 neuen Karten in einer vergleichsweise kurzen Zeit zu Beginn des Semesters bereitgestellt werden, weil in Zukunft eine Reihe von Anwendungen sofort benutzt werden (z. B. bargeldloses Bezahlen in der Mensa, Informationszugang im Hochschulbereich).

Es wird erwartet, dass die Chipkarte der Studierenden in absehbarer Zeit auch den Mitarbeitern der Universität zur Verfügung gestellt wird. Anstelle der Gruppenkennung „Studierender (1)“ und der Matrikelnummer tritt nur die Gruppenkennung „Mitarbeiter (2)“ und die Personalnummer. Die Festlegung der Ausweisnummern-Struktur wurde mit den Bibliotheksverbund für die Hochschulen des Landes Hessen einheitlich festgelegt.

Informationen zur Chipkarte der **J**ustus-**L**iebig-**U**niversität Gießen (**JLU**-Card) sind zu finden unter http://www.uni-giessen.de/chipkarte/.

Diese Information umfasst allgemeine Angaben zur Chipkarte als auch solche für den Betrieb (Statusanzeige, Sperrantrag, Anleitung zur Installation von Chipkartenleser-Software usw.)

14.3.2
Datenschutzrechtliche Bewertung

Die datenschutzrechtliche Bewertung stützt sich auf die folgenden Säulen:

– die Vorabkontrolle

– die Satzung

– das Verfahrensverzeichnis

– das Informationsblatt.

Der Einsatz von Chipkarten stellt besondere Anforderungen an den Datenaustausch. Deshalb hatte ich im Vorfeld folgende Forderungen formuliert:

1. Transparenz für den Nutzer über seine gespeicherten personenbezogenen Daten, ausreichende Zahl von Lesegeräten,
2. umfangreiche Informationen der Nutzer über ihre Rechte und die Möglichkeit der Wahrnehmung,
3. klare Beschreibung aller technischen Details des Verfahrens.

Diesen Anforderungen wurde der Entwurf der umfangreichen Vorabkontrolle, die Satzung und das ausführliche Informationsblatt gerecht. Die Vorabkontrolle beinhaltet Informationen über

1. datenverarbeitende Stellen,
2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung,
3. Art der gespeicherten Daten,
4. Kreis der Betroffenen,
5. Art regelmäßig übermittelter Daten, deren Empfänger sowie Art und Herkunft regelmäßig empfangener Daten,
6. zugriffsberechtigte Personen und Personengruppen,
7. technische und organisatorische Maßnahmen nach § 10 HDSG,
8. Technik des Verfahrens,
9. Fristen der Löschung,
10. Prüfung auf Zweckbestimmung, Rechtsgrundlage, Datensparsamkeit,
11. Prüfung, ob die Rechte der Betroffenen nach § 8 HDSG gewährleistet sind.

Ausführlich wird das Missbrauchsrisiko und die Beurteilung der Folgen der missbräuchlichen Nutzung beleuchtet. Die Satzung, die in Zusammenarbeit mit mir erarbeitet wurde, ist am 19. November 2002 verabschiedet worden. Das Kurzinformationsblatt für die Studenten enthält alle erforderlichen Informationen klar und übersichtlich. Die Vorabkontrolle wurde auf Anregung des internen Datenschutzbeauftragten in einigen Punkten ergänzt. Für den betroffenen Personenkreis sind keine unzumutbaren Risiken zu erkennen. In diesem Jahr werde ich prüfen, ob alle vorgesehenen Maßnahmen umgesetzt sind.

15. Schulverwaltung und Schulen

15.1
Ergebnisse der Prüfung eines staatlichen Schulamtes

Auch Fach- und Rechtsaufsichtsbehörden für Schulen, wie staatliche Schulämter, sind nicht frei von verbreiteten datenschutzrechtlichen Mängeln in der Verwaltung.

Im Juni 2002 stattete ich dem staatlichen Schulamt Fulda einen Prüfbesuch ab. Die wesentlichen Ergebnisse der Prüfung stelle ich kurz dar, da ich annehme, dass ähnliche Mängel auch bei anderen Stellen auftreten.

15.1.1
Vorabkontrolle und Verfahrensverzeichnis

Das Schulamt setzt Verwaltungsprogramme ein, die zum Beispiel die Kontrolle der Arbeitszeit (Chipkarte) und Abrechnung der Telefonkosten steuern. Für diese neuen Programme ist – seit Geltung des neuen Hessischen Datenschutzgesetzes (HDSG) – eine so genannte Vorabkontrolle nach § 7 Abs. 6 HDSG und ein Verfahrensverzeichnis nach § 6 HDSG notwendig.

Da weder eine Vorabkontrolle noch ein Verfahrensverzeichnis vorlagen, habe ich das Schulamt gebeten, dieses nachzuholen.

§ 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.

§ 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.

15.1.2
Informationspflicht

Eine Prüfung der verwendeten Datenerhebungsformulare (zum Beispiel Personaldaten) ergab, dass die in § 12 Abs. 4 HDSG vorgesehenen Informationen fehlten.

§ 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 aufgrund 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.

Zwar sieht diese Vorschrift für die Aufklärung nicht die Schriftform vor, diese stellt aber regelmäßig die „geeignete Weise“ dar. Deshalb habe ich um entsprechende Ergänzung der Formulare gebeten.

15.1.3
Aufbewahrungsfristen

Für einen Teil der Altakten waren die von Gesetzen oder Erlassen vorgegebenen Aufbewahrungsfristen abgelaufen, ohne dass sie dem zuständigen hessischen Staatsarchiv zur eventuellen Archivierung angeboten worden waren. Dies fordert jedoch § 10 Abs. 1 Hessisches Archivgesetz (HArchivG).

§ 10 Abs. 1 HArchivG

Die in § 6 genannten Stellen sind verpflichtet, alle Unterlagen, die zur Erfüllung ihrer Aufgaben nicht mehr erforderlich sind, unverzüglich auszusondern und dem zuständigen Archiv zur Übernahme anzubieten. Dies soll im Regelfall 30 Jahre nach Entstehung der Unterlagen erfolgen. Anzubieten sind auch Unterlagen, die besonderen Rechtsvorschriften über Geheimhaltung oder über den Datenschutz unterworfen sind. Unberührt bleiben gesetzliche Vorschriften über die Löschung oder Vernichtung unzulässig erhobener oder verarbeiteter Daten oder Unterlagen.

Ich habe das Schulamt gebeten, Aussonderung und Anbietung der Unterlagen nachzuholen.

15.1.4
Aufbewahrung von Personalakten

Die Personalakten der vom Schulamt betreuten Lehrkräfte befanden sich in einem nicht abschließbaren, offenen Schrank. § 10 Abs. 3 HDSG verlangt jedoch Maßnahmen, die den Zugriff Unbefugter auch bei der Aufbewahrung der Unterlagen verhindern.

§ 10 Abs. 3 HDSG

Werden personenbezogene Daten nicht automatisiert verarbeitet, dann sind insbesondere Maßnahmen zu treffen, um den Zugriff Unbefugter bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung zu verhindern.

Für Personalakten ist standardmäßig ein abschließbarer Schrank zu verlangen. Das Schulamt sagte zu, im Rahmen der bevorstehenden Neugestaltung der räumlichen Unterbringung dieser Forderungen gerecht zu werden.

15.1.5
Datensicherheitsmaßnahmen

Da dem Amt wegen der räumlichen Zusammenlegung mit drei Studienseminaren eine künftige Neustrukturierung der Informationstechnik und des Netzes bevorstand, habe ich mich insoweit auf Hinweise hinsichtlich der Einhaltung der Forderungen nach Datensicherheitsmaßnahmen aus den üblichen Regelwerken (z. B. BSI-Grundschutzhandbuch) beschränkt.

15.2
Datenschutz in Schulen

Das Thema Datenschutz in Schulen ist jetzt auf meiner Homepage verfügbar. Auf diesem Weg stehen Schulen und Schulaufsicht ständig aktualisierte Informationen zur Verfügung.

Das Thema „Datenschutz in Schulen“ geht Schulleiter, schulische Datenschutzbeauftragte und Schulaufsichtsbehörden gleichermaßen etwas an. Dieser Kreis kann aber nur langsam durch Schulungen und Informationsmaterial über die rechtlichen Besonderheiten, Neuerungen etc. aktuell und laufend informiert werden. Um den Interessierten den schnellen Zugriff auf grundsätzliche Aussagen zu ermöglichen, habe ich meine Homepage um das Thema „Datenschutz in Schulen“ ergänzt. Verfügbar ist neben der allen hessischen Schulen schon vorliegenden Broschüre „Daten-

schutz in Schulen“ und den internen Dienstanweisungen des Hessischen Landesinstituts für Pädagogik zum Datenschutz eine Zusammenstellung von Informationen, die gerade dem schulischen Datenschutzbeauftragten die Arbeit erleichtern sollen. Neben der Aufzählung seiner Aufgaben und den häufig anzutreffenden Mängeln an Schulen kann auf die einschlägigen schulrechtlichen Normen zurückgegriffen werden.

Die zunehmende Nutzung des Internets in der hessischen Schulverwaltung wirft eine Vielzahl von Rechtsfragen auf, die in einem Grundsatzpapier des Hessischen Kultusministeriums weitgehend dargestellt worden sind. Dieses ist auf der Internetseite verfügbar, ebenso ein Muster für eine Nutzungsordnung der Schulleitung für die Computereinrichtungen an Schulen. Hier wird beispielsweise als Regelung empfohlen, den Schülerinnen und Schülern diese Internet-Nutzung nur zu schulischen Zwecken zu erlauben. Die weitergehende Nutzung auch zu privaten Zwecken würde die Anwendung des Teledienstegesetzes auf dieses Nutzungsverhältnis bewirken.

Eine permanente Aktualisierung und Ergänzung dieses Themenbereiches ist angestrebt. Der regelmäßige Zugriff darauf ist also allen empfohlen, die sich mit dem Thema „Datenschutz in Schulen“ auseinandersetzen müssen. Die direkte Internetadresse lautet http://www.datenschutz.hessen.de\F06t63.htm.

16. Archivwesen

Ergebnisse der Prüfung eines Staatsarchives

Bei hessischen Staatsarchiven liegt ein Schwerpunkt datenschutzrechtlicher Verantwortung bei der Sicherheit des Archivgutes.

Eine Prüfung des Hessischen Staatsarchivs in Marburg hinterließ den Gesamteindruck einer weitgehend korrekten Beachtung datenschutzrechtlicher Vorschriften.

Die wesentlichen angetroffenen Mängel beschränken sich auf folgende Punkte:

16.1
Vorabkontrolle

Die Archivverwaltung benutzt verschiedene elektronische Datenbanken wie die Benutzerkartendatei, die Telefonverbindungsdatei und die Arbeitszeitkontenverwaltung, die erst nach dem 10. November 1998 eingeführt wurden. Das seit diesem Tag geltende neue Hessische Datenschutzgesetz (HDSG) erfordert jedoch in § 7 Abs. 6 eine so genannte Vorabkontrolle vor dem Einsatz solcher Verwaltungsprogramme.

§ 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.

Die Vorabkontrolle war nicht durchgeführt worden.

Die Archivverwaltung sagte mir zu, die notwendigen Vorabkontrollen nachzuholen und die Vorschrift auch bei einer künftigen wesentlichen Verfahrensänderung oder der Einführung eines neuen Verfahrens zu beachten.

16.2
Information der Nutzer

Vor der erstmaligen Nutzung des Archivs füllt der Benutzer zunächst ein Formular aus, das verschiedene Informationen über ihn abfragt (Name, Vorname usw.). Das Formular enthielt nur einen Teil der Informationen, die die Verwaltung den Betroffenen bei der Datenerhebung zukommen lassen muss, wie es § 12 Abs. 4 HDSG vorsieht. So fehlten beispielsweise die Hinweise auf die rechtliche Auskunftspflicht nach der Benutzungssatzung und auf die Rechte nach § 8 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 aufgrund 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.

§ 10 Abs. 3 HDSG

Werden personenbezogene Daten nicht automatisiert verarbeitet, dann sind insbesondere Maßnahmen zu treffen, um den Zugriff Unbefugter bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung zu verhindern.

Die Verwaltung sagte mir eine Überarbeitung des Formulars zu.

16.3
Räumliche Sicherheit

Im Erdgeschoss des Archivs bestand eine erhebliche Einbruchsgefahr vom öffentlichen Straßenraum aus, weil die Fenster nur aus einfacher Standardverglasung bestanden und eine Alarmanlage fehlte. Gerade für Archive hat die Sicherung des gesamten, auch personenbezogenen Archivgutes gegen Einbruch eine besondere Bedeutung. Eine Behörde hat alle angemessenen technischen und organisatorischen Maßnahmen zu ergreifen, um den Datenbestand vor dem Zugriff Unbefugter zu bewahren. Dies sieht § 10 Abs. 3 HDSG vor.

Mit der Archivleitung wurde dies besprochen.

Da dem Archiv aus anderen Gründen größere Umbauarbeiten bevorstanden, wurde versichert, dass umgehend im Erdgeschossbereich eine entsprechende Sicherheitsverglasung eingesetzt wird.

17. Gesundheitswesen

17.1
Wiesbadener Forum Datenschutz: Gesundheitssystem und Datenschutz

Auf dem 11. Wiesbadener Forum Datenschutz wurde über die datenschutzrechtlichen Aspekte der vielfältigen – teils bereits umgesetzten – Reformüberlegungen im Gesundheitsbereich diskutiert. Die Ausgestaltung der Reformen ist auch für die Entwicklung des Patientendatenschutzes von zentraler Bedeutung.

Seit Jahren wird über Reformen der gesetzlichen Krankenversicherung diskutiert. Zahlreiche Modellvorhaben laufen, gesetzliche Regelungen wurden bereits verabschiedet, weitere sind geplant. Die Reformen betreffen stets auch Umfang, Zweck und Art und Weise der Verarbeitung personenbezogener sensitiver Daten der Versicherten. Etwa 90 % der Bevölkerung Deutschlands gehören der gesetzlichen Krankenversicherung an und sind damit von den Reformen betroffen. Vor diesem Hintergrund ist es eine für die Entwicklung des Patientendatenschutzes wesentliche Frage, ob für die Reformen datenschutzgerechte Modelle entwickelt werden und das Vertrauensverhältnis zwischen Patient und Arzt aufrechterhalten wird.

Das am 19. September 2002 vom Präsidenten des Hessischen Landtags und mir gemeinsam veranstaltete 11. Forum Datenschutz zum Thema „Gesundheitssystem und Datenschutz“ hat insbesondere drei aktuelle Schwerpunkte der Reformdiskussion aufgegriffen:

– **Zentraler Datenpool in der gesetzlichen Krankenversicherung**

  Die Verwendung der verfügbaren Mittel in der gesetzlichen Krankenversicherung ist gegenwärtig nicht transparent. Es gibt keine valide Datenbasis für eine Analyse der Mittelverwendung und deswegen keine zielgerichtete Systemsteuerung. Zur Herstellung von Transparenz wird vom Bundesgesundheitsministerium eine sektoren- und kassenübergreifende Zusammenführung der Leistungs- und Abrechnungsdaten der Versicherten in einem zentralen Datenpool angestrebt (zu den Einzelheiten s. Ziff. 17.2). Aus datenschutzrechtlicher Sicht bedürfen Umfang, Zweck und Organisation des Datenpools der Klärung. Die Reidentifizierung von Versicherten muss sicher ausgeschlossen werden.

– **Einführung elektronischer Gesundheitskarten als Krankenversichertenkarte der zweiten Generation**

  Die vom Bundesgesundheitsministerium für diese Legislaturperiode geplante elektronische Gesundheitskarte soll eine Chipkarte mit Mikroprozessor sein und verschiedene Funktionen erfüllen. Insbesondere ist vorgesehen, dass die Chipkarte Speicher für Notfallinformationen, Arztbriefe, Arzneimitteldokumentation und elektronisches Rezept (s. BTDrucks. 14/8255) sein soll. Der Einsatz der Gesundheitskarte soll zunächst freiwillig sein. Unklar ist allerdings bisher, worauf sich die freie Entscheidung der Versicherten beziehen wird. Es darf auf keinen Fall dazu kommen, dass der Versicherte rechtlich oder faktisch gezwungen ist, seine medizinischen Daten überall im Gesundheitssystem pauschal zu offenbaren. Die technische Ausgestaltung der Chipkarte muss eine differenzierte

Kommunikation im Gesundheitsbereich ermöglichen, wie sie auch unter den gegenwärtigen Rahmenbedingungen selbstverständlich ist.

– **Einführung strukturierter Behandlungsprogramme bei den Krankenkassen**

  Im Dezember 2001 hat der Bundestag das Gesetz zur Reform des Risikostrukturausgleichs in der gesetzlichen Krankenversicherung verabschiedet. Durch die neuen Regelungen soll u. a. die Versorgung chronisch kranker Versicherter verbessert werden. Zu diesem Zweck soll die Durchführung strukturierter Behandlungsprogramme (sog. Disease-Management-Programme) im Risikostrukturausgleich unter den Krankenkassen finanziell gefördert werden. Verantwortlich für die Durchführung der Programme sind die Krankenkassen. Sie erhalten dafür von den Kassenärztlichen Vereinigungen erstmals detaillierte personenbezogene medizinische Daten der Patienten. Die Neuregelungen werfen nicht nur Fragen hinsichtlich der künftigen Abgrenzung der Aufgaben auf, sondern berühren auch die Befugnisse zur Verarbeitung personenbezogener Patientendaten der Ärzte einerseits und der Krankenkassen andererseits (s. Ziff. 17.3).

Auf dem Forum wurden die datenschutzrechtlichen Konsequenzen der Reformüberlegungen aus verschiedenen Perspektiven intensiv diskutiert. Die Vorträge und Diskussionsbeiträge werden als Tagungsband im NOMOS-Verlag veröffentlicht.

17.2
Aufbau eines zentralen Datenpools in der gesetzlichen Krankenversicherung

Durch einen zentralen Datenpool soll in der gesetzlichen Krankenversicherung Transparenz des Leistungsgeschehens hergestellt werden. Umfang, Zweck und Organisation des geplanten Datenpools im Einzelnen sind noch klärungsbedürftig. In jedem Fall muss eine Reidentifizierung von Versicherten sicher ausgeschlossen werden.

Wegen der finanziellen Probleme in der gesetzlichen Krankenversicherung wird bereits seit Jahren darüber diskutiert, wie mehr Transparenz des gesamten Leistungsgeschehens hergestellt werden kann. Etwa 140 Mrd. Euro werden derzeit jährlich von den gesetzlichen Krankenkassen aufgewandt. Durch die getrennte Letzterfassung der Leistungs- und Abrechnungsdaten bei den ca. 400 Krankenkassen einerseits und der ärztlichen beziehungsweise zahnärztlichen Leistungsdaten bei den 23 Kassenärztlichen beziehungsweise Kassenzahnärztlichen Vereinigungen andererseits ist die Verwendung der Ausgaben derzeit nicht transparent. Eine sektoren- und kassenübergreifende Zusammenführung von Leistungs- und Abrechnungsdaten für systematische übergreifende Analysen des Versorgungsgeschehens ist gegenwärtig nicht zugelassen. Deswegen hat die 73. Gesundheitsministerkonferenz die Bundesregierung aufgefordert, ein Datentransparenzgesetz für die gesetzliche Krankenversicherung zu erarbeiten, damit die im System vorhandenen Daten in einer geeigneten Form erfasst, aufbereitet, zusammengeführt und ausgewertet werden können.

Nach intensiven vorangegangenen Diskussionen hat das Bundesgesundheitsministerium (BMG) im Januar 2002 einen Workshop mit den Spitzenverbänden der Krankenkassen, der Kassenärztlichen Bundesvereinigung und der Deutschen Krankenhausgesellschaft sowie den Datenschutzbeauftragten veranstaltet, um ein Konzept für ein Datentransparenzgesetz zu erarbeiten. Vom BMG wird eine sektoren- und kassenübergreifende Zusammenführung der Leistungs- und Abrechnungsdaten der Versicherten in einem zentralen Datenpool bei einer sog. Datenaufbereitungsstelle angestrebt. Die Datenaufbereitungsstelle soll die ihr übermittelten Daten speichern und für die verschiedenen Zugriffsberechtigten zur Auswertung zur Verfügung stellen. Auf diese Weise soll eine valide Datenbasis für eine zielgerichtete Systemsteuerung durch Selbstverwaltung, Politik auf Bundes- und Landesebene, Gesundheitsberichterstattung und Forschung aufgebaut werden.

Zu dem nach dem Workshop vom BMG entwickelten Konzept habe ich – wie auch andere Datenschutzbeauftragte – Stellung genommen. Das Ziel der Reformüberlegungen wird von mir und meinen Kollegen nicht in Frage gestellt. Sorgfältig geprüft werden muss aber die Frage, in welchem Umfang, zu welchem Zweck und in welchem Verfahren die Versichertendaten konkret verarbeitet werden dürfen. Bei den Abrechnungs- und Leistungsdaten der Versicherten handelt es sich um sehr sensitive medizinische Daten von ca. 70 Millionen Bürgerinnen und Bürgern. Übereinstimmend mit meinen Kollegen habe ich daher insbesondere die folgenden Anforderungen an den Aufbau eines Datenpools gestellt:

– Personenbezogene Versichertendaten sind zu pseudonymisieren. Eine Reidentifizierung von Versichertendaten – durch ein technisch unzureichendes Pseudonymisierungsverfahren oder etwa auch durch zu umfangreiche Datensätze – muss sicher ausgeschlossen sein.

– Die Pseudonymisierung muss durch unabhängige, rechtlich selbständige Stellen nach § 35 SGB I erfolgen. Pseudonymisierungsstelle (Vertrauensstelle) und Datenaufbereitungsstelle müssen räumlich, organisatorisch und personell von den Krankenkassen und deren Verbänden, den Kassenärztlichen Vereinigungen und der Kassenärztlichen Bundesvereinigung sowie sonstigen abrufberechtigten Stellen getrennt sein.

– Die Zwecke der Datenaufbereitung und die Zugriffsberechtigung sind abschließend im Gesetz festzulegen.

– Für die Vertrauensstellen und die Datenaufbereitungsstelle ist die öffentlich-rechtliche Rechtsform vorzusehen.

Wesentliche Punkte dieser Forderungen sind in das derzeitige Konzept des BMG eingeflossen. Das Konzept bedarf jedoch noch einer Konkretisierung. Insbesondere sind die folgenden Punkte aus meiner Sicht noch klärungsbedürftig:

– **Notwendigkeit einer zentralen Speicherung der Daten aller Versicherten**

  Es sollte zunächst geprüft werden, ob die angestrebten Ziele auch bei einer Beschränkung der Datenerhebungen auf Stichproben erreicht werden können.

– **Datensatz für die zentrale Speicherung**

  Unklar ist noch, welche Daten für den Aufbau eines zentralen Datenpools gespeichert werden sollen. Der Datensatz muss sich strikt am Erforderlichkeitsgrundsatz orientieren. Es muss Reidentifizierungsrisiken ausschließen.

– **Organisation und Verfahren der Datenzusammenführung und -auswertung im Einzelnen**

  Geklärt werden muss insbesondere, welche Stellen die Aufgaben der Vertrauensstelle und der Datenaufbereitungsstelle wahrnehmen. Auch das technische Verfahren der Pseudonymisierung ist noch nicht festgelegt.

– **Nutzungsberechtigte des Datenpools**

  Es muss rechtsverbindlich festgelegt werden, welche Stellen in welchem Umfang und in welchem Verfahren die Berechtigung zum Zugriff auf den Datenbestand erhalten.

Wenn das BMG sein Konzept konkretisiert hat, werde ich erneut zu der Thematik Stellung nehmen.

17.3
Einführung von Disease-Management-Programmen durch die gesetzliche Krankenversicherung

Die Krankenkassen erhalten für die Durchführung der neuen strukturierten Behandlungsprogramme umfangreiche und detaillierte medizinische Daten chronisch kranker Patientinnen und Patienten. Für welche Zwecke diese Daten genau verwendet werden, bedarf noch der Klärung.

Im Dezember 2001 hat der Bundestag das Gesetz zur Reform des Risikostrukturausgleichs in der gesetzlichen Krankenversicherung verabschiedet (BGBl. I S. 3465). Durch die neuen Regelungen soll u. a. die Versorgung chronisch kranker Versicherter verbessert werden. Zu diesem Zweck soll die Durchführung strukturierter Behandlungsprogramme für chronisch Kranke (so genannter Disease-Management-Programme, DMP) im Risikostrukturausgleich zwischen den Krankenkassen finanziell gefördert werden. Verantwortlich für die Einführung und Durchführung der DMP sind die Krankenkassen. Die Behandlungen der chronisch Kranken, die sich in ein strukturiertes Behandlungsprogramm einschreiben, sind besonders zu dokumentieren und zu evaluieren. Den Krankenkassen werden in diesem Zusammenhang neue Befugnisse zur Verarbeitung personenbezogener medizinischer Versichertendaten eingeräumt:

– Gemäß § 284 Abs. 1 Ziff. 11 Sozialgesetzbuch (SGB) V sind die Krankenkassen jetzt befugt, zur Gewinnung von Versicherten, der Vorbereitung und der Durchführung von strukturierten Behandlungsprogrammen personenbezogene Versichertendaten zu erheben.

– Gemäß § 295 Abs. 2 SGB V sind die Kassenärztlichen Vereinigungen verpflichtet, die Daten zu den strukturierten Behandlungsprogrammen und über die von den Ärzten abgerechneten Leistungen (die sonst fallbezogen, nicht versichertenbezogen an die Krankenkassen übermittelt werden) versichertenbezogen zu übermitteln.

Zunächst ist die Einführung von strukturierten Behandlungsprogrammen für Diabetes mellitus Typ 1 und 2, chronische Atemwegserkrankungen, Brustkrebs und koronare Herzkrankheiten vorgesehen. Die im Rahmen strukturierter Behandlungsprogramme für Diabetes mellitus Typ 2 und Brustkrebs zu erhebenden Daten werden in den Anlagen 2 und 4 der Vierten Verordnung zur Änderung der Risikostruktur-Ausgleichsverordnung (RSAV) konkretisiert (BGBl. 2002 I S. 2286 ff.). Trotz kritischer Stellungnahmen von an-deren Datenschutzbeauftragten und mir ist es bedauerlicherweise in § 28f Abs. 3 RSAV bei der Regelung geblieben, dass die Krankenkassen dann alle umfangreichen Daten als Anlage 2a und 4a erhalten, wenn die Durchführung der strukturierten Behandlungsprogramme ohne Beteiligung der Kassenärztlichen Vereinigungen erfolgt. Für diesen Fall ist allerdings aufgrund der geäußerten Kritik vorgesehen worden, dass die Teilnehmer an den strukturierten Behandlungsprogrammen in jede einzelne Übermittlung ihrer Gesundheitsdaten, die vom Arzt beziehungsweise von der Ärztin oder anderen Leistungserbringern an die Krankenkasse erfolgt, gesondert schriftlich einwilligen müssen. Dadurch wird sichergestellt, dass die Betroffenen vorher informiert werden, welche sensiblen Patientendaten unmittelbar an die Krankenkasse weitergegeben werden. Die Patientinnen und Patienten werden sich so der Bedeutung der Übermittlung ihrer Gesundheitsdaten bewusst.

In § 28d Abs. 1 RSAV sind die Anforderungen und Voraussetzungen am Verfahren der Einschreibung der Versicherten in ein strukturiertes Behandlungsprogramm einschließlich der Dauer der Teilnahme festgelegt. Unter datenschutzrechtlichen Aspekten ist insbesondere hervorzuheben, dass Verträge über ein strukturiertes Behandlungsprogramm nur dann genehmigt werden, wenn sie vorsehen, dass die Versicherten in die Teilnahme einwilligen, über Programminhalte und die Verarbeitung ihrer personenbezogenen Daten informiert werden und ihre Einwilligung schriftlich bestätigen.

§ 28d Abs. 1 RSAV

...

2. nach § 137f Abs. 3 des Fünften Buches Sozialgesetzbuch in die Teilnahme einwilligt und
3. über die Programminhalte, insbesondere auch darüber, dass zur Durchführung des strukturierten Behandlungsprogramms Befunddaten an die Krankenkasse übermittelt werden und diese Daten von der Krankenkasse zur Unterstützung der Betreuung des Versicherten im Rahmen des strukturierten Behandlungsprogramms verarbeitet und genutzt werden können, die Aufgabenteilung zwischen den Versorgungsebenen und die Versorgungsziele, die Freiwilligkeit der Teilnahme am Programm und die Möglichkeit des Widerrufs der Einwilligung sowie über seine im Programm aufgeführten Mitwirkungspflichten zur Erreichung der Ziele und darüber, wann eine fehlende Mitwirkung das Ende der Teilnahme an dem Programm zur Folge hat, informiert wird und diese Information schriftlich bestätigt.

Zu diesen Regelungen ist zugleich festgelegt, dass die an die Krankenkassen übermittelten personenbezogenen Versichertendaten ausschließlich für die Durchführung der strukturierten Behandlungsprogramme verwendet werden dürfen. Dies entspricht einer Forderung der Datenschutzbeauftragten. Ungeachtet dessen besteht jedoch nach wie vor Klärungsbedarf, in welchem Umfang und zu welchen Zwecken im Einzelnen die personenbezogenen Versichertendaten bei den Krankenkassen verarbeitet werden sollen. Die Neuregelungen werfen Fragen hinsichtlich der künftigen Abgrenzung der Aufgaben und Befugnisse zur Verarbeitung personenbezogener Patientendaten der Ärzte einerseits und der Krankenkassen andererseits auf. Ziel der Kassen ist es, detaillierte medizinische personenbezogene Daten zur Steuerung der Behandlungsprogramme zu erhalten. Die individuelle Therapieentscheidung soll allerdings nach wie vor dem behandelnden Arzt oder der behandelnden Ärztin obliegen.

Sobald 2003 strukturierte Behandlungsprogramme in Hessen durchgeführt werden, werde ich stichprobenhaft bei den Krankenkassen überprüfen, ob die medizinischen personenbezogenen Versichertendaten ausschließlich für die Durchführung der strukturierten Behandlungsprogramme verwendet werden, die Rechte der Versicherten gewahrt und die rechtlichen Vorgaben eingehalten werden.

17.4
Medizinalkartei der Gesundheitsämter

Durch die Beschwerde eines Arztes bin ich darauf aufmerksam geworden, dass die bei den hessischen Gesundheitsämtern nach dem Gesetz über die Vereinheitlichung des Gesundheitswesens vorhandene Medizinalkartei unterschiedlich geführt und gepflegt wird.

17.4.1
Die Beschwerde des Arztes

Ein Arzt hatte vom Gesundheitsamt des Landkreises Offenbach ein Schreiben erhalten, in dem er gebeten wurde, eine beigefügte Meldekarte ausgefüllt zurückzusenden. Der Arzt sollte Angaben über den Beschäftigungsort machen, eine Meldebestätigung seines Erstwohnsitzes beifügen und in Fotokopie die Approbationsurkunde, Promotionsurkunde und Facharztanerkennung übersenden. Dagegen erhob der Arzt Einwände und bat mich um eine datenschutzrechtliche Klärung.

17.4.2
Verpflichtung der Gesundheitsämter zur Führung der Medizinalkartei

Bei der Medizinalkartei handelt es sich um eine bei den Gesundheitsämtern manuell geführte Kartei. Die Verpflichtung zur Erhebung der Daten ergibt sich aus § 1 Abs. 1 der Dritten Durchführungsverordnung zum Gesetz über die Vereinheitlichung des Gesundheitswesens (Dienstordnung für die Gesundheitsämter).

Dritte Durchführungsverordnung zum Gesetz über die Vereinheitlichung des Gesundheitswesens (Dienstordnung für die Gesundheitsämter – Besonderer Teil vom 30. März 1935, zuletzt geändert durch Verordnung vom 18. Dezember 1987)

(1) Das Gesundheitsamt führt Listen über diejenigen Personen, die in seinem Bezirk selbständig oder in abhängiger Stellung Behandlung, Pflege oder gesundheitliche Fürsorge am Menschen ausüben ...

(2) Für jede Berufsart ist eine besondere Liste zu führen; die Führung als Kartei ist statthaft.

Die Gesundheitsämter führen also Listen, Karteien u. a. über Personen, die in ihrem Bezirk selbständig, z. B. als Arzt tätig sind.

17.4.3
Verpflichtung der Ärzte, sich beim Gesundheitsamt zu melden

Ärzte sind als Kammerangehörige einer Zwangsmitgliedschaft unterworfen. Nach § 2 Abs. 2 des Heilberufsgesetzes haben sie sich binnen eines Monats, bei vorübergehender Berufsausübung in fünf Tagen nach Aufnahme der beruflichen Tätigkeit unter Vorlage ihrer Berechtigungsnachweise bei der zuständigen Kammer und beim zuständigen Gesundheitsamt anzumelden. Auch haben die Kammerangehörigen die Beendigung ihrer Berufsausübung und den Wohnsitz- und Niederlassungswechsel anzuzeigen.

§ 2 Heilberufsgesetz

(1) Den Kammern gehören als Berufsangehörige an alle

1. Ärztinnen und Ärzte,
2. Zahnärztinnen und Zahnärzte,

...

die in Hessen ihren Beruf ausüben...

(2) Kammerangehörige haben sich binnen eines Monats, bei vorübergehender Berufsausübung in fünf Tagen nach Aufnahme der beruflichen Tätigkeit unter Vorlage ihrer Berechtigungsnachweise bei der zuständigen Kammer und bei dem zuständigen Gesundheitsamt oder, wenn sie Berufsangehörige im Sinne des Abs. 1 Satz 1 Nr. 3 sind, dem zuständigen Staatlichen Amt für Lebensmittelüberwachung, Tierschutz und Veterinärwesen anzumelden; sie haben diesen die Beendigung ihrer Berufsausübung und den Wohnsitz- und Niederlassungswechsel anzuzeigen sowie den Ladungen der Kammer Folge zu leisten.

(3) Die Kammern dürfen Daten ihrer Kammerangehörigen nur verarbeiten, soweit dies für die Wahrnehmung der ihnen in diesem Gesetz zugewiesenen Aufgaben erforderlich ist. Für jeden Kammerangehörigen wird eine Akte angelegt. Das Nähere, insbesondere den Umfang der von den Kammerangehörigen bei der Meldung anzugebenden Daten und vorzulegenden Unterlagen, den Umfang der Datenweitergabe bei einer Verlegung der Tätigkeit der Kammerangehörigen innerhalb oder außerhalb Hessens sowie die Dauer der Speicherung der Daten über die Kammerangehörigen, regelt eine Satzung (Meldeordnung). Für die Kammern gelten die Bestimmungen des Hessischen Datenschutzgesetzes in der jeweils geltenden Fassung. Die Kammern übermitteln den zuständigen Behörden gegen Erstattung der Kosten für die von diesen nach der Dienstordnung für die Gesundheitsämter – Besonderer Teil – vom 30. März 1935 (RMBl. S. 327, 435), geändert durch Verordnung vom 18. Dezember 1987 (GVBl. 1988 I S. 11), zu führenden Listen über die Berufsangehörigen nach § 2 Abs. 1 Nr. 1 bis 3 halbjährlich nachfolgende Angaben:

1. Name und Vorname,
2. Dienstanschrift,
3. Anerkannte Bezeichnungen nach den Weiterbildungsordnungen.

Ihren Meldepflichten kommen viele Ärzte jedoch nicht, zeitlich verspätet oder nur unvollständig nach.

17.4.4
Vorgehensweise der Gesundheitsämter

Die Gesundheitsämter haben diesen Missstand in der Vergangenheit unterschiedlich bewältigt. Einige Stellen haben die Führung der Medizinalkartei – obwohl gesetzlich dazu verpflichtet – de facto eingestellt. Andere haben einen erheblichen Aufwand betrieben und die Ärzte ermittelt. Sie haben sich mittels zeitaufwändiger Recherchen aus Zeitungsanzeigen, Telefonbüchern und sonstigen öffentlichen Quellen die erforderlichen Informationen, z. B. über eine Praxisneueröffnung beschafft und daraufhin den betroffenen Arzt angeschrieben.

Das Gesundheitsamt Offenbach hat diesen Weg eingeschlagen, allerdings mehr Daten erhoben, als es der § 2 Abs. 3 des Heilberufsgesetzes vorsieht. Aufgrund der bislang gemachten Erfahrungen und nach Gesprächen, die ich im Jahre 1999 mit Vertretern des Sozialministeriums, der Landesärztekammer sowie des Landkreistages geführt habe, hat man das Gesetz im Januar 2001 geändert. Danach können die Gesundheitsämter jetzt von den Kammern bestimmte Daten der Ärzte erhalten: Namen, Vornamen, Dienstanschrift sowie anerkannte Bezeichnungen nach den Weiterbildungsverordnungen. Diese Angaben genügen, um den gesetzlichen Verpflichtungen des öffentlichen Gesundheitsdienstes Rechnung zu tragen. Allerdings war die Novellierung des Gesetzes vielen Ämtern verborgen geblieben.

Die Offenbacher Behörde bezog sich bislang jedoch, was Umfang und Inhalt der vom Arzt zu übermittelnden Unterlagen anbelangt, auf § 2 Abs. 2 Satz 1 des Gesetzes. Darin steht, dass sich Kammerangehörige unter Vorlage ihrer Berechtigungsnachweise bei dem zuständigen Gesundheitsamt anzumelden haben. Unter diese nicht näher bestimmte Formulierung subsumierte das Amt alle relevanten Unterlagen, die notwendig sind, um dem Auftrag der Behörde nachzukommen, der Folgendes umfasst:

- die Berechtigung zur Führung einer Praxis und Behandlung zu prüfen,
- im Katastrophenfall gezielt auf Ärzte bestimmter Fachrichtungen beziehungsweise auf Ärzte generell zugreifen zu können und
- nach § 36 Abs. 2 Infektionsschutzgesetz (Einhaltung der Infektionshygiene) die Möglichkeit zur Überwachung von u. a. Arztpraxen, in denen invasive Eingriffe vorgenommen werden.

17.4.5
Rechtliche Bewertung

Die vom Gesundheitsamt Offenbach gegenüber dem Arzt geforderten Angaben gingen darüber hinaus, was seit Januar 2001 im geänderten Heilberufsgesetz als für dessen Aufgaben erforderlich festgelegt ist. Eine Befragung diverser hessischer Gesundheitsämter hatte allerdings ergeben, dass die Verfahrensweise im Zusammenhang mit der Führung der Medizinalkartei erhebliche Unterschiede aufzeigte.

17.4.6
Antwort des Sozialministeriums

Das Ministerium hat mir auf Anfrage mitgeteilt, dass von den Gesundheitsämtern keine über die von der Landesärztekammer übermittelten Daten hinaus von Betroffenen beziehungsweise von Dritten für die Erfüllung ihrer Aufgaben benötigt würden, da die dort gesammelten und erfassten Daten bezüglich der Ärztinnen und Ärzte vollständig und ausreichend seien. Die Gesundheitsämter seien erneut auf die Einhaltung der Bestimmungen des Heilberufsgesetzes hingewiesen worden. Das Gesundheitsamt des Landkreises Offenbach erhebe keine zusätzlichen Daten mehr.

17.4.7
Sichtweise des Gesundheitsamtes des Landkreises Offenbach

Das Gesundheitsamt des Landkreises Offenbach hat sich nach Gesprächen mit dem Medizinalreferat des Regierungspräsidiums Darmstadt sowie im Rahmen einer Amtsleiterversammlung bereit erklärt, nur noch die im Heilberufsgesetz genannten Daten anzufordern beziehungsweise zu erheben. Diskutiert wurde noch, ob die private Anschrift des Arztes erforderlich sei, um im Katastrophenfall eine zügige Anforderung von benötigten Ärzten zu ermöglichen. Nach einer Erörterung unter den Amtsleitern ist man jedoch zu der Auffassung gelangt, auf dieses Merkmal verzichten zu können. Im Übrigen hätte es hierzu auch einer Ergänzung im Heilberufsgesetz bedurft.

18. Sozialwesen

18.1
„Offensiv-Gesetz“

Auf der Grundlage (des Entwurfs) des „Offensiv-Gesetzes“ sozialpolitische Pilot-Projekte durchzuführen, verstößt gegen das geltende Sozialdatenschutzrecht.

Die hessische Landesregierung hatte einen mit dem Schlagwort „Wisconsin-Modell“ gekennzeichneten Entwurf zu einem „Offensiv-Gesetz“ auf den Weg gebracht (vgl. Pressemitteilung vom 24. Januar 2002), der die Errichtung sogenannter Job-Center zum Gegenstand hatte. Die Datenübermittlung der Arbeitsverwaltung und Sozialhilfeträger an die Job-Center sollte auf der Grundlage des Bundesdatenschutzgesetzes (BDSG) stattfinden (§§ 190c Sozialgesetzbuch [SGB] III, 18e Bundessozialhilfegesetz [BSHG] des Entwurfs).

Ich habe die hessische Landesregierung frühzeitig – ohne Erfolg – darauf hingewiesen, dass die Bezugnahme auf das BDSG datenschutzrechtlich systemwidrig ist, vielmehr das geltende Sozialdatenschutzrecht (§§ 35 SGB I, 67 ff. SGB X) den korrekten Maßstab für die Datenübermittlung an die Job-Center bilden muss. Die Bezugnahme auf das BDSG ist deshalb nicht sachgerecht, weil sowohl die Arbeitsverwaltung als auch die Sozialhilfeträger an das SGB gebunden sind und dessen auf die Belange der Sozialverwaltung und der Hilfeempfänger abgestimmter Sozialdatenschutz ein dem BDSG überlegenes datenschutzrechtliches Regelungswerk bereitstellt. Da nach dem „Offensiv-Gesetz“ Daten zwischen Arbeitsverwaltung und Sozialhilfeträgern nach Maßgabe des SGB ausgetauscht und verarbeitet werden sollen (§§ 190c SGB III, 18e BSHG des Entwurfs), ist der Verweis auf das BDSG für die Datenübermittlung an die Job-Center ein datenschutzrechtlicher Systembruch. Die datenschutzrechtliche Flankierung des so genannten „Hartz-Konzepts“ verfolgt dagegen zutreffend die Anbindung an das Sozialdatenschutzrecht (§§ 402 SGB III, 18 BSHG des Gesetzentwurfs; BTDrucks. 15/26).

Nachdem die von Hessen ausgehende Bundesratsinitiative im Bundestag auch in der vergangenen Legislaturperiode gescheitert ist, hat das hessische Sozialministerium in der Folgezeit über die Presse verlauten lassen, dass, angelehnt an den Entwurf für ein „Offensiv-Gesetz“, in Hessen Pilot-Projekte durchgeführt werden sollen. Dem steht entgegen,

dass ein Tätigwerden von Job-Centern im Sinne des „Offensiv-Gesetzes“ auf der Grundlage nach dem BDSG übermittelter Daten einen Verstoß gegen das Sozialdatenschutzrecht darstellt. Die auszutauschenden Informationen sind Sozialdaten, die nach geltendem Recht nur aufgrund der Ermächtigungen des SGB übermittelt werden dürfen.

Vor diesem Hintergrund werde ich die weitere Entwicklung aufmerksam verfolgen.

18.2
Dienstaufsicht und Sozialdatenschutz

Der Sozialdatenschutz steht der Wahrnehmung der Dienstaufsicht auch im Kinder- und Jugendhilferecht grundsätzlich nicht entgegen.

Der Landkreis Kassel hat mich um Stellungnahme gebeten, ob es aus datenschutzrechtlicher Sicht zulässig ist, dass die Amtsleitung eines Jugendamtes von den Mitarbeiterinnen und Mitarbeitern die Bekanntgabe der Außendiensttermine mit Namen und Adressen der Klienten verlangen kann, insbesondere wenn der Verdacht auf Erledigung privater Angelegenheiten während der Dienstzeit besteht.

Das habe ich unter Hinweis auf den datenschutzrechtlichen Erforderlichkeitsgrundsatz bejaht. Es bestehen keine Zweifel, dass auch die Terminierung der Gespräche mit Klienten sowie deren Namen und Adressen personenbezogene Daten im Sinne des Sozialdatenschutzes sind; denn es handelt sich um Angaben über Personen, die durch die Aufgabenwahrnehmung nach dem Kinder- und Jugendhilferecht betroffen werden (§ 67 Abs. 1 Sozialgesetzbuch X [SGB X]). Der Gesetzgeber hat den Kinder- und Jugendhilfebereich als datenschutzrechtlich besonders sensiblen Bereich bewertet und ihn demzufolge strengeren, vom allgemeinen Sozialdatenschutzrecht abweichenden bereichsspezifischen Sonderregelungen unterstellt (§§ 61 ff. SGB VIII – Kinder- und Jugendhilfegesetz).

Markantester Ausdruck der datenschutzrechtlichen Sonderstellung des Kinder- und Jugendhilferechts ist § 65 SGB VIII, der zugunsten des „besonderen Vertrauensschutzes“ in der persönlichen und erzieherischen Hilfe ein „behördeninternes Weitergabeverbot“ verfügt.

§ 65 SGB VIII

(1) Sozialdaten, die dem Mitarbeiter eines Trägers der öffentlichen Jugendhilfe zum Zweck persönlicher und erzieherischer Hilfe anvertraut worden sind, dürfen von diesem nur weitergegeben werden

1. mit der Einwilligung dessen, der die Daten anvertraut hat, oder
2. dem Vormundschafts- oder dem Familiengericht zur Erfüllung der Aufgaben nach § 50 Abs. 3, wenn angesichts einer Gefährdung des Wohls eines Kindes oder eines Jugendlichen ohne diese Mitteilung eine für die Gewährung von Leistungen notwendige gerichtliche Entscheidung nicht ermöglicht werden könnte, oder
3. unter den Voraussetzungen, unter denen eine der in § 203 Abs. 1 oder 3 des Strafgesetzbuches genannten Personen dazu befugt wäre.

Gibt der Mitarbeiter anvertraute Sozialdaten weiter, so dürfen sie vom Empfänger nur zu dem Zweck weiter gegeben werden, zu dem er diese befugt erhalten hat.

(2) § 35 Abs. 3 des Ersten Buches gilt auch, soweit ein behördeninternes Weitergabeverbot nach Absatz 1 besteht.

Dies ist im Hinblick auf die Struktur des öffentlichen Dienstrechts eine besondere Privilegierung datenschutzrechtlicher Interessen im Kinder- und Jugendhilfebereich; denn selbst das allgemeine Sozialdatenschutzrecht geht davon aus, dass eine Zweckänderung der Datenverarbeitung dann nicht gegeben ist, wenn sie u. a. für die Wahrnehmung von Aufsichts-, Kontroll- und Disziplinarbefugnissen erforderlich ist (§ 67c Abs. 3 SGB X).

Daraus folgt, dass eine durch „behördeninternes Weitergabeverbot“ geschaffene kontrollfreie Enklave nur in ganz engen Ausnahmefällen akzeptabel ist. Der Gesetzgeber hat dies im Kinder- und Jugendhilfebereich für den Fall besonders „anvertrauter“ Sozialdaten so vorgesehen. Freilich liegt auf der Hand, dass diese datenschutzrechtliche Privilegierung eines „besonderen Vertrauensschutzes“ nicht überdehnt werden darf. Außendiensttermine mit Namen und Adressen der Klienten sind keine besonders anvertrauten Daten und unterliegen keinem behördeninternen Weitergabeverbot. Wie bei allen Datenübermittlungen ist allerdings auch im Rahmen von Aufsichtsmaßnahmen zu beachten, dass keine Daten weitergegeben werden, die zur Erfüllung des Kontrollzwecks nicht erforderlich sind. „Auf Vorrat“ dürfen auch Informationen über Termine nicht übermittelt werden.

Ich habe dem Landkreis Kassel in diesem Sinne Auskunft gegeben.

18.3
Auskunftsansprüche im Kinder- und Jugendhilferecht

Die leiblichen Eltern haben auch dann prinzipiell einen Auskunftsanspruch hinsichtlich der Daten ihres Kindes, wenn sie nicht sorgeberechtigt sind.

Im Rahmen meiner Tätigkeit ist im kinder- und jugendhilferechtlichen Sozialdatenschutz (§§ 61 ff. Sozialgesetzbuch [SGB] VIII) die Frage aufgetreten, ob die nicht sorgeberechtigten, leiblichen Eltern auf Antrag Auskunft über die zu ihrem Kind in Akten oder auch sonstigen Datenträgern gespeicherten Daten verlangen können.

Zweifel ergeben sich zum einen deshalb, weil §§ 67 SGB VIII, 83 SGB X den Auskunftsanspruch auf die zur Person des Betroffenen gespeicherten Daten beschränken, und zum anderen, weil § 8 SGB I im Kontext der Kinder- und Jugendhilfe speziell von Personensorgeberechtigten spricht. § 68 Abs. 3 SGB VIII befasst sich hingegen ausschließlich mit dem Auskunftsanspruch des Pfleglings oder Mündels.

Meines Erachtens darf diesen Regelungen aber keine Ausschlusswirkung beigemessen werden. Den leiblichen Eltern muss ein Auskunftsanspruch hinsichtlich ihres Kindes prinzipiell zustehen. Die informationelle Abschottung gegenüber dem Kind würde – von Missbrauchsfällen abgesehen – mit verfassungsrechtlichen Vorgaben kollidieren. Art. 6 Abs. 2 Satz 1 Grundgesetz (GG) verfügt, dass Pflege und Erziehung der Kinder das natürliche Recht der Eltern und die zuvörderst ihnen obliegende Pflicht sind. Mit dieser Vorgabe wäre es nicht vereinbar, wenn ein Informationsanspruch der leiblichen Eltern auf Auskünfte über ihr Kind gänzlich verneint würde. Erst die durch Ausübung des Auskunftsrechts erlangten Informationen können die leiblichen Eltern in die Lage versetzen, notfalls mit Rechtsbehelfen einzugreifen, falls nach ihrem Eindruck gegen das Kindeswohl verfahren wird.

Zwar hat gemäß Art. 6 Abs. 2 Satz 2 GG die staatliche Gemeinschaft hinsichtlich der Wahrnehmung elterlicher Pflichten einen Überwachungsauftrag, der auch zur Entziehung des Sorgerechts führen kann; das vermag aber nicht zu rechtfertigen, dass die staatliche Gemeinschaft die leiblichen Eltern von jedem Informationsfluss, der ihr Kind betrifft, ausschließt. Auch im Sozialrecht wird einleitend explizit betont, dass es dazu beitragen soll, die Familie zu schützen und zu fördern (§ 1 Satz 2 dritter Teilsatz SGB I). Diese Pflicht, die Familie zu schützen und zu fördern, hat ein entsprechendes Informationsrecht der leiblichen Eltern zur Folge.

Es ist zu konzedieren, dass ein Informationsrecht der leiblichen Eltern dort seine Grenzen haben muss, wo zu erwarten ist, dass durch die Auskunft an die leiblichen Eltern das Wohl des Kindes beeinträchtigt oder notwendige Maßnahmen konterkariert werden. § 1 Abs. 3 Nr. 3 SGB VIII legt denn auch der Jugendhilfe ausdrücklich auf, Kinder und Jugendliche vor Gefahren für ihr Wohl zu schützen. Die Verwaltungspraxis ist aus Gründen der Transparenz gehalten, die Gründe für die Ablehnung aktenkundig zu machen, um die notwendige Nachprüfbarkeit zu gewährleisten.

Das Sozialministerium, das ich um Stellungnahme gebeten habe, hat zwar Vorbehalte hinsichtlich der verfassungsrechtlichen Herleitung meiner Auffassung geäußert, ist aber im Ergebnis mit mir der Ansicht, dass eine am Kindeswohl orientierte Jugendhilfe die leiblichen Eltern soweit in den Hilfeprozess für ein Kind einzubinden und zu informieren hat, wie dies mit dem Kindeswohl vereinbar ist. Insofern gibt es für die Zukunft eine gemeinsame Richtschnur für die Jugendämter, die sowohl vom Sozialministerium als auch von mir hinsichtlich des Auskunftsanspruchs leiblicher Eltern vertreten wird.

18.4
Datenschutz im Adoptionsvermittlungsverfahren

Der Datenschutz im Adoptionsvermittlungsverfahren ist nunmehr vorrangig im Adoptionsvermittlungsgesetz geregelt; ergänzend gilt das allgemeine Sozialdatenschutzrecht.

Von Jugendämtern wird des Öfteren die Frage aufgeworfen, wonach sich der Datenschutz bei der Adoptionsvermittlung richte.

Dass diese Frage überhaupt gestellt wird, überrascht nicht, weil durch einen Verweis an recht versteckter Stelle geregelt gewesen ist, welche datenschutzrechtlichen Regelungen für die Adoptionsvermittlung maßgebend waren: § 68 Sozialgesetzbuch (SGB) I bestimmt nämlich, dass das Adoptionsvermittlungsgesetz bis zur Einordnung in das Sozialgesetzbuch als dessen besonderer Teil gilt (Nr. 12). Damit war zugleich angeordnet, dass der Sozialdatenschutz der §§ 35 SGB I, 67 ff. SGB X auch im Adoptionsvermittlungsverfahren gilt.

Mittlerweile ist im Adoptionsvermittlungsrecht der Datenschutz bereichsspezifisch, speziell geregelt. Hintergrund ist die Neufassung des Adoptionsvermittlungsgesetzes, die am 1. Januar 2002 (BGBl. I S. 354) in Kraft getreten ist. Maßgeblich für den Datenschutz ist insofern der neue § 9d Adoptionsvermittlungsgesetz (AdVermiG), der die amtliche Überschrift „Datenschutz“ trägt:

§ 9d AdVermiG

(1) Für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten gilt das Zweite Kapitel des Zehnten Buches Sozialgesetzbuch mit der Maßgabe, dass Daten, die für Zwecke dieses Gesetzes erhoben worden sind, nur für Zwecke der Adoptionsvermittlung oder Adoptionsbegleitung, der Anerkennung, Zulassung oder Beaufsichtigung von Adoptionsvermittlungsstellen, der Überwachung von Vermittlungsverboten, der Verfolgung von Verbrechen oder anderen Straftaten von erheblicher Bedeutung oder der internationalen Zusammenarbeit auf diesen Gebieten verarbeitet oder genutzt werden dürfen. Die Vorschriften über die internationale Rechtshilfe bleiben unberührt.

(2) Die Bundeszentralstelle übermittelt den zuständigen Stellen auf deren Ersuchen die zu den in Absatz 1 genannten Zwecken erforderlichen personenbezogenen Daten. In dem Ersuchen ist anzugeben, zu welchem Zweck die Daten benötigt werden.

(3) Die ersuchende Stelle trägt die Verantwortung für die Zulässigkeit der Übermittlung. Die Bundeszentralstelle prüft nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben der ersuchenden Stelle liegt, es sei denn, dass ein besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht.

(4) Bei der Übermittlung an eine ausländische Stelle oder an eine inländische nicht-öffentliche Stelle weist die Bundeszentralstelle darauf hin, dass die Daten nur für den Zweck verarbeitet und genutzt werden dürfen, zu dem sie übermittelt werden.

(5) Fügt eine verantwortliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, so finden die §§ 7 und 8 des Bundesdatenschutzgesetzes Anwendung.

Aus datenschutzrechtlicher Sicht äußerst bedeutsam ist ferner § 9b AdVermiG, der die Aufbewahrungsdauer (Abs. 1) sowie das Einsichtsrecht (Abs. 2) in Vermittlungsakten betrifft:

§ 9b AdVermiG

(1) Aufzeichnungen und Unterlagen über jeden einzelnen Vermittlungsfall (Vermittlungsakten) sind, gerechnet vom Geburtsdatum des Kindes an, 60 Jahre lang aufzubewahren. Wird die Adoptionsvermittlungsstelle aufgelöst, so sind die Vermittlungsakten der Stelle, die nach § 2 Abs. 1 Satz 3 oder Satz 4 ihre Aufgabe übernimmt, oder der zentralen Adoptionsstelle des Landesjugendamtes, in dessen Bereich die Adoptionsvermittlungsstelle ihren Sitz hatte, zur Aufbewahrung zu übergeben. Nach Ablauf des in Satz 1 genannten Zeitraums sind die Vermittlungsakten zu vernichten.

(2) Soweit die Vermittlungsakten die Herkunft und die Lebensgeschichte des Kindes betreffen oder ein sonstiges berechtigtes Interesse besteht, ist dem gesetzlichen Vertreter des Kindes und, wenn das Kind das 16. Lebensjahr vollendet hat, auch diesem selbst auf Antrag unter Anleitung durch eine Fachkraft Einsicht zu gewähren. Die Einsichtnahme ist zu versagen, soweit überwiegende Belange eines Betroffenen entgegenstehen.

Wichtig ist insbesondere § 9b Abs. 2 AdVermiG, weil nach wie vor das Recht der Adoptierten auf Kenntnis der eigenen Abstammung in der Praxis eine große Rolle spielt. Ein solches Recht hat das Bundesverfassungsgericht schon vor Jahren bejaht, worauf ich in meinem 25. Tätigkeitsbericht ausdrücklich hingewiesen habe (Ziff. 6.3). Der Gesetzgeber hat daraus die Folgerung gezogen, dass die adoptierte Person bereits ab dem 16. Lebensjahr selbst berechtigt ist, den Antrag auf Einsicht in die Adoptionsvermittlungsakte zu stellen und das Einsichtsrecht wahrzunehmen. Soweit in den Adoptionsvermittlungsakten Daten Dritter aufgeführt sind, die für die Herkunft und die Lebensgeschichte des Adoptierten unerheblich sind – das kann etwa dann der Fall sein, soweit es um Personen geht, die nicht die leiblichen Eltern sind –, ist das Einsichtsrecht in § 9b Abs. 2 Satz 2 AdVermiG gegenständlich begrenzt. Praktisch kann das bedeuten, dass den Adoptierten teilgeschwärzte Kopien der Akte vorgelegt werden dürfen. Ich habe die Jugendämter bei Beratungsgesprächen und Schulungsveranstaltungen über die datenschutzrechtlichen Maßstäbe bei der Adoptionsvermittlung unterrichtet.

19. Personalwesen

19.1
Weitergabe dienstlicher Unterlagen bei der Anrufung des Hessischen Datenschutzbeauftragten durch einen Personalrat

Wird der Hessische Datenschutzbeauftragte von Bediensteten einer öffentlichen Stelle angerufen, dürfen ihm personenbezogene Akten zur Begründung des Prüfungsverfahrens übergeben werden. Nachteilige Sanktionen gegen Bedienstete wegen vermeintlichen Bruchs von Dienstgeheimnissen sind gesetzlich untersagt.

Der Personalrat einer öffentlichen Stelle hat sich unter Vorlage eines Prüfungsberichts der zuständigen Prüfinstanz, aus denen die Verarbeitung personenbezogener Daten ersichtlich war, mit der Bitte um datenschutzrechtliche Prüfung und Bewertung an mich gewandt. Im weiteren Verlauf teilte die Vorsitzende des Personalrats mir mit, dass der Leiter der öffentlichen Stelle die Auffassung vertreten habe, die Weiterleitung der Unterlagen an mich sei nicht erforderlich gewesen und stelle einen Bruch des Betriebsgeheimnisses dar. Die Vorsitzende äußerte die Befürchtung, dass sich durch die Einschaltung meiner Dienststelle nachteilige Folgen für die Personalratsarbeit ergeben könnten. Der Leiter der öffentlichen Stelle hat im Verlauf meiner Prüfung geäußert, dass mit der Übersendung von Unterlagen durch die Personalvertretung an meine Dienststelle Dienstgeheimnisse verletzt würden.

Die Auffassung des Leiters der öffentlichen Stelle beruht auf einem groben Fehlverständnis des Hessischen Datenschutzgesetzes (HDSG). Die Einschaltung meiner Dienststelle, unter Vorlage der für meine Tätigkeit relevanten Unterlagen, ist datenschutzrechtlich durch § 28 HDSG legitimiert und damit auch zulässig.

§ 28 HDSG

(1) Jeder kann sich an den Hessischen Datenschutzbeauftragten wenden, wenn er annimmt, bei der Verarbeitung seiner personenbezogenen Daten durch datenverarbeitende Stellen, ausgenommen die Gerichte, soweit sie nicht in Verwaltungsangelegenheiten tätig werden, in seinen Rechten verletzt worden zu sein. Niemand darf dafür gemaßregelt oder benachteiligt werden, dass er sich aufgrund tatsächlicher Anhaltspunkte für einen Verstoß gegen dieses Gesetz oder andere Vorschriften über den Datenschutz an den Hessischen Datenschutzbeauftragten wendet.

(2) Beschäftigte öffentlicher Stellen können sich ohne Einhaltung des Dienstweges an den Hessischen Datenschutzbeauftragten wenden. Die dienstrechtlichen Pflichten der Beschäftigten bleiben im Übrigen unberührt.

Die Übermittlung der vollständigen Unterlagen – konkret handelt es sich um einen Prüfbericht der zuständigen Kontrollbehörde zur Einstufung und Vergütung des Personals der Dienststelle – war zulässig. Die Trennung der personenbezogenen Daten von den übrigen Angaben wäre nur mit unverhältnismäßig großem Aufwand möglich gewesen. In solchen Fällen lässt § 11 Abs. 2 HDSG die Weitergabe von Akten zu, die auch nicht erforderliche Daten enthalten. Eine Verletzung von Betriebs- beziehungsweise Geschäftsgeheimnissen durch die Weitergabe – wie sie der Leiter der Dienststelle in der Weiterleitung der Unterlagen gerügt hatte – liegt schon deshalb nicht vor, weil auch meine Dienststelle eine öffentliche Stelle und zudem zur Verschwiegenheit verpflichtet ist.

Für die Daten, die nicht dem Zweck der Verarbeitung dienen, gilt ein Verwertungsverbot nach § 13 Abs. 2, 3 HDSG. Dies wird von mir selbstverständlich beachtet.

Ich habe sowohl den Leiter der öffentlichen Stelle als auch den Personalrat von meiner Rechtsauffassung unterrichtet und dabei ausdrücklich auf § 28 Abs. 1 Satz 2 HDSG hingewiesen.

19.2
Übertragung der Zuständigkeit für Untersuchungen zur Dienstfähigkeit von Beamtinnen und Beamten in der hessischen Landesverwaltung auf die Versorgungsämter

Bei der Übertragung der Dienstunfähigkeitsuntersuchungen von Landesbeamten auf die Versorgungsverwaltung wurden datenschutzrechtliche Fragen nicht zufriedenstellend gelöst. So gibt es keine spezifische Rechtsgrundlage für die Tätigkeit der Versorgungsämter. Auch bei der praktischen Umsetzung fehlt es der Versorgungsverwaltung an eindeutigen Vorgaben.

19.2.1
Der Kabinettsbeschluss

Das Hessische Ministerium des Innern und für Sport hatte im April 2001 eine Kabinettvorlage erarbeitet, wonach Dienstunfähigkeitsuntersuchungen (DU-Untersuchungen) der Landesbeamten und Richter künftig vom ärztlichen Dienst von hessischen Ämtern für Versorgung und Soziales erfolgen sollten. Mit der Umsetzung der Maßnahme wurde das Sozialministerium beauftragt. Das Kabinett hatte der Vorlage durch Beschluss vom 8. Mai mit der Maßgabe zugestimmt, dass die neue Regelung zum 1. Juni 2001 in Kraft tritt.

19.2.2
Bisherige Verfahrensweise bei DU-Untersuchungen in den Gesundheitsämtern

Bisher waren die Gesundheitsämter der Städte und Landkreise für DU-Untersuchungen von Beamten und Richtern in Hessen – mit Ausnahme der Beamten im Polizeivollzugsdienst – zuständig. Mit dem Übergang auf die hessische Versorgungsverwaltung, die jetzt verantwortlich für den gesamten Bereich der Landesverwaltung ist, haben die Gesundheitsämter einen Teil ihrer Aufgaben verloren; sie führen aber weiterhin DU-Untersuchungen im Kommunalbereich durch. Rechtsgrundlage für DU-Untersuchungen ist § 51 Abs. 1 Satz 3 HBG und § 18a der zweiten Durchführungsverordnung zum Gesetz über die Vereinheitlichung des Gesundheitswesens (Dienstordnung – Allgemeiner Teil) – GVBl. I S. 197 vom 23. Mai 1986. § 51 Abs. 3 HBG regelt die Pflicht des Beamten zur DU-Untersuchung.

§ 51 Abs. 1 Satz 3 HBG

Bestehen Zweifel über die Dienstunfähigkeit des Beamten, so ist er verpflichtet, sich nach Weisung der Behörde ärztlich untersuchen und, falls ein Amtsarzt dies für erforderlich hält, auch beobachten zu lassen.

In § 18a Abs. 1 ist festgelegt, in welchem Umfang Untersuchungsergebnisse von den Gesundheitsämtern an die den Auftrag erteilende Stelle übermittelt werden dürfen. Dazu gibt es verbindliche Formularvordrucke, die von den Gesundheitsämtern zu verwenden sind. Diese Vordrucke sind als Anlagen 1 und 2 der Verordnung angefügt.

§ 18a Dienstordnung – Allgemeiner Teil

(1) In dienst- und arbeitsrechtlichen Angelegenheiten ist das amtsärztliche Gutachten nach den Mustern der Anlagen 1 und 2 auszustellen. Dem Auftraggeber hat das Gesundheitsamt grundsätzlich nur das Gesundheitszeugnis nach Anlage 2 zu übermitteln, soweit in Abs. 2 nichts anderes bestimmt ist. Die untersuchte Person ist berechtigt, Einsicht in die anlässlich der Untersuchung gemachten Aufzeichnungen zu nehmen. Einsichtsrechte nach anderen Rechtsvorschriften bleiben unberührt.

(2) Bei konkreten Zweifeln an der Vollständigkeit und Aussagefähigkeit des Gesundheitszeugnisses oder dem darin festgestellten Ergebnis der Beurteilung ist die auftraggebende Stelle berechtigt, Aufklärung von dem untersuchenden Arzt zu verlangen, soweit sie dies unter Beachtung des Grundsatzes der Verhältnismäßigkeit für erforderlich hält. Das Gesundheitsamt ist verpflichtet, ihr die für das Gesundheitszeugnis maßgeblichen Einzeldaten zu übermitteln.

...

19.2.3
Verfahrensweise bei den hessischen Versorgungsämtern

Auf die Änderung der Zuständigkeiten und die sich daraus ergebenden datenschutzrechtlichen Konsequenzen wurde ich erst im Berichtsjahr aufmerksam. Deshalb habe ich im August 2002 das Sozialministerium angeschrieben und um Stellungnahme gebeten. Unabhängig davon habe ich die Ämter für Versorgung und Soziales in Wiesbaden, Fulda und Frank-furt am Main aufgesucht, um in den Dienststellen die Verfahrensweise zu prüfen.

Die Rechtsgrundlage für die Datenerhebung durch die untersuchenden Ärzte der Versorgungsverwaltung ist zweifelhaft. In den beamtenrechtlichen Vorschriften des § 51 Abs. 1 HBG ist die DU-Untersuchung Ärzten vorbehalten. Die Anordnung einer Beobachtung darf ausdrücklich nur dann erfolgen, wenn ein Amtsarzt sie für erforderlich hält. Nach der einschlägigen Kommentierung ist dies der Amtsarzt beim Gesundheitsamt (v. Roetteken/Rothländer, Hessisches Bedienstetenrecht IV, § 51 Rdnr. 76). Es bestehen erhebliche Zweifel, ob durch einen Kabinettsbeschluss die Funktion des Amtsarztes auf Ärzte der Versorgungsverwaltung übertragen werden konnte. Ggf. wäre eine Änderung oder Ergänzung des § 51 HBG erforderlich gewesen. § 18a Dienstordnung hätte geändert werden müssen, da diese Regelung die Gesundheitsämter für zuständig erklärt hat.

Mit der inhaltlichen Umsetzung der bislang von den Gesundheitsämtern durchgeführten Maßnahmen hatten die Versorgungsämter Probleme. Die Handlungsanweisungen vom Ministerium beziehungsweise vom Landesamt für Versorgung und Soziales sind teilweise unvollständig. Das betrifft z. B. die Frage, in welchem Umfang Daten bei Betroffenen erhoben werden oder wie deren Einverständnis zur Einholung von Auskünften oder zur Beiziehung von Akten hergestellt wird. Dazu gibt es unterschiedliche Formularsätze, die zum Teil von den Gesundheitsämtern übernommen worden sind. Der Anamnesebogen ist nicht einheitlich gestaltet. Die Unterrichtung und persönliche Erklärung der Betroffenen ist von unterschiedlichem Inhalt und Umfang. An sich hätte es sich angeboten, im Zuge der Übertragung auf die sechs Versorgungsämter allen Stellen einheitliche Unterlagen zur Verfügung zu stellen.

Keine klare Vorstellung hatten die Ärzte der Versorgungsämter dazu, in welcher Form sie bereits vorhandene Unterlagen bei den Gesundheitsämtern anfordern können. Mittlerweile liegen mir von mehreren Gesundheitsämtern Anfragen vor, ob einzelne Datenanforderungen der Versorgungsverwaltung zulässig sind, insbesondere ob sie inhaltlich hinreichend begründet und auf den Einzelfall bezogen klar genug definiert sind.

In allen Fällen hätten klare Vorgaben und Anweisungen die Unsicherheit vermeiden können, wie ich sie im Verlauf meiner Gespräche festgestellt habe.

19.2.4
Datenschutzrechtliche Forderungen

19.2.4.1
Rechtliche Grundlage für die Versorgungsverwaltung

Die Rechtsgrundlage, auf deren Basis die Versorgungsverwaltung im Zusammenhang mit DU-Untersuchungen tätig wird, ist teilweise nicht schlüssig. Zwar ist in § 51 Abs. 1 HBG festgeschrieben, dass bei Zweifeln über die weitere Dienstunfähigkeit der Beamte verpflichtet ist, sich nach Weisung der Behörde ärztlich untersuchen zu lassen. Die nähere Ausführung der Vorschrift ist in § 18a Dienstordnung zu finden. Danach ist in dienst- und arbeitsrechtlichen Angelegenheiten das amtsärztliche Gutachten nach den Mustern der Anlagen 1 und 2 auszustellen. Das bedeutet, dass der Auftraggeber nur das Ergebnis der Begutachtung erhält und keinen Anspruch auf die Übermittlung medizinischer Daten erheben kann.

Eine dem § 18a Dienstordnung inhaltlich entsprechende ausdrückliche Regelung für die Versorgungsämter ist unerlässlich. Die analoge Anwendung dieser – für die Tätigkeit der Gesundheitsämter geschaffenen – Vorschrift auf die Versorgungsämter lässt sich nicht rechtfertigen.

Anlage 1

Gesundheitsamt
des Kreises/der Stadt . . .

Ort, Datum:

Telefon Durchwahl:

A. ANGABEN ZUR VORGESCHICHTE
(soweit zur Durchführung des Untersuchungsauftrages erforderlich)

Name (ggf. auch Geburtsname)
Vorname
wohnhaft, Straße, Nr.
Wohnort
Geburtsdatum
Gutachterauftrag vom /Az.
auf Veranlassung
wegen
ausgewiesen durch

Wurden Sie bereits in einem Gesundheitsamt untersucht?

nein ☐ ja ☐ Wann? _____ Wo? _____

Weshalb? _____

_____

1. Hat es in Ihrer engeren Familie ernsthafte Erkrankungen gegeben?
(Eltern, Geschwister, Kinder)

☐ hoher Blutdruck ☐ Herzkrankheiten ☐ Zuckerkrankheiten ☐ Gicht

☐ chronischer Rheumatismus ☐ Allergien ☐ Tuberkulose ☐ Krebs

☐ Suchtkrankheiten ☐ Nerven- oder Geisteskrankheiten, auch Selbstmord/Versuche

☐ Sonstiges _____

☐ keine ernsten Krankheiten

2. Eigene Vorgeschichte,

folgende Krankheiten/Krankheiten folgender Organe/Behinderungen lagen vor/
liegen noch vor

☐ Herzerkrankungen ☐ hoher/niedriger Blutdruck ☐ Bronchien/Lunge ☐ Asthma

☐ Tuberkulose ☐ Allergien ☐ Haut ☐ Mandelentzündungen

☐ Diphtherie ☐ Scharlach ☐ Rheuma ☐ Schilddrüse

☐ Leber ☐ Röteln ☐ Gallenblase ☐ Gelbsucht

☐ Magen und Darm ☐ Nieren ☐ Harnblase ☐ Knochen- und Gelenksystem Wirbelsäule

☐ Nerven- oder Geisteskrankheiten (auch Anfälle und Selbstmordversuche) ☐ körperliche/geistige/seelische Behinderung

☐ keine ernsthaften Krankheiten oder Behinderungen ☐ Diabetes ☐ Gehirnerschütterung

☐ Knochenbruch ☐ Krampfadern, Thrombose Embolie ☐ Geschlechtskrankheiten ☐ Gicht

Name: _____

Zeitpunkt	Krankheit/Sanatoriums-aufenthalt/Heilkur	Zeitdauer	Behandelnder Arzt o. Krankenhaus Kurarzt o. Sanatoriumsarzt
Beispiel: Sommer 69 Winter 70	Scharlach Unterarmbruch rechts	4 Wochen 3 Wochen	Dr. Meyer, Melsungen St. Marien-Hospital, Marburg

3. Welche Folgen sind von den Krankheiten oder Verletzungen zurückgeblieben?

_____

_____

4. Jetzige Beschwerden oder Krankheiten

☐ Sehstörungen ☐ Augenbeschwerden ☐ Kopfschmerzen ☐ Schwindel

☐ Schwerhörigkeit ☐ Hals/Nase/Ohren* ☐ Anfälle ☐ Zittern

☐ Schlafstörungen ☐ Schmerzen ☐ Husten ☐ Atemnot

☐ Nachtschweiß ☐ Appetitlosigkeit ☐ Gewichtsabnahme ☐ Verdauungsbeschwerden

☐ schmerzhaftes Wasserlassen ☐ rheumatische Beschwerden ☐ Herzbeschwerden ☐ Gelenkbeschwerden

☐ Rückenschmerzen ☐ nervöse Beschwerden ☐ Stimmungs- und Antriebsschwankungen

☐ Sonstiges _____

_____

_____

5. Haben Sie eine Rente beantragt?

☐ nein ☐ ja, weshalb _____ MdE _____ %

6. Sind Sie schwerbehindert?

☐ nein ☐ ja, weshalb _____ MdE _____ %

* Unzutreffendes streichen

Name: _____

7. Wurden früher Röntgenuntersuchungen durchgeführt?

☐ nein ☐ ja (nach Möglichkeit bitte Bilder und Befunde zum Untersuchungstermin mitbringen)

8. Sind Sie zur Zeit in Behandlung?

☐ nein ☐ ja, weshalb _____

9. Nehmen Sie zur Zeit Medikamente ein?

☐ nein ☐ ja, welche _____

_____ seit _____

10. Namen der behandelnden Ärzte _____

_____

11. Fühlen Sie sich gesund und leistungsfähig? ☐ ja ☐ nein

12. Betätigen Sie sich sportlich? ☐ ja ☐ nein

13. Tragen Sie eine Sehhilfe?

☐ nein ☐ ja ☐ Brille ☐ Haftschalen

14. Rauchen Sie? ☐ nein ☐ ja, seit _____ tägliche Menge _____

15. Nehmen Sie regelmäßig alkoholische Getränke (einschließlich Bier) zu sich?

☐ nein ☐ ja, seit _____ tägliche Menge _____

16. Haben Sie im letzten Jahr regelmäßig Medikamente oder Drogen eingenommen?

☐ nein ☐ ja, seit _____

17. Wurden Sie schon einmal auf Ihre gesundheitliche Eignung untersucht (z. B. Musterung)?

☐ nein ☐ ja, wo _____

Ergebnis _____

Unterrichtung und persönliche Erklärung:

1. Die Datenerhebung bei dieser Untersuchung erfolgt auf Grund von §§ 18, 18a der Zweiten Durchführungsverordnung zum Gesetz über die Vereinheitlichung des Gesundheitswesens in Verbindung mit den einschlägigen arbeits- und beamtenrechtlichen Vorschriften.
2. Ich habe dem untersuchenden Arzt zu meinem Gesundheitszustand vollständige Angaben gemacht.
3. Das Gesundheitsamt übersendet der auftraggebenden personalführenden Stelle grundsätzlich nur ein Gesundheitszeugnis, das in der Regel lediglich das zusammenfassende Ergebnis der Untersuchung zu den im Gutachtenauftrag gestellten Fragen enthält.
4. Bei konkreten Zweifeln an der Vollständigkeit oder Aussagefähigkeit des Gesundheitszeugnisses oder dem darin festgestellten Ergebnis der Beurteilung ist die auftraggebende Stelle berechtigt und das Gesundheitsamt verpflichtet, die für das Gesundheitszeugnis maßgeblichen Einzeldaten zu übermitteln. Dies gilt auch, wenn die Einzeldaten für gerichtliche Streitverfahren benötigt werden.
5. Bei Einstellungsuntersuchungen gilt Nr. 4 nur dann, wenn ich vor der Übermittlung vom untersuchenden Arzt über Inhalt und Umfang der gutachterlichen Feststellungen aufgeklärt worden bin und mich schriftlich mit der Übermittlung einverstanden erklärt habe.
6. Ich bin weiter darüber informiert, daß ich Einsicht in die bei meiner Untersuchung gemachten Aufzeichnungen nehmen kann.
7. Soweit zur Durchführung der Untersuchung die Beiziehung von Unterlagen von Ärzten oder Krankenhäusern, die mich behandelt oder untersucht haben, erforderlich ist, erfolgt die Entbindung von der Schweigepflicht auf gesonderten Formularen, die den betroffenen Arzt, den Untersuchungszweck sowie die angeforderten Unterlagen im einzelnen bezeichnen.

_____

Datum/Unterschrift

B. UNTERSUCHUNGSBEFUND

_____ Name
Vorname
wohnhaft, Straße, Nr.
Wohnort
_____ Geburtsdatum

Größe (ohne Schuhe) in cm _____ Gewicht (leicht bekleidet) in kg _____

Brustumfang in cm _____/_____ Urin Z: _____ E: _____ Ubg: _____ Sed: _____

Zu 4: Fernvisus
ohne/mit Glas re. _____/li. _____

Nahvisus
ohne/mit Glas, Nieden Nr. re. _____/li. _____

Farbensinn

☐ tüchtig ☐ gestört

Zu 5: Hörvermögen: Flüstersprache re. _____m/li. _____m

Umgangssprache re. _____m/li. _____m oder Audiogramm

Zu 10: Puls: _____/ _____/min. Blutdruck RR _____/ _____mmHg

falls erforderliche Belastung: Art der Belastung _____

Normalbefund	Von der Norm abweichende Befunde (mit Bezugsnummer)
1. Gesamteindruck ☐ ☐ schl. ☐ musk. ☐ adipös ☐ kachektisch	
2. Gangbild ☐	
3. Ernährungszustand ☐	
4. Augen/Sehvermögen ☐	
5. Ohren/Hörorgan ☐	
6. Sprachorgan ☐	
7. Haut und sichtbare Schleimhäute und Lymphknoten ☐	
8. Hals, Mundhöhle (mit NAP und Schilddrüse) ☐	
9. Gebiß nicht saniert ☐ Parodontose ☐ saniert ☐ gesund ☐	
10. Herz und Kreislauf/ periphere Durchblutung ☐	
11. Atmungsorgane ☐	
12. Bauchorgane ☐	
13. Harn- und Geschlechtsorgane (Nierenlager) ☐	
14. Bewegungsapparat (Zustand und Funktion von Gliedmaßen und Wirbelsäule) ☐	
15. Neurologischer Befund ☐	
16. Psychischer Befund ☐	
17. a) Röntgen-Thorax ☐ b) soweit erforderlich: Tuberkulintest (negativ) ☐	

Ergänzende Befunde
(mit Untersuchungsdatum und -stelle)

Bei Frauen, die einem erhöhten Rötelninfektionsrisiko ausgesetzt sind:

Eine Untersuchung auf Rötelnantikörper ☐ wurde durchgeführt

☐ wurde nicht durchgeführt, weil _____

_____ ggf. Rötelntiter: _____

DIAGNOSE: .....

☐ Kein von der Norm abweichender Befund

Ort, Datum

Gesundheitsamt
Im Auftrag:

_____
(Unterschrift des (Amts)Arztes)

Anlage 2

Gesundheitsamt
des Kreises/der Stadt . . .

Ort, Datum:

Telefon Durchwahl:

AMTSÄRZTLICHES GESUNDHEITSZEUGNIS

Name (ggf. auch Geburtsname)
Vorname
wohnhaft, Straße, Nr.
Wohnort
Geburtsdatum
Gutachterauftrag vom /Az.
auf Veranlassung
wegen
ausgewiesen durch

Beurteilung:

(Zusammenfassendes Ergebnis der Untersuchung unter Berücksichtigung der von der auftraggebenden Stelle gestellten Fragen bzw. von ihr bezeichneten Anforderungen. Bei uneingeschränkter Eignung genügt in der Regel die Mitteilung dieser Tatsache ohne nähere Begründung.)

Die der Beurteilung zugrundeliegenden Aufzeichnungen und Befunde bleiben im Gesundheitsamt. Bei konkreten Zweifeln an der Vollständigkeit oder Aussagefähigkeit des Gesundheitszeugnisses oder dem darin festgestellten Ergebnis der Beurteilung kann die auftraggebende Stelle die Übermittlung der für das Gesundheitszeugnis maßgeblichen Einzeldaten verlangen.

Gebühr DM
Tarifstelle

Im Auftrag:

(Unterschrift des (Amts)Arztes)

19.2.4.2
Einwilligungserklärungen

Die von den Versorgungsämtern verwendeten Einwilligungserklärungen, mit denen ärztliche Unterlagen bei anderen Stellen angefordert werden, sind unterschiedlich abgefasst und gehen teilweise über das erforderliche Maß hinaus. So verwendet das Amt in Wiesbaden ein Formular, das den ärztlichen Dienst ermächtigt, Auskünfte bei Ärzten, Krankenanstalten, Behörden und Trägern der Sozialversicherung einzuholen und Unterlagen beizuziehen. Diese Art allumfassender Einwilligung, die der Betroffene abgeben soll, um das Versorgungsamt pauschal von der ärztlichen Schweigepflicht zu entbinden, halte ich für nicht vertretbar. Eine datenschutzgerechtere Lösung hat das Amt in Frankfurt gefunden. Dort willigt der zu Untersuchende ganz konkret in die Datenübermittlung einer ganz bestimmten Stellen, etwa in die Datenübermittlung vom Gesundheitsamt an das Versorgungsamt ein. Dieses Verfahren sorgt einerseits für die notwendige Transparenz und veranlasst andererseits die untersuchende Behörde, sich zuvor über die Erforderlichkeit der Maßnahme klar zu werden.

19.2.4.3
Unterrichtung und persönliche Erklärung auf dem Anamnesebogen

Die vom Betroffenen zu unterschreibende „Unterrichtung und persönliche Erklärung“ genügt den datenschutzrechtlichen Anforderungen nicht. So wird der Untersuchte angehalten, mit seiner Unterschrift die Vollständigkeit der Angaben zu erklären. Gleichzeitig wird er über die Rechtsgrundlagen der Datenerhebung unterrichtet. Außerdem wird ihm eine pauschale Einwilligung in die Übermittlung von Einzeldaten des Gesundheitszeugnisses für den Fall abverlangt, dass der Auftraggeber Zweifel an der Vollständigkeit oder den inhaltlichen Aussagen des Gutachtens anmeldet. Schließlich entbindet der Betroffene Ärzte und Krankenhäuser von der Schweigepflicht, soweit zur Durchführung der Untersuchung die Beiziehung von deren Unterlagen erforderlich ist.

Die Verquickung unterschiedlicher Einwilligungen zur Datenübermittlung Dritter an das Versorgungsamt sowie zur Übermittlung von Einzeldaten Betroffener durch das Amt an den Auftraggeber ist unzulässig. Vielmehr sind zu trennen

a) die Bestätigung der eigenen Angaben,

b) die Anforderung von Unterlagen bei Dritten,

c) die Übermittlung von weiteren Daten über das Gutachten hinaus.

Bei der Anforderung von Unterlagen bei anderen Stellen sind diese genau zu bezeichnen und eine Einwilligung gilt dann nur für diesen Bereich. Schließlich darf die untersuchende Behörde, wendet man die Vorschrift des § 18a analog an, nur konkrete und einzelne Nachfragen des Auftraggebers beantworten. Das schließt die pauschale Weitergabe medizinischer Daten aus.

19.2.5
Konsequenzen meiner Prüfungen

Die notwendigen Schritte ergeben sich aus meinen Feststellungen:

a) Die Tätigkeit der Versorgungsverwaltung bei Dienstunfähigkeitsuntersuchungen ist auf eine tragfähige Grundlage zu stellen.

b) Die Einwilligungserklärungen für die Datenanforderung bei dritten Stellen sind zu vereinheitlichen und datenschutzgerecht zu gestalten.

c) Die Unterrichtung und Erklärung auf dem Anamnesebogen müssen voneinander getrennt und in Teilen neu formuliert werden.

Das Sozialministerium ist vom Ergebnis meiner Untersuchungen unterrichtet worden.

20. Verkehrswesen

Inhalt von Führerscheinakten

Entscheidungen, die in örtlichen Fahrerlaubnisregistern enthalten und auch im Verkehrszentralregister einzutragen sind, unterliegen den in § 29 Straßenverkehrsgesetz näher bezeichneten Tilgungsfristen. Die neue Regelung wird von einigen Fahrerlaubnisbehörden noch nicht beachtet.

Wiederholte Eingaben an meine Behörde im Berichtsjahr haben gezeigt, dass die – im Rahmen der Novellierung des Straßenverkehrsgesetzes (StVG) – neu aufgenommene Regelung des § 29 StVG zu den Tilgungsfristen von den für die Fahrerlaubnis zuständigen Behörden noch nicht überall beachtet wird, sondern alle Entscheidungen nach wie vor „lebenslänglich“ aufbewahrt werden.

So wurde z. B. einem Verkehrsteilnehmer im Jahr 1963 der Führerschein entzogen. Gemäß § 28 Abs. 3 Satz 2 StVG wurde die rechtskräftige Entscheidung des Strafgerichts, die die Entziehung der Fahrerlaubnis anordnete, im Verkehrszentralregister und im örtlichen Fahrzeugregister gespeichert. Die Speicherung im örtlichen Fahrzeugregister wurde auch nach Ablauf der Fristen nach § 29 StVG aufrechterhalten. Das war unzulässig.

Fahrerlaubnisbehörden führen gemäß § 48 Abs. 1 Nr. 2 StVG im Rahmen ihrer örtlichen Zuständigkeit ein Register, in dem unter anderem Entscheidungen enthalten sind, die Bestand, Art und Umfang von Fahrerlaubnissen betreffen. In § 50 Abs. 2 StVG ist geregelt, welche Daten darüber hinaus in diesen örtlichen Fahrerlaubnisregistern enthalten sein dürfen, nämlich z. B. der Widerruf und die Rücknahme der Fahrerlaubnis, Fahrverbote und die Sicherstellung und Verwahrung von Führerscheinen.

Grundsätzlich gilt für die in den örtlichen Fahrzeugregistern enthaltenen Registerauskünfte, Führungszeugnisse, Gutachten und Gesundheitszeugnisse, dass diese gem. § 2 Abs. 9 StVG nach zehn Jahren zu vernichten sind, es sei denn, dass mit ihnen im Zusammenhang stehende Eintragungen im Verkehrszentralregister oder im zentralen Fahrerlaubnisregister nach den Bestimmungen für diese Register zu einem späteren Zeitpunkt zu tilgen oder zu löschen sind. In diesem Fall ist für die Vernichtung oder Löschung der spätere Zeitpunkt maßgeblich. Ist aufgrund der besonderen Art der Führung der Akten die Vernichtung nicht oder nur mit unverhältnismäßigem Aufwand möglich, ist zumindest eine Sperrung der Daten notwendig. Das bedeutet, dass die entsprechenden Daten dann zwar noch in der Akte enthalten sind, jedoch dem Verwertungsverbot unterliegen.

Sind – wie im beschriebenen Fall – in den örtlichen Fahrerlaubnisregistern Entscheidungen enthalten, die auch im Verkehrszentralregister einzutragen sind, gelten gemäß § 61 Abs. 3 StVG die in § 29 StVG geregelten Tilgungsfristen auch für die im örtlichen Register gespeicherten Eintragungen.

§ 29 StVG

(1) Die im Register gespeicherten Eintragungen werden nach Ablauf der in Satz 2 bestimmten Fristen getilgt. Die Tilgungsfristen betragen

1. zwei Jahre

   bei Entscheidungen wegen einer Ordnungswidrigkeit,

2. fünf Jahre

   a) bei Entscheidungen wegen Straftaten mit Ausnahme von Entscheidungen wegen Straftaten nach § 315c Abs. 1 Nr. 1 Buchstabe a, den §§ 316 und 323a des Strafgesetzbuches und Entscheidungen, in denen die Entziehung der Fahrerlaubnis nach den §§ 69 und 69b des Strafgesetzbuches oder eine Sperre nach § 69a Abs. 1 Satz 3 des Strafgesetzbuches angeordnet worden ist,

   b) bei von der Fahrerlaubnisbehörde verhängten Verboten oder Beschränkungen, ein fahrerlaubnisfreies Fahrzeug zu führen,

   c) bei der Teilnahme an einem Aufbauseminar oder einer verkehrspsychologischen Beratung.

3. zehn Jahre

   in allen übrigen Fällen

...

(6) Sind im Register mehrere Entscheidungen nach § 28 Abs. 3 Nr. 1 und 9 über eine Person eingetragen, so ist die Tilgung einer Eintragung vorbehaltlich der Regelungen in den Sätzen 2 bis 5 erst zulässig, wenn für alle betreffenden Eintragungen die Voraussetzungen der Tilgung vorliegen. Eintragungen von Entscheidungen wegen Ordnungswidrigkeiten hindern nur die Tilgung von Entscheidungen wegen anderer Ordnungswidrigkeiten. Die Eintragung einer Entscheidung wegen einer Ordnungswidrigkeit – mit Ausnahme von Entscheidungen wegen einer Ordnungswidrigkeit nach § 24a – wird spätestens nach Ablauf von fünf Jahren getilgt. Die Tilgung einer Eintragung einer Entscheidung wegen einer Ordnungswidrigkeit unterbleibt in jedem Fall so lange, wie der Betroffene im Zentralen Fahrerlaubnisregister als Inhaber einer Fahrerlaubnis auf Probe gespeichert ist. Wird eine Eintragung getilgt, so sind auch die Eintragungen zu tilgen deren Tilgung nur durch die betreffende Eintragung gehemmt war.

...

Allerdings darf eine Eintragung erst dann getilgt werden, wenn für alle betreffenden Eintragungen die Voraussetzungen für die Tilgung vorliegen. Dies war im beschriebenen Fall eindeutig.

Gemäß § 61 Abs. 3 StVG in Verbindung mit den in § 29 StVG aufgeführten Tilgungsfristen, hätte die Speicherung über die Entziehung der Fahrerlaubnis unmittelbar nach In-Kraft-Treten der Novellierung des StVG bereits gelöscht werden müssen. Meine Prüfung ergab jedoch, dass die Angaben über den Entzug der Fahrerlaubnis im Jahr 1963 nach wie vor im örtlichen Fahrerlaubnisregister gespeichert waren. Die zuständige Behörde löschte die Daten nach meinem Hinweis auf die gesetzlich vorgeschriebene Frist.

21. Vermessungswesen

Erste Erfahrungen mit dem zum 1. Juli 2002 geänderten Hessischen Vermessungsgesetz

Mit der Novellierung des Hessischen Vermessungsgesetzes wurde die Liegenschaftskataster-Abrufverordnung vom 28. November 2000 aufgehoben. Statt dessen enthalten jetzt die Vorschriften des § 16 und § 16a Hessisches Vermessungsgesetz die Regelungen zur Einsicht beziehungsweise Auskunft aus dem Liegenschaftskataster sowie die Voraussetzungen für einen automatisierten Datenabruf.

Im Gegensatz zur früheren Regelung ist nach dem jetzigen § 16 Hessisches Vermessungsgesetz (HVG) für die Auskunft oder Einsicht in das Liegenschaftskataster nur noch dann ein berechtigtes Interesse glaubhaft zu machen, wenn auf personenbezogene Daten zugegriffen werden soll. Personenbezogene Daten sind hierbei die Namen von natürlichen Personen, deren Geburtsdatum sowie deren Anschrift. Alle anderen Daten des Liegenschaftskatasters können von jeder Person oder Stelle eingesehen werden.

§ 16 HVG

(1) Jede Person oder Stelle kann das Liegenschaftskataster und seine Unterlagen sowie die Ergebnisse der Landesvermessung einsehen, Auskunft und auf Antrag Auszüge daraus erhalten.

(2) Die Einsicht in die personenbezogenen Daten sowie das Erteilen von entsprechenden Auskünften und Auszügen ist nur zulässig, wenn der Nutzer ein berechtigtes Interesse an der Kenntnis dieser Daten glaubhaft macht. Personenbezogene Daten im Sinne dieses Gesetzes sind die Namen von natürlichen Personen, deren Geburtsdatum und deren Anschrift.

(3) Abs. 2 gilt nicht für

1. Gemeinden, Landkreise und Finanzbehörden, soweit die personenbezogenen Daten zur rechtmäßigen Erfüllung ihrer Aufgaben benötigt werden. Unter den gleichen Voraussetzungen dürfen die Angaben innerhalb der Gemeinde und Kreisverwaltungen weitergegeben werden.
2. sonstige öffentlichen Stellen, Öffentlich bestellte Vermessungsingenieurinnen und -ingenieure sowie Notarinnen und Notare, soweit die personenbezogenen Daten im Einzelfall zur rechtmäßigen Erfüllung ihrer Aufgaben erforderlich sind.

(4) Über die Angaben und Ergebnisse hinaus, die nach Abs. 1 bis 3 zulässigerweise abgegeben werden dürfen, dürfen auch andere mit diesen verbundene personenbezogene Angaben und Ergebnisse abgegeben werden, wenn die Trennung der verbundenen von den abzugebenden personenbezogenen Angaben und Ergebnissen nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.

(5) Die Angaben des Liegenschaftskatasters und die Ergebnisse der Landesvermessung dürfen nur für den Zweck verwendet werden, für den sie erteilt wurden. Eine Verwendung für andere Zwecke ist nur mit ausdrücklicher Genehmigung der abgebenden Kataster- und Landesvermessungsbehörden zulässig.

(6) Angaben aus dem Zahlenwerk des Liegenschaftskatasters dürfen nur den Vermessungsstellen nach § 15 Abs. 1 uneingeschränkt überlassen werden. Beratende Ingenieurinnen und Ingenieure der Fachrichtung Vermessungswesen und fachlich vergleichbare Stellen dürfen Angaben aus dem Zahlenwerk des Liegenschaftskatasters zur Erfüllung ihrer Aufgaben erhalten, wenn Sie den Verwendungszweck darlegen und gewährleistet ist, dass die Angaben sachgerecht sowie nicht für die Ausführung von Katastervermessungen oder entsprechende Gutachten verwendet werden. Die oberste Kataster- und Vermessungsbehörde kann im Einzelfall Ausnahmen zulassen.

...

Die Daten des Liegenschaftskatasters können auch in automatisierter Form übermittelt werden. Hierbei muss eine Teilnahme am automatisierten Abrufverfahren über personenbezogene Daten vom Hessischen Landesvermessungsamt genehmigt werden. Soll die Genehmigung einer anderen Stelle als Gemeinden, Landkreisen, Finanzbehörden, sonstigen öffentlichen Stellen beziehungsweise öffentlich bestellten Vermessungsingenieurinnen und -ingenieuren oder Notarinnen und Notaren erteilt werden, so ist der Hessische Datenschutzbeauftragte vor Erteilung dieser Genehmigung zu hören.

§ 16a HVG

(1) Die Daten des Liegenschaftskatasters und die Ergebnisse der Landesvermessung können nach Maßgabe der Abs. 2 bis 5 auch in automatisierter Form abgegeben werden.

(2) Die Daten können regelmäßig übermittelt oder in einem automatisierten Abrufverfahren bereitgestellt werden.

(3) Die Teilnahme an einem automatisierten Abrufverfahren über personenbezogene Daten bedarf der Genehmigung. Die Genehmigung wird auf Antrag von der oberen Kataster- und Landesvermessungsbehörde unter den Bedingungen

des § 16, erforderlichenfalls mit Auflagen und unter dem Vorbehalt des Widerrufs, erteilt und auf den im Antrag zu benennenden Verwendungszweck begrenzt. Die Genehmigung darf nur erteilt werden, wenn sichergestellt ist, dass auf Seiten des Anwenders die Grundsätze einer ordnungsgemäßen Datenverarbeitung, das Datenschutzrecht und die Bestimmungen der für die Informations- und Kommunikationsdienste einschlägigen Normen eingehalten werden. An Stelle einer Genehmigung kann ein öffentlich-rechtlicher Vertrag abgeschlossen werden. Vor der Erteilung der Genehmigung an eine andere, in § 16 Abs. 3 nicht genannte Stelle oder vor Abschluss eines entsprechenden öffentlich-rechtlichen Vertrags ist der Hessische Datenschutzbeauftragte zu hören.

...

Bisher haben fünf Einrichtungen eine Genehmigung zur Teilnahme am automatisierten Abrufverfahren über personenbezogene Daten des Liegenschaftskatasters beantragt. Im einen Fall handelt es sich um ein Unternehmen, das auch bisher für städtebauliche Sanierungs- und Entwicklungsmaßnahmen Auszüge aus dem Liegenschaftskataster erhalten hat. Gegen die Erteilung der beantragten Genehmigung hatte ich keine datenschutzrechtlichen Bedenken. Im Fall eines Bankvereins konnte ich aufgrund der eingereichten Unterlagen zunächst keine Erforderlichkeit für die Erteilung einer Genehmigung erkennen, da jegliche Darlegung eines berechtigten Interesses fehlte.

Mit dem Landesvermessungsamt wurde vereinbart, dass mir das Amt die von den einzelnen Antragstellern vorgetragenen Gründe für die Zulassung eines Online-Zugriffs zuleitet, so dass das Vorliegen eines berechtigten Interesses seitens der Antragsteller überprüft werden kann.

Im Freigabebescheid, den das Landesvermessungsamt der abrufberechtigten Stelle erteilt, sind die Voraussetzungen genau festgelegt, unter denen für diese Stelle der Datenabruf im Einzelfall rechtlich zulässig sein soll. Alle Datenabrufe werden gemäß § 16a Abs. 4 HVG protokolliert. Die Protokollierung beinhaltet auch den Verwendungszweck.

§ 16a Abs. 4 HVG

Die Abrufe sind zum Zweck der Kontrolle zu protokollieren. Dabei werden die Benutzererkennung, Datum und Uhrzeit, der Verwendungszweck (Aktenzeichen oder Bearbeitungs- oder Auftragsnummer) und die Ordnungsmerkmale der abgerufenen Daten (Gemarkungsname und -nummer, Flur- und Flurstücksnummer oder Grundbuchblattnummer) erfasst. Die Protokollierung erfolgt durch die Kataster- und Landesvermessungsbehörden oder durch die von diesen mit der Verarbeitung der Daten beauftragten Stelle. Die Protokolle sind nach Ablauf von zwölf Monaten seit ihrer Erfassung zu löschen.

Mit dem Hessischen Ministerium für Wirtschaft, Verkehr und Landesentwicklung habe ich vereinbart, dass im Frühjahr 2003 mehrere Institutionen, denen eine Abrufberechtigung personenbezogener Daten aus dem Liegenschaftsbuch erteilt worden ist, daraufhin überprüft werden, ob die getätigten Abrufe innerhalb des bei Antragstellung benannten Verwendungszwecks erfolgt sind und auch nur für diesen weiterverarbeitet werden.

22. Kammern

Hessisches Architekten- und Stadtplanergesetz

Änderung des Ingenieurkammergesetzes

Mit dem Gesetz zur Reform über die Führung der Berufsbezeichnung in den Bereichen der Architektur und der Stadtplanung wurde das Hessische Architektengesetz von 1977 und das Ingenieurkammergesetz umfassend novelliert.

In Abstimmung mit dem Hessischen Datenschutzbeauftragten wurden in beide Gesetze ausführliche Datenverarbeitungsregelungen aufgenommen.

Das Gesetz zur Reform über die Führung der Berufsbezeichnung in den Bereichen der Architektur und der Stadtplanung vom 23. Mai 2002 (GVBl. I S. 182) ist am 1. August 2002 in Kraft getreten. Es handelt sich um ein Artikelgesetz. Artikel 1 enthält das Hessische Architekten- und Stadtplanergesetz (HASG), in Artikel 2 findet sich ein Gesetz zur Änderung des Ingenieurkammergesetzes.

22.1
Hessisches Architekten- und Stadtplanergesetz

Entsprechend meiner langjährigen Forderung hat der Gesetzgeber in § 3 Abs. 2 HASG detailliert festgelegt, welche personenbezogenen Architektendaten in das von der Architektenkammer zu führende Berufsverzeichnis (bislang Architektenliste genannt) aufzunehmen sind. Maßstab war dabei, welche Daten die Kammer für interne Angelegenheiten, die Überwachung der Obliegenheiten und Berufspflichten der Kammermitglieder und für die Erfüllung berechtigter Informationswünsche Dritter, hier in erster Linie der Auftraggeber der Architekten, benötigt. Neben diesem

Pflichtkatalog können mit Einwilligung der Betroffenen zusätzliche im Gesetz definierte Daten in das Berufsverzeichnis aufgenommen werden (§ 3 Abs. 2 HASG). Auf EU-rechtlichen Vorgaben basiert § 3 Abs. 4 HASG. Die Vorschrift listet einige Daten auf, die für statistische Zwecke erhoben werden müssen und separat von den übrigen Daten in das Berufsverzeichnis einzutragen sind.

Das Gesetz regelt in § 4 Abs. 4 HASG die Auskunftspflichten der Betroffenen und bestimmt, welche Nachweisdokumente sie der Kammer vorzulegen haben. Im Unterschied zur bisherigen Datenerhebung für die Architektenliste erfolgt damit die Datenerhebung für das Berufsverzeichnis auf einer ausreichenden Rechtsgrundlage.

Für die Datenverarbeitung im Zusammenhang mit der Durchführung der Teilnahme an einer Versorgungseinrichtung schafft § 10 Abs. 6 HASG die notwendige gesetzliche Verarbeitungsbefugnis.

Der Architektenkammer werden erstmals präzise Löschungsfristen vorgeschrieben. Fünf Jahre nach der Löschung der Eintragung in einem Berufsverzeichnis oder Beendigung der Mitgliedschaft müssen alle gespeicherten Daten gelöscht werden (§ 16 Abs. 3 HASG); die personenbezogenen Daten zu einem Berufsordnungsverfahren und einer Rüge sind fünf Jahre nach Bestandskraft oder Einstellung zu löschen (§ 18 Abs. 10 HASG).

Die Datenübermittlungen der Kammern an Dritte, insbesondere die Veröffentlichung von Mitgliederdaten, hat der Gesetzgeber in § 16 Abs. 4 HASG geregelt. Die Kammer darf Mitgliederdaten nur veröffentlichen, wenn die Betroffenen zuvor schriftlich zugestimmt haben.

22.2
Ingenieurkammergesetz

Die Änderung des Ingenieurkammergesetzes (Art. 2 des Artikelgesetzes vom 23. Mai 2002) sieht an die Verarbeitungsvorschriften des HSAG angelehnte Regelungen vor.

23. Bilanz

23.1
Einsatz des so genannten IMSI-Catchers durch Strafverfolgungsbehörden und Polizei (30. Tätigkeitsbericht, Ziff. 13.2)

Der Gesetzgeber hat im Laufe des Jahres die Regelungen in der Strafprozessordnung zur Überwachung der Telekommunikation überarbeitet. Dabei wurde mit § 100i Strafprozessordnung (StPO) auch die von mir seit langem geforderte gesetzliche Grundlage zum Einsatz des so genannten IMSI-Catchers durch die Strafverfolgungsbehörden geschaffen.

§ 100i Abs. 1 bis 4 StPO

(1) Durch technische Mittel dürfen

1. zur Vorbereitung einer Maßnahme nach § 100a die Geräte- und Kartennummer sowie
2. zur vorläufigen Festnahme nach § 127 Abs. 2 oder Ergreifung des Täters aufgrund eines Haftbefehls oder Unterbringungsbefehls der Standort eines aktiv geschalteten Mobilfunkendgerätes ermittelt werden.

(2) Die Maßnahme nach Absatz 1 Nr. 1 ist nur zulässig, wenn die Voraussetzungen des § 100a vorliegen und die Durchführung der Überwachungsmaßnahme ohne die Ermittlung der Geräte- oder Kartennummer nicht möglich oder wesentlich erschwert wäre. Die Maßnahme nach Absatz 1 Nr. 2 ist nur im Falle einer Straftat von erheblicher Bedeutung und nur dann zulässig, wenn die Ermittlung des Aufenthaltsortes des Täters auf andere Weise weniger erfolgversprechend oder erschwert wäre; § 100c Abs. 2 Satz 2 gilt entsprechend. Die Maßnahme nach Absatz 1 Nr. 2 ist im Falle einer Straftat von erheblicher Bedeutung auch zulässig, wenn die Ermittlung des Aufenthaltsortes des Täters zur Eigensicherung der zur vorläufigen Festnahme oder Ergreifung eingesetzten Beamten des Polizeidienstes erforderlich ist.

(3) Personenbezogene Daten Dritter dürfen anlässlich solcher Maßnahmen nur erhoben werden, wenn dies aus technischen Gründen zur Erreichung des Zwecks nach Absatz 1 unvermeidbar ist. Über den Datenabgleich zur Ermittlung der gesuchten Geräte- und Kartennummer hinaus dürfen sie nicht verwendet werden und sind nach Beendigung der Maßnahme unverzüglich zu löschen.

(4) § 100b Abs. 1 gilt entsprechend; ...

§ 100b Abs. 1 StPO

Die Überwachung und Aufzeichnung der Telekommunikation (§ 100a) darf nur durch den Richter angeordnet werden. Bei Gefahr im Verzug kann die Anordnung auch von der Staatsanwaltschaft getroffen werden. Die Anordnung der Staatsanwaltschaft tritt außer Kraft, wenn sie nicht binnen drei Tagen von dem Richter bestätigt wird.

Meine Bedenken wegen des Fehlens einer Rechtsgrundlage sind damit beseitigt.

Vor Einsätzen des IMSI-Catchers ist zu bedenken, dass die technischen Bedingungen zwangsläufig dazu führen, dass eine Vielzahl von Telefonverbindungen rechtstreuer Bürgerinnen und Bürger mit erfasst werden. Außerdem wird die bestimmungsgemäße Nutzung des Mobiltelefons für den Zeitraum des Einsatzes unterbunden, obwohl die üblichen Gesprächskosten anfallen. Die richterliche Entscheidung muss daher Ermittlungszwecke und Datenschutz abwägen und insbesondere hinsichtlich der Dauer der Maßnahme berücksichtigen.

23.2
Neue Informationssysteme für die Polizei
(30. Tätigkeitsbericht, Ziff. 8.1)

Wie im letzten Jahr angekündigt, ist das neue Informationssystem für die Polizei – POLAS – nunmehr hessenweit in Betrieb.

Das Sicherheitskonzept für die Hessische Polizei, das auch den Betrieb von POLAS abdeckt, liegt seit Dezember 2001 vor. Es wurde von einer Unternehmensberatung auf Grundlage des IT-Sicherheitshandbuchs und des IT-Grundschutzhandbuchs des Bundesamts für die Sicherheit in der Informationstechnik (BSI) erstellt. Es verbietet sich, an dieser Stelle einzelne konkrete Maßnahmen aus dem Konzept darzustellen. Einige generelle Maßnahmen sollen jedoch genannt werden, da sie für den Erfolg entscheidend sein können.

– Es wird ein IT-Sicherheitsmanagement-Team gebildet, welches sämtliche Belange der IT-Sicherheit regelt und Pläne, Vorgaben und Richtlinien erarbeitet beziehungsweise koordiniert. Dabei müssen insbesondere für die Polizei die Verantwortlichkeiten geklärt und die Kommunikationswege festgelegt werden. Es handelt sich um einen wesentlichen Schritt, wenn eine adäquate IT-Sicherheit erreicht und beibehalten werden soll.
– Es wird ein IT-Sicherheitsbeauftragter bei der hessischen Polizei benannt. Diese Funktion ist im IT-Sicherheitsmanagement von zentraler Bedeutung.
– Das Sicherheitskonzept wird fortgeschrieben. Ein Sicherheitskonzept ist kein statisches Gebilde. Es muss an technische und organisatorische Veränderungen und an neue Bedrohungslagen angepasst werden. Dabei gibt es in der Praxis oft Probleme. Die tägliche Arbeit, den Betrieb aufrecht zu erhalten, lässt nicht genug Zeit für konzeptionelle Tätigkeiten. So müssen beispielsweise Firewalls stetig überprüft und gegenüber neuen Angriffstechniken angepasst werden. Die erforderliche Ergänzung oder Änderung des Konzepts erfolgt erfahrungsgemäß zu selten.
– Regelmäßige Überprüfungen der IT-Sicherheitsmaßnahmen sollen gewährleisten, dass das angestrebte Sicherheitsniveau nicht nur erreicht, sondern auch beibehalten wird.
– Durch Schulungen und andere Maßnahmen sollen die Bediensteten, die mit POLAS arbeiten, für die Thematik sensibilisiert werden.

Um das Konzept umzusetzen, wurde eine Arbeitsgruppe unter Leitung des Präsidiums für Technik, Logistik und Verwaltung eingerichtet. An den Sitzungen dieser Arbeitsgruppe nimmt ein Mitarbeiter meiner Dienststelle als beratendes Mitglied teil.

Im Jahr 2002 ist auch die zweite Komponente der Informationssysteme in Betrieb gegangen, die computerunterstützte Vorgangsbearbeitung „ComVor“. Diese soll helfen, die Papierflut in den Polizeidienststellen einzudämmen und das Erfassen von neuen Sachverhalten wie etwa Strafanzeigen zu beschleunigen. Den Bürgerinnen und Bürgern soll dies durch verkürzte Wartezeiten zu Gute kommen.

Dieses Verfahren erleichtert für die Dienststellen den Zugriff auf einzelne Vorgänge, die in anderen Dienststellen federführend bearbeitet werden. Das Verfahren ist aus datenschutzrechtlichen Gründen so konstruiert, dass immer nur ein konkreter Vorgang erschließbar ist. So ist es z. B. nicht möglich, hessenweit zu suchen, ob und in welcher Rolle (Verdächtiger, Opfer, Zeuge) eine Person in verschiedenen Ermittlungsverfahren auftaucht.

Bis jetzt sind mir aus der polizeilichen Praxis keine datenschutzrechtlichen Probleme mit diesem Verfahren bekannt geworden.

23.3
Projekt „Elektronische Fußfessel“
(28. Tätigkeitsbericht, Ziff. 6, 29. Tätigkeitsbericht, Ziff. 20.2)

Anlässlich einer Prüfung der Hessischen Zentrale für Datenverarbeitung – Außenstelle Hünfeld – haben meine Mitarbeiter auch die dortige Abwicklung des Projektes „Elektronische Fußfessel“ überprüft.

Dabei wurde festgestellt, dass die inhaltlichen Festlegungen, welche Daten in Hünfeld und wie lange verarbeitet werden, nicht immer im ausreichenden Maße vom Ministerium vorgegeben werden, sondern vom Rechenzentrum als Auftragnehmer entschieden wurden.

Darüber hinaus hat sich meines Erachtens deutlich gezeigt, dass – entgegen der Auffassung des Ministeriums – keine Notwendigkeit besteht, alle im Laufe des Tages im System anfallenden Meldungen längerfristig aufzubewahren. Not-

wendig ist dies nur für die sog. Alarmmeldungen, in denen Unregelmäßigkeiten beziehungsweise Abweichungen vom vorgesehenen Tagesplan dokumentiert werden. Das Ministerium hat nunmehr die Hessische Zentrale für Datenverarbeitung angewiesen, alle anderen Daten umgehend zu löschen.

Nach Abschluss der zweijährigen Modellphase soll nunmehr der Einsatz der elektronischen Fußfessel schrittweise auf alle Landgerichtsbezirke ausgedehnt werden. Zur Rechtfertigung beruft sich der Justizminister u. a. auf die Ergebnisse des begleitenden Forschungsprojektes. Details der Begleitforschung sind mir leider nicht bekannt. Insbesondere die Fragestellung, wie sich die besonderen Rahmenbedingungen, insbesondere die freiwillige Teilnahme der Probanden und die Einbeziehung möglicher Familienangehöriger ausgewirkt haben, wären auch aus Sicht des Datenschutzes interessant.

Ich habe zudem den Hessischen Justizminister nochmals darauf hingewiesen, dass aus meiner Sicht eine ausreichende Rechtsgrundlage für einen so schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung nicht vorhanden ist. Die Fußfessel nähert sich hinsichtlich der Eingriffsintensität der Führungsaufsicht und bedarf daher zwingend der gesetzlichen Regelung.

23.4
Richtlinien für kriminalpolizeiliche personenbezogene Sammlungen
(30. Tätigkeitsbericht, Ziff. 8.4)

Die Richtlinien für kriminalpolizeiliche personenbezogene Sammlungen wurden zum 1. Oktober 2002 neu gefasst. Von meinen Änderungsvorschlägen zu dem Entwurf, über die ich in meinem letzten Bericht informierte, hat das Innenministerium einen Teil berücksichtigt, einen anderen Teil verworfen.

Nicht berücksichtigt wurde u. a. meine Forderung, die Aufbewahrung von erkennungsdienstlichen Unterlagen an strengere Voraussetzungen zu knüpfen, als sie für die Aufbewahrung von sonstigen Akten gelten. Nach den Richtlinien genügt für die weitere Aufbewahrung, dass ein Anfangsverdacht nicht ausgeräumt wurde.

Da die Richtlinien nicht zwischen erkennungsdienstlichen Unterlagen und sonstigen Akten unterscheiden, ist damit zu rechnen, dass künftig erkennungsdienstliche Unterlagen auch dann aufbewahrt werden, wenn „nur“ diese Voraussetzung erfüllt ist. Tatsächlich hat aber die Rechtsprechung zu § 81b Strafprozessordnung (StPO) die Voraussetzung entwickelt, dass zu Zwecken des Erkennungsdienstes (also nach Abschluss des Ermittlungsverfahrens) die Weiterspeicherung nur dann erforderlich und zulässig ist, wenn nach der Art und Schwere der Straftat ein besonderes kriminalistisches Interesse besteht.

Maßgebend ist, ob nach kriminalistischer Erfahrung Anhaltspunkte dafür vorliegen, dass der Beschuldigte künftig strafrechtlich in Erscheinung treten wird und dass die angefertigten Unterlagen dann die Ermittlungen der Polizei fördern können (dazu beispielsweise Kleinknecht/Meyer-Goßner, StPO, § 81b Rdnr. 18). Diese Prognose zu stellen, sieht die Richtlinie nicht vor. Rechtsverstöße scheinen daher vorprogrammiert.

23.5
Modellprojekt Mammographie-Screening
(30. Tätigkeitsbericht, Ziff. 11.1)

Im letzten Jahr hatte ich von dem Modellprojekt zur Einführung einer qualitätsgesicherten Brustkrebsfrüherkennung mittels Mammographie-Screening in Wiesbaden berichtet. Gegenstand des Modellprojekts ist die praktische Erprobung von Strukturen, innerhalb derer künftig qualitätsgesichertes Mammographie-Screening in Deutschland flächendeckend durchgeführt werden kann.

Die Umsetzung des Konzepts haben das für den privaten Bereich – und damit auch für den Verein Mammographie-Screening – zuständige Dezernat Datenschutz des Regierungspräsidiums Darmstadt und ich soweit es grundsätzliche Fragen des Konzepts betrifft überprüft.

Bei der Prüfung der getroffenen technischen und organisatorischen Sicherungsmaßnahmen konnten wir feststellen, dass die im Datenschutzkonzept vorgesehenen Maßnahmen weitgehend umgesetzt waren. Die beiden wesentlichen vorgefundenen Mängel sind wie folgt zu skizzieren.

- Das Konzept sah eine personelle Trennung von zwei Administrationsfunktionen vor. Ein Administrator sollte die Datenbank mit den medizinischen Daten betreuen, ein anderer die Datenbank mit den Einladungsdaten. Zum Zeitpunkt der Prüfung musste jedoch eine Person in Personalunion die Aufgaben wahrnehmen. Es wurde dazu mitgeteilt, dass eine Mitarbeiterin beziehungsweise ein Mitarbeiter eingestellt werden soll, um entsprechend dem Konzept zu verfahren.
- Entgegen dem Konzept waren die BIOS-Einstellungen der Server so, dass ein Booten von Disketten aus möglich war. An einem der Server war das BIOS auch nicht durch ein Passwort gegen unbefugte Änderungen geschützt. Kurze Zeit vorher hatte eine Wartung stattgefunden. Es wurde daher vermutet, dass der Techniker die ursprünglichen Einstellungen für die Wartung geändert hatte, ohne sie anschließend wieder zurück zu setzen. Die nach dem Konzept erforderlichen Einstellungen wurden noch während der Prüfung vorgenommen. Ausreichende räumliche

Sicherungsmaßnahmen waren getroffen, denn die Server sind in abgeschlossenen Serverschränken in einem nur wenigen Personen zugänglichen Raum untergebracht. Der beschriebene Mangel konnte kaum durch Personen ohne Zutrittsrechte ausgenutzt werden.

Im Ergebnis war das Konzept in einer Art und Weise umgesetzt, dass ich keine Bedenken wegen unzureichender Sicherungsmaßnahmen habe, wenn Einwohnermeldeämter dem Verein die vorgesehenen Daten übermitteln.

23.6
Datenschutz in der Abgabenordnung
(30. Tätigkeitsbericht, Ziff. 10.2 und 27.7)

In den Novellierungsprozess der Abgabenordnung unter datenschutzrechtlichen Gesichtspunkten ist Bewegung gekommen.

Der Bundesdatenschutzbeauftragte hat im August 2002 – in Zusammenarbeit mit den Datenschutzbeauftragten der Länder dem Bundesfinanzministerium einen ausführlichen Anforderungskatalog mit den aus datenschutzrechtlicher Sicht notwendigen Änderungen vorgelegt. Aufgrund dieses Schreibens ist es zu einem ersten Besprechungstermin zwischen den Vertretern der Datenschutzbeauftragten des Bundes und der Länder sowie der Steuerverwaltung auf Bundes- und Landesebene gekommen. Das bisherige Ergebnis ist dahin zusammenzufassen, dass beide Seiten jeweils vor dem Hintergrund ihres Verfassungsauftrages (Gleichmäßigkeit und Vollständigkeit der Besteuerung beziehungsweise Wahrung des Persönlichkeitsrechts auf informationelle Selbstbestimmung) ihre Standpunkte verdeutlichten, gleichwohl aber eine gemeinsame Zielrichtung erarbeiteten:

1. Der Wunsch der Regierungsvertreter, eine bereichsspezifische Regelung in der Abgabenordnung zu treffen, ist von Seiten des Datenschutzes akzeptiert worden.
2. Die bestehenden Lücken in der Abgabenordnung sollen geschlossen werden. Dies gilt beispielsweise für Regelungen über ein Akteneinsichtsrecht, Datensammlungen und Kontrollmitteilungen.
3. Schon heute bestehende Durchbrechungen des Steuergeheimnisses durch interne Querinformationen innerhalb der Finanzverwaltung sollen auf normenklare Ermächtigungen umgestellt werden, da die Generalklausel des § 88a Abgabenordnung (AO) den Anforderungen der verfassungsgerichtlichen Judikatur nicht entspricht (etwa für Kontrollmitteilungen außerhalb von § 194 Abs. 3 AO und Vorratsspeicherungen).
4. Neuere Erlasse – etwa zum Verfahren ZAUBER (**Z**entrale Datenbank zur Speicherung und **A**uswertung von **U**msatzsteuer-**B**etrugsfällen und **E**ntwicklung von **R**isikoprofilen) sollen hinsichtlich der Eingriffsrechte und der Befugnisse zu Ergänzungen überarbeitet werden. Auch die Steuerdatenabrufverordnung soll diesen datenschutzrelevanten Forderungen angepasst werden.

Eine Fortsetzung der Koordinierungsgespräche ist für die nächste Zeit in Aussicht genommen.

23.7
Zusammenarbeit bei der Produktion von Fernsehsendungen – Reality-TV
(30. Tätigkeitsbericht, Ziff. 8.2)

In meinem 30. Tätigkeitsbericht hatte ich darauf hingewiesen, dass eine Zusammenarbeit zwischen der Polizei und Fernseheinrichtungen bei polizeilichen Einsätzen nur unter bestimmten, genau festgelegten Richtlinien, erfolgen darf. Die durch Erlass vom 21. Dezember 1999 festgelegten Richtlinien über Mitteilungen der Polizei an die Presse und den Rundfunk wurden deshalb unter meiner Mitwirkung um Regelungen über die Zusammenarbeit mit Fernseheinrichtungen per Erlass vom 10. Mai 2001 ergänzt.

Im laufenden Berichtsjahr wurde eine Beschwerde an mich herangetragen, wonach bei einer durchgeführten Geschwindigkeitskontrolle durch Beamte einer Polizeiautobahnstation in Osthessen, bei der ein Fernsehteam anwesend war, Filmaufnahmen gemacht worden seien, obwohl der Betroffene widersprochen habe. Dieser Beschwerde bin ich nachgegangen. Meine datenschutzrechtliche Prüfung ergab, dass die Polizeiautobahnstation die bestehenden Erlasse eingehalten hat. Die Mitarbeiter des Fernsehteams wurden vor Beginn des Einsatzes durch die zuständigen Polizeibeamten ausdrücklich darauf hingewiesen, dass Verkehrsteilnehmer nur dann gefilmt oder interviewt werden dürfen, wenn diese der Maßnahme zustimmen. Da der Betroffene seine Zustimmung zu Interviews und Filmaufnahmen verweigerte, wurden durch das Fernsehteam weder Daten noch Filmaufnahmen gespeichert beziehungsweise aufgezeichnet. Die Beschwerde war somit unbegründet. Eine Verletzung datenschutzrechtlicher Belange erfolgte nicht.

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

24.1
Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. März 2002

Biometrische Merkmale in Personalausweisen und Pässen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eingehend über Geeignetheit, Erforderlichkeit und Angemessenheit der beabsichtigten Einführung biometrischer Merkmale in Ausweisen und Pässen diskutiert. Sie hat ein Positionspapier des Arbeitskreises Technik, das detaillierte Prüfpunkte für die Erprobungsphase einer solcher Maßnahme nennt, zustimmend zur Kenntnis genommen. Für den Fall, dass das Vorhaben trotz noch bestehender Bedenken realisiert werden sollte, hat sie übereinstimmend folgende Anforderungen formuliert:

1. Fälschliche Zurückweisungen berechtigter Personen durch automatisierte Personenerkennungssysteme sind auch bei ständiger Verbesserung der Technik prinzipiell nicht zu vermeiden. Es dürfen deshalb nur Verfahren in Betracht gezogen werden, bei denen die Fehlerquote zumutbar gering ist. In Fehlerfällen muss dafür Sorge getragen werden, dass eine die Betroffenen nicht diskriminierende rasche Aufklärung erfolgt.
2. Zu berücksichtigen ist, dass bei der Anwendung biometrischer Verfahren Zusatzinformationen anfallen können (z. B. Krankheits-, Unfall-, Beschäftigungsindikatoren). Es muss sichergestellt werden, dass die gespeicherten und verarbeiteten Daten keine Rückschlüsse auf zusätzliche personenbezogene Merkmale erlauben.
3. Systeme, die biometrische Daten aus Ausweisen ohne Kenntnis der Betroffenen verarbeiten (sog. passive Systeme), sind abzulehnen.
4. Der Gesetzgeber hat die Verwendung biometrischer Daten in Ausweisen und Pässen grundsätzlich auf die Feststellung beschränkt, dass die dort gespeicherten Daten mit den Merkmalen der jeweiligen Ausweisinhaber und -inhaberinnen übereinstimmen; dies muss erhalten bleiben. Die Verwendung der biometrischen Merkmale für andere öffentliche Zwecke (außer der gesetzlich zugelassenen Verwendung aus dem Fahndungsbestand) wie auch für privatrechtliche Zwecke (Versicherung, Gesundheitssystem) ist auszuschließen. Deshalb hat der Gesetzgeber zu Recht die Einrichtung zentraler Dateien ausgeschlossen. Diese gesetzgeberische Entscheidung darf nicht durch den Aufbau dezentraler Dateien umgangen werden.
5. Die Entscheidung über das auszuwählende biometrische Erkennungssystem verlangt ein abgestimmtes europäisches Vorgehen.

24.2
Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. März 2002

Umgang mit personenbezogenen Daten bei Anbietern von Tele-, Medien- und Telekommunikationsdiensten

Mit der rasch wachsenden Nutzung des Internet kommt dem datenschutzgerechten Umgang mit den dabei anfallenden Daten der Nutzerinnen und Nutzer immer größere Bedeutung zu. Die Datenschutzbeauftragten haben bereits in der Vergangenheit (Entschließung der 59. Konferenz „Für eine freie Telekommunikation in einer freien Gesellschaft“) darauf hingewiesen, dass das Telekommunikationsgeheimnis eine unabdingbare Voraussetzung für eine freiheitliche demokratische Kommunikationsgesellschaft ist. Seine Geltung erstreckt sich auch auf Multimedia- und E-Mail-Dienste.

Die Datenschutzbeauftragten betonen, dass das von ihnen geforderte in sich schlüssige System von Regelungen staatlicher Eingriffe in das Kommunikationsverhalten, das dem besonderen Gewicht des Grundrechts auf unbeobachtete Telekommunikation unter Beachtung der legitimen staatlichen Sicherheitsinteressen Rechnung trägt, nach wie vor fehlt. Die Strafprozessordnung (und seit dem 1. Januar 2002 das Recht der Nachrichtendienste) enthält ausreichende Befugnisse, um den Strafverfolgungsbehörden (und den Nachrichtendiensten) im Einzelfall den Zugriff auf bei den Anbietern vorhandene personenbezogene Daten zu ermöglichen. Für eine zusätzliche Erweiterung dieser Regelungen z. B. hin zu einer Pflicht zur Vorratsdatenspeicherung besteht nicht nur kein Bedarf, sondern eine solche Pflicht würde dem Grundrecht auf unbeobachtete Kommunikation nicht gerecht, weil damit jede Handlung (jeder Mausklick) im Netz staatlicher Beobachtung unterworfen würde.

In keinem Fall sind Anbieter von Tele-, Medien- und Telekommunikationsdiensten berechtigt oder verpflichtet, generell Daten über ihre Nutzerinnen und Nutzer auf Vorrat zu erheben, zu speichern oder herauszugeben, die sie zu keinem Zeitpunkt für eigene Zwecke (Herstellung der Verbindung, Abrechnung) benötigen. Sie können nur im Einzelfall berechtigt sein oder verpflichtet werden, bei Vorliegen ausdrücklicher gesetzlicher Voraussetzungen Nachrichteninhalte, Verbindungsdaten und bestimmte Daten (Nutzungsdaten), die sie ursprünglich für eigene Zwecke benötigt haben und nach den Bestimmungen des Multimedia-Datenschutzrechts löschen müssten, den Strafverfolgungsbehörden (oder Nachrichtendiensten) zu übermitteln.

24.3
Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. März 2002

Datenschutzgerechte Nutzung von E-Mail und anderen Internet-Diensten am Arbeitsplatz

Immer mehr Beschäftigte erhalten die Möglichkeit, das Internet auch am Arbeitsplatz zu nutzen. Öffentliche Stellen des Bundes und der Länder haben beim Umgang mit den dabei anfallenden personenbezogenen Daten der Beschäftigten und ihrer Kommunikationspartner bestimmte datenschutzrechtliche Anforderungen zu beachten, die davon abhängen, ob den Bediensteten neben der dienstlichen die private Nutzung des Internet am Arbeitsplatz gestattet wird. Der Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat detaillierte Hinweise hierzu erarbeitet.

Insbesondere gilt Folgendes:

1. Die Arbeitsplätze mit Internet-Zugang sind so zu gestalten, dass keine oder möglichst wenige personenbezogene Daten erhoben werden. Die Nutzung des Internet am Arbeitsplatz darf nicht zu einer vollständigen Kontrolle der Bediensteten führen. Präventive Maßnahmen gegen eine unbefugte Nutzung sind nachträglichen Kontrollen vorzuziehen.
2. Die Beschäftigten sind umfassend darüber zu informieren, für welche Zwecke sie einen Internet-Zugang am Arbeitsplatz nutzen dürfen und auf welche Weise der Arbeitgeber die Einhaltung der Nutzungsbedingungen kontrolliert.
3. Fragen der Protokollierung und einzelfallbezogenen Überprüfung bei Missbrauchsverdacht sind durch Dienstvereinbarungen zu regeln. Die Kommunikation von schweigepflichtigen Personen und Personalvertretungen muss vor einer Überwachung grundsätzlich geschützt bleiben.
4. Soweit die Protokollierung der Internet-Nutzung aus Gründen des Datenschutzes, der Datensicherheit oder des ordnungsgemäßen Betriebs der Verfahren notwendig ist, dürfen die dabei anfallenden Daten nicht zur Leistungs- und Verhaltenskontrolle verwendet werden.
5. Wird den Beschäftigten die private E-Mail-Nutzung gestattet, so ist diese elektronische Post vom Telekommunikationsgeheimnis geschützt. Der Arbeitgeber darf ihren Inhalt grundsätzlich nicht zur Kenntnis nehmen, und hat dazu die erforderlichen technischen und organisatorischen Vorkehrungen zu treffen.
6. Der Arbeitgeber ist nicht verpflichtet, die private Nutzung des Internet am Arbeitsplatz zu gestatten. Wenn er dies gleichwohl tut, kann er die Gestattung unter Beachtung der hier genannten Grundsätze davon abhängig machen, dass die Beschäftigten einer Protokollierung zur Durchführung einer angemessenen Kontrolle der Netzaktivitäten zustimmen.
7. Die gleichen Bedingungen wie bei der Nutzung des Internet müssen prinzipiell bei der Nutzung von Intranets gelten.

Die Datenschutzbeauftragten fordern den Bundesgesetzgeber auf, auch wegen des Überwachungspotentials moderner Informations- und Kommunikationstechnik am Arbeitsplatz die Verabschiedung eines umfassenden Arbeitnehmerdatenschutzgesetzes nicht länger aufzuschieben.

24.4
Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. März 2002

Neues Abrufverfahren bei den Kreditinstituten

Nach der Novelle des Gesetzes über das Kreditwesen soll die zuständige Bundesanstalt die von den Kreditinstituten vorzuhaltenden Daten, wer welche Konten und Depots hat, ohne Kenntnis der Kundinnen und Kunden zur eigenen Aufgabenerfüllung oder zu Gunsten anderer öffentlicher Stellen abrufen können. Dies ist ein neuer Eingriff in die Vertraulichkeit der Bankbeziehungen.

Dieser Eingriff in die Vertraulichkeit der Bankbeziehungen muss gegenüber den Kundinnen und Kunden zumindest durch eine aussagekräftige Information transparent gemacht werden. Die Konferenz fordert daher, dass zugleich mit der Einführung dieses Abrufverfahrens eine Verpflichtung der Kreditinstitute zur generellen Information der Kundinnen und Kunden vorgesehen wird und diese die Kenntnisnahme schriftlich bestätigen. Dadurch soll zugleich eine effektive Wahrnehmung des Auskunftsrechts der Kundinnen und Kunden gewährleistet werden.

Die Erweiterung der Pflichten der Kreditinstitute, Kontenbewegungen auf die Einhaltung gesetzlicher Bestimmungen mit Hilfe von EDV-Programmen zu überprüfen, verpflichtet die Kreditinstitute außerdem zu einer entsprechend intensiven Kontenüberwachung (sog. „know your customer principle“). Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass die Überprüfung in einer Weise stattfindet, die ein datenschutzkonformes Vorgehen sicherstellt.

24.5

Entschließung der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24./25. Oktober 2002

Umgang mit personenbezogenen Daten in Sachakten des Verfassungsschutzes

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass bei den von Verfassungsschutzämtern geführten Personen- und Sachakten Unterschiede bei der Löschung beziehungsweise Vernichtung auftreten. Während Personenakten nach Ablauf der gesetzlichen Fristen unter Beachtung archivrechtlicher Regelungen regelmäßig gelöscht oder vernichtet werden, geschieht dies bei Sachakten, die in der Regel auch personenbezogene Daten enthalten, oftmals nicht. Dies darf aber nicht dazu führen, dass diese Daten anders als die Daten in Personenakten noch weiter verwandt werden dürfen.

Die Konferenz fordert, dass in Sachakten personenbezogene Angaben, die nicht mehr erforderlich sind, auch in Ländern ohne gesetzliches Löschungsgebot zumindest zu sperren sind.

24.6

Entschließung der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24./25. Oktober 2002

Speicherung und Veröffentlichung der Standortverzeichnisse von Mobilfunkantennen

Die Speicherung und die Veröffentlichung der Standortdaten von Mobilfunkantennen durch die Kommunen oder andere öffentliche Stellen stehen zur Zeit in verstärktem Maße in der öffentlichen Diskussion. Mehrere kommunale Spitzenverbände haben sich diesbezüglich bereits an die jeweiligen Landesdatenschutzbeauftragten gewandt. Unbeschadet bereits bestehender Landesregelungen und der Möglichkeit, Daten ohne Grundstücksbezug zu veröffentlichen, fordert die 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder aufgrund der bundesweiten Bedeutung der Frage den Bundesgesetzgeber auf, im Rahmen einer immissionsschutzrechtlichen Regelung über die Erstellung von Mobilfunkkatastern zu entscheiden.

Dabei ist zu bestimmen, wie derartige Kataster erstellt werden sollen. Die gegenwärtige Regelung des Bundesimmissionsschutzgesetzes sieht keine ausdrückliche Ermächtigung zur Schaffung von Mobilfunkkatastern vor, so dass deren Erstellung und Veröffentlichung ohne Einwilligung der Grundstückseigentümer und -eigentümerinnen und der Antennenbetreiber keine ausdrückliche gesetzliche Grundlage hat. Bei der Novellierung ist insbesondere zu regeln, ob und unter welchen Bedingungen eine Veröffentlichung derartiger Kataster im Internet oder in vergleichbaren Medien zulässig ist. Individuelle Auskunftsansprüche nach dem Umweltinformationsgesetz oder den Informationsfreiheitsgesetzen bleiben davon unberührt.

24.7

Entschließung der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24./25. Oktober 2002

Datenschutzgerechte Vergütung für digitale Privatkopien im neuen Urheberrecht

Zur Umsetzung der EU-Urheberrechtsrichtlinie wird gegenwärtig über den Entwurf der Bundesregierung für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft beraten. Hierzu hat der Bundesrat die Forderung erhoben, das bisherige System der Pauschalabgaben auf Geräte und Kopiermedien, die von den Verwertungsgesellschaften auf die Urheberinnen und Urheber zur Abgeltung ihrer Vergütungsansprüche verteilt werden, durch eine vorrangige individuelle Lizenzierung zu ersetzen. Zugleich hat der Bundesrat die Gewährleistung eines ausreichenden Schutzes der Nutzerinnen und Nutzer vor Ausspähung personenbezogener Daten über die individuelle Nutzung von Werken und die Erstellung von Nutzungsprofilen gefordert.

Die Datenschutzbeauftragten des Bundes und der Länder weisen in diesem Zusammenhang auf Folgendes hin: Das gegenwärtig praktizierte Verfahren der Pauschalvergütung beruht darauf, dass der Bundesgerichtshof eine individuelle Überprüfung des Einsatzes von analogen Kopiertechniken durch Privatpersonen zur Durchsetzung von urheberrechtlichen Vergütungsansprüchen als unvereinbar mit dem verfassungsrechtlichen Schutz der persönlichen Freiheitsrechte der Nutzerinnen und Nutzer bezeichnet hat. Diese Feststellung behält auch unter den Bedingungen der Digitaltechnik und des Internets ihre Berechtigung. Die Datenschutzkonferenz bestärkt den Gesetzgeber, an diesem bewährten, datenschutzfreundlichen Verfahren festzuhalten. Sollte der Gesetzgeber – wie es der Bundesrat fordert – jetzt für digitale Privatkopien vom Grundsatz der Pauschalvergütung (Geräteabgabe) tatsächlich abgehen wollen, so kann er den verfassungsrechtlichen Vorgaben nur entsprechen, wenn er sicherstellt, dass die urheberrechtliche Vergütung aufgrund von statistischen oder anonymisierten Angaben über die Nutzung einzelner Werke erhoben wird. Auch technische Systeme zur digitalen Verwaltung digitaler Rechte (Digital Rights Management) müssen datenschutzfreundlich gestaltet werden.

24.8
Entschließung der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24./25. Oktober 2002

Systematische verdachtslose Datenspeicherung in der Telekommunikation und im Internet

Gegenwärtig werden sowohl auf nationaler als auch auf europäischer Ebene Vorschläge erörtert, die den Datenschutz im Bereich der Telekommunikation und der Internetnutzung und insbesondere den Schutz des Telekommunikationsgeheimnnisses grundlegend in Frage stellen.

Geplant ist, alle Anbieter von Telekommunikations- und Multimediadiensten zur verdachtslosen Speicherung sämtlicher Bestands-, Verbindungs-, Nutzungs- und Abrechnungsdaten auf Vorrat für Mindestfristen von einem Jahr und mehr zu verpflichten, auch wenn sie für die Geschäftszwecke der Anbieter nicht (mehr) notwendig sind. Das so entstehende umfassende Datenreservoir soll dem Zugriff der Strafverfolgungsbehörden, der Polizei und des Verfassungsschutzes bei möglichen Anlässen in der Zukunft unterliegen. Auch auf europäischer Ebene werden im Rahmen der Zusammenarbeit der Mitgliedstaaten in den Bereichen „Justiz und Inneres“ entsprechende Maßnahmen – allerdings unter weitgehendem Ausschluss der Öffentlichkeit – diskutiert.

Die Datenschutzbeauftragten des Bundes und der Länder treten diesen Überlegungen mit Entschiedenheit entgegen. Sie haben schon mehrfach die Bedeutung des Telekommunikationsgeheimnisses als unabdingbare Voraussetzung für eine freiheitliche demokratische Kommunikationsgesellschaft hervorgehoben. Immer mehr menschliche Lebensäußerungen finden heute in elektronischen Netzen statt. Sie würden bei einer Verwirklichung der genannten Pläne einem ungleich höheren Überwachungsdruck ausgesetzt als vergleichbare Lebensäußerungen in der realen Welt. Bisher muss niemand bei der Aufgabe eines einfachen Briefes im Postamt seinen Personalausweis vorlegen oder in einer öffentlichen Bibliothek registrieren lassen, welche Seite er in welchem Buch aufschlägt. Eine vergleichbar umfassende Kontrolle entsprechender Online-Aktivitäten (E-Mail-Versand, Nutzung des WorldWideWeb), wie sie jetzt erwogen wird, ist ebenso wenig hinnehmbar.

Zudem hat der Gesetzgeber erst vor kurzem die Befugnisse der Strafverfolgungsbehörden erneut deutlich erweitert. Die praktischen Erfahrungen mit diesen Regelungen sind von unabhängiger Seite zu evaluieren, bevor weitergehende Befugnisse diskutiert werden.

Die Konferenz der europäischen Datenschutzbeauftragten hat in ihrer Erklärung vom 11. September 2002 betont, dass eine flächendeckende anlassunabhängige Speicherung sämtlicher Daten, die bei der zunehmenden Nutzung von öffentlichen Kommunikationsnetzen entstehen, unverhältnismäßig und mit dem Menschenrecht auf Achtung des Privatlebens unvereinbar wäre. Auch in den Vereinigten Staaten sind vergleichbare Maßnahmen nicht vorgesehen.

Mit dem deutschen Verfassungsrecht ist eine verdachtslose routinemäßige Speicherung sämtlicher bei der Nutzung von Kommunikationsnetzen anfallender Daten auf Vorrat nicht zu vereinbaren. Auch die Rechtsprechung des Europäischen Gerichtshofs lässt eine solche Vorratsspeicherung aus Gründen bloßer Nützlichkeit nicht zu.

Die Konferenz fordert die Bundesregierung deshalb auf, für mehr Transparenz der Beratungen auf europäischer Regierungsebene einzutreten und insbesondere einer Regelung zur flächendeckenden Vorratsdatenspeicherung nicht zuzustimmen.

24.9
Umlaufentschließung der Datenschutzbeauftragten des Bundes und der Länder vom 7. Januar 2003

Entwurf des Steuervergünstigungsabbaugesetzes lässt sorgfältige Abwägung zwischen Steuergerechtigkeit und informationellem Selbstbestimmungsrecht vermissen

Gesetzesgerechte Steuererhebung und grundrechtlicher Persönlichkeitsschutz stehen in einer Wechselbeziehung, die sorgfältiger Abwägung bedarf. Im Gegensatz zu Bereichen wie Sozialleistungen und Rentenversicherungen, wo es gelungen ist, eine Balance zwischen der wirksamen Erfüllung der staatlichen Aufgaben und dem individuellen Persönlichkeitsrecht des Einzelnen, das sich auch in dem Grundrecht auf informationelle Selbstbestimmung manifestiert, zu finden, lässt der Entwurf des Steuervergünstigungsabbaugesetzes diese Abwägung vermissen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die gesetzgebenden Stellen auf, bei den geplanten Maßnahmen zur Sicherung der Steuergerechtigkeit eine datenschutzkonforme Abwägung zwischen diesen Verfassungsprinzipien vorzunehmen und die Datenschutzrechte der Bürger angemessen zu berücksichtigen. Im Einzelnen machen sie auf Folgendes aufmerksam:

– Die Aufhebung des § 30a AO führt zu einem Wegfall des Bankgeheimnisses und damit zu einer deutlichen Störung des Vertrauensverhältnisses zwischen Banken und Kunden. Dass künftig auch verdachtunabhängige Prüfungen in Banken angeordnet werden können, schafft den „gläsernen Bankkunden“ und erweckt den Anschein, als sei jeder Steuerpflichtige ein potentieller Steuerverkürzer. Das datenschutzrechtliche Prinzip, dass Daten grundsätzlich bei Betroffenen zu erheben sind (§ 93a AO), wird außer Kraft gesetzt.

– Der Vertrauensverlust in der Bevölkerung wird durch die automatische Meldepflicht verschärft, die die Banken und andere Finanzdienstleister künftig gegenüber dem Bundesamt für Finanzen (BfF) haben.

– Nach § 23a EStG-E haben die Kreditinstitute Kontrollmitteilungen an das BfF über private Veräußerungsgeschäfte, insbesondere bei Wertpapieren, aber auch bei anderen Wirtschaftsgütern, z. B. Antiquitäten, mit Namen, Anschaffungs- und Veräußerungsbeträgen sowie Anzahl zu senden.

– Gemäß § 45d EStG-E sollen die Banken alle Kapitalerträge, bei denen ein Abzug von Steuern vorgesehen ist, mit Namen, Beträgen und Freistellungssummen dem BfF anzeigen.

– Da die umfangreichen Datenübermittlungen unter einem einheitlichen Identifikationsmerkmal (§ 139a AO-E) beim BfF zusammengeführt werden sollen, entsteht die Sorge, dass für alle Staatsbürger ein einheitliches Personenkennzeichen ins Auge gefasst wird. Dies widerspricht dem Urteil des Bundesverfassungsgerichts zur Volkszählung vom 15. Dezember 1983, wonach die Erschließung von Datenverbunden durch ein einheitliches Personenkennzeichen oder sonstiges Ordnungsmerkmal nicht zulässig ist.

– Die Zusammenführung der Daten beim Bundesamt der Finanzen schafft eine bundesweite Datensammlung über alle Differenzgewinne und Kapitalerträge sowie sonstige Veräußerungsgewinne und verstärkt die Entwicklung des BfF zum zentralen Datenpool. Es besteht erfahrungsgemäß die Gefahr, dass auch andere Behörden auf solche riesigen Datenbestände zugreifen wollen.

– Die geplante Ausweitung der Befugnis zu Kontrollmitteilungen durch die Neufassung des § 194 Abs. 3 AO verstößt gegen das verfassungsrechtliche Übermaßverbot. Unabhängig von einer zulässigen Verwertung von Zufallsfunden müssen Kontrollmitteilungen über alle steuerpflichtigen Staatsbürger daran gebunden werden, dass tatsächliche Anhaltspunkte für den Verdacht einer Steuerverkürzung bereits entstanden sind. Die gegenwärtig geplante verdachtunabhängige Befugnis zu Kontrollmitteilungen ist unverhältnismäßig.

  In diesem Zusammenhang müsste es gesetzlich ausgeschlossen werden, dass kopierte Unterlagen der Betriebe i. S. des § 147 Abs. 6 AO in den Finanzämtern für die massenhafte Herstellung von Kontrollmitteilungen verwendet werden. Da die bisherige Einschränkung des § 194 Abs. 3 AO aufgegeben wird, stehen gesetzlich keine Hindernisse gegen eine solche Auswertung der betrieblichen EDV im Wege. Dies wäre ebenfalls ein Verstoß gegen das verfassungsrechtliche Prinzip der Verhältnismäßigkeit.

Die Konferenz der Datenschutzbeauftragten von Bund und Ländern weist in diesem Zusammenhang darauf hin, dass eine Abgeltungssteuer wie in anderen europäischen Staaten (etwa Österreich und Schweiz) zu vergleichbarem Steueraufkommen führen wird, ohne dass die Banken zu umfassenden Anzeigepflichten über alle Steuerpflichtigen gezwungen werden. Die neuen Überlegungen der Bundesregierung gehen offenbar in diese Richtung und würden damit die Voraussetzungen schaffen, dass Kontrollmitteilungen entfielen, das Bankgeheimnis gewahrt bliebe und es bei Betriebsprüfungen weiterhin ausschließlich um die zulässige Verwertung von Zufallskunden ginge.

24.10
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. Mai 2002

Geplanter Identifikationszwang in der Telekommunikation

Das Bundesministerium für Wirtschaft und Technologie hat einen Entwurf zur Änderung des Telekommunikationsgesetzes veröffentlicht. Der Entwurf hat das Ziel, jeden Anbieter, der geschäftsmäßig Telekommunikationsdienste erbringt, dazu zu verpflichten, Namen, Anschriften, Geburtsdaten und Rufnummern seiner Kundinnen und Kunden zu erheben. Die Kundinnen und Kunden werden verpflichtet, dafür ihren Personalausweis vorzulegen, dessen Nummer ebenfalls gespeichert werden soll. Die beabsichtigten Änderungen sollen in erster Linie dazu führen, auch Nutzerinnen und Nutzer von Prepaid-Karten (also die Erwerberinnen und Erwerber von SIM-Karten ohne Vertrag) im Mobilfunk erfassen zu können. Die erhobenen Daten sollen allein dem Zweck dienen, den Sicherheitsbehörden zum jederzeitigen Online-Abruf über die Regulierungsbehörde für Telekommunikation und Post bereitzustehen. Im gleichen Zuge sollen die Zugriffsmöglichkeiten der Sicherheitsbehörden auf diese Daten dadurch erheblich erweitert werden, indem auf die Kundendateien nach abstrakten Merkmalen zugegriffen werden kann.

Die Datenschutzbeauftragten des Bundes und der Länder lehnen dieses Vorhaben ab. Unter der unscheinbaren Überschrift „Schließen von Regelungslücken“ stehen grundlegende Prinzipien des Datenschutzes zur Disposition. Kritikwürdig an dem geplanten Gesetz sind insbesondere die folgenden Punkte:

- Der geplante Grundrechtseingriff ist nicht erforderlich, um die Ermittlungstätigkeit der Sicherheitsbehörden zu erleichtern. Seine Eignung ist zweifelhaft: Auch die Gesetzesänderung wird nicht verhindern, dass Straftäterinnen und Straftäter bewusst und gezielt in kurzen Zeitabständen neue Prepaid-Karten erwerben, Strohleute zum Erwerb einsetzen, die Karten häufig – teilweise nach jedem Telefonat – wechseln oder die Karten untereinander tauschen. In der Begründung wird nicht plausibel dargelegt, dass mit dem geltenden Recht die Ermittlungstätigkeit tatsächlich behindert und durch die geplante Änderung erleichtert wird. Derzeit laufende Forschungsvorhaben beziehen diese Frage nicht mit ein.
- Der Entwurf widerspricht auch dem in den Datenschutzrichtlinien der Europäischen Union verankerten Grundsatz, dass Unternehmen nur solche personenbezogenen Daten verarbeiten dürfen, die sie selbst zur Erbringung einer bestimmten Dienstleistung benötigen.
- Die Anbieter würden eine Reihe von Daten auf Vorrat speichern müssen, die sie selbst für den Vertrag mit ihren Kunden nicht benötigen. Die ganz überwiegende Zahl der Nutzerinnen und Nutzer von Prepaid-Karten, darunter eine große Zahl Minderjähriger, würde registriert, obwohl sie sich völlig rechtmäßig verhalten und ihre Daten demzufolge für die Ermittlungstätigkeit der Strafverfolgungsbehörden nicht benötigt werden. Das Anhäufen von sinn- und nutzlosen Datenhalden wäre die Folge.

- Die gesetzliche Verpflichtung, sich an dem Ziel von Datenvermeidung und Datensparsamkeit auszurichten, würde konterkariert. Gerade die Prepaid-Karten sind ein gutes praktisches Beispiel für den Einsatz datenschutzfreundlicher Technologien, da sie anonymes Kommunizieren auf unkomplizierte Weise ermöglichen. Die Nutzung dieser Angebote darf deshalb nicht von der Speicherung von Bestandsdaten abhängig gemacht werden.
- Mit der Verpflichtung, den Personalausweis vorzulegen, würden die Anbieter zusätzliche Informationen über die Nutzerinnen und Nutzer erhalten, die sie nicht benötigen, z. B. die Nationalität, Größe oder Augenfarbe. Die vorgesehene Pflicht, auch die Personalausweisnummern zu registrieren, darf auch künftig keinesfalls dazu führen, dass die Ausweisnummern den Sicherheitsbehörden direkt zum Abruf bereit gestellt werden und sie damit diese Daten auch für die Verknüpfung mit anderen Datenbeständen verwenden können.
- Auch Krankenhäuser, Hotels, Schulen und Hochschulen sowie Unternehmen und Behörden, die ihren Mitarbeiterinnen und Mitarbeitern das private Telefonieren gestatten, sollen verpflichtet werden, die Personalausweisnummern der Nutzerinnen und Nutzer zu registrieren.
- Die Befugnis, Kundendateien mit unvollständigen oder ähnlichen Suchbegriffen abzufragen, würde den Sicherheitsbehörden eine Vielzahl personenbezogener Daten unbeteiligter Dritter zugänglich machen, ohne dass diese Daten für ihre Aufgaben erforderlich sind. Die notwendige strikte Beschränkung dieser weitreichenden Abfragebefugnis durch Rechtsverordnung setzt voraus, dass ein entsprechender Verordnungsentwurf bei der Beratung des Gesetzes vorliegt.

Der Formulierungsvorschlag des Bundeswirtschaftsministeriums lässt eine Auseinandersetzung mit dem Recht auf informationelle Selbstbestimmung der Kundinnen und Kunden der Telekommunikationsunternehmen weitgehend vermissen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung und den Gesetzgeber auf, auf die geplante Änderung des Telekommunikationsgesetzes zu verzichten und vor weiteren Änderungen die bestehenden Befugnisse der Sicherheitsbehörden durch unabhängige Stellen evaluieren zu lassen.

25. Materialien

25.1
AK Technik

Positionspapier zu technischen Aspekten biometrischer Merkmale in Personalausweisen und Pässen

1. Ausgangslage

Mit dem Terrorismusbekämpfungsgesetz wurden in § 4 Passgesetz und § 1 Personalausweisgesetz nahezu gleichlautende Regelungen folgenden Inhalts aufgenommen:

– Pässe und Personalausweise dürfen neben dem Lichtbild und der Unterschrift weitere biometrische Merkmale von
  • Fingern,
  • Händen oder
  • Gesicht

  des Inhabers enthalten.
– Alle biometrischen Merkmale und die Angaben über die Person dürfen auf den Ausweispapieren verschlüsselt gespeichert werden. Durch ein Bundesgesetz ist Folgendes zu regeln:
  • Arten der biometrischen Merkmale,
  • Einzelheiten der Einbringung von Merkmalen und Angaben in verschlüsselter Form,
  • Art der Speicherung und
  • Art ihrer sonstigen Verarbeitung und Nutzung.
– Die biometrischen Merkmale dürfen nur verwendet werden, um die Echtheit des Dokumentes und die Identität des Inhabers zu prüfen.
– Eine bundesweite Datei darf nicht eingerichtet werden.

Um beurteilen zu können, ob diese Maßnahmen geeignet und angemessen sind, müssen die verschiedenen biometrischen Verfahren aus Datenschutzsicht bewertet werden. Im Folgenden werden verschiedene Verfahren beschrieben und die Risiken aufgezeigt, die im Zusammenhang mit einem flächendeckenden Einsatz biometrischer Merkmale in Ausweisdokumenten zu erkennen sind.

2. Technische Möglichkeiten

2.1 Nutzung vorhandener biometrischer Merkmale

Bevor neue Merkmale in Ausweisen gespeichert werden, sollte geklärt werden, ob die vorhandenen nicht bereits ausreichen, um die Identität des Ausweisinhabers zu prüfen. Auf die Erhebung neuer personenbezogener Daten muss dann verzichtet werden. Könnten Verfahren eingesetzt werden, die bereits vorhandene biometrische Merkmale nut-

zen, wäre eine geringere Eingriffstiefe in das Recht auf informationelle Selbstbestimmung als bei der Verwendung eines völlig neuen Merkmals ausreichend.

Lichtbild
Mit dem Foto des Inhabers enthalten deutsche Ausweisdokumente bereits biometrische Daten. Mit heute vorhandener Technik ist es grundsätzlich möglich, das Foto auf dem Personalausweis automatisch mit dem Gesicht der Person zu vergleichen, die den Ausweis vorlegt.

Möglicherweise können die zurzeit verwendeten Passbilder die Qualitätsanforderungen an eine automatisierte Verarbeitung nicht in vollem Umfang erfüllen. Bisher gibt es allerdings keine verlässlichen Aussagen über die Bildqualität, die für biometrische Verfahren erforderlich ist. Ebenso wenig ist bisher geklärt, wie sich biometrische Merkmale im Laufe der Zeit ändern. Möglicherweise müsste die Gültigkeitsdauer von Personalausweisen wesentlich verkürzt werden, damit die Verifikation anhand des Passbildes im Ausweis über die gesamte Gültigkeitsdauer sichergestellt werden kann.

Unterschrift
Die Unterschrift des Inhabers ist ein weiteres biometrisches Merkmal, das schon jetzt auf jedem deutschen Ausweisdokument vorhanden ist. Ein automatischer Vergleich der vorhandenen mit einer bei der Kontrolle geleisteten Unterschrift wäre jedoch wenig sinnvoll, weil die zur Erkennung erforderlichen dynamischen Daten der Unterschrift (Druckverlauf, Schreibpausen) im Ausweis nicht gespeichert sind.

2.2 Biometrische Vermessung des Gesichtes

Sollen biometrische Daten des Gesichtes neu erhoben und in den Ausweispapieren maschinenlesbar beispielsweise als Barcode oder elektronischer Datensatz gespeichert werden, sind hohe Qualitätsanforderungen an die Erfassungs- und Kontrollsysteme zu stellen, um eine ausreichende Wiedererkennungsrate sicherzustellen. Für gute Ergebnisse sind gleichmäßig ausgeleuchtete Frontalaufnahmen von Gesichtern erforderlich. In der Praxis werden diese Anforderungen nur mit hohem Aufwand realisierbar sein.

2.3 Papillarmuster der Finger

Werden nur die Merkmale eines bestimmten Fingers genutzt, entstehen Probleme, wenn dieser bei der Erfassung oder bei Vergleichen verletzt oder anderweitig stark beansprucht ist (z. B. bei Bauarbeitern). Die Erfassung von Daten mehrerer Finger und alternative Vergleiche bei Kontrollen sind sehr aufwändig. Außerdem zeigen Tests, dass ein signifikanter (statistisch aber noch nicht abschließend verifizierter) Prozentsatz von Papillarmustern aus physiologischen Gründen nicht nutzbar ist (siehe Punkt 3.2).

2.4 Handgeometrie und Handlinien

Bei der Vermessung der Handgeometrie handelt es sich um ein System, das in den USA bereits im Einsatz ist. Über die Erkennungsqualität gibt es keine verlässlichen Angaben. Über die Möglichkeiten der Nutzung der Handlinien gibt es ebenfalls keine gesicherten Erkenntnisse. Die Problematik der Verletzungen oder sonstigen Einschränkungen der Nutzung einer Hand und der sich daraus ergebenden Notwendigkeit der Alternativdaten ist vergleichbar mit der bei der Papillarmusterverwendung. Unklar ist zurzeit auch die Wiedererkennungsqualität bei Handveränderungen durch Arbeits- und Alterungsprozesse.

2.5 Iris- und Retinastruktur

Die gesetzliche Formulierung „Gesicht“ lässt eine Erfassung detaillierter Merkmale der Augen nicht zu. Ungeachtet dessen ist festzustellen, dass diese Verfahren bisher noch nicht im größeren Stil eingesetzt worden sind. Sie sind sowohl technisch als auch organisatorisch sehr aufwändig. Bisher ist eine genaue Kopfpositionierung erforderlich, so dass fraglich ist, ob sie durch „Ungeübte“ in den Erfassungsstellen und an den Kontrollstellen praktiziert werden können. Sofern das Gesicht, die Iris oder die Retina durch ein Infrarot- oder Lasersystem abgetastet wird, ist damit zu rechnen, dass derartige Systeme auf eine signifikante Ablehnung durch die Betroffenen stoßen.

2.6 Weitere biometrische Merkmale

Aus technischer Sicht ist nicht auszuschließen, dass zur Prüfung der Identität Betroffener auch andere biometrische Merkmale verwendet werden könnten (z. B. Stimme, Bewegungsmuster). Diese Merkmale werden hier jedoch nicht weiter betrachtet, weil laut Pass- und Personalausweisgesetz neben dem Lichtbild und der Unterschrift nur biometrische Merkmale von Fingern, Händen oder dem Gesicht des Inhabers verwendet werden dürfen (siehe 1.).

3. Allgemeine technische Randbedingungen

3.1 Vorgaben aus der bestehenden Rechtslage

Aus dem rechtlichen Rahmen ergeben sich für die zu schaffenden Regelungen aus technischer Sicht, unabhängig von der Art der genutzten biometrischen Merkmale, folgende Vorgaben:

- Die Kontrollsysteme bestehen aus vier Komponenten, die untrennbar und unbeeinflussbar miteinander verknüpft sein müssen:
  - Leseeinheit für die aktuellen biometrischen Merkmale,
  - Leseeinheit für die Ausweispapiere,
  - Entschlüsselungs- und Vergleichseinheit und
  - Einheit zur Freigabe beziehungsweise Sperrung der Passage.
- Um Manipulationen ausschließen zu können, müssen die biometrischen Systeme bei der Kontrolle stand-alone arbeiten.
- Die enthaltenen Softwarekomponenten sollten zertifiziert (z. B. nach Common Criteria oder ITSEC) und signiert sein. Das gilt auch für Hardwarekomponenten, soweit mit ihnen Entschlüsselungen vorgenommen werden.
- Eine Speicherung von personenbezogenen Daten auf den Datenträgern der Kontrollsysteme über den Abschluss des Kontrollvorgangs hinaus ist nicht zulässig.
- Die Zahl der Personen, die Kontrollen trotz falscher Identität passieren können, muss möglichst gering sein (vgl. FAR unter 3.2).
- Eine regelmäßige Falsch-Rückweisung durch Unzulänglichkeiten bei den gespeicherten Daten muss vor der Ausgabe der Ausweise und Pässe schon durch die örtlichen Ausweisbehörden ausgeschlossen werden. Bevor die ausgebende Stelle den Ausweis aushändigt, muss sie ihn daher mit einem entsprechenden Referenz-Kontrollsystem prüfen.
- Die Verschlüsselung kann wahlweise bei der örtlichen Behörde oder in der Bundesdruckerei erfolgen.
- Der Verschlüsselungsalgorithmus muss wissenschaftlich anerkannt sein und dem Stand der Technik entsprechend als sicher gelten (mindestens für den Zeitraum der Gültigkeit der Ausweise).
- Der Schlüssel darf Unbefugten nicht bekannt werden.
- Wird auf eine Verschlüsselung der Daten verzichtet, müssen die gespeicherten Werte auf andere Weise gegen Missbrauch gesichert werden.

3.2 Stand der wissenschaftlichen Erkenntnisse zu biometrischen Verfahren

- Bisher gibt es keine wissenschaftlich gesicherten Erkenntnisse zu biometrischen Verfahren bei großen Anwendergruppen. Es können lediglich Erfahrungen mit kleineren Systemen (z. B. die automatisierte Kontrolle der Einwanderungsbehörde auf amerikanischen Flughäfen [Handgeometrie] oder auf den Flughäfen Schiphol und Frankfurt [Irisscan]) herangezogen werden.
- Die Leistungsfähigkeit biometrischer Systeme wird durch ihre Zurückweisungsrate berechtigter Personen (FRR False Rejection Rate) und ihre Überwindungssicherheit gegenüber unberechtigten Personen (FAR False Acception Rate) beschrieben. Beide Raten stehen in einem engen Zusammenhang. Je größer die Überwindungssicherheit ist, um so mehr berechtigte Personen werden abgewiesen. Die Ermittlung der FAR und der FRR und der Beziehung zueinander ist sehr aufwändig. Für große Anwendergruppen gibt es deshalb bisher keine herstellerneutralen Untersuchungen.
- Biometrische Systeme sind bislang hinsichtlich der FRR und der FAR nicht ausreichend überprüft, um flächendeckend eingesetzt zu werden. Das betrifft auch Fragen der Manipulationssicherheit des Gesamtsystems. Von besonderer Bedeutung ist die Verbindung zwischen Rechner und Sensor, da bei unzureichender Sicherung biometrische Merkmale durch Einspielen (Replay) entsprechender Datensätze vorgetäuscht werden können.
- Auch die Lebenderkennung ist bisher wenig ausgereift. Es ist deshalb nicht auszuschließen, dass biometrische Systeme durch die Präsentation nachgebildeter Merkmale (Silikonabdruck eines Fingerabdrucks, Foto eines Gesichtes usw.) überwunden werden können.
- Zur FER (False Enrollment Rate), die den Anteil der Personen nennt, bei denen das jeweilige biometrische Merkmal nicht geeignet ist oder nicht zur Verfügung steht, gibt es bisher keine gesicherten wissenschaftlichen Erkenntnisse. Eine FER von 1% bedeutet beispielsweise bei bundesweiten Ausweisdokumenten, dass mehr als 500.000 Personen bei Kontrollen immer mit Fehlermeldungen rechnen müssen, da sie durch das System nicht erkannt werden. In jedem Fall muss ein Rückfallsystem für die Nutzer vorhanden sein, die eine sehr schlechte Merkmalsausprägung besitzen oder überhaupt nicht erfasst werden können.

4. Einheitliches Personenkennzeichen

Mit neu erfassten biometrischen Merkmalen beziehungsweise mit den daraus generierten Datensätzen lässt sich eine Vielzahl unterschiedlicher Dateien erschließen und verknüpfen. Deshalb muss ausgeschlossen werden, dass die zusätzlichen biometrischen Merkmale der Ausweise sowohl für weitere staatliche Zwecke (z. B. Strafverfolgung) als auch im privatrechtlichen Bereich (z. B. für Vertragsabschlüsse) verwendet werden. Ein derartiges Merkmal käme sehr schnell einem einheitlichen Personenkennzeichen gleich, das gemäß dem Volkszählungsurteil des Bundesverfassungsgerichts unzulässig ist (BVerfGE 65,1, 53).

In Bereichen, in denen Biometrie für andere als die in § 4 Passgesetz und § 1 Personalausweisgesetz genannten Zwecke zum Einsatz kommt (z. B. Zugangskontrolle), wäre eine Verknüpfung der verschiedenen Daten technisch möglich. Dies könnte zum einen durch Verwendung der im Ausweis gespeicherten Daten als Referenzmaterial für solche Zwecke erfolgen. Zum anderen könnten gespeicherte biometrische Daten mit denen abgeglichen werden, die zum Zwecke der Ausweiserstellung verwendet werden. Dies wäre, auch wenn es keine durchgängig verwendeten Standards für die Codierung biometrischer Daten gibt, verfahrensübergreifend prinzipiell durchführbar.

5. Speicherung biometrischer Daten

Zur Vermeidung der unbefugten Nutzung von Ausweisdokumenten ist nur eine biometrische Verifikation erforderlich, d. h. der Abgleich der biometrischen Merkmale einer konkreten Person mit den auf einem Ausweis gespeicherten Daten. Eine Speicherung außerhalb des Ausweises ist dafür nicht erforderlich. Das Ziel der Erkennung von „Doppelidentitäten“ durch Abgleich biometrischer Daten einer unbekannten Person mit denjenigen anderer Personen (Identifikation) setzt die Speicherung personenbezogener Daten in zentralen Referenzdateien voraus. Aus Sicht des Datenschutzes ist eine solche Datensammlung insbesondere im Hinblick auf die Bildung eines einheitlichen Personenkennzeichens und die unvermeidlichen Missbrauchsmöglichkeiten jedoch abzulehnen.

Für die Ausweise selbst besteht die Möglichkeit, die Referenzdaten als Rohdaten oder als biometrischen Datensatz zu speichern. Während Rohdaten ggf. auch grafisch gespeichert werden können (z. B. das Bild eines Fingerabdrucks), muss für elektronische Biometriedaten („Template“, „Vektor“) der Ausweis mit einem maschinenlesbaren Datenträger (Barcode, Speicherchip etc.) versehen werden. Um einen Missbrauch dieser Daten zu verhindern, kommt insbesondere eine verschlüsselte Speicherung in Betracht. Während dies gegen einen alltäglichen Zugriff schützen mag, kann bei der Vielzahl von Geräten, in denen der Entschlüsselungsschlüssel vorhanden sein muss (bei Polizei und Grenzkontrollbehörden), jedoch kaum davon ausgegangen werden, dass die verschlüsselt gespeicherten Daten auf Dauer vor interessierten Dritten verborgen bleiben (siehe 3.1).

6. Überschießende Daten

Einige biometrische Merkmale lassen neben der Nutzung zur Identifizierung auch völlig andere Auswertungen zu. So kann möglicherweise auf bestimmte gesundheitliche Zustände oder Dispositionen, auf Faktoren wie Stress, Betrunkenheit oder Müdigkeit geschlossen werden. Bekannt ist dies von Bildern des Gesichts, der Hand und des Augenhintergrunds, von verhaltensbasierten biometrischen Merkmalen (Sprache, Unterschrift) sowie in besonderer Weise von genetischen Daten.

In der Regel sind nur aus den biometrischen Rohdaten solche Zusatzinformationen ableitbar, nicht aber aus den daraus gewonnenen Templates. Aus diesem Grund dürfen insbesondere die Rohdaten selbst nicht zentral gespeichert werden. Außerdem sind im Verarbeitungsprozess einer biometrischen Kontrolle die Rohdaten möglichst früh zu löschen, um die Gefahr einer Zweckentfremdung zu verringern.

7. Eignung für die Überwachung

Die Speicherung biometrischer Merkmale außerhalb des Ausweises birgt neue Gefahren für das Grundrecht auf informationelle Selbstbestimmung. Gelingt es, biometrische Daten im Alltag zu erfassen und diese mit einer zentralen Datenbank abzugleichen, können weitgehende Bewegungsprofile der Betroffenen erstellt werden. Im Gegensatz zu einer Erfassung eines biometrischen Merkmals unter Mitwirkung des Betroffenen handelt es sich hierbei um nichtkooperative Vorgänge, die dem Betroffenen womöglich nicht einmal bewusst sind. Dafür sind Merkmale geeignet, die kontaktlos und über eine gewisse Distanz erfasst werden können. Dies trifft zur Zeit vor allem auf die Gesichtserkennung zu, die bei geeignetem Blickwinkel mittels gewöhnlicher Kameras erfolgen kann. Da es datenschutzrechtlich geboten ist, sensitive Daten nur in Kenntnis der Betroffenen zu erheben, sind nichtkooperative passive Systeme abzulehnen.

Demgegenüber ist die flächendeckende Erfassung des Fingerabdrucks oder der Handgeometrie ohne Wissen und Mitwirkung des Betroffenen nicht oder nur unter sehr großem Aufwand möglich. Zwar können Fingerabdrücke auch heimlich von berührten Gegenständen abgenommen werden. Dies eignet sich jedoch – wegen des hierfür erforderlichen Aufwands – nur zur Behandlung von Einzelfällen und ist daher mit einer Überwachung nicht vergleichbar.

8. Ergebnis

Im Ergebnis zeigt sich, dass keines der weiteren biometrischen Merkmale unproblematisch ist. Vor der Entscheidung, ob ein bestimmtes biometrisches Merkmal in Ausweise aufgenommen werden soll, müssen die verschiedenen Risiken daher sorgfältig gegeneinander abgewogen werden.

Vor der gesetzlichen Einführung neuer biometrischer Merkmale ist eine Evaluation durch einen Großversuch geboten. Dabei wären Ausweise mit zusätzlichen Sicherheitsmerkmalen (z. B. Hologramm) ohne biometrische Merkmale zu erproben und zu bewerten und mit Ausweisen zu vergleichen, die ebenso ausgestaltet sind, jedoch biometrische Merkmale enthalten. Zu prüfen wäre auch, wie hoch das Risiko für Bürgerinnen und Bürger wäre, wegen Gerätedefekten bei hard- oder softwaregestützter Erkennung der Merkmale beziehungsweise wegen statistisch zu erwartenden Falscherkennungen bei der Ausweiskontrolle trotz eines echten eigenen Ausweises aufgehalten und intensiver überprüft zu werden, als sonst notwendig.

25.2
Arbeitskreis Medien[1]

Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz

Immer mehr Beschäftigte erhalten die Möglichkeit, das Internet auch am Arbeitsplatz zu nutzen. Öffentliche Stellen des Bundes und der Länder haben beim Umgang mit den dabei anfallenden personenbezogenen Daten der Beschäftigten und ihrer Kommunikationspartner bestimmte datenschutzrechtliche Anforderungen zu beachten, die davon abhängen, ob den Bediensteten neben der dienstlichen die private Nutzung des Internet am Arbeitsplatz gestattet wird. E-Mail und andere Internetdienste sind geeignet, das Verhalten und die Leistung der Beschäftigten zu überwachen. Die Orientierungshilfe stellt die bei der Nutzung dieser Dienste geltenden datenschutzrechtlichen Anforderungen dar.

I. Allgemeines

a) Bei der Nutzung von E-Mail und anderen Internetdiensten durch die Beschäftigten sind die eingesetzten Verfahren technisch so zu gestalten, dass von vornherein so wenige personenbezogene Daten wie möglich verarbeitet werden (Grundsatz von Datenvermeidung und Datensparsamkeit). Hierzu bietet es sich an, datenschutzfreundliche Verfahren einzusetzen. Ebenso ist die Kontrolle der Nutzung dieser Dienste durch den Arbeitgeber[2] so zu gestalten, dass sie zunächst ohne, zumindest aber mit so wenigen personenbezogenen Daten wie möglich durchgeführt wird. Dabei sind präventive Maßnahmen gegen unbefugte Nutzung nachträglichen Kontrollen vorzuziehen.

b) Die Bediensteten sind mit den technischen Möglichkeiten vertraut zu machen, wie die eingesetzten Verfahren datenschutzgerecht angewendet werden können. Um Art und Umfang der Verarbeitung ihrer personenbezogenen Daten nachvollziehen zu können, sind die Bediensteten umfassend darüber zu informieren (Grundsatz der Transparenz).

c) Es sind geeignete Maßnahmen zu treffen, um die Vertraulichkeit und Integrität der Kommunikation zu gewährleisten. Insbesondere sollte jeder internetfähige PC mit leicht bedienbarer, auch bei den Kommunikationspartnern vorhandener Verschlüsselungssoftware ausgestattet sein, um zu verhindern, dass aus Bequemlichkeit personenbezogene oder andere sensible Daten unverschlüsselt übertragen werden.

d) Automatisierte zentrale und wegen einer Verschlüsselung auch lokale Virenchecks sind notwendig. Um aktive Inhalte zu überprüfen, empfiehlt sich der Einsatz von lokaler Sandbox-Software.

II. Dienstliche Nutzung

a) Gestattet der Arbeitgeber die Nutzung von E-Mail und Internet ausschließlich zu dienstlichen Zwecken, ist er nicht Anbieter im Sinne des Telekommunikations- (TK-) beziehungsweise Teledienstegesetzes (vgl. § 1 Abs. 1 Nr. 1 Teledienstedatenschutzgesetz, TDDSG); die Erhebung und Verarbeitung von Daten über das Nutzungsverhalten der Beschäftigten richtet sich in diesen Fällen nach den einschlägigen Vorschriften des Beamtenrechts beziehungsweise des BDSG (für Tarifbedienstete des Bundes) oder den Landesdatenschutzgesetzen (für Tarifbedienstete der Länder).

b) Der Arbeitgeber hat grundsätzlich das Recht, stichprobenartig zu prüfen, ob das Surfen beziehungsweise E-Mail-Versenden der Beschäftigten dienstlicher Natur ist. Eine automatisierte Vollkontrolle durch den Arbeitgeber ist als schwerwiegender Eingriff in das Persönlichkeitsrecht der Beschäftigten hingegen nur bei konkretem Missbrauchsverdacht im Einzelfall zulässig. Es wird empfohlen über die Nutzung von E-Mail und Internet eine Dienstvereinbarung mit dem Personalrat abzuschließen, in der die Fragen der Protokollierung, Auswertung und Durchführung von Kontrollen eindeutig geregelt werden. Auf mögliche Überwachungsmaßnahmen und in Betracht kommende Sanktionen sind die Beschäftigten hinzuweisen.

[1] Die Orientierungshilfe wurde unter Beteiligung des AK Personalwesen erstellt. Sie richtet sich in erster Linie an öffentliche Stellen des Bundes und der Länder. Die hier dargestellten Grundsätze können auch auf den nichtöffentlichen Bereich übertragen werden.

c) Bei Beschäftigten, denen in ihrer Tätigkeit persönliche Geheimnisse anvertraut werden und die deshalb in einem besonderen Vertrauensverhältnis zu den betroffenen Personen stehen (z. B. Psychologen, Ärzte, Sozialarbeiter und -pädagogen), muss entsprechend der Rechtsprechung des Bundesarbeitgerichtes zu Verbindungsdaten über dienstliche Telefonate eine Kenntnisnahme des Arbeitgebers vom Inhalt der Nachrichten und den Verbindungsdaten, die einen Rückschluss auf die betroffenen Personen zulassen, ausgeschlossen werden.

d) Der Arbeitgeber darf die Nutzungs- und Verbindungsdaten der Personalvertretung nur insoweit kontrollieren, als dies im Einzelfall aus Gründen der Kostenkontrolle erforderlich ist. Soweit allerdings nur unerhebliche Kosten bei der Nutzung von Internet und E-Mail anfallen – was überwiegend der Fall sein wird –, ist eine Auswertung dieser Daten unzulässig.

e) Soweit die grundlegenden Datenschutzprinzipien eingehalten werden, kann die Dienstvereinbarung Regelungen enthalten, die im Einzelfall hinter den unter a) genannten Vorschriften zurückbleiben. Weder das BDSG noch die Landesdatenschutzgesetze beziehungsweise die beamtenrechtlichen Vorschriften schließen dies von vornherein aus. Nur wenn eine gesetzliche Regelung unabdingbar ist, kommt eine Abweichung zuungunsten der Beschäftigten nicht in Betracht.

f) Im Regelfall sollte darauf verzichtet werden, die Verarbeitung von Protokolldaten auf die Einwilligung der Beschäftigten zu stützen, da sie aufgrund des Abhängigkeitsverhältnisses zum Arbeitgeber nicht immer freiwillig entscheiden können. Nur ausnahmsweise ist auch die Einwilligung der Beschäftigten in eine Verarbeitung der Protokolldaten über die unter a) genannten Vorschriften hinaus möglich. Die Beschäftigten können z. B. die Verwertung ihrer Protokolldaten verlangen, um den Verdacht einer unbefugten Internetnutzung auszuräumen.

g) Soweit die Nutzung von E-Mail und Internet zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherung des ordnungsgemäßen Betriebs der Verfahren protokolliert wird, dürfen diese Daten nach dem BDSG, den Landesdatenschutzgesetzen und dem Beamtenrecht des Bundes und der Länder auch nur zu diesen Zwecken genutzt werden, nicht aber zur Verhaltens- und Leistungskontrolle der Beschäftigten.

h) Von ein- und ausgehenden dienstlichen E-Mails seiner Beschäftigten darf der Arbeitgeber im selben Maße Kenntnis nehmen wie von deren dienstlichem Schriftverkehr. Beispielsweise könnte der Vorgesetzte verfügen, dass ihm jede ein- oder ausgehende E-Mail seiner Mitarbeiter zur Kenntnis zu geben ist.

i) Aus Gründen der Datensicherheit dürfen Teilinhalte oder Anlagen von E-Mails unterdrückt werden, die gefährlichen oder verdächtigen ausführbaren Code enthalten (also insbesondere html-Seiten als Mail-body, Dateien mit den Erweiterungen *.exe, *.bat, *.com oder gepackte Dateien wie *.zip, *.arj, *.lha).

III. Private Nutzung

1. Allgemeines

a) Wenn ein Arbeitgeber den Beschäftigten die private Nutzung von Internet oder E-Mail erlaubt, ist er ihnen gegenüber TK- beziehungsweise Teledienste-Anbieter.

b) Vom Arbeitgeber beauftragte Zugangsanbieter (Access Provider) sind zwar diesem gegenüber TK- beziehungsweise Teledienste-Anbieter, gegenüber den privat nutzenden Beschäftigten sind die Provider aber lediglich Auftragnehmer des dann als Anbieter zu qualifizierenden Arbeitgebers.

c) Der Arbeitgeber ist den Beschäftigten gegenüber zur Einhaltung des Telekommunikationsgeheimnisses verpflichtet. Daher gelten die gleichen Bedingungen wie beim privaten Telefonieren.

d) Es gelten die Regelungen der Telekommunikations-Datenschutzverordnung, des Teledienstedatenschutzgesetzes beziehungsweise des Mediendienste-Staatsvertrages.

e) Der Arbeitgeber ist nicht verpflichtet, den Beschäftigten die private Nutzung des Internet zu erlauben. Entschließt er sich jedoch dazu, muss es ihm grundsätzlich möglich sein, diese Erlaubnis an einschränkende Voraussetzungen zu knüpfen (z. B. eine angemessene Art der Kontrolle durchzuführen). Beschäftigte, die diese Voraussetzungen nicht erfüllen wollen, können ihre Einwilligung ohne jeden dienstlichen Nachteil verweigern.

f) Der Umfang der privaten Nutzung, ihre Bedingungen sowie Art und Umfang der Kontrolle, ob diese Bedingungen eingehalten werden, müssen – am sinnvollsten durch Dienstvereinbarung oder -anweisung – unter Beteiligung des Personalrats eindeutig geregelt werden.

g) Eine Protokollierung darf ohne Einwilligung erfolgen, wenn sie zu Zwecken der Datenschutzkontrolle, der Datensicherung, zur Sicherung des ordnungsgemäßen Betriebs der Verfahren oder zu Abrechnungszwecken erforderlich ist.

2. Besonderheiten bei E-Mail

a) Private E-Mails sind wie private schriftliche Post zu behandeln. So sind eingehende private, aber fälschlich als Dienstpost behandelte E-Mails den betreffenden Mitarbeitern unverzüglich nach Bekanntwerden ihres privaten Charakters zur alleinigen Kenntnis zu geben.

b) Der Arbeitgeber sollte vor dem Hintergrund des von ihm zu wahrenden Telekommunikationsgeheimnisses entweder für die Beschäftigten separate E-Mail-Adressen zur privaten Nutzung einrichten oder – falls privates Surfen erlaubt ist – sie auf die Nutzung eines (kostenlosen) Web-Mail-Dienstes verweisen.

c) Wie bei der dienstlichen Nutzung (s. II.i) dürfen aus Gründen der Datensicherheit eingegangene private E-Mails oder deren Anhänge unterdrückt werden, wenn sie ein Format aufweisen, das ausführbaren Code enthalten kann. Die Verfahrensweise ist den Beschäftigten zuvor bekannt zu geben. Generell sind die Beschäftigten darüber zu unterrichten, wenn an sie gerichtete oder von ihnen abgesendete E-Mail ganz oder teilweise unterdrückt werden oder virenverseucht sind. Eine Untersuchung von virenverseuchten E-Mails mit Kenntnisnahme des Inhalts, etwa durch den Systemadministrator, ist nur unter Einbeziehung der betreffenden Beschäftigten zulässig.

d) Eine darüber hinaus gehende inhaltliche Kontrolle ist nicht zulässig.

25.3
Arbeitskreis Medien

Orientierungshilfe zum Umgang mit personenbezogenen Daten bei Internetdiensten

Übersicht

1. Allgemeines

Bei der Nutzung von Internetdiensten fallen bei Diensteanbietern eine Fülle personenbezogener Daten an. Die Rechtsgrundlagen zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten ergeben sich für Tele- und Mediendienste aus dem Teledienstedatenschutzgesetz (TDDSG) beziehungsweise aus dem Mediendienste-Staatsvertrag (MDStV). Darüber hinaus handelt es sich bei der Vermittlung des Zugangs zum Internet (access providing) sowie bei E-Mail-Diensten zumindest teilweise auch um die Erbringung eines Telekommunikatonsdienstes i. S. d. TKG. Soweit sich die folgenden Ausführungen auf die Verarbeitung personenbezogener Daten bei E-Mail-Diensten oder der Zugangsvermittlung beziehen, müssen daher auch das Telekommunikationsgesetz (TKG) und die Telekommunikations-Datenschutzverordnung (TDSV) zugrunde gelegt werden. Bei der Beurteilung der Zulässigkeit der Datenerhebung, Verarbeitung und Nutzung ist auch der Grundsatz der **Datenvermeidung** und **Datensparsamkeit** nach § 3a BDSG zu beachten.

Bei den einzelnen Diensten können unterschiedliche Arten personenbezogener Daten (Bestands-, Verbindungs-, Nutzungs-, Abrechnungs- und Inhaltsdaten) anfallen, deren Verwendung sich nach unterschiedlichen Regelungen richtet:

– **Teledienste** (hierunter fällt die Zugangsvermittlung nur zum Teil; s. 3.1)
– § 5 TDDSG: Bestandsdaten
– § 6 TDDSG: Nutzungs- und Abrechnungsdaten

– **Mediendienste**
– § 19 Abs. 1 MDStV: Bestandsdaten
– § 19 Abs. 2 bis 9 MDStV: Nutzungs- und Abrechnungsdaten

– **E-Mail-Dienste** sowie z. T. die Zugangsvermittlung (s. 3.1)
– § 89 Abs. 2 TKG i. V. m. § 5 TDSV unter Beachtung des § 89 Abs. 6 u. 10 Satz 1 TKG: Bestandsdaten
– § 89 Abs. 2 TKG i. V. m. § 6 Abs. 1 TDSV: Verbindungsdaten

Soweit eine staatliche Stelle die Herausgabe von personenbezogenen Daten beziehungsweise die Überwachung eines E-Mail-Anschlusses verlangt, muss sie gegenüber dem Diensteanbieter die Rechtsgrundlage ihrer Forderung darlegen und ggf. notwendige richterliche Anordnungen beibringen. Der Diensteanbieter hat sich von der Einhaltung der formalen Anforderungen an eine entsprechende Maßnahme zu vergewissern, einer Verpflichtung zur inhaltlichen Prüfung der entsprechenden Anordnungen unterliegt er jedoch grundsätzlich nicht. Gegenüber Strafverfolgungsbehörden ist er verpflichtet, entsprechende Anordnungen zur Überwachung umzusetzen; dagegen ist er gegenüber Nachrichtendiensten unter den gesetzlichen Voraussetzungen zur Auskunft berechtigt, aber nicht verpflichtet.

2. Datentypen

2.1 Bestandsdaten

Bestandsdaten sind Daten für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses über die Nutzung von Tele-, Medien- und Telekommunikationsdiensten. Dies können sein: Name, Anschrift, E-Mail-Adresse, Telefon- oder Telefaxnummer, Geburtsdatum, Bankverbindung, Kreditkartennummer, öffentlicher Schlüssel, User-ID, aber auch statische IP-Adressen und ähnliche Angaben. Welche Bestandsdaten im Einzelnen erhoben, verarbeitet oder genutzt werden dürfen, ist im Wesentlichen abhängig von der technischen Ausgestaltung des Dienstes und von dem Inhalt der jeweiligen Verträge. Die Definition dieser Daten ist für die Bereiche der Teledienste, Mediendienste und Telekommunikationsdienste identisch.

In welchem Umfang Bestandsdaten erhoben werden, ist am **Grundsatz der Erforderlichkeit** auszurichten, d. h., Daten, die für die genannten Zwecke nicht zwingend erforderlich sind, dürfen nicht erhoben, verarbeitet oder genutzt werden.

So dürfen z. B. bei der kostenlosen Bereitstellung von Informationen für die Allgemeinheit grundsätzlich **keine Bestandsdaten** erhoben werden, weil kein Vertragsverhältnis vorliegt und die Daten für die Abwicklung solcher Angebote nicht erforderlich sind.

Dennoch werden bei kostenlosen Diensten wie der Anforderung beziehungsweise Bestellung von Newslettern von den Anbietern häufig neben der E-Mail-Adresse auch noch andere personenbezogene Daten erhoben. Dies ist in der Regel nicht zulässig, da diese Daten für die Erbringung der Leistung (Übersendung einer E-Mail) nicht notwendig sind. Ihre Nutzung würde ggf. zudem gegen das Koppelungsverbot (§ 3 Abs. 4 TDDSG, § 17 Abs. 4 MDStV, § 89 Abs. 10 TKG) verstoßen.

Bestandsdaten werden bei Zugangs-Providern und bei solchen Telediensteanbietern erhoben, die eine Vertragsbeziehung zwischen dem Anbieter und den Nutzenden voraussetzen, also im Wesentlichen bei kostenpflichtigen Diensten.

In diesem Zusammenhang muss auf die Abgrenzung zwischen Bestandsdaten, die unter das TDDSG beziehungsweise die TDSV fallen, und Daten, die auf Grundlage des BDSG oder einer bereichsspezifischen Rechtsvorschrift erhoben werden, hingewiesen werden. Solche Daten, die z. B. bei der Bestellung einer kommunalen Dienstleistung (Müllabfuhr) oder eines materiellen Guts in einem Online-Shop angegeben werden, sind keine Bestandsdaten i. S. d. TDDSG, sondern sog. Inhaltsdaten, die zur Offline-Abwicklung (Lieferung der Ware, Zusendung der Rechnung) des Vertrags erforderlich und daher nach BDSG zu beurteilen sind.

Löschungsfristen

Die Pflicht zur frühestmöglichen Löschung von Bestandsdaten ergibt sich für Tele- und Mediendiensteanbieter aus dem Erforderlichkeitsgrundsatz. Soweit Bestandsdaten nicht mehr zur Begründung, Ausgestaltung und Änderung des Vertragesverhältnisses erforderlich sind, etwa weil das Vertragsverhältnis beendet ist und nachvertragliche Ansprüche nicht mehr bestehen, müssen sie gelöscht werden. Die Löschungspflicht ergibt sich darüber hinaus aus § 35 Abs. 2 Nr. 3 BDSG.

Bestandsdaten, die im Zusammenhang mit der Erbringung von Telekommunikationsdiensten (E-Mail-Dienste beziehungsweise Zugangsvermittlung) erhoben wurden, sind spätestens gem. § 5 Abs. 3 Satz 1 TDSV mit Ablauf des auf die Beendigung des Vertrages folgenden Kalenderjahres zu löschen. Ausnahmen hiervon ergeben sich aus § 35 Abs. 3 BDSG hinsichtlich einer fortdauernden Speicherung von personenbezogenen Daten im Rahmen gesetzlicher Aufbewahrungsbestimmungen. In diesem Fall sind die Daten vom operativen Datenbestand zu trennen und für eine Verwendung außerhalb der Dokumentationsverpflichtung zu sperren.

2.2 Nutzungsdaten

Nutzungsdaten fallen im Regelfall bei jedem Tele- und Mediendiensteanbieter an. Nutzungsdaten sind gem. § 6 Abs. 1 TDDSG beziehungsweise § 19 Abs. 2 MDStV Daten, die erforderlich sind, um die Inanspruchnahme von Telediensten zu ermöglichen und diese abzurechnen. Es handelt sich hierbei insbesondere um Merkmale zur Identifikation des

Nutzers, Angaben über Beginn und Ende sowie Umfang der jeweiligen Nutzung und Angaben über die von den Nutzenden in Anspruch genommenen Teledienste.

Die Regelungen sind abschließend, d. h. die Erhebung, Verarbeitung oder Nutzung der Nutzungs- und Abrechnungsdaten durch die Diensteanbieter ist nur zulässig, soweit sie durch die Vorschriften erlaubt wird. Nutzungsdaten dürfen außerhalb dieser Bestimmungen nur verarbeitet werden, wenn eine gesetzliche Spezialregelung dies ausdrücklich erlaubt oder der Betroffene eingewilligt hat.

Die Aussagekraft der Nutzungsdaten bei Tele- und Mediendiensten ist bisweilen größer als etwa bei Verbindungsdaten der Sprachtelekommunikation. Während Verbindungsdaten lediglich Auskunft darüber geben, wer wann mit wem kommuniziert hat, offenbaren Nutzungsdaten häufig darüber hinaus, welche Inhalte übertragen wurden. Dies gilt insbesondere in Bezug auf aus dem Web abgerufene Ressourcen und auf Anfragen bei Suchmaschinen.

Löschungsfristen

Nach § 6 Abs. 4 TDDSG darf der Diensteanbieter Nutzungsdaten über das Ende des Nutzungsvorgangs hinaus verarbeiten und nutzen, soweit sie für Zwecke der Abrechnung erforderlich sind. Im Umkehrschluss bedeutet dies, dass alle übrigen Nutzungsdaten frühestmöglich, spätestens unmittelbar nach Ende der Nutzung zu löschen sind. Eine entsprechende Regelung liefert § 19 Abs. 5 MDStV.

– Nutzungsdaten, die nicht zu Abrechnungszwecken erforderlich sind

  Zur Abrechnung von Telediensten werden die entsprechenden Daten über die beim Provider „eingehende“ Telefonnummer oder eine im Vorfeld zugeteilte User-ID den Nutzenden zugeordnet. Die IP-Adressen werden hierfür aber nicht benötigt, zudem wären sie als Ordnungskriterium nicht geeignet, da sie in den meisten Fällen dynamisch vergeben werden und im Laufe einer Internet-Sitzung mehrfach wechseln können. Somit ist die **Speicherung von IP-Adressen über die Nutzungsdauer hinaus unzulässig** (zum Personenbezug von IP-Adressen s. u. 3.1). Gleiches gilt auch für die Angaben über die von den Nutzenden in Anspruch genommenen Teledienste (URLs).

– Abrechnungsdaten (Nutzungsdaten, die zur Abrechnung erforderlich sind)

  Abrechnungsdaten sind diejenigen Nutzungsdaten, die für die Abrechnung von Tele- und Mediendiensten verwendet werden. Üblicher Weise werden für Abrechnungszwecke Nutzungsdaten mit Bestandsdaten kombiniert und zur Rechnungsstellung verwendet. Der Gestaltung der Abrechnungsmodalitäten kommen im Hinblick auf die Erforderlichkeit der Verarbeitung personenbezogener Daten und der daraus resultierenden datenschutzrechtlichen Probleme besondere Bedeutung zu. Abrechnungsverfahren sollten nach Möglichkeit so gestaltet werden, dass für Abrechnungszwecke so wenig wie möglich personenbezogene Daten erhoben, gespeichert und genutzt werden. Die Speicherung von Nutzungsdaten auf IP-Ebene ist im Regelfall für Abrechnungszwecke nicht erforderlich. Gleiches gilt für andere technische Angaben, die die Hardware-Ausstattung des Nutzers oder die von ihm eingesetzte Software betreffen. Ebenfalls nicht erforderlich und damit im Regelfall unzulässig ist die Speicherung einzelner Inhalte oder deren Adressen, die der Nutzer abgerufen oder angesteuert hat.

  Abrechnungsdaten sind zu löschen, sobald sie für Zwecke der Abrechnung nicht mehr erforderlich sind. Eine Abrechnung mit detailgenauen Angaben (etwa Bezeichnung einer aus dem WWW abgerufenen Ressource, Bezeichnungen von Newsgroups, die in Anspruch genommen wurden) ist nur zulässig, wenn der Nutzer einen derartigen Einzelnachweis ausdrücklich verlangt (§ 6 Abs. 6 letzter Halbsatz TDDSG). Im Falle des Einzelnachweises dürfen Abrechnungsdaten höchstens bis zum Ablauf von sechs Monaten (§ 6 Abs. 7 TDDSG, § 19 Abs. 8 MDStV) nach Versendung der Rechnung gespeichert werden. Lediglich in den Fällen, in denen die Nutzer oder die Nutzerinnen gegen die Entgeltforderung fristgerecht Einwendungen erhoben oder diese trotz Zahlungsaufforderung nicht beglichen haben, dürfen die Abrechnungsdaten aufbewahrt werden, bis die Einwendungen abschließend geklärt sind oder die Entgeltforderung beglichen wurde.

2.3 Verbindungsdaten bei E-Mail-Diensten

Bei dem Angebot zur Übermittlung von **E-Mails** handelt es sich um einen Telekommunikationsdienst. Die bei der Erbringung dieses Dienstes anfallenden Daten sind Verbindungsdaten im Sinne des Telekommunikationsrechts (§ 2 Nr. 4 TDSV). Verbindungsdaten bei E-Mail-Diensten sind insbesondere E-Mail-Adressen (die auch Bestandsdaten sein können, s. o. 2.1), Zeitpunkte der Sendung beziehungsweise Zustellung und Routing-Informationen (Angaben über diejenigen Rechner, die eine E-Mail durchgeleitet haben). Nicht zu den Verbindungsdaten gehören z. B. Bezeichnungen von Datei-Anlagen und über den „Betreff“.

Zulässig ist die Verarbeitung zur Entgeltermittlung und Entgeltabrechnung (§ 7 TDSV), für den Einzelverbindungsnachweis (§ 8 TDSV) und zur Erkennung und Abwehr von Störungen von Telekommunikationsanlagen und des Missbrauchs von Telekommunikationsdiensten (§ 9 TDSV).

Hiervon zu unterscheiden sind die Informationen, die ein Nutzer oder eine Nutzerin beispielsweise im persönlichen Mail-Adressbuch zur dauerhaften Nutzung abspeichert. Eine Verarbeitung oder Nutzung der Verbindungsdaten darf nur erfolgen, soweit sie zum Aufbau weiterer Verbindungen oder zu Abrechnungszwecken erforderlich sind.

Löschungsfristen

Sofern die Verarbeitung oder Nutzung der Verbindungsdaten aus vorgenannten Gründen nicht erforderlich ist, sind sie vom Diensteanbieter spätestens am Tag nach Beendigung der Verbindung unverzüglich zu löschen, wenn die Nutzenden die E-Mail abgerufen haben, und keine weitere Speicherung wünschen.

Angesichts der derzeitigen Tarifmodelle für E-Mail-Dienste ist eine längerfristige Speicherung von Verbindungsdaten nicht erforderlich und damit unzulässig, da die Daten nicht zu Abrechnungszwecken benötigt werden.

2.4 Inhaltsdaten

Die Beurteilung der Rechtmäßigkeit zur Erhebung, Verarbeitung und Nutzung von Inhaltsdaten bei Tele- und Mediendiensten richtet sich nach den jeweiligen spezialgesetzlichen Regelungen (z. B. die Erhebung von Sozialdaten nach den Vorschriften des Sozialgesetzbuches, Auskünfte zum Meldewesen nach dem Meldegesetz etc.) und nach dem Bundesdatenschutzgesetz. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, sind zusätzlich zu beachten.

3. Anbieter (Provider)

Welche Daten zu welchem Zweck ein Provider erheben, verarbeiten und nutzen darf, hängt vom angebotenen Dienst und den jeweiligen Tarifmodellen ab. In jedem Fall ist zu beachten, dass beim Angebot mehrerer Dienste die rechtliche Beurteilung für jeden Dienst separat zu betrachten ist. Auch darf nicht eine Zusammenführung von z. B. Bestandsdaten aus den Bereichen des Telekommunikations- und des Teledienstes erfolgen.

3.1 Zugangs-Anbieter (Access-Provider)

Die Aufgabe des Zugangs-Providers liegt darin, den Zugang zu Informationen beziehungsweise Diensten gegen Entgelt zu vermitteln beziehungsweise die entsprechenden Inhalte an den Nutzer durchzuleiten. Nach § 2 Abs. 2 Nr. 3 TDG ist das Angebot zur Nutzung des Internets oder weiterer Netze ein Teledienst. Dies wurde bisher von den meisten Datenschutzaufsichtsbehörden so interpretiert, dass hierunter auch die reine Zugangsvermittlung (access providing) fällt. In der Praxis wird diese Auffassung hingegen überwiegend abgelehnt und das access providing in erster Linie als Telekommunikationsdienst angesehen (vgl. HansOLG Hamburg MMR 2000, 611, 613). Aus folgenden Gründen ist dieser Auffassung nunmehr zuzustimmen:

Der Gesetzgeber hatte bei der Regelung des § 2 Abs. 2 Nr. 3 TDG in erster Linie das Angebot von Navigationshilfen und Suchmaschinen, nicht aber die reine Zugangsvermittlung im Sinn. Zudem sprechen auch technische Gründe dafür, die mit der Vermittlung des Zugangs verbundene Datenübertragung als Telekommunikationsdienst anzusehen. Nach dem OSI-Referenzmodell, das der Kommunikation im Internet zugrunde gelegt wird, wird erst auf der Ebene des Transmission Control Protocol (TCP) die virtuelle Verbindung zwischen den beteiligten Endgeräten hergestellt. TCP wird der Schicht 4 (Transportschicht) des OSI-Modells zugeordnet. Daraus folgt, dass Schicht 4 sowie alle darunter liegenden Schichten (auch die der Schicht 3 zugeordnete IP-Ebene) zum technischen Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten zu zählen sind und damit als Telekommunikation i. S. v. § 3 Nr. 16 TKG betrachtet werden müssen. Dagegen unterliegen nach dem Hypertext Transport Protocol (http) übermittelte Informationen als Nutzungsdaten dem Tele- und Mediendiensterecht. Soweit der Zugangs-Anbieter seine Dienste mit der von § 3 Nr. 5 TKG geforderten Nachhaltigkeit anbietet, besteht grundsätzlich die Verarbeitungsbefugnis für Bestands- und Nutzungsdaten nach der TDSV. Bestandsdaten dürfen lediglich in dem Umfang gespeichert werden, wie sie für das Vertragsverhältnis erforderlich sind und zum Zwecke der Abrechnung benötigt werden. Zur Vermittlung erforderliche Verbindungsdaten (auch die IP-Adresse) dürfen nur für die Phase der Inanspruchnahme gespeichert werden. Sie sind nach der Inanspruchnahme grundsätzlich unverzüglich, spätestens aber am Tage nach Beendigung der Verbindung nach § 6 Abs. 2 Satz 2 TDSV zu löschen, es sei denn, einzelne Verbindungsdaten werden zu den in §§ 7 bis 10 TDSV genannten Zwecken (insbesondere Abrechnungszwecken) benötigt. Im Einzelnen ist dies abhängig von dem Tarifmodell, nach dem die Abrechnung erfolgt. Im Falle einer Flatrate dürfen keine Verbindungsdaten gespeichert werden, da für die Nutzung ein Pauschalpreis zu bezahlen ist. Erfolgt die Abrechnung dagegen nach Zeit- oder Mengentarifen, so sind entweder die Zeittakte oder aber die Mengendaten zu speichern. Um die Zuordnung der für die Abrechnung gespeicherten Verbindungsdaten zu den jeweiligen Nutzenden herzustellen, muss darüber hinaus ein eindeutiges Zuordnungsmerkmal (Bestandsdatum), also entweder die Telefonnummer oder die User-ID, mitgespeichert werden. Eine Speicherung beider Zuordnungsmerkmale ist unter dem Gebot der Datensparsamkeit nicht zulässig.

Die Frage, ob IP-Nummern personenbezogen sind, wird kontrovers diskutiert. Sie ist deshalb von großer Bedeutung, weil an verschiedenen Stellen des Internet (insb. bei Access Providern, Content Providern, Hosting Services) IP-Adressen – teilweise zusammen mit anderen Nutzungsdaten – protokolliert werden.

Zugangs-Provider (Access Provider) können – unabhängig von der bei der Vergabe der IP-Adressen verwendeten Technik, also auch bei dynamischer Vergabe – die IP-Nummer einzelnen Nutzenden zuordnen. Sie sind somit perso-

nenbezogene Daten. Dies gilt auch, wenn der Zugang (Access) beispielsweise über das LAN eines Unternehmens beziehungsweise einer Behörde erfolgt oder über Firewallsysteme eine Adressumsetzung erfolgt.

Betrachtet man die Möglichkeiten anderer Anbieter (beispielsweise Inhalts-Anbieter) eine Identifikation anhand der IP-Adresse vorzunehmen, so sind hier die Möglichkeiten der Zusammenführung der personenbezogenen Daten im Internet zu berücksichtigen. Mit Hilfe Dritter ist es bereits jetzt ohne großen Aufwand in den meisten Fällen möglich, Internet-Nutzer und -Nutzerinnen aufgrund ihrer IP-Adresse zu identifizieren. Wenn z. B. für Inhalte-Anbieter der Personenbezug von IP-Adressen verneint und das TDDSG beziehungsweise die TDSV nicht für anwendbar erklärt werden, hätte dies nicht nur die mit dem Grundrechtsschutz unvereinbare Konsequenz, dass der Diensteanbieter die Daten unbegrenzt selbst verarbeiten oder nutzen könnte, sondern er dürfte diese Daten auch ohne Restriktionen an Dritte übermitteln, die ihrerseits die Möglichkeit hätten, den Nutzer aufgrund der IP-Adresse zu identifizieren. Es bedarf keiner näheren Begründung, dass dies dem Schutzgedanken des Datenschutzrechts diametral zuwiderlaufen würde. Dynamische IP-Adressen sind daher personenbezogene Daten, da sie durch Zusammenführung mit den dahinter stehenden Zuordnungstabellen den Rückschluss auf bestimmbare Personen zulassen (vgl. §§ 3 Abs. 1 BDSG, 1 Abs. 2 TDDSG).

Auf jeden Fall sind statische IP-Adressen personenbezogene Daten, da diese einen direkten und andauernden Bezug zu den Nutzenden enthalten und auf diesen ohne weiteres rückschließen lassen. Beim Zugangsanbieter (und nur bei diesem) gehören sie allerdings zu den Bestandsdaten (s. o. 2.1)

Als Folge dessen sind für das Erheben, Verarbeiten, Nutzen und auch Löschen von IP-Adressen die Vorschriften für Verbindungs- beziehungsweise Nutzungsdaten anzuwenden.

3.2 Proxybetrieb

Inhalte, die von Nutzern aus dem Internet abgerufen wurden, werden von Betreibern von Proxy-Diensten auf Proxy-Servern zwischengespeichert und können bei wiederholtem Zugriff derselben oder anderer Nutzer ohne erneute Inanspruchnahme anderer Internet-Provider dem Nutzer zugestellt werden. Deshalb kann von ihnen das Surfverhalten der Nutzer einschließlich der dabei übertragenen Inhalte nachvollzogen werden.

Hinsichtlich der Einordnung dieser Dienste gilt das oben unter 3.1 zu den Zugangsanbietern Gesagte entsprechend. Bis einschließlich zur TCP-Ebene ist das Betreiben eines Proxy-Dienstes als Übermittlung von Nachrichten Telekommunikation i. S. v. § 3 Nr. 16 TKG.

Bei Betreibern von Proxydiensten gem. § 10 TDG dürften, sofern dieser Dienst nicht in Verbindung mit anderen Diensten angeboten wird, keine Bestandsdaten anfallen.

Verbindungs- beziehungsweise Nutzungsdaten dürfen nur gespeichert werden, sofern sie zur Erbringung der Leistung erforderlich sind. Dies können allenfalls die URL (Nutzungsdatum) beziehungsweise die IP-Adresse (Verbindungsdatum) von angefragten Angeboten sein. Eine darüber hinaus gehende Speicherung dieser Daten, insbesondere die IP-Adresse der Nutzer oder Nutzerinnen, ist unzulässig, da sie zur Erbringung des Proxy-Dienstes nicht erforderlich sind. Eine Speicherung von Inhaltsdaten kann unter Bezug auf § 10 Ziffer 3 TDG für maximal 24 Stunden toleriert werden. Eine darüber hinaus gehende Speicherung ist nicht erforderlich und dementsprechend unzulässig.

3.3 Inhalts-Anbieter (Content-Provider)

Bei Inhalts-Providern können sowohl Bestandsdaten als auch Nutzungsdaten anfallen. Bestandsdaten dürfen gespeichert werden, soweit es sich um Identifikationsangaben handelt. Des weiteren wird auf die Ausführungen zu den Bestandsdaten unter 3.1 verwiesen.

Welche Nutzungsdaten im Einzelnen gespeichert werden dürfen, ist von dem jeweiligen Dienst abhängig. Auch hier gilt das Erforderlichkeitsprinzip, d. h., im Falle eines kostenlosen Angebots dürfen keine Nutzungsdaten gespeichert werden, ansonsten nur die Daten, die zur Abrechnung erforderlich sind. Wird beispielsweise für das Herunterladen von Dokumenten abgerechnet, so darf nur der Preis des Dokumentes gespeichert werden, nicht aber seine Bezeichnung.

3.4 Webhosting

Beim sogenannten Webhosting überträgt der Anbieter eines Dienstes die technische Abwicklung seines Angebotes einem Dritten (host). Dieser Dienstleister kann auf unterschiedliche Weise in die Abläufe einbezogen sein. Bei der Verarbeitung personenbezogener Daten im Rahmen des Angebots (etwa bei elektronischen Bestellungen) handelt es sich im Regelfall um Datenverarbeitung im Auftrag des Diensteanbieters, der als Auftraggeber die Verantwortung für die personenbezogenen Daten des Nutzers trägt (§ 11 BDSG). Er ist Adressat aller Datenschutzrechte, die Betroffene (z. B. auf Auskunft) geltend machen können. Soweit der Betreiber des Hosting-Service in eigener Verantwortung personenbezogene Daten erhebt, verarbeitet oder nutzt (z. B. in Logdateien), treffen ihn selbst auch datenschutzrechtliche Pflichten (z. B. zur Information des Nutzers, § 4 Abs. 3 BDSG).

4. Übermittlung von Daten an Strafverfolgungsbehörden und Nachrichtendienste

Das Fernmeldegeheimnis gem. Art. 10 GG, § 85 TKG schützt die Inhalte und auch die „näheren Umstände der Telekommunikation“ (Verbindungsdaten). Das Grundrecht beschränkt ferner die Verwendung und Weitergabe von Daten, die unter Aufhebung des Fernmeldegeheimnisses erlangt worden sind. Ferner schützt Art. 10 GG, § 85 TKG die gesamte Telekommunikation einschließlich der auf ihr basierenden Dienste. Soweit weitere personenbezogene Daten, wie etwa Bestandsdaten, betroffen sind, ist der Schutz aus dem Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) einschlägig. Wegen der Grundrechtsrelevanz von Ermittlungshandlungen im Rahmen der Strafverfolgung bedarf es für die Erhebung von personenbezogenen Daten in jedem Falle spezieller gesetzlicher Befugnisse.

Generell gilt, dass Anbieter weder berechtigt noch verpflichtet sind, vorauseilend für Zwecke der Strafverfolgung oder der Nachrichtendienste personenbezogene Daten zu speichern, die sie nach den oben beschriebenen Bestimmungen von TKG, TDSV, TDDSG und MDStV nicht verarbeiten dürften.

4.1 Zugangs-Anbieter (Access Provider)

Da es sich bei den Zugangs-Anbietern wie unter 3.1 ausgeführt um Anbieter von Telekommunikationsdiensten handelt, richtet sich die Herausgabe von **Bestandsdaten** nach § 89 Abs. 6 TKG. Die für den Dienst erhobenen Bestandsdaten dürfen nach Maßgabe dieser Vorschrift im Einzelfall auf Ersuchen an die zuständigen Stellen übermittelt werden, soweit dies für die Verfolgung von Straftaten und Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgabe der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des militärischen Abschirmdienstes sowie des Zollkriminalamtes erforderlich ist. Eine richterliche Anordnung ist nicht erforderlich. Darunter fallen auch Auskünfte über Inhaber statischer IP-Adressen, da dies zu den Bestandsdaten des Nutzers gehört. Allerdings darf nicht über alle Bestandsdaten Auskunft verlangt werden, sondern nur solche, die einen spezifischen Telekommunikationsbezug aufweisen (also zwar z. B. Name und Anschrift, nicht aber Bankverbindung des Nutzers). Auskünfte über Inhaber dynamischer IP-Adressen können hingegen nicht nach § 89 Abs. 6 TKG erlangt werden, da es sich insoweit um Verbindungsdaten handelt (s. u.).

Die bei der Nutzung eines Zugangs-Dienstes entstehenden **Verbindungsdaten** unterliegen als „nähere Umstände der Telekommunikation“ dem Fernmeldegeheimnis nach § 85 TKG. Die Herausgabe von Verbindungsdaten über die zugrunde liegende Telekommunikation erfolgt aufgrund der §§ 100g und 100h Strafprozessordnung (StPO), die den Zugriff auf Verbindungsdaten gegenüber der früheren Rechtslage nach § 12 Fernmeldeanlagengesetz (FAG) teilweise beschränken, teilweise aber auch erweitern. So kann ein Richter (und bei Gefahr im Verzug die Staatsanwaltschaft) diejenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, zur Auskunft über die Verbindungsdaten verpflichten. Voraussetzung ist, dass bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine Straftat von erheblicher Bedeutung, insbesondere eine Katalogstraftat nach § 100a Satz 1 StPO, oder mittels einer Endeinrichtung eine beliebige Straftat begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht oder durch eine Straftat vorbereitet hat. Die Anordnung darf nur Verbindungsdaten des Beschuldigten oder eine der sonstigen in § 100a StPO genannten Personen betreffen und kann (im Gegensatz zum bisherigen Rechtszustand) auch für zukünftige Telekommunikationsverbindungen angeordnet werden.

Als Verbindungsdaten zu betrachten sind gem. § 100g Abs. 3 StPO im Falle einer Verbindung Berechtigungskennungen, Kartennummern, Standortkennung sowie Rufnummer oder Kennung des anrufenden und angerufenen Anschlusses oder der Endeinrichtung, Beginn und Ende der Verbindung nach Datum und Uhrzeit, vom Kunden in Anspruch genommene Telekommunikationsdienstleistung, Endpunkte festgeschalteter Verbindungen, ihr Beginn und ihr Ende nach Datum und Uhrzeit. Aus der Formulierung „im Falle einer Verbindung“ folgt, dass Daten über erfolglose Verbindungsversuche, die nach § 85 Abs. 1 Satz 3 TKG ebenfalls dem Telekommunikationsgeheimnis unterliegen, nicht an die Strafverfolgungsbehörden herauszugeben sind. Für einen Zugangsanbieter bedeutet dies konkret, dass er Auskunft über folgende Verbindungsdaten erteilen muss: verwendetes Protokoll (z. B. http), IP-Nummer beziehungsweise Domain-Name von Quell- und Zielserver, Datum und Uhrzeit des Abrufes. Außerdem muss er Auskünfte über Inhaber dynamischer IP-Adressen erteilen. Dazu gehört sowohl die Information, welche IP-Adressen innerhalb eines bestimmten Zeitraumes einem bekannten Nutzer zugewiesen waren beziehungsweise zukünftig zugeordnet werden, als auch wem eine bestimmte IP-Adresse zu einem bestimmten Zeitpunkt zugeordnet war.

§ 100g StPO ermöglicht jedoch nur die Herausgabe von Verbindungsdaten, nicht den strafverfolgungsbehördlichen Zugriff auf Inhaltsdaten der Kommunikation. Inhaltsdaten sind in diesem Zusammenhang nicht nur die eigentlichen Inhalte der aufgerufenen Internet-Seiten, sondern auch solche Bestandteile der URL (Uniform Resource Locator), die inhaltliche Angaben aufweisen. Demzufolge kann von einem Zugangsanbieter im Rahmen von § 100g StPO nur eine Auskunft über bestimmte Teilkomponenten der URL – namentlich Bezeichnung des Dienstes (http, ftp, pop etc.), des Hosts (IP-Adresse beziehungsweise Domain-Name) und ggf. Port-Nummer – verlangt werden. Alle weiteren Bestandteile der URL wie Dateipfade, Inhalte von Anfragen oder Web-Formularen sind Inhalte der Telekommunikation

und dürfen nur gem. §§ 100a, 100b StPO herausgegeben werden, wenn zuvor der Richter oder bei Gefahr im Verzuge die Staatsanwaltschaft mit binnen drei Tagen einzuholender richterlicher Bestätigung wegen des Verdachts einer in § 100a StPO genannten Katalogtat die Überwachung der Telekommunikation für die Zukunft angeordnet haben. Die Hilfsbeamten der Staatsanwaltschaft (Polizei) können diese Auskunft nicht verlangen.

4.2 E-Mail-Dienst

Die für den E-Mail-Dienst erhobenen **Bestandsdaten** dürfen – ebenso wie beim Zugangs-Anbieter – nach Maßgabe des § 89 Abs. 6 TKG im Einzelfall auf Ersuchen an die zuständigen Stellen übermittelt werden, soweit dies für die Verfolgung von Straftaten und Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgabe der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des militärischen Abschirmdienstes sowie des Zollkriminalamtes erforderlich ist. Eine richterliche Anordnung ist nicht erforderlich. Der E-Mail-Anbieter kann insbesondere Auskunft über die Zuordnung einer bestimmten Person zu einer bestimmten E-Mail-Adresse erteilen.

Inhaltsdaten und **Verbindungsdaten** von E-Mails unterliegen dem Fernmeldegeheimnis. Zu den Inhaltsdaten gehören auch der Betreff und die Bezeichnung von Dateianlagen. Die Überwachung der Inhalte ist dem entsprechend nur auf Basis der einschlägigen spezialgesetzlichen Eingriffsnormen zulässig. Rechtsgrundlage für diese Maßnahmen finden sich in den §§ 100a ff. StPO, § 39 Außenwirtschaftsgesetz (AWG) und dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G10). Die Anordnung nach § 100a StPO darf nur durch den Richter oder bei Gefahr im Verzuge auch durch die Staatsanwaltschaft, nicht aber durch deren Hilfsbeamte, getroffen werden. Die angeordneten Maßnahmen berechtigen nicht zum Zugriff auf vergangene Telekommunikationsvorgänge.

Für die Weitergabe der **Verbindungsdaten** bei E-Mail-Diensten an die Strafverfolgungsbehörden gelten die §§ 100g, 100h StPO. Daten mit Inhaltsbezug (etwa Betreff, Bezeichnung von Dateianlagen) dürfen aufgrund dieser Regelungen (vgl. § 100g Abs. 3 StPO) nicht an Strafverfolgungsbehörden übermittelt werden (s. o. 4.1).

Nach der Rechtsprechung des BGH stellt ein Zugriff von Strafverfolgungsbehörden auf Inhalte von E-Mail-Postfächern ebenfalls eine Telekommunikationsüberwachung dar. Das Eindringen in E-Mail-Systeme des Anbieters kann nicht auf die strafprozessualen Befugnisse der Beschlagnahme von Gegenständen oder zur Durchsuchung von Räumen gestützt werden, insbesondere weil der Zugriff anders als bei den vorgenannten Maßnahmen im Regelfall heimlich erfolgt und auch die zukünftige Kommunikation umfasst. Dies gilt auch dann, wenn z. B. ein Webmail-Anbieter Kopien bereits durch den Nutzer vom Server abgerufener E-Mails auf seinem Server speichert. Anders als bei einem Anrufbeantworter oder den auf dem PC des Nutzers gespeicherten abgerufenen E-Mails gilt hier weiterhin das Fernmeldegeheimnis, weil dies noch Bestandteil des vom Anbieter angebotenen E-Mail-Dienstes ist und der Nutzer zu Recht darauf vertraut, dass das Fernmeldegeheimnis für die gesamte Dauer der Erbringung des Dienstes (langfristige Bereithaltung von E-Mails auch zum wiederholten Abruf) gilt.

4.3 Inhalts-Anbieter (Content Provider)

§ 6 Abs. 5 Satz 5 TDDSG erlaubt es den Diensteanbietern, nach Maßgabe der hierfür geltenden Bestimmungen der Strafprozessordnung, Auskunft an Strafverfolgungsbehörden und Gerichte für Zwecke der Strafverfolgung zu erteilen.

Bestandsdaten im Bereich der Tele- und Mediendienste dürfen nur aufgrund einer Beschlagnahmeanordnung, die vom Richter und bei Gefahr im Verzuge auch durch die Staatsanwaltschaft oder ihre Hilfsbeamten erlassen werden kann, gem. §§ 94 ff. StPO herausgegeben werden.

Inhaltsdaten, die bei der Nutzung von Tele- und Mediendiensten anfallen und mittels Telekommunikation übermittelt werden, unterliegen ebenso wie die Inhaltsdaten der Telekommunikation dem Fernmeldegeheimnis. Sie können durch die Strafverfolgungsbehörden nur mittels Überwachung und Aufzeichnung der Telekommunikation ermittelt werden. Rechtsgrundlagen für diese Maßnahmen finden sich in den §§ 100a ff. StPO, § 39 Außenwirtschaftsgesetz (AWG) und dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G 10). Die Anordnung im Strafverfahren darf nur durch den Richter und bei Gefahr im Verzuge auch durch die Staatsanwaltschaft mit binnen drei Tagen einzuholender richterlichen Bestätigung erfolgen. Die angeordneten Maßnahmen berechtigen nur zum Zugriff auf zukünftig übertragene Inhalte.

4.4 Befugnisse der Nachrichtendienste

Mit dem Terrorismusbekämpfungsgesetz vom 9. 1. 2002 sind (befristet bis zum 10. 1. 2007) zusätzliche Erhebungsbefugnisse der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes (BND) und des Militärischen Abschirmdienstes (MAD) bei Anbietern von Telekommunikations- und Telediensten (nicht Mediendiensten) geschaffen worden. Die Nachrichtendienste dürfen im Einzelfall zur Erfüllung ihrer Aufgaben und unter der Voraussetzung, dass tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand bestimmte Staatsschutzdelikte oder Kapitalverbrechen plant, begeht oder begangen hat, von denjenigen, die geschäftsmäßig Telekommunikations- oder Teledienste erbringen oder daran mitwirken, unentgeltlich Auskünfte über Telekommunikations-

verbindungsdaten und Teledienstenutzungsdaten einholen. Dies setzt eine Anordnung des Bundesinnenministeriums beziehungsweise einer entsprechenden obersten Landesbehörde oder (im Fall des BND) des Chefs des Bundeskanzleramtes voraus. Die Auskunft kann auch in Bezug auf eine zukünftige Nutzung dieser Dienste verlangt werden. Eine Auskunftspflicht der Diensteanbieter gegenüber den Nachrichtendiensten besteht jedoch nicht, da der Gesetzgeber (anders als im Strafprozessrecht) einen entsprechenden Grundrechtseingriff nicht angeordnet hat.

Die Nachrichtendienste dürfen nur Auskunft über folgende Daten verlangen: Berechtigungskennungen, Kartennummern, Standortkennung sowie Rufnummer oder Kennung des anrufenden und angerufenen Anschlusses oder der Endeinrichtung, Beginn und Ende der Verbindung nach Datum und Uhrzeit, Angaben über die Art der vom Kunden in Anspruch genommenen Telekommunikations- und Teledienst-Dienstleistungen, Endpunkte festgeschalteter Verbindungen, ihr Beginn und ihr Ende nach Datum und Uhrzeit (§§ 8 Abs. 8 Satz 3 BVerfSchG, 8 Abs. 3a Satz 3 BNDG, 10 Abs. 3 Satz 3 MADG).

Anbieter von Tele-, Medien- oder Telekommunikationsdiensten werden durch die Strafprozessordnung oder das Recht der Nachrichtendienste (Verfassungsschutzgesetze des Bundes und der Länder, BNDG, MADG) weder berechtigt noch verpflichtet, generell Daten über ihre Nutzer auf Vorrat zu erheben oder zu speichern, die sie zu keinem Zeitpunkt für ihre eigenen Zwecke (Herstellung der Verbindung, Abrechnung) benötigen. Sie können nur im Einzelfall berechtigt sein oder verpflichtet werden, bei Vorliegen ausdrücklicher gesetzlicher Voraussetzungen (§§ 100a ff. StPO; 8 Abs. 8 BVerfSchG; 3 Abs. 1, 5 Abs. 1 G 10; 8 Abs. 3a BNDG; 10 Abs. 3 MADG; 39, 40 AWG) Nachrichteninhalte aufzuzeichnen und bestimmte Daten, die sie ursprünglich für eigene Zwecke benötigt haben und nach dem Multimedia- oder Telekommunikationsrecht löschen müssten, weiter vorzuhalten und den Strafverfolgungsbehörden oder Nachrichtendiensten zu übermitteln.

Die Landesämter für Verfassungsschutz können Auskünfte über Telekommunikationsverbindungsdaten und Teledienstenutzungsdaten nur dann einholen, wenn die Landesgesetzgeber das Antragsverfahren, die Beteiligung der G-10-Kommission, die Verarbeitung der erhobenen Daten und die Mitteilung an den Betroffenen sowie eine parlamentarische Kontrolle gleichwertig wie im Bundesverfassungsschutzgesetz geregelt haben.

25.4

Orientierungshilfe zu Rechtsfragen bei der Einführung häuslicher Telearbeitsplätze

Stand: 17. Oktober 2002

Diese Orientierungshilfe spricht nicht nur datenschutzrechtliche Fragestellungen an, sondern enthält auch Hinweise auf andere rechtliche Aspekte, die vor der Einführung von Telearbeit zu klären sind. Soweit einzelne Themenkreise doppelt angesprochen werden, ist dies darin begründet, dass manche Themenkomplexe mehrfach relevant sind.

1. Schwachstellen von Telearbeitsplätzen

Bei der Telearbeit gibt es im Vergleich zum Büroarbeitsplatz zusätzliche 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) Der Arbeitsplatzrechner ist unberechtigten Zugriffen eher ausgesetzt.

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

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

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

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

2. Regelungsbereiche

Für die Telearbeit sind zu verschiedenen Bereichen dienstliche Anordnungen, allgemeine Weisungen und technische Vorgaben nötig:

Die Anordnungen und Vorgaben zur Nutzung der dienstlichen Einrichtungen sind für folgende Bereiche erforderlich:

a) zur Nutzung der dienstlichen Einrichtungen am Telearbeitsplatz und

b) zu den Befugnissen des zu Hause arbeitenden Bediensteten im Netz des Dienstherrn

c) zur häuslichen Umgebung des Arbeitsplatzes

d) zur Ausstattung des Arbeitsplatzes

e) zur Absicherung der Kommunikation mit der Dienststelle

f) zum Zugang in das Verwaltungsnetz und dessen Absicherung

g) zu den Protokolldaten und deren Auswertung

h) zu notwendigen Änderungen und deren Vorabanzeige.

Die mit den Bediensteten zu schließenden Einzelvereinbarungen sind in Form von Musterverträgen vorzubereiten.

3. Verantwortlichkeit

a) Die datenverarbeitende Stelle bleibt für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich.

b) Die datenverarbeitende Stelle hat die technischen und organisatorischen Maßnahmen nach § 10 HDSG vorzugeben. Sie muss die vom Mitarbeiter zugesicherten Maßnahmen ausdrücklich bestätigen.

c) Sie muss die Einhaltung aller Maßnahmen kontrollieren.

4. Grundpflichten und -rechte der Bediensteten

Die Bediensteten dürfen die personenbezogenen Daten nur im Rahmen der Weisungen des Dienstherren verarbeiten. Weisungen muss es insbesondere geben

a) zum Verbot der Bearbeitung mit und der Übertragung auf eigene DV-Anlagen

b) zur Nutzung des dienstlichen PC und der über ihn erreichbaren Speicher

c) zur Verwahrung und zur Herausgabe von Arbeitsunterlagen und entsprechenden Dateien

d) zu den Löschungspflichten und deren Befristung

e) zur Internetnutzung und E-Mail über dienstliche PC

f) zur Sicherung des PC gegen unbefugte Nutzung

g) zur Handhabung der vorgegebenen Verschlüsselungstechnik (ggf. durch technische unausweichliche Vorgaben)

h) zum Administratoreneinsatz einschließlich der Kontrollrechte am Telearbeitsplatz

i) zur Verwendung von Programmen nach Auswahl der Dienststelle (Ausschluss der Nutzung eigener Software)

j) zur Verfügbarkeit der Daten und deren Aktualisierung

Es muss organisatorisch und technisch sichergestellt werden, dass am Telearbeitsplatz verarbeitete Daten der Dienststelle ausreichend aktuell zur Verfügung stehen. (Speicherung der Daten auf einem Server der Dienststelle, tägliche Übertragung der Daten zur Dienststelle, evtl. Abrufrecht der Dienststelle ...)

5. Einzelvertraglich zu regelnde Sachverhalte

Folgende Punkte müssen zusätzlich zu in 4. genannten Grundpflichten in den Einzelvereinbarungen mit den Bediensteten geklärt werden:

a) Art der zu verarbeitenden Daten. Hier sind Einschränkungen zu beachten, die sich aus Amts- oder besonderen Berufsgeheimnissen ergeben (Personaldaten, Patientendaten, Sozialdaten).

b) Zutrittsrechte des behördlichen Datenschutzbeauftragten vor Arbeitsaufnahme und während der Telearbeit. Insbesondere sind die vom Bediensteten vorgesehenen Datensicherheitsmaßnahmen zu überprüfen.

c) Zutrittsrechte der behördlichen Administratoren zur Wartung, Behebung von Störungen und bei Veränderungen der Hard- oder Software.

d) Kontrollrechte der Dienststelle, insbesondere das Zutrittsrecht zur Wohnung. Geregelt werden muss, was geschieht, wenn der Zutritt verweigert wird. Es ist sinnvoll, die Möglichkeit vorzusehen, dass das Telearbeitsverhältnis außerordentlich beendet wird.

e) Rückholrechte des dienstlichen Geräts, auch zu Prüfzwecken.

f) Kontrollrechte des Hessischen Datenschutzbeauftragten. Insbesondere müssen die Zutrittsrechte durch Unterwerfungserklärung der mit dem Mitarbeiter entsprechend § 4 Abs. 3 Satz 1 HDSG vereinbart werden. Wenn die Einwilligung verweigert wird, darf ein Telearbeitsplatz nicht eingerichtet werden. Für den Fall, dass der Zutritt durch den Bediensteten im Einzelfall verweigert wird, sollte die Möglichkeit der Beendigung des Telearbeitsplatzes vorgesehen werden.

g) Datensicherung. Festzulegen ist insbesondere die Verantwortung für die Datensicherung (Backup). (Etwa zentraler Datenbeistand bei der Dienststelle, lokaler Datenbestand beim Bediensteten.)

h) Pflicht zur Anzeige von Änderungen im häuslichen Bereich. Grundsatz der Vorabgenehmigung durch die Dienststelle.

i) Hinweis auf die einzuhaltenden Sicherheitsvorkehrungen, die die Dienststelle vorgegeben hat
   - technische und organisatorische Maßnahmen
   - Passwortschutz
   - arbeitsplatzspezifische Sicherheitsvorkehrungen
   - Aufbewahrungs- und Verwahrungspflichten
   - Sicherheit beim Transport von Datenträgern
   - Verschlüsselungsmethoden
   - Löschung von Datenträgern nach Weisung der Dienststelle
   - Verbot, private Rechner mit dienstlichen Anschlüssen zu verbinden
   - Verbot, Dritten Zugriffe auf das Arbeitsgerät zu gestatten.

Diese Hinweise sind in einem Merkblatt zusammenzufassen.

a) Vertraglich festzulegen sind überdies
   - Arbeitsort
   - Arbeitszeit
   - Arbeitsauftrag
   - Arbeitsbemessung bei Stücklohnvereinbarung

b) Kostenerstattung durch die Dienststelle (Umfang, Nachweispflichten und Verfahren im Streitfall)

6. Abstimmung mit dem Personalrat

Grundsätzlich ist der Personalrat bei der Einführung von Telearbeitsmodellen zu beteiligen. Das gilt insbesondere für beabsichtigte Maßnahmen, die zur Überwachung des Bediensteten geeignet sind. Sollen Protokollierungen vorgenommen werden, die über die Aufzeichnungen, die am Arbeitsplatz vorgenommen werden, hinausgehen, so müssen diese mit dem Personalrat angestimmt werden.

7. Technische Sicherungsmaßnahmen

7.1 Standardsicherungen

a) Soweit möglich muss durch technische und organisatorische Maßnahmen die Vertraulichkeit von dienstlichen Unterlagen am Telearbeitsplatz erreicht werden.

b) Das Verwaltungsnetz muss gegen unbefugte Zugriffe geschützt werden. Soweit möglich muss der Dienstherr gewährleisten, dass nur berechtigte Personen vom Telearbeitsplatz aus auf dienstliche Daten zugreifen können.

c) Durch technische Sicherungsmaßnahmen müssen die Vertraulichkeit und die Integrität der zwischen dem Telearbeitsplatz und der Dienststelle übertragenen Daten gewahrt sein.

d) Die Zugriffsrechte müssen auf das erforderliche Maß reduziert sein.

e) Das gesamte Verfahren muss revisionssicher sein.

7.2 Sicherheitsbedingte Einzelmaßnahmen

7.2.1 Sicherungen am Telearbeitsplatz

a) Die Dienststelle stellt die gesamte IT-Ausstattung zur Verfügung. Der Telearbeiter darf keine Änderungen bei Soft- und Hardwarekomponenten vornehmen (können). Software darf nur mit Genehmigung der Dienststelle eingespielt werden.

b) Die Möglichkeit zur verschlüsselten Speicherung von Dateien oder die Verschlüsselung der gesamten Festplatte ist bei sensiblen Daten vorzusehen. Dabei ist ein anerkanntes kryptografisches Verfahren zu nutzen.

c) Durch das Betriebssystem oder zusätzliche Sicherheits-Hard- und Software müssen die Benutzer (Telearbeiter, Administrator) unterschieden werden. Sie dürfen nur im erforderlichen Umfang Zugriffsrechte besitzen. Zur Authentisierung müssen zumindest Passwörter verlangt werden.

d) Generell ist zu empfehlen, zusätzliche technische Einrichtungen wie chipkartenbasierter Logon oder biometrische Verfahren zu nutzen.

e) Wie bei einem Arbeitsplatz im Büro muss der Bildschirmschoner aktiviert und ein Virenscanner installiert sein.

f) Der Dienstherr muss Behältnisse zur sicheren Lagerung der Datenträger zur Verfügung stellen.

g) Datenträger müssen an die Dienststelle zurückgegeben werden. Es darf kein Zurückbehaltungsrecht im Streitfall geben. Die Dienststelle muss die datenschutzgerechte Vernichtung vornehmen.

7.2.2 Sicherung der Kommunikation und des Dienstellennetzes

a) In einem Sicherheitskonzept sind die Maßnahmen zum Schutz des Dienststellennetzes festzulegen (ggf. auf Basis des Grundschutzhandbuchs). Insbesondere muss die Sicherheit des Kommunikationsrechners gewährleistet werden.

b) Für die Telearbeit sollten spezielle Benutzerkennungen eingerichtet werden, um für die Telearbeit gezielt Berechtigungsprofile einrichten zu können. Die Zugriffsrechte müssen restriktiv vergeben werden. Wurde eine Kennung längere Zeit nicht genutzt, sollte sie gesperrt werden.

c) Die Anbindung des Telearbeitsplatzes muss durch Einrichtung einer geschlossenen Benutzergruppe auf Telekommunikationsebene, virtual private network (VPN) oder andere Sicherheitsfunktionen (Rufnummernprüfung, Call-Back) gesichert werden.

d) Die Datenübertragung muss verschlüsselt erfolgen (anerkanntes kryptografisches Verfahren). Dies gilt für Kommunikationsleitungen, aber auch für Disketten und vergleichbare Datenträger (Akten: in verschlossenen Behältern).

e) Ein direkter Zugang zum Internet oder anderen Online-Diensten vom Telearbeitsplatz aus muss unterbunden werden. Wenn dienstlich ein Zugang erforderlich ist, muss er über einen zentralen, durch eine Firewall gesicherten Punkt, der von der Dienststelle festgelegt ist, erfolgen.

f) Es muss protokolliert werden, wer wann auf welche Datenbestände mit Hilfe des Telearbeitsplatzes zugegriffen hat und welche Daten zwischen Dienststelle und Telearbeitsplatz übertragen wurden (Empfehlung: Dauer der Speicherung von Protokolldaten sechs Monate).

25.5
Mustersatzung zur Evaluation an Hochschulen

§ 1 Geltungsbereich

Diese Satzung gilt für die Datenverarbeitung (§ 2 Abs. 2 HDSG) von personenbezogenen Daten, die zur Evaluation von Leistungen in den Bereichen

– Forschung
– künstlerische Entwicklung
– Lehre (einschließlich Lehrangebot, Studienorganisation etc.)
– Förderung des wissenschaftlichen Nachwuchses
– Durchsetzung der Gleichberechtigung von Frauen und Männern

verwendet werden.

§ 2 Evaluation

(1) Der Evaluation im Sinne dieser Satzung dienen Verfahren, die die Verarbeitung personenbezogener Daten vorsehen, um Leistungen der Hochschule, der ihr angehörenden Forscher und Forscherinnen, der an der Hochschule Lehrenden, des wissenschaftlichen Nachwuchses und das Studienverhalten bewerten zu können.

(2) Evaluationsverfahren werden durchgeführt zur Qualitätssicherung und -verbesserung der Aufgabenerfüllung durch die Mitglieder und Angehörigen der Hochschule, zur Verbesserung des Lehr- und Studienangebots und zur Rechenschaftslegung der Hochschule gegenüber der Öffentlichkeit.

(3) Evaluationsergebnisse dienen der Information und Entscheidung
  – von hochschulinternen Gremien
  – von Stellen mit Aufsichts- oder Steuerungsfunktionen
  – der Öffentlichkeit.

(4) Die Erhebung und Weiterverarbeitung von Daten zum Zweck der Ressourcenzuteilung einschließlich der Ausstattung von Fachbereichen, Professuren und Einrichtungen richtet sich nach den allgemeinen Vorschriften. § 7 Abs. 1 Satz 3 bleibt unberührt.

§ 3 Grundsätze

(1) Personenbezogene Daten dürfen bei Evaluationsverfahren nur verarbeitet werden, soweit dies für den Evaluationszweck unter Beachtung des Grundsatzes der Verhältnismäßigkeit erforderlich ist.

(2) Sie sind möglichst frühzeitig zu anonymisieren, sobald dies der Evaluationszweck zulässt.

(3) Mehrfacherhebungen werden nur durchgeführt, soweit dies methodisch geboten ist.

(4) Daten, die der Privatsphäre zuzurechnen sind (Alter, Wohnort, Geburtsort, Familienstand, Kinderzahl), dürfen nur in zwingend notwendigen Fällen erhoben und weiterverarbeitet werden. Sie sind auf typische Merkmale zu beschränken.

(5) Die Verarbeitung von personenbezogenen Daten, die zur Evaluation erhoben worden sind, erfolgt getrennt von anderen Verwaltungsverfahren.

(6) Die Übermittlung von Daten an Vorgesetzte oder andere zur Steuerung von Aufgabenbereichen gemäß § 1 berufene Stellen ist zulässig.

(7) Soweit in Gremien personenbezogene Daten behandelt werden, geschieht dies in nicht-öffentlicher Sitzung. Die Beteiligten sind auf das Datengeheimnis nach § 9 HDSG sowie die Straf- und Ordnungswidrigkeitstatbestände in §§ 40, 41 HDSG besonders hinzuweisen.

(8) Eine Weiterverarbeitung personenbezogener Daten für andere Zwecke als der Evaluation und der daraus abzuleitenden Maßnahmen der Steuerung und Aufsicht ist unzulässig.

§ 4 Datenarten

Zu Zwecken der Evaluation dürfen folgende Arten von Daten verarbeitet werden:

1. Studienbezogene Daten:
   - Immatrikulationsdaten (§§ 2 und 3 HDVVO)
   - Art des Studienzugangs (z. B. Hochschulauswahlverfahren)
   - Anzahl von Studierenden und Studienanfängern beziehungsweise -anfängerinnen eines Fachbereichs
   - Studium in und außerhalb der Regelstudienzeit
   - Verteilung der Studiendauern
   - Abbruchsquoten
   - Bestehen von Zwischenprüfungen und von Pflichtübungen und -seminaren
   - Examenszahlen, -ergebnisse und -quoten
   - Alter bei Studienbeginn und -abschluss
   - Finanzierung des Studiums und soziale Lage von Studierenden
   - Notenverteilung;

   dabei kann nach Studiengängen, Haupt- und Nebenfachstudierenden unterschieden werden;

2. Lehrbezogene Daten:
   - Vorbereitung von Lehrveranstaltungen
   - Qualität von Arbeitspapieren
   - Einhaltung der Veranstaltungsgliederung
   - Qualität des Vortrags
   - aktive Einbeziehung von Studierenden
   - Prüfungsanforderungen
   - Prüferfolge
   - Teilnehmerzahl, Schwundquote
   - Anzahl betreuter Studienabschlussarbeiten pro Professur
   - Studienbegleitung (Beratung, Betreuung)
   - Studienstruktur und -bedingungen
   - zeitliche Lage von Lehrveranstaltungen;

3. Daten zum Wissenschaftlichen Nachwuchs:
   - Anzahl von begonnenen und abgeschlossenen Promotionen
   - Alter von Doktoranden und Doktorandinnen bei Beginn und Abschluss der Promotionsphase
   - Studienabschluss vor Promotion

- Anzahl betreuter Doktoranden und Doktorandinnen und abgeschlossener Promotionen pro Professur
- Finanzierungsarten von Promotionsvorhaben
- Angaben zur Betreuungsqualität
- entsprechende Angaben zu Habilitationen und zur Postdocphase
- zu gleichwertigen postgradualen künstlerischen Leistungen;

4. Forschungsbezogene Daten:
   - Verwendung zugeteilter Finanzmittel
   - Höhe, Herkunft und Zweckbindung von Drittmitteln
   - Publikationen
   - Zitationen
   - Gutachtertätigkeiten
   - Vorträge
   - Gastaufenthalte, wissenschaftliche Kooperationspartner
   - Herausgeberschaft von Zeitschriften und vergleichbarer Veröffentlichungen
   - Patente
   - Ausstellungen
   - Wettbewerbe
   - Preise
   - Beteiligung an Sonderforschungsbereichen
   - Leitungsfunktionen in Einrichtungen (Instituten, Kliniken);

5. Gruppenspezifische und soziale Daten von Studierenden und wissenschaftlichem Nachwuchs:
   - Alter
   - Geschlecht
   - Familienstand
   - Kinderzahl
   - Berufstätigkeit außerhalb der Hochschule
   - Nationalität, Regionalität
   - Hochschulzugangsberechtigung.

§ 5 Verfahren

(1) Die Mitglieder und Angehörigen der Hochschule haben an der Evaluation mitzuwirken.

(2) Soweit personenbezogene Daten verarbeitet werden, sind die betroffenen Personen oder der betroffene Personenkreis vorab über den Gegenstand des Evaluationsverfahrens und das angewandte Verfahren zu informieren. Ihnen ist Gelegenheit zur Stellungnahme zu geben.

(3) Die Information erfolgt gegenüber der betroffenen Person oder in allgemein zugänglicher Form, z. B. durch öffentlichen Aushang im Fachbereich.

(4) Bei Zweifeln über die datenschutzrechtliche Zulässigkeit der Verarbeitung von personenbezogenen Daten entscheidet das Präsidium auf Antrag; § 7 Abs. 2 bleibt unberührt.

(5) Vor einer Entscheidung gemäß Abs. 4 ist dem beziehungsweise der behördlichen Datenschutzbeauftragten Gelegenheit zur Stellungnahme zu geben.

§ 6 Erhebung

(1) Die Erhebung personenbezogener Daten erfolgt in erster Linie durch Auswertung schriftlicher oder elektronisch gespeicherter Unterlagen sowie durch Befragung der betroffenen Person oder Dritter mit Bezug zu dem Evaluationszweck.

(2) Soweit die Erhebung personenbezogener Daten durch Befragung Dritter erfolgt, hat das ausschließlich nach Kriterien zu erfolgen, über die die betroffene Person vorab informiert worden ist.

(3) Vor Erhebungen sind sowohl die betroffene Person selbst als auch der Personenkreis, der sich zu Evaluationszwecken äußern soll, über Gegenstand, Zweck und Verfahren der jeweiligen Untersuchung und der vorgesehenen Auswertung zu unterrichten.

§ 7 Weitere Verarbeitung

(1) Die weitere Verarbeitung personenbezogener Daten erfolgt durch Bewertung der erhobenen Daten. Sie ist auf den vorab festgelegten Evaluationszweck zu beschränken. Zweck kann auch die Ressourcenzuteilung sein.

(2) Übermittlungen erfolgen ausschließlich zur Auswertung von Evaluationsergebnissen im Rahmen der Zuständigkeit der empfangenden Stelle. Diese hat die Zweckbindung der Daten zu beachten und darf die Daten nur dann an andere Stellen weiterleiten, wenn diese ihrerseits Evaluationen auswerten. In Konfliktfällen entscheidet der Präsident beziehungsweise die Präsidentin nach Stellungnahme des oder der behördlichen Datenschutzbeauftragten.

(3) Im Falle der Übermittlung personenbezogener Daten ist die Herkunft der Daten durch geeignete Kennzeichnung deutlich zu machen.

§ 8 Löschung

(1) Spätestens ein Jahr nach der Erhebung von Evaluationsdaten ist zu prüfen, ob eine weitere personenbezogene Speicherung notwendig ist. Die Prüfung und ihr Ergebnis sind zu dokumentieren.

(2) Archivrechtliche Vorschriften bleiben unberührt.

§ 9 Veröffentlichung

(1) Eine Veröffentlichung von personenbezogenen Daten, die zu Evaluationszwecken erhoben worden sind, ist nur mit Einwilligung zulässig.

(2) Zur Information der Öffentlichkeit dürfen nur anonymisierte Evaluationsergebnisse verwendet werden.

(3) Formen der Veröffentlichung können insbesondere sein: öffentliche Sitzungen, Einstellen in elektronische Netze, Aushang und Druck. Die Form der Bekanntmachung ist entsprechend dem Evaluationszweck unter Beachtung der Schutzbelange der Personen zu bestimmen, deren Daten verwendet wurden.