Landtag von Baden-Württemberg
12. Wahlperiode

Drucksache 12 / 750
04. 12. 96

Mitteilung

des Landesbeauftragten für den Datenschutz

**Siebzehnter Tätigkeitsbericht des
Landesbeauftragten für den Datenschutz in Baden-Württemberg**

Der Tätigkeitsbericht wurde dem Landtag von Baden-Württemberg mit Schreiben vom 3. Dez. 1996 Az. C 2310 vorgelegt.

Eingegangen: 04. 12. 96 / Ausgegeben: 17. 12. 96

Siebzehnter Tätigkeitsbericht des Landesbeauftragten für den Datenschutz in Baden-Württemberg

INHALTSVERZEICHNIS

2. Teil: Öffentliche Sicherheit

3. Teil: Gesundheit

4. Teil: Soziale Leistungen

5. Teil: Rund ums Rathaus

6. Teil: Weitere Schwerpunkte

Zur Situation

Datenschutz in der Entwicklung

Datenschutz ist keine ein für allemal fixierte Größe. Als Instrument der Sicherung des Selbstbestimmungsrechts der Menschen hat er sich vielmehr ständig den Risiken anzupassen, die sich aus den sich wandelnden politischen, gesellschaftlichen und wirtschaftlichen Gegebenheiten und der Entwicklung der Technik ergeben.

– Modernisierung des Datenschutzrechts – ein Gebot der Stunde
Hand in Hand mit der rasant zunehmenden internationalen Verflechtung der Wirtschaft findet auch ein immer stärker werdender weltweiter Informationsaustausch statt. Ermöglicht und unterstützt wird dieser durch den Einsatz der modernen Informations- und Kommunikationstechniken und dem damit verbundenen Ausbau von Datennetzen wie z.B. dem Internet. Dieser unaufhaltsame Marsch in eine globale Informationsgesellschaft, in der Menschen aller Kontinente über diese Netze miteinander kommunizieren und Informationen austauschen können, ist für viele ein Faszinosum, über dem sie allzu leicht außer acht lassen, daß dabei eine für unsere Gesellschaft und die von ihr verkörperten Werte wesentliche Errungenschaft, nämlich ein das Selbstbestimmungsrecht der Menschen wahrender Datenschutz, in Gefahr gerät, auf der Strecke zu bleiben. Denn das Datenschutzniveau ist in den meisten Ländern dieser Erde wesentlich niederer als bei uns. Not tut deshalb, darauf hinzuwirken, daß der Datenschutz nicht an den Grenzen haltmacht, sondern sich dort in möglichst gleicher Qualität fortsetzt. Einen wichtigen Schritt in diese Richtung stellt die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Okt. 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. Nr. L281/31) dar, die sog. EU-Datenschutzrichtlinie. Diese verpflichtet die Mitgliedstaaten, ihr Datenschutzrecht binnen drei Jahren auf einem relativ hohen Niveau zu harmonisieren.

  Die Umsetzung dieser Richtlinie wird in der nächsten Zeit gesetzgeberische Aktivitäten sowohl im Bund als auch in den Ländern notwendig machen. Die Datenschutzbeauftragten von Bund und Ländern haben dies zum Anlaß genommen, in einer Entschließung (vgl. Anhang 3) an den Gesetzgeber in Bund und Ländern zu appellieren, sich nicht, wie leider zu befürchten ist, mit einer bloßen Anpassung des geltenden Rechts zu begnügen und sich damit auf das notwendige Minimum zu beschränken. Statt dessen sollten sie die Gelegenheit als Chance nutzen, das deutsche Datenschutzrecht umfassend zu modernisieren. Denn eines muß man klar sagen: Unser Datenschutzrecht beruht noch weitgehend auf Vorstellungen der 70er und 80er Jahre und berücksichtigt den Stand der Informations- und Kommunikationstechnik der damaligen Zeit. Seither haben sich aber die Verhältnisse sehr stark verändert. Stichwortartig seien einige dieser neuen Entwicklungen genannt:
  * Immer deutlicher wird, daß die Gefahren für das Selbstbestimmungsrecht der Menschen nicht nur von einem Daten sammelnden und auswertenden Staat ausgehen, sondern in ständig steigendem Maße auch von Datensammlungen privater Stellen. Denn der Einsatz der modernen Informations- und Kommunikationstechniken und die sich ständig verändernde Medienwelt führen dazu, daß der Mensch immer mehr Spuren hinterläßt, die zu sammeln, miteinander in Beziehung zu setzen, auszuwerten und zur Beeinflussung und Lenkung von Menschen zu benutzen allein schon aus wirtschaftlichen Gründen ein erheblicher Anreiz besteht. Um welche Dimensionen es dabei geht, nur ein Beispiel: Schon jetzt bietet ein in dieser Branche tätiges Unternehmen in Baden-Württemberg Werbung treibenden Firmen 35 Millionen Privatadressen an und zwar aufgeschlüsselt nach Kaufkraft, Konsumneigung und Wohnsituation, wobei alle Merkmale miteinander kombinierbar sind.
  * Die herkömmliche strikte Trennung zwischen Datenschutz im öffentlichen und Datenschutz im privaten Bereich verliert immer mehr ihre Berechtigung. In einer Zeit, in der der Staat zu einer veritablen Schlankheitskur genötigt wird, hängt es häufig nur noch von organisatorischen Zufälligkeiten ab, ob ein und dieselbe Aufgabe von einer privaten oder einer öffentlichen Stelle bewältigt wird.

* An die Stelle der früher vorherrschenden Konzentration der Datenverarbeitung in großen Rechenzentren ist eine Dezentralisierung und Miniaturisierung getreten. Der Siegeszug des PC hat die Datenverarbeitung zurück an den Arbeitsplatz gebracht.
* Die damit einhergehende wachsende Vernetzung und die ständige Steigerung der Leistungsfähigkeit der Netze ermöglichen einen Datenaustausch auf Knopfdruck in Sekundenschnelle zwischen all diesen „kleinen Brüdern", der früher nicht vorstellbar war.
* Der zunehmende Einsatz der Chipkarten-Technik nötigt die Datenschutzrechtsexperten zu Interpretationskunststücken, die Akrobaten alle Ehre machen würden. Man denke nur an die für das geltende Datenschutzrecht zentrale Frage nach der speichernden, für die Datenverarbeitung letztlich verantwortliche Stelle, auf die bei Chipkarten eine Antwort zu finden, wenn man ehrlich ist, gar nicht möglich ist.

All dies macht Reaktionen notwendig, soll erreicht werden, daß der Einzelne auch in Zukunft möglichst weitgehend selbst die Verwendung seiner Daten, die ja ihn selbst in all seinen Erscheinungs- und Betätigungsformen widerspiegeln, bestimmen kann. Anzustreben ist u.a. folgendes:

* Das Datenschutzrecht für den öffentlichen und privaten Bereich sollte möglichst weitgehend vereinheitlicht werden, damit in beiden Bereichen ein gleichwertiges, hohes Datenschutzniveau erreicht wird. Die bisherige stiefmütterliche Behandlung des Datenschutzes im privaten Bereich kann nicht länger beibehalten werden.
* Verbesserungen sind aber auch bei der Datenschutzkontrolle notwendig. Weil sich die Unterschiede zwischen öffentlichem und privatem Bereich immer mehr verwischen und eine Abgrenzung oft genug kaum noch sinnvoll möglich ist, ist eine weitgehende Vereinheitlichung der Datenschutzkontrolle notwendig. So ist z.B. überhaupt nicht einzusehen, weshalb, wie in Baden-Württemberg, ein von einer GmbH des Landkreises geführtes Kreiskrankenhaus wie auch andere Krankenhäuser in privater Trägerschaft eine Datenschutzkontrolle durch das Innenministerium als Aufsichtsbehörde für den privaten Datenschutz nur akzeptieren muß, wenn und soweit die Aufsichtsbehörde Grund zur Annahme hat, daß ein Datenschutzverstoß begangen worden ist, während die Datenverarbeitung eines Kreiskrankenhauses, das vom Landkreis selbst betrieben wird, auch ohne konkreten Anlaß vom Landesbeauftragten für den Datenschutz überprüft werden kann. Aber nicht nur die Kontrollbefugnis sollte angeglichen werden. Wenn schon die Übertragung beider Kontrollzuständigkeiten auf eine unabhängige Stelle aus verfassungsrechtlichen Gründen für problematisch erachtet wird, sollte zumindest eine enge Kooperation angestrebt werden, damit in beiden Bereichen möglichst einheitliche Kontrollmaßstäbe angelegt werden. Schließlich muß der ständig zunehmende Einsatz der EDV und anderer moderner Informations- und Kommunikationstechniken auch seinen Niederschlag in der Ausstattung der Datenschutzkontrolle mit technischem Sachverstand finden. Auch in einer Zeit knappster Haushaltsmittel geht es nicht an, auf der einen Seite den IuK-Einsatz zu forcieren und auf der anderen Seite die Datenschutzkontrolle im öffentlichen wie im privaten Bereich an der kurzen Leine zu halten.
* Es wäre eine Illusion zu glauben, allein schon mit der Existenz der unabhängigen Datenschutzkontrolle sei die Einhaltung der Datenschutzbestimmungen bei den Behörden gesichert. Insbesondere kann auf diese Weise der ordnungsgemäße Einsatz der EDV nicht überwacht werden. Deshalb sollte auch im öffentlichen Bereich eine effektive Eigenkontrolle durch qualifizierte interne Beauftragte für den Datenschutz angestrebt werden. Dies würde u.a. auch ermöglichen, auf die Führung des Datenschutzregisters durch unser Amt und den damit verbundenen aufwendigen Meldedienst der Behörden zu verzichten.
* Schließlich gilt es, die Vorschriften zur Datensicherheit den geänderten technischen Gegebenheiten anzupassen und dabei z.B. den Einsatz von Verschlüsselungstechniken beim Transport von Daten in ausgewählten Bereichen zwingend vorzuschreiben.

– Gefordert ist auch die Technik
Eine Modernisierung des datenschutzrechtlichen Instrumentariums, für die die Datenschutzbeauftragten des Bundes und der Länder in ihrer bereits erwähnten Entschließung noch eine ganze Reihe weitere Vorschläge auf den Tisch

gelegt haben, reicht aber nicht aus, um den aktuellen und künftigen Gefährdungen des Rechts der Menschen, selbst über die Preisgabe und Verwendung ihrer Daten zu bestimmen, wirksam zu begegnen. Gefordert ist vielmehr auch die Technik selbst. Ob beim Einsatz von Chipkarten, bei Multimediadiensten oder anderen elektronischen Dienstleistungen, überall sollte der möglichst auch im Datenschutzrecht noch ausdrücklich zu verankernde Grundsatz der Datensparsamkeit und die Forderung nach Wahrung größtmöglicher Anonymität ein zentrales Anliegen sein, dem es durch eine datenschutzgerechte Ausgestaltung der Technik Rechnung zu tragen gilt, soweit dies irgend möglich ist. Dazu können und sollten gerade auch die Datenschutzbeauftragten einiges beitragen, indem sie, wie dies schon jetzt in vielfältiger Weise geschieht, beratend an der Entwicklung von Projekten mitwirken, dazu Vorgaben machen und auf die Datenschutzimplikationen hinweisen. Aber nicht nur dies: Kraft des bei ihnen angesiedelten Sachverstands und ihrer Akzeptanz bei den Bürgern sind sie prädestiniert dazu, nicht nur diejenigen, die an der Entwicklung und der Entscheidung über den Einsatz der neuen Techniken mitwirken, zu beraten und auf möglichst datenschutzkonforme Lösungen zu drängen, sondern verstärkt auch generell in der Öffentlichkeit auf mögliche Risiken und Konsequenzen hinzuweisen. Dies könnte dazu beitragen, daß die, die sich später der neuen technischen Möglichkeiten bedienen sollen, für diese Risiken sensibilisiert werden und daß effektiver Datenschutz und ausreichende Datensicherheit zu Recht immer mehr als Qualitätsmerkmale einer neuen Technik und einer neuen Dienstleistung empfunden werden. Damit wiederum würde für diejenigen, die diese produzieren und an ihrem Einsatz interessiert sind, ein zusätzlicher Anreiz geschaffen werden, sich um möglichst datenschutzgerechte Lösungen zu bemühen und so auch den erhofften wirtschaftlichen Erfolg zu erzielen.

Das Amt

Das Berichtsjahr war für unser Amt ein außergewöhnliches Jahr, endete doch am 31. März 1996 die Amtszeit von Frau Dr. Ruth Leuze, der ersten Landesbeauftragten für den Datenschutz in Baden-Württemberg. Bei ihrem Ausscheiden fand ihre Arbeit in den vergangenen 16 Jahren zu Recht vielfältige Anerkennung. Zwar gibt es nach wie vor Auseinandersetzungen darüber, wieviel oder wie wenig Datenschutz notwendig ist und gerade in der heutigen Zeit hat er nicht gerade Hochkonjunktur. Doch sind jedenfalls die Zeiten vorbei, in denen, wie noch zu Beginn der 80er Jahre, der Datenschutz insgesamt in Frage gestellt wurde und z.B. in Baden-Württemberg ein Ministerium in aller Offenheit davon reden konnte, von einem Datenschutzbedürfnis der Allgemeinheit könne man allenfalls insoweit sprechen, „als es ihr interessierte Seiten mit Erfolg aufdrängen“ (vgl. 3. Tätigkeitsbericht, LT-Drs. 8/3450, S. 15). Dieser Wandel ist zu einem guten Teil dem konsequenten und von großem persönlichen Einsatz geprägten Bemühen von Frau Dr. Leuze zu verdanken, dem Datenschutz den ihm gebührenden Rang zu verschaffen.

Aber auch das Amt selbst hat durch ihre Amtsführung eine Bedeutung erlangt, wie dies jedenfalls bei seinem Start im April 1980 nicht zu erwarten war. So läßt sich vielleicht erklären, weshalb trotz zahlreicher Bewerber die Nachfolgefrage in unserem kleinen Amt 8 Monate nach Ende der Amtszeit von Frau Dr. Leuze immer noch nicht gelöst ist.

Für die Arbeit unseres Amtes war diese Vakanz freilich alles andere als erfreulich, zumal außerdem seit 1. Jan. 1996 eine Referentenstelle und seit 1. Mai 1996 eine weitere von insgesamt 16 im Haushaltsplan ausgewiesenen Stellen nicht mehr besetzt waren. Logische Folge war, daß wir uns weitgehend darauf beschränken mußten, auf Anstöße von außen zu reagieren statt aus eigenem Antrieb zu agieren. Insbesondere waren deshalb systematische, nicht durch konkrete Anlässe ausgelöste Kontrollen vor Ort nicht in dem Maße möglich, wie dies eigentlich wünschenswert gewesen wäre. Dies alles ist, nicht zuletzt wegen der eingangs angesprochenen drängenden Fragen, vor die sich der Datenschutz in der heutigen Zeit gestellt sieht, wahrlich kein Zustand, der noch lange andauern darf.

1. Teil: Datenschutz und Technik

1. Internet und Intranets

Alles redet vom Internet, das nach wie vor boomt. Daneben gewinnen aber zunehmend auch Abkömmlinge des Internets, nämlich die sog. Intranets an Bedeutung. Dabei handelt es sich um interne Computernetzwerke von Behörden, Unternehmen oder anderen Institutionen, die zur Datenübertragung die Internet-Technik einsetzen, salopp ausgedrückt also um Internets en miniature. Intranets müssen nicht zugleich mit dem Internet gekoppelt sein, sind es aber häufig. Nachdem wir uns im vergangenen Jahr mit dem Internet, seiner Struktur und Funktionsweise sowie mit den damit verbundenen grundlegenden datenschutzrechtlichen Risiken befaßt hatten (vgl. 16. Tätigkeitsbericht, LT-Drs. 11/6900, S. 45 ff.), nahmen wir uns dieses Jahr der spezifischen Risiken an, denen es beim Anschluß von internen Netzen, insbesondere von Intranets an das Internet zu begegnen gilt.

1.1 Gesicherte Anschlüsse an das Internet
Wer ein internes Computernetz betreibt, in dem auch personenbezogene Daten transportiert werden, muß beim Anschluß dieses Netzes an das Internet dafür sorgen, daß Internet-Nutzer nicht unbefugt in das eigene Netz eindringen und dort personenbezogene Daten lesen oder ändern können. Dafür ist es unabdingbare Voraussetzung, daß die Stelle, die den Anschluß herstellen will, zunächst einmal ihren individuellen Kommunikationsbedarf ermittelt und ein Sicherheitskonzept erarbeitet. Darin sind sowohl das zu schützende System als auch die durch die beabsichtigte Koppelung hervorgerufenen Risiken genau zu beschreiben und festzulegen, welche technischen und organisatorischen Maßnahmen zur Abwehr der Risiken zu ergreifen sind.

1.1.1 Zentrale oder dezentrale Schutzmaßnahmen?
Vor einer Koppelung gilt es zu entscheiden, ob man alle internen Computer einzeln schützen oder aber die Sicherungsmaßnahmen auf einen zentralen Übergang zwischen dem eigenen Netz und dem Internet konzentrieren will. Da die Einrichtung und der Betrieb aufeinander abgestimmter dezentraler Sicherheitsmaßnahmen in aller Regel aufwendiger und fehlerträchtiger sein wird als die Einrichtung und der Betrieb einer zentralen Sicherungsstelle, der sog. Firewall, empfiehlt sich in aller Regel, die gewünschte Netzkoppelung durch eine Firewall zu sichern.

1.1.2 Was sollte eine Firewall leisten?
Bei der Auswahl der am Markt erhältlichen unterschiedlichen Firewall-Produkte sollte man darauf achten, daß die Firewall zumindest folgendes leistet:
- Sie prüft die Zulässigkeit einzelner Datenverbindungen zwischen dem internen Netz und dem Internet. Diese Prüfung muß vor allem der Frage nachgehen, wer die gewünschte Datenverbindung für welche Anwendung nutzen will und welche Internet-Adressen die beteiligten Computer haben. Bei dieser Prüfung ist von dem Grundsatz auszugehen, daß alles verboten ist, was nicht ausdrücklich erlaubt ist.
- Sie verhindert, daß Internet-Teilnehmer Informationen über das interne Netz, beispielsweise die Namen der internen Computer, ausforschen können, die unter Umständen Rückschlüsse auf deren Aufgaben oder die eingesetzte Technik zulassen.
- Sie protokolliert die Nutzung zugelassener Dienste sowie besondere sicherheitsrelevante Ereignisse wie
  * abgewiesene Verbindungsversuche;
  * zurückgewiesene Datenpakete;
  * erfolgreiche und abgewiesene Versuche des Systemverwalterzugriffs auf Firewall-Komponenten;

* Versuche, vom Internet aus Datenpakete durch die Firewall zu schleusen, die als Absenderangabe die Internet-Adresse eines internen Computers tragen (sog. IP-Spoofing-Attacken).

– Sie benachrichtigt darüber hinaus bei sicherheitsrelevanten Ereignissen sofort die Systemverantwortlichen.

1.1.3 Paket- und Anwendungsfilter im Dienste der Sicherheit

Um zulässige von unzulässigen Kommunikationswünschen zu unterscheiden, bedient sich eine Firewall in der Regel eines Paketfilters sowie eines Anwendungsfilters, häufig auch als „Application Level Gateway“ tituliert.

Um zu verstehen, wie ein Paketfilter arbeitet, sollte man sich folgendes vergegenwärtigen: Verfaßt ein Internet-Nutzer eine elektronische Post, surft er durch das World Wide Web (WWW) oder nutzt er einen der zahlreichen anderen Dienste, die das Internet bietet, so werden die dabei zu übertragenden Daten, also beispielsweise ein elektronischer Brief, nicht an einem Stück durch das Internet gesandt. Vielmehr wird der Brief oder werden die gewünschten WWW-Daten automatisch und ohne daß der Internet-Nutzer hiervon etwas bemerkt, in gleichgroße Bruchstücke zerlegt, mit einem „elektronischen Umschlag“ versehen und auf diese Weise zu Datenpaketen geschnürt, die dann einzeln ihren Weg durch das Internet antreten. Ein Paketfilter vergleicht die auf dem elektronischen Umschlag genannten Informationen, z.B. die Adressen der Herkunfts- und Zielcomputer mit Listen, in denen die Stelle, die die Firewall betreibt, die Herkunfts- und Zieladressen zulässiger Pakete hinterlegt hat. Stimmen die entsprechenden Angaben nicht überein, läßt der Paketfilter das fragliche Paket nicht passieren. Ein gravierender Nachteil eines Paketfilters liegt darin, daß seine Schutzfunktion durch Manipulationen der Absenderadresse unterlaufen werden kann. Ferner protokollieren viele Paketfilter nur unzureichend.

Diese Defizite lassen sich durch den zusätzlichen Einsatz eines Anwendungsfilters beheben. Mehr noch: Ein Anwendungsfilter greift auf die in den Paketen enthaltenen Daten, insbesondere auf Angaben über die Identität der Internet-Nutzer und die von ihnen gewählten Dienste zu und kann damit auch darüber wachen, welche Personen welche Anwendungen nutzen können.

1.1.4 Welche Firewall darf es sein?

Wer eine Firewall installieren will, hat zum einen die auf den ersten Blick verlockende Möglichkeit, die erforderlichen Programme kostenlos über das Internet zu beziehen. Damit kann man nicht nur Geld sparen, sondern erhält auch Einblick in den gesamten Programmcode und kann diesen Zeile für Zeile überprüfen. Zudem werden dessen Schwachstellen in der Fachöffentlichkeit offen erörtert, so daß, wenn nötig, rasche Abhilfe möglich ist. Wer ein solches Produkt einsetzen will, sollte allerdings darauf achten, daß er es von einer vertrauenswürdigen Quelle bezieht und etwa durch verschlüsselte Übertragung ausgeschlossen wird, daß das Produkt unterwegs unbemerkt manipuliert werden kann. Möglich ist es aber auch, Firewalls auf dem Markt zu kaufen. Dabei ist jedoch zu bedenken, daß deren Programmcode geheimgehalten wird, was einer offenen Diskussion etwaiger Produktmängel entgegensteht. Statt dessen ist man auf einen guten Kundendienst angewiesen und muß darauf vertrauen, daß der Hersteller der Firewall stets umgehend über die ihm bekanntgewordenen Sicherheitsmängel informiert.

Bei all dem darf man jedoch nie außer acht lassen, daß die Anbindung eines internen Netzes an das Internet in jedem Fall die Datenschutzrisiken für die im internen Netz befindlichen Daten erhöht. Selbst wenn man eine nach allen Regeln der Kunst gestaltete Firewall einsetzt, läßt sich damit ledig-

lich die Zunahme des Risikos begrenzen, ganz auf den Status quo ante zurückführen läßt es sich aber nicht.

1.2 Verwaltungsnetze am Internet – Erfahrungen aus der Praxis
Um einen Eindruck davon zu gewinnen, wie öffentliche Stellen beim Anschluß ihrer internen Netze an das Internet vorgehen, führten wir zwei Kontrollbesuche durch. Dabei zeigten sich folgende Mängel:

1.2.1 Fehlendes oder unvollständiges Sicherheitskonzept
Eine der beiden überprüften Stellen konnte zwar eine Dokumentation der von ihr getroffenen Sicherheitsvorkehrungen vorlegen. Daraus war jedoch nicht zu ersehen, von welchen Risiken diese Stelle bei der Erstellung ihres Sicherheitskonzepts ausgegangen war. Prompt hatte sie auch einige sicherheitsrelevante Punkte nicht bedacht. Die andere Stelle meldete in puncto Dokumentation sogar Fehlanzeige. Weil zur Anbindung eines internen Netzes an das Internet viele komplexe Regelungen und Maßnahmen zu treffen sind, ist das Fehlen eines zu Papier gebrachten vollständigen Sicherheitskonzepts ein gravierender Mangel, der nahezu zwangsläufig auch zu Mängeln bei der praktischen Umsetzung der Schutzvorkehrungen führt.

1.2.2 Schutzmöglichkeiten der Paketfilter nicht oder nur unzureichend genutzt
Die Firewall einer der überprüften Stellen enthielt zwei, die der anderen einen sog. Router, die auch als Paketfilter genutzt werden können. Beide Stellen hatten von dieser Möglichkeit entweder gar keinen oder nur unzureichend Gebrauch gemacht. Dazu im einzelnen:

– Filterfunktionen nicht genutzt
Bei einer Stelle bestand die Firewall aus zwei Routern und einem dazwischen angeordneten Computer, auf dem ein Paket- und ein Anwendungsfilter eingerichtet war. Diese Geräte waren so miteinander verbunden, daß Daten auf dem Weg vom Internet ins interne Netz zunächst den äußeren Router, dann den Computer und schließlich den inneren Router passieren mußten. Die Router führten, obgleich technisch dazu in der Lage, keine Paketfilterung durch. Damit hätten Angreifer aus dem Internet Datenpakete bis zu dem in der Firewall installierten Computer leiten und dort ihre Angriffsversuche starten können. Bei richtiger Einstellung und fehlerfreier Funktion der Firewall wäre das auch nicht weiter problematisch. Da aber technische Fehler oder Störungen nie ganz auszuschließen sind, empfahlen wir dieser Stelle gleichwohl, auch die von den Routern bereitgestellten Filterfunktionen zu nutzen, um unerwünschte Verbindungsversuche so frühzeitig und so weitgehend wie möglich abzuwehren.

– Filterregeln zu großzügig gewählt
Die Firewall der anderen Stelle bestand aus einem Router mit einem Paketfilter. Dessen Einstellungen ließen es zu, daß mehr Datenpakete ins interne Netz gelangen konnten, als unbedingt erforderlich. Gesetzt den Fall, die Systemkonfiguration eines im internen Netz angeschlossenen Computers wäre entsprechend geändert worden, was aufgrund der unzureichenden Sicherung der vernetzten PC durchaus möglich gewesen war, so hätte sogar vom Internet aus eine unberechtigte Verbindung mit einem internen Computer aufgebaut werden können. Wir forderten daher die Stelle auf, restriktiver zu filtern und die PC des internen Netzes vor unerwünschten Änderungen an den Systemeinstellungen zu schützen.

1.2.3 Zu viele Informationen über das interne Netz preisgegeben
Bei einer Stelle war es jedem Internet-Teilnehmer möglich, aus bestimmten internen Computern eine Liste abzurufen, in der die Namen einzelner Rechner, ihre Internet-Adressen sowie einige weitere Informationen über die einzelnen Rechner genannt waren. Um zu vermeiden, daß Angreifer von diesen Informationen profitieren können, forderten wir die betroffene Dienststelle auf, dafür zu sorgen, daß nicht mehr Informationen über das eigene Netz nach außen dringen können als unbedingt notwendig.

1.2.4 Protokollierung ungenügend
Beide Stellen protokollierten nur unzulänglich. Die Firewall der einen Stelle zählte lediglich, wie viele Datenpakete insgesamt zwischen welchen Geräten ausgetauscht wurden. Wer dabei welche Anwendung nutzte, war daraus jedoch nicht zu entnehmen. Gravierender war noch, daß abgewiesene Datenpakete oder Verbindungsversuche nicht erfaßt wurden und diese Stelle daher keine Hinweise auf etwaige Unregelmäßigkeiten erhalten konnte. Die Firewall der anderen Stelle protokollierte zwar die Nutzung einzelner Dienste, registrierte aber ebenfalls nicht die abgewiesenen Verbindungsversuche. Auch zurückgewiesene Versuche, mit der Systemverwalterberechtigung auf Firewall-Komponenten zuzugreifen, wurden nicht protokolliert. Wir mahnten daher bei beiden Stellen eine aussagekräftigere Protokollierung an.

1.2.5 Mängel bei der Administration der Firewall-Komponenten
Die Qualität des mit einer Firewall erreichten Schutzes steht und fällt damit, daß die Einstellungen der Firewall entsprechend den individuellen Notwendigkeiten des Betriebs des internen Netzes gewählt werden. Deshalb sind an die Systemverwaltung, die die Einstellung der Firewall-Komponenten vorzunehmen hat, besonders strenge Sicherheitsanforderungen zu stellen. Unsere Kontrollen machten auch in diesem Bereich Defizite deutlich:

- Fehlende Terminalbeschränkung für Systemverwalter
  In einem Fall konnten sich die Systemverwalter von allen am internen Netz angeschlossenen Computern aus an einem zur Firewall gehörenden Computer anmelden. Da sich bei aller Sorgfalt nie ganz ausschließen läßt, daß ein Systemverwalterpaßwort einmal einem Dritten bekannt wird, ist es wichtig, daß diese Funktion nicht von einem beliebigen PC in einem „stillen Kämmerlein“, sondern nur von möglichst wenigen Computern aus ausgeübt werden kann. Abhilfe war notwendig.

- Übertragene Administrationsdaten schützen
  Die Systemverwaltung der Paketfilter durfte in einem Fall nur von ausgewählten Computern aus erfolgen. Diese befanden sich in einem Segment des internen Netzes, das insgesamt ca. 50 Anschlüsse umfaßte. In diesem Netzsegment standen alle Datenpakete prinzipiell allen angeschlossenen Computern zur Verfügung. Zwar pickt sich jeder Computer normalerweise nur die Datenpakete heraus, die für ihn bestimmt sind. Durch eine Veränderung der Computereinstellungen kann man allerdings erreichen, daß ein Computer auch solche Datenpakete aufgreift, die für einen anderen Computer bestimmt sind. Um zu vermeiden, daß auf diesem Weg Administrationsdaten unberechtigt abgehört oder manipuliert werden können, forderten wir dazu auf, den Administrationszugang für den Paketfilter besonders zu sichern. Dies könnte dadurch geschehen, daß entweder alle Firewall-Administrationsarbeitsplätze in einem eigenen Netzsegment zusammengefaßt oder aber die Administrationsdaten nur verschlüsselt übertragen werden.

1.2.6 Nicht von der Firewall gesicherte Internet-Anbindungen
Eine Stelle ließ es zu, daß außer über die Firewall auch auf mehr als 50 anderen, über öffentliche Netze führenden Wegen Daten zwischen internen Computern und externen Stellen ausgetauscht werden konnten. Dabei war nicht auszuschließen, daß über diese Wege auch einmal eine Verbindung zwischen dem internen Netz und dem Internet zustande kommen konnte. Jeder, der solche Verbindungen zuläßt, muß bedenken, daß die beste Firewall nichts wert ist, wenn auch nur über eine einzige andere Verbindung Daten ungehindert zwischen Internet und internem Netz hin- und herfließen können. Wir hielten die betroffene Stelle daher dazu an, möglichst bald ein bislang lediglich geplantes Projekt zu verwirklichen und künftig alle Verbindungen zwischen internem Netz und externen Netzen über ihre Firewall abzuwickeln.

Leider ist damit das Problem ungesicherter Verbindungen noch nicht völlig aus der Welt, denn auch dann, wenn unserer Aufforderung Rechnung getragen ist, gehen weiterhin Gefahren von Internet-Anschlüssen aus, die von einzelnen Mitarbeitern ohne Wissen der EDV-Verantwortlichen etwa mit Hilfe eines Modems hergestellt werden können. Um diesen Gefahren zu begegnen, muß jede Stelle, die eine Firewall betreibt, ihre Mitarbeiterinnen und Mitarbeiter klipp und klar darauf hinweisen, daß es unzulässig ist, solche Verbindungen herzustellen. Einen darüber hinausgehenden technischen Schutz kann man erreichen, indem man in seinem internen Netz sog. private Internet-Adressen verwendet, die einen von seiten des Internet gewünschten Zugriff auf interne Computer zumindest erschweren. Wir forderten beide überprüfte Stellen auf, derartige private Adressen in ihren internen Netzen künftig zu verwenden.

1.2.7 Programme aus dem Internet: ein Risiko
Immer mehr WWW-Angebote halten nicht nur Informationen in Form von Texten, Bildern und Querverweisen bereit, sondern sind auch in der Lage, vom Internet-Teilnehmer eingegebene Daten, z.B. über seine Einkommensverhältnisse, zu erfassen und daraus – um im Bild zu bleiben – die fällige Steuerbelastung zu berechnen. Wenn jemand ein solches WWW-Angebot nutzt, so geschieht folgendes: Der Computer, auf dem das Angebot gespeichert ist, sendet nicht nur die zum Angebot gehörenden Texte und Bilder an den Internet-Teilnehmer, sondern auch das zur Verarbeitung der eingegebenen Daten erforderliche Programm, das dann – ohne weiteres Zutun des Internet-Teilnehmers – automatisch auf dessen Computer gestartet wird.

Wer, wie eine überprüfte Stelle, dagegen keine Schutzvorkehrungen ergreift, verliert den Überblick darüber, wann auf internen Rechnern welche Programme mit welchen Funktionen ablaufen und gerät in Gefahr, daß sicherheitsrelevante Einstellungen interner Computer oder dort gespeicherte personenbezogene Daten geändert oder Dritten mitgeteilt werden. Deshalb sollten aus dem Internet kommende automatisch startende Programme möglichst nur auf Computern laufen können, die gegenüber anderen internen Computern so abgeschottet sind, daß die Vertraulichkeit und Integrität personenbezogener oder sicherheitsrelevanter Daten durch den Programmablauf nicht beeinträchtigt werden können.

1.3 Aufbau ressortspezifischer Intranets im Bereich der Landesverwaltung
Die Behörden von Land und Kommunen stehen derzeit vor der schwierigen Aufgabe, ihren EDV-Betrieb trotz leerer Kassen nicht nur aufrechtzuerhalten, sondern ihn auch mit den sich ständig wandelnden Anforderungen Schritt halten zu lassen. Hohe Erwartungen setzt dabei so manche Behörde auf Verwaltungsintranets, also den

verwaltungsinternen Einsatz der Internet-Übertragungsstandards sowie darauf abgestimmter Programme. Der besondere Reiz dieser Intranets liegt darin, daß Programme für unterschiedlichste Computertypen zur Verfügung stehen, was bei der bunten EDV-Landschaft der Landesverwaltung von nicht zu unterschätzendem Wert ist, und sie zudem vielfach kostenlos und bequem über das Internet erhältlich sind. Da auch beim Datentransport in einem Intranet eine ausreichende Datensicherheit gewährleistet sein muß, kam dem vom Innenministerium in diesem Jahr auf den Tisch gelegten Konzept einer Fortschreibung des schon lange existierenden Datenschutz- und Sicherheitskonzepts für das Landesverwaltungsnetz erhebliche Bedeutung zu. Ging es dabei doch darum, der Landesverwaltung Hinweise zum Aufbau von Intranets und zur Nutzung des Internet zu geben. Unter anderem sollen danach Intranets einzelner Landesressorts sowohl untereinander als auch mit Intranets des Bundes oder von Kommunen verknüpft werden dürfen, sofern der Übergang durch eine sog. standardisierte Firewall abgesichert wird. Auch soll bei Bedarf jeder Arbeitsplatzcomputer eine Verbindung zum Internet erhalten können.

Bei allem Verständnis dafür, daß ein solches Konzept nicht jedes Detail aufgreifen kann, war die im ersten Entwurf des Innenministeriums enthaltene Beschreibung der standardisierten Firewall und die Darstellung der Maßnahmen zur Sicherung der Arbeitsplatzcomputer doch gar zu knapp ausgefallen. Deshalb war es für uns besonders wichtig zu erreichen, daß für jedes Intranet und dessen Koppelungen mit anderen Netzen ein auf die jeweilige konkrete Gegebenheit abgestimmtes Sicherheitskonzept erstellt wird, das sowohl die relevanten Risiken als auch die gebotenen Schutzmaßnahmen beim Namen nennt. Das Innenministerium nahm daraufhin diese Forderung in sein Konzept auf. Des weiteren konnten wir noch folgende Klarstellungen und Ergänzungen erreichen:

- Paketfilter sind so zu betreiben, daß sie alle Kommunikationswünsche zurückweisen, die nicht ausdrücklich erlaubt wurden.
- Eine standardisierte Firewall muß, anders als zunächst vorgesehen, die Kommunikationsvorgänge angemessen protokollieren.

Weiteren Ergänzungs- und Änderungsvorschlägen, die u.a. darauf gerichtet waren,

- das Einschleusen von Datenpaketen mit offensichtlich manipulierten Adressen technisch zu unterbinden,
- mit Hilfe der Firewall die interne Struktur der daran angebundenen Intranets zu verbergen,
- zu verhindern, daß über einen gleichzeitig an einem Landesintranet und dem Internet angeschlossenen Arbeitsplatzcomputer automatisiert Daten hin- und herfließen können,

blieb dagegen der Erfolg versagt. Weder das Innenministerium noch der Landessystemausschuß, der im Herbst der Fortschreibung des Datenschutz- und Sicherheitskonzepts für das Landesverwaltungsnetz zustimmte, trugen ihnen Rechnung.

2. Verschlüsselung

Wie kann jemand einem anderen eine nur für diesen bestimmte Nachricht so zukommen lassen, daß ihr Inhalt für Dritte nicht erkennbar ist, auch wenn ihm die Nachricht in die Hände fällt? Mit dieser Frage befaßt sich seit eh und je die Kryptographie. Lange Zeit war diese Disziplin der Informatik fast ausschließlich eine Domäne von Militärs und Geheimdiensten, die ihre Nachrichten und Informationen geheimhalten wollten. Das hat sich inzwischen wesentlich geändert. Mit der zunehmenden Computerisierung und Vernetzung hat sich das Betätigungsfeld der Kryptographie wesentlich erweitert. Immer öfter wird Verschlüsselung auch in einem Atemzug mit effektiverem technischen Datenschutz genannt.

2.1 Was bedeutet Verschlüsselung?
Mit der Verschlüsselung soll erreicht werden, daß nur derjenige

Nachrichten entschlüsseln, also im Klartext wieder lesbar machen kann, der über nur ihm bekanntes Wissen, den Schlüssel, verfügt, während anderen die Entschlüsselung nicht möglich ist. Ob dies gelingt, hängt wesentlich davon ab, welcher Schlüssel gewählt wird und ob es möglich ist, ihn geheimzuhalten. Würde z.B. der Begriff *„Kryptographie“* durch *„Lszquphsbqijf“* ersetzt, hätte derjenige, dem diese verschlüsselte Information in die Hände fällt, keine große Mühe herauszufinden, daß jeder Buchstabe des Alphabets durch den nächsten ersetzt ist. Verschlüsselungsverfahren, die die ihnen zugedachte Funktion erfüllen und denen auch Experten nicht so leicht auf die Schliche kommen, sind natürlich sehr viel trickreicher und komplizierter aufgebaut und benötigen eine Vielzahl von Rechenoperationen. Sie lassen sich in zwei Klassen einteilen:

– Symmetrische Verschlüsselungsverfahren
Hier gilt die Regel: Wer verschlüsseln kann, kann immer auch entschlüsseln. Notwendig dabei ist, daß Absender und Empfänger einer Nachricht den gleichen nur ihnen bekannten Schlüssel besitzen, mit dem sie sowohl verschlüsseln als auch entschlüsseln können. Neben dem nie ganz auszuschließenden Risiko, daß der Schlüssel Dritten bekannt wird, hat dieses Verfahren den Nachteil, daß bei einer Vielzahl von Kommunikationsvorgängen mit unterschiedlichen Partnern auch viele Schlüssel benötigt werden und der Aufwand für die Schlüsselverwaltung dementsprechend groß ist.

– Asymmetrische Verschlüsselungsverfahren
Verschlüsselungsverfahren auf ganz anderer Basis wurden Mitte der 70er Jahre entwickelt und seither auch angewandt. Dabei benötigt jeder Kommunikationspartner ein Schlüsselpaar, unabhängig davon, mit wie vielen anderen Partnern Nachrichten ausgetauscht werden sollen. Einen dieser beiden Schlüssel bewahrt er bei sich auf und hält ihn geheim. Der andere ist öffentlich. Ihn darf er beliebig vielen bekanntgeben und z.B. auch unter seinem Namen in einem elektronischen Telefonbuch veröffentlichen. Die Verschlüsselung funktioniert so: Der Absender verschlüsselt die Nachricht mit dem öffentlichen Schlüssel des gewünschten Empfängers. Die Nachricht entschlüsseln kann aber nur der Empfänger mit seinem geheimen Schlüssel. Zwei Vorteile gegenüber symmetrischen Verfahren springen sofort ins Auge: Erstens müssen Absender und Empfänger nicht erst einen geheimen Schlüssel verabreden, bevor sie verschlüsselt Daten austauschen können und zweitens ist die Anzahl der insgesamt benötigten Schlüssel wesentlich geringer, weil jeder Kommunikationspartner nur ein einziges Schlüsselpaar braucht. Der Teufel steckt aber auch hier im Detail, denn das Problem der Schlüsselverwaltung ist noch nicht zufriedenstellend gelöst: Wer es auf nicht für ihn, sondern für eine andere Person oder Stelle bestimmte Informationen abgesehen hat, kann seinen öffentlichen Schlüssel unter deren Namen veröffentlichen und die an sie gerichteten Nachrichten abfangen und lesen. Zumindest in größeren Datennetzen ist deshalb eine Vertrauensinstanz, ein sog. Trust Center, unverzichtbar, die garantiert, daß mit der Schlüsselverwaltung, also der Erzeugung, Verteilung, Veröffentlichung, Speicherung, Sperrung und Löschung von Schlüsseln alles seine Ordnung hat. Eine besondere Stärke asymmetrischer Verschlüsselungsverfahren besteht darin, daß sich mit ihnen eine digitale Signatur, auch elektronische Unterschrift genannt, realisieren läßt. Wer dem Empfänger eines Dokuments dessen Echtheit garantieren möchte, verschlüsselt es mit seinem geheimen Schlüssel und versendet es anschließend unter seinem Namen. Gelingt es dem Empfänger, das Dokument mit dem zugehörigen öffentlichen Schlüssel des Absenders zu entschlüsseln, ist die Authentizität nachgewiesen.

u

2.2 Was bringt Verschlüsselung für den Datenschutz?
Wer personenbezogene Daten automatisiert verarbeitet, muß Siche-

rungsvorkehrungen treffen, die sicherstellen, daß die Datenverarbeitung auch nur so erfolgt, wie dies das Datenschutzrecht zuläßt. Solche Maßnahmen sind notwendig, um insbesondere folgenden Risiken entgegenzuwirken:

– Gefährdung der Vertraulichkeit
  Ein zentrales Anliegen des Datenschutzes lautet: Personenbezogene Daten dürfen nur denjenigen bekannt werden, für die sie bestimmt sind. Automatisch sichergestellt ist dies jedoch nicht:
  * Personenbezogene Daten, die unverschlüsselt in Datennetzen fließen, sind offen lesbar wie auf einer Postkarte. Wer Datenleitungen abhört oder in das Datennetz eindringt, kann sie sich mühelos verschaffen. Besonders groß ist diese Gefahr in Datennetzen wie dem Internet, die jedermann zugänglich sind. Problematisch sind aber auch die sog. „Broadcast"-orientierten Netzwerke, in denen jedes darin übertragene Datenpaket jeweils für alle angeschlossenen Rechner zugänglich ist. Funktioniert alles ordnungsgemäß, so kopiert sich ein Rechner nur dann ein Datenpaket und verarbeitet es weiter, wenn es an ihn adressiert ist. Ein Rechner läßt sich aber auch auf relativ einfache Weise so manipulieren, daß er jedes Datenpaket, also auch die nicht für ihn bestimmten, aufnimmt. Auf diese Weise kann man den gesamten Datenverkehr in dem Netzwerk abhören. Beinahe unbegrenzte Möglichkeiten hat der Systemverwalter des Netzbetreibers. Er hat in aller Regel keine Mühe, z.B. eine elektronische Post zu lesen.
  * Gefährdet ist aber auch die Vertraulichkeit von personenbezogenen Daten, die unverschlüsselt auf der Festplatte eines P C gespeichert sind. Wird der Computer entwendet – bei einem mobilen PC wie einem Laptop oder Notebook kann dies leicht passieren –, so kann jeder die Daten lesen.

– Kann man elektronisch übertragenen Daten trauen?
  Wer Daten per Datenfernübertragung erhält, will sicher sein, daß sie wirklich vom angegebenen Absender stammen und unverfälscht bei ihm ankommen. Die Realität sieht anders aus:
  * Dem, der eine elektronische Post verschicken will, bereitet es in aller Regel keine allzu große Mühe, sie mit einer falschen Absenderangabe zu versehen.
  * Personenbezogene Daten können in Datennetzen aber auch verändert werden. Da solche Manipulationen häufig sogar keine Spuren hinterlassen, läßt sich dies meist nicht einmal im nachhinein feststellen. So hat z.B. der Empfänger einer elektronischen Post keine Gewähr, daß ihr Inhalt unverfälscht ist. Das gleiche gilt auch für den, der Programme von einem fremden Rechner auf seinen eigenen Rechner kopiert, wie dies z.B. bei der Nutzung des Internet gang und gäbe ist. Jedes Programm kann manipuliert und mit einem Virus behaftet sein. Schließlich könnte auch der Systemverwalter eines Netzbetreibers seine Macht mißbrauchen und z.B. elektronische Post verändern und dann weiterschicken.

– Schwäche des herkömmlichen Paßwortschutzes
  Mit dem Computer darf nur der Daten verarbeiten, der dazu auch legitimiert ist. Um dies sicherzustellen, setzt man heutzutage vor allem auf den Paßwortschutz. Ohne Schwächen ist dieser klassische Schutzmechanismus freilich nicht:
  * Häufig kommen Paßwörter zum Einsatz, die nicht den allgemein anerkannten Regeln für deren Gestaltung entsprechen (vgl. z.B. 10. Tätigkeitsbericht, LT-Drs. 10/2730, S. 140 ff. und 14. Tätigkeitsbericht, LT-Drs. 11/2900, S. 112 ff.). Solche Paßwörter bieten keinen ausreichenden Schutz. In Zeiten, in denen mehr und mehr Stellen ihre Netze an weltweite Computernetze anschließen, erhalten diese Mängel eine ganz neue Dimension. Die Zahl derjenigen, die sich diese zunutze machen könnten, wächst damit nämlich explosionsartig an.

* Fließen, wie dies häufig der Fall ist, Benutzerkennung und Paßwort unverschlüsselt über die Datenleitungen, können sie durch Abhören ausgespäht werden. Selbst deren Verschlüsselung besitzt keinerlei ausreichende Sicherheit. Denn wer sie abhört, kann sie auch unverändert wieder einspielen und sich damit Zugang zu den Daten verschaffen.

Diesen Risiken gilt es wirksam zu begegnen. Dabei führt kein Weg am Einsatz geeigneter Verschlüsselungstechniken vorbei:
- Werden Daten verschlüsselt gespeichert oder übertragen, so kann der, für den sie nicht bestimmt sind, nichts damit anfangen, solange er sie nicht entschlüsseln kann.
- Die digitale Signatur kann sicherstellen, daß der Empfänger die Daten unverfälscht und von demjenigen erhalten hat, der als Absender angegeben ist.
- Schließlich kann der Einsatz geeigneter Verschlüsselungstechniken weitaus wirksamer als der herkömmliche Paßwortschutz gewährleisten, daß sich nur der an einem Computer anmelden kann, der dazu auch berechtigt ist.

Der Verschlüsselung kommt damit eine zentrale Rolle zu, wenn es um die Gewährleistung von Vertraulichkeit, Unversehrtheit und Zurechenbarkeit personenbezogener Daten geht. Verschlüsselungsverfahren, die inzwischen für immer mehr Rechnerplattformen und Anwendungsbereiche zur Verfügung stehen, eröffnen die Chance, daß der Einsatz moderner Technik zu einer Verbesserung des Persönlichkeitsschutzes führt. Verschlüsselung wird damit zu einem Grundpfeiler eines effektiven technischen Datenschutzes.

2.3 Was folgt daraus?
Weil die Verschlüsselung zu einer wesentlichen Verbesserung des Datenschutzes, insbesondere in Datennetzen beitragen kann, haben wir schon in der Vergangenheit für den Einsatz von Verschlüsselungstechniken im Landesverwaltungsnetz und bei der elektronischen Post plädiert (vgl. 15. Tätigkeitsbericht, LT-Drs. 11/5000, S. 115 ff.). Auch die Datenschutzbeauftragten des Bundes und der Länder haben sich wiederholt für einen verstärkten Einsatz von Verschlüsselungsverfahren bei der Übertragung von Daten ausgesprochen (vgl. Anhang 5). Diesen Forderungen sollten die datenverarbeitenden Stellen nicht nur Rechnung tragen, wenn sie Daten über öffentliche Netze leiten, sondern auch dann, wenn sie dafür Verwaltungsnetze benutzen. Denn auch dort bestehen die beschriebenen Risiken. In Zeiten, in denen die öffentliche Verwaltung mehr und mehr Daten automatisiert verarbeitet, die Zahl der an die Behördennetze angeschlossenen Teilnehmer stetig wächst und Verwaltungsnetze mit öffentlichen Netzen wie dem Internet gekoppelt werden, nehmen sie sogar noch zu. Hinzu kommt, daß für den Transport der Daten verwendete Übertragungsstrecken in der Regel von privaten Netzbetreibern angemietet sind. Die von ihnen ergriffenen Sicherheitsmaßnahmen, die für die Sicherheit des gesamten Datennetzes eine Rolle spielen, sind oft ganz oder teilweise unbekannt. Aus diesen Gründen halten wir es für vordringlich, bei der Einführung neuer Verfahren als Regelfall die Verschlüsselung der zu übertragenden Daten vorzusehen. Aber auch bei bestehenden Verfahren sollte so vorgegangen werden. Ein besonders dringlicher Handlungsbedarf besteht dabei generell bei Verfahren, die die Übertragung von Personal-, Steuer-, Polizei-, Sozialdaten, medizinischen oder ähnlich sensiblen Daten vorsehen. Inzwischen hat sich der Landessystemausschuß, der die EDV-Aktivitäten der Landesverwaltung zu koordinieren hat, mit dem Thema Verschlüsselung beschäftigt und Grundsätze zum Einsatz der Verschlüsselung aufgestellt. Dabei konnten wir ihn wenigstens dazu bewegen festzulegen, daß künftig vor dem Einsatz eines Verfahrens zur Übertragung personenbezogener Daten zu prüfen ist, ob die Daten verschlüsselt übertragen werden müssen. Dies ist zweifellos ein Schritt in die richtige Richtung, dem aber weitere folgen sollten. Damit die Verschlüsselung den ihr zugedachten Effekt bewirken kann, ist beim Beschaffen und dem Einsatz der Verschlüsselungsverfahren folgendes zu beachten:

- Verschlüsselungsprodukte, die aufgrund von Exportbeschränkungen einzelner Staaten nur mit einer verkürzten Schlüssellänge betrieben werden dürfen, sind problematisch, denn durch die Verringerung der Schlüssellänge wird die Sicherheit des Verfahrens reduziert. Empfehlenswert sind deshalb nur Verschlüsselungsprodukte, bei denen diese Einschränkung nicht besteht.
- Die Schlüsselverwaltung muß sicher sein. Es nützt beispielsweise gar nichts, ein sicheres Verschlüsselungsverfahren einzusetzen und dabei einen geheimen Schlüssel auf einem ungesicherten PC zu speichern.
- Schließlich erfordert Verschlüsselung ein Gesamtkonzept. Auf Dauer ergäbe es wenig Sinn, wenn jeder Anwender seine eigene Insellösung realisieren würde. Der Einsatz der Verschlüsselung in einem Datennetz, das jedem Teilnehmer den Datenaustausch mit vielen anderen Teilnehmern sowie die Nutzung einer ganzen Reihe von EDV-Verfahren ermöglicht, erfordert ein abgestimmtes Vorgehen. Unverzichtbar ist dabei festzulegen, welche Verschlüsselungstechniken zum Einsatz kommen sollen und wie sie mit den noch zu entwickelnden oder bereits eingesetzten EDV-Verfahren zusammenwirken sollen. Die Grundsätze für die Verschlüsselung im Bereich der Landesverwaltung sehen dazu eine ressortübergreifende Koordinierung der Verschlüsselung vor. Absprachen dürften aber auch mit den Kommunen sowie mit anderen Bundesländern und dem Bund notwendig sein. Auf Dauer wird auch kein Weg an einem oder mehreren Trust Centern vorbeiführen, um eine professionelle Schlüsselverwaltung zu gewährleisten.

3. Beratung

Fehler zu beheben, ist meistens schwieriger, als sie von vornherein zu vermeiden. Deshalb bemühten wir uns auch im vergangenen Jahr darum, trotz der damit verbundenen erheblichen Arbeitsbelastung schon im Status nascendi von EDV-Verfahren darauf hinzuwirken, daß sie am Ende datenschutzgerecht zum Einsatz kommen. So nahmen wir u.a. gegenüber dem Innen-, dem Justiz-, dem Finanz-, dem Kultusministerium und dem Ministerium Ländlicher Raum beratend zu geplanten EDV-Verfahren Stellung. Einige der dabei angesprochenen Fragen können auch andernorts für die Planung vernetzter Computersysteme relevant sein.

3.1 Sichere Anmeldung im Netz ermöglichen

Wer ein Computernetzwerk plant, in dem sich einzelne Nutzer von ihrem Arbeitsplatzcomputer aus bei anderen Computern anmelden können, sollte ein Anmeldeverfahren wählen, bei dem Paßwörter nicht im Klartext über das Netz transportiert werden. Auch sollte dabei bedacht werden, daß selbst verschlüsselte Paßwörter unterwegs abgehört und dann beliebig wieder eingespielt werden können. Schließlich sollte eine solche Anmeldung nur von möglichst wenigen, nicht von allen Arbeitsplatzcomputern aus möglich sein.

3.2 Sicherung der Arbeitsplatzcomputer

An modernen Computernetzen, die nach dem sog. Client/Server-Konzept aufgebaut sind, hängen zum einen Computer, die umfangreiche Datenbestände speichern und zur Nutzung durch Netzteilnehmer bereithalten (Server), und zum anderen Arbeitsplatzcomputer (Clients), von denen aus die auf den Servern gespeicherten Daten verarbeitet werden. Während die Server meistens gut gesichert sind, wird die Sicherung bei Arbeitsplatzcomputern immer wieder vernachlässigt. So kann bei ihnen vielfach jeder Nutzer unbeschränkt auf das Betriebssystem zugreifen, sicherheitsrelevante Systemeinstellungen ändern oder eigene Programme installieren, mit denen unter Umständen bestehende Sicherungsvorkehrungen des Netzwerks unterlaufen werden können. Um dies zu verhindern, sollten normale Benutzer nicht uneingeschränkt auf der Betriebssystemebene arbeiten und keine sicherheitsrelevanten Einstellungen ändern können. Diskettenlaufwerke, die normale Benutzer nicht für ihre tägliche Arbeit benötigen, sollten verriegelt werden.

3.3 Anschlüsse an andere Netze
Wer sein Computernetz mit einem oder mehreren anderen Netzen koppelt, um z.B. elektronische Post auszutauschen oder eine Wartung der eingesetzten Hard- und Software durch ein Wartungsunternehmen zu ermöglichen, muß dafür sorgen, daß Daten nur in dem Umfang zwischen dem eigenen und den angeschlossenen Netzen hin- und herfließen, wie dies zuvor festgelegt worden ist. Soweit die Koppelung durch eine Wählverbindung hergestellt werden soll, müssen flankierende Sicherungsvorkehrungen getroffen werden. Dafür kommt insbesondere die Einrichtung eines automatischen Rückrufverfahrens oder die Bildung einer geschlossenen Benutzergruppe in Betracht.

3.4 Benutzerservice
In weiträumigen Computernetzen gibt es häufig einen zentralen Benutzerservice, an den sich wenden kann, wer Probleme mit der Bedienung seines Arbeitsplatzcomputers oder eines Anwendungsprogramms hat. Da die gewünschte Hilfe um so besser möglich ist, je genauer der Benutzerservice weiß, was mit dem Computer des hilfebedürftigen Nutzers los ist, halten es manche Stellen für geboten, daß sich der Benutzerservice dort aufschalten und dadurch zum einen alles sehen kann, was am Bildschirm angezeigt wird, und zum anderen dort auch Eingaben tätigen kann. Ein solches System sollte insbesondere das Aufschalten auf einen Bildschirm deutlich und dauerhaft an dem jeweiligen Bildschirm signalisieren. Ferner sollten die Bildschirmaufschaltung und die am Computer des hilfebedürftigen Nutzers vorgenommenen Eingaben protokolliert werden.

3.5 Protokollierung
Für die Überprüfung des ordnungsgemäßen Umgangs mit personenbezogenen Daten leistet eine Protokollierung vielfach wertvolle Dienste. Unabhängig davon, was im einzelnen protokolliert wird, sollte folgendes beachtet werden:
- Bei allen zu protokollierenden Aktivitäten sollten in der Regel nicht nur die erfolgten Nutzungen, sondern auch abgewiesene Nutzungsversuche erfaßt werden können.
- Die Protokolldaten sollten möglichst vor nachträglichen Änderungen geschützt sein.
- Angesichts des großen Umfangs anfallender Protokolldaten empfiehlt es sich ferner, geeignete Programme zur systematischen Auswertung der Protokolldaten und zum Absetzen von Alarm-Meldungen bei sicherheitskritischen Ereignissen einzusetzen.

3.6 Datenbankentwurf mit Weitblick
Wer eine Datenbank einrichtet, muß, bevor er mit dem Einspeichern einzelner Daten beginnen kann, ein Datenbankschema entwerfen, das festlegt, welche Datenarten später einmal gespeichert werden sollen. Dieses Datenbankschema sollte sorgfältig geplant werden. Denn wenn erst einmal zahlreiche Daten in der Datenbank erfaßt sind, erfordert eine Änderung des Datenbankschemas mitunter Änderungen in jedem einzelnen gespeicherten Datensatz. Bei der Planung eines Datenbankschemas ist daher zum einen zu prüfen, ob die betreffende Stelle alle im Schema enthaltenen personenbezogenen Daten speichern darf. Zum anderen ist zu klären, ob für Zwecke des Datenschutzes besondere Datenfelder in das Datenbankschema aufgenommen werden müssen. Dies könnten beispielsweise Datenfelder sein, in denen registriert wird, wer auf welche personenbezogenen Daten zugreifen darf oder wer wann zugegriffen hat.

2. Teil: Öffentliche Sicherheit

1. Die verdachts- und ereignisunabhängige Personenkontrolle

Konnten sich in der vergangenen Legislaturperiode des Landtags die damaligen Regierungsparteien noch nicht auf die Einführung verdachts-

und ereignisunabhängiger Personenkontrollen verständigen, sah dies nach der Landtagswahl und den geänderten Mehrheitsverhältnissen ganz anders aus. Schon in ihrer Koalitionsvereinbarung schrieben die jetzt die Regierung tragenden Parteien die Einführung dieser Kontrolle fest. Bei der Realisierung dieser Absprache eilte es offenbar sehr. Weil das Innenministerium meinte, unsere Position aus unserer Äußerung zu der Frage, was von einer am bayerischen Vorbild orientierten Regelung zu halten sei, hinreichend zu kennen, leitete es uns seinen Gesetzentwurf zur Änderung des Polizeigesetzes erst gar nicht zu. Wir sahen uns deshalb veranlaßt, dem Landtag unsere Stellungnahme unmittelbar zukommen zu lassen und ihm dabei zu empfehlen, von dem Gesetzesvorhaben Abstand zu nehmen. Die wesentlichen Gründe für diese Empfehlung waren auf einen kurzen Nenner gebracht folgende:

Keine Frage: Das Vorzeigen eines Ausweises ist – wie Befürworter der Gesetzesänderung gerne argumentieren – keine allzu gravierende Angelegenheit. Bei näherem Hinsehen ist jedoch rasch klar: So einfach liegen die Dinge nicht. Zum einen brauchen Identitätsfeststellungen keineswegs immer so glimpflich abzulaufen. Wenn jemand seinen Ausweis nicht eingesteckt hat – dazu ist man bekanntlich nicht verpflichtet – kann die Polizei bei der Kontrolle die zur Feststellung seiner Identität erforderlichen Maßnahmen treffen; sie kann ihn insbesondere anhalten, ihn und die mitgeführten Sachen nach Gegenständen durchsuchen, die zur Identitätsfeststellung dienen, und ihn sogar in Gewahrsam nehmen und erkennungsdienstlich behandeln. Zum anderen ist die Identitätsfeststellung für die Polizei ein "Schlüssel", der ihr ermöglicht, die kontrollierte Person durch Computerabfragen gründlich vor allem danach abzuchecken, ob sie bereits einmal in ein strafrechtliches Ermittlungsverfahren verwickelt war, ob sie aus welchem Grund auch immer im Fahndungscomputer steht, ob sie tatsächlich Halter des Autos ist, mit dem sie unterwegs ist, oder was über sie im Ausländerzentralregister beim Bundesverwaltungsamt in Köln steht. Solche Abfragen können wiederum Auslöser für weitere Maßnahmen wie etwa Nachfragen bei anderen Polizeidienststellen oder sonstigen Behörden, Durchsuchungen, Sicherstellungen oder gar Festnahmen sein. Treffen können solche Maßnahmen jedermann, also nicht nur Personen, die tatsächlich oder vermeintlich etwas mit der grenzüberschreitenden Kriminalität zu tun haben. Damit liegt auf der Hand, daß solche verdachts- und ereignisunabhängige Personenkontrollen, die die Polizei den Kontrollierten gegenüber in keiner Weise rechtfertigen muß, ganz erheblich in das in Art. 1 Abs. 1 i.V. mit Art. 2 Abs. 1 des Grundgesetzes verankerte Grundrecht auf informationelle Selbstbestimmung eingreifen. Solche Eingriffe darf der Gesetzgeber nach der seit dem Volkszählungsurteil von 1983 ständigen Rechtsprechung des Bundesverfassungsgerichts aber nur im überwiegenden Allgemeininteresse unter Beachtung des Verhältnismäßigkeitsgrundsatzes zulassen. Konkret heißt dies: Lediglich die nicht durch Fakten abgesicherte Hoffnung, daß verdachts- und ereignisunabhängige Personenkontrollen etwas zur Verbesserung der Situation der Polizei beitragen können, reicht hierfür nicht. Notwendig ist vielmehr, daß sie einen zusätzlichen bedeutsamen Beitrag zur Bekämpfung der grenzüberschreitenden Kriminalität über das hinaus leisten, was die Polizei mit ihren bisherigen vielfältigen Kontrollmöglichkeiten sowieso schon kann. Daran zu zweifeln, besteht aus folgenden Gründen Anlaß:

– Der in der Diskussion über das Für und Wider so gern bemühte Verweis auf das Vorbild Bayern hilft nicht weiter. Zum einen ist die Rechtslage dort eine andere als bei uns, weil in Bayern die Grenzkontrolle und damit insbesondere die Verhinderung illegaler Grenzübertritte seit jeher Sache der Polizei und nicht wie in Baden-Württemberg Sache des Bundesgrenzschutzes ist. Der Bundesgrenzschutz kann aber in Baden-Württemberg schon bisher wie in Bayern die Polizei im Grenzgebiet verdachts- und ereignisunabhängige Personenkontrollen durchführen und tut dies, was auch in Protokollen über Landtagsdebatten der vergangenen Legislaturperiode nachgelesen werden kann, mit Erfolg. Zum anderen gibt es aus Bayern keine konkreten Angaben darüber, wie viele von den nach den dortigen "Erfolgsmeldungen" festgestellten Tatverdächtigen und Straftätern überhaupt der grenz-

überschreitenden Kriminalität zuzurechnen sind und wie viele von ihnen der Polizei ohne die Befugnis zu verdachts- und ereignisunabhängigen Personenkontrollen nicht ins Netz gegangen wären.
- Auch die Erfahrungen aus den bisherigen monatlichen Großfahndungen, bei denen die Polizei des Landes mit erheblichem Aufwand nach illegal aufhältlichen Ausländern fahndet, eignen sich nicht als Kronzeuge. 1994 hat sie beispielsweise bei insgesamt 824 Kontrollen, zu denen mehr als 8 900 Polizeibeamte notwendig waren, insgesamt lediglich 187 Ausländer ohne Aufenthaltserlaubnis ermittelt. Wenn aber schon diese eingehend vorbereiteten und ganz gezielten Fahndungen nicht mehr Effekt haben, ist doch sehr die Frage, ob verdachts- und ereignisunabhängige Personenkontrollen, die ja praktisch ins Blaue hinein erfolgen und der Suche nach der Stecknadel im Heuhaufen gleichen, überhaupt noch irgendeinen zusätzlichen polizeilichen Erfolg bringen können.
- So gar nicht ins Bild paßt auch, daß das Innenministerium als das für die Polizei zuständige Fachministerium bei gleicher Sachlage, die jetzt zum Beleg für die angebliche Notwendigkeit der Einführung von verdachts- und ereignisunabhängigen Personenkontrollen herangezogen wurde, nicht allzulange vorher auch gegenüber dem Landtag immer wieder betont hatte, daß das geltende Polizeigesetz der Polizei einen ausreichend weiten Handlungsspielraum für Personenkontrollen eröffnet und sich aus den Erfahrungen der Praxis kein Beleg dafür ergibt, daß weitere Kontrollmöglichkeiten notwendig seien.

Die Landtagsmehrheitsfraktionen schlossen sich unseren Argumenten nicht an. Die sodann beschlossene Änderung des Polizeigesetzes trat am 1. Sept. 1996 in Kraft. Seitdem kann die Polizei in Baden-Württemberg über die ihr bereits eingeräumten weitgehenden Möglichkeiten hinaus „zum Zwecke der Bekämpfung der grenzüberschreitenden Kriminalität in öffentlichen Einrichtungen des internationalen Verkehrs sowie auf Durchgangsstraßen (Bundesautobahnen und Europastraßen und anderen Straßen von erheblicher Bedeutung für die grenzüberschreitende Kriminalität)" die Identität einer Person feststellen, und zwar ohne daß irgend etwas über sie vorliegen müßte. Näheres hierzu regelte das Innenministerium Anfang August 1996 in einer langen Verwaltungsvorschrift. Auch dieses Mal sah es von einer Beteiligung unseres Amtes ab, obwohl in den Vorschriftenrichtlinien der Landesregierung klipp und klar steht, daß es uns frühzeitig Gelegenheit geben muß, zu Entwürfen, die Auswirkungen auf die Verarbeitung personenbezogener Daten durch Behörden oder sonstige öffentliche Stellen haben, Stellung zu nehmen. Dies ist um so bedauerlicher, als in der Verwaltungsvorschrift eine Regelung fehlt, wem bei der Polizei die Feststellung obliegt, bei welchen konkreten Straßen es sich um eine andere Straße von erheblicher Bedeutung im Sinne der neuen Regelung handelt. Weil dies nicht Sache des einzelnen Polizeibeamten sein kann, schrieben wir Ende September 1996 dem Herrn Innenminister, daß diese Entscheidung den Leitern der Polizeidienststellen überantwortet und jeweils von vornherein befristet werden sollte. Vor kurzem bekamen wir Antwort: In der Frage, was eine andere Straße von erheblicher Bedeutung im Sinne der neuen Regelung sei, gehe man mit uns d'accord; ergänzen wolle man allerdings die Verwaltungsvorschrift nicht. Zum Entwurf seiner Verwaltungsvorschrift habe uns das Innenministerium nicht zu hören brauchen, weil diese neben der Änderung des Polizeigesetzes keine eigenständigen Auswirkungen auf die Verarbeitung personenbezogener Daten habe. Dem können wir schon deshalb nicht zustimmen, weil wir meinen, daß das Innenministerium es uns hätte überlassen sollen, sich wegen dieser Frage den Kopf zu zerbrechen.

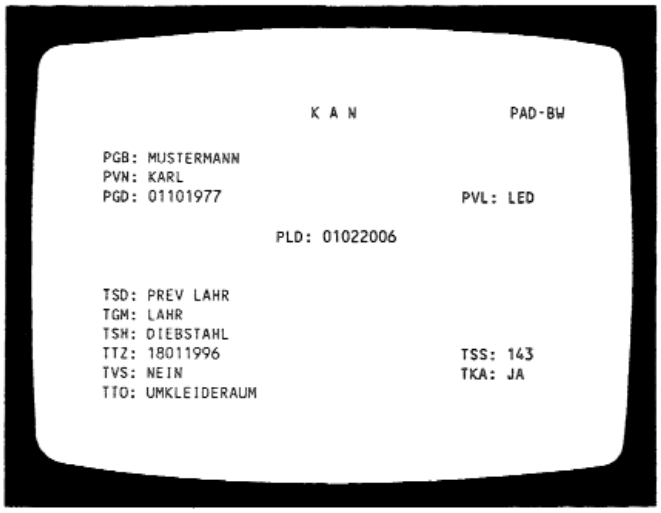
2. Probleme mit der PAD

1973 nahm die Polizei des Landes ihre automatisiert geführte Personenauskunftsdatei (PAD) in Betrieb. Sie läuft auf dem Rechner des Landeskriminalamts, das sie in eigener Regie entwickelt hat. In der PAD speichert die Polizei alle zur Straftatenbekämpfung wichtigen Daten über

mutmaßliche und tatsächliche Straftäter; sie gibt auch Auskunft über Vermißtenfälle und dient der Erstellung der polizeilichen Kriminalstatistik. Jeder Polizeibeamte kann über die breit gefächerten dezentralen Zugriffsmöglichkeiten die PAD rund um die Uhr abfragen. Beinahe regelmäßig tauchte die PAD aus unterschiedlichen Gründen in unseren Tätigkeitsberichten auf: Mal ging es darum, wie die Polizei sie im Alltag handhabt, mal ging es um Fehler im System, was ihr Änderungen und Umprogrammierungen eintrug. 1990 war z.B. die unverhältnismäßige PAD-Fristenspirale eines der Themen (vgl. 11. Tätigkeitsbericht, LT-Drs. 10/4540, S. 40 f.). Um ihre Spitze zu kappen, berichtete die Landesregierung im Januar 1992 dem Landtag, die Regelspeicherfrist in der PAD werde bei tatverdächtigen Erwachsenen von 10 auf 5 Jahre abgesenkt und nur bei schweren Straftaten verbleibe es bei der 10jährigen Maximalfrist. Davon, wie die Polizei mit der PAD-Maximalfrist in der Praxis verfährt, und von anderen PAD-Problemen ist heuer zu berichten:

2.1 Die Speicherung von KAN-Merkern in der PAD – Kleiner Handgriff mit großen Folgen

Ein Ladendiebstahl ist kein Fall eines besonders schweren Diebstahls und ein solcher Diebstahl ist kein Bankraub. Zudem ist nicht jedes in Baden-Württemberg geführte Ermittlungsverfahren für die Polizei in Hamburg, Berlin oder sonstwo in der Bundesrepublik von Bedeutung. Dies muß die Polizei bedenken, wenn sie festlegt, ob sie einen mutmaßlichen oder tatsächlichen Straftäter in der Personenauskunftsdatei (PAD) mit der 10jährigen Maximalfrist speichert und ihn zugleich auch in den auf dem Computer des Bundeskriminalamts geführten Kriminalaktennachweis (KAN) der Polizeien des Bundes und der Länder, den bundesweit alle Polizeibeamten rund um die Uhr in Sekundenschnelle abfragen können, einstellt. Um beides möglichst rationell erledigen zu können, ist die PAD so programmiert, daß sie bei bestimmten Tatvorwürfen automatisch einen sog. KAN-Merker setzt, und bei anderen Tatvorwürfen den Polizeibeamten Raum läßt, im Einzelfall einen KAN-Merker zu vergeben. Das sieht am PAD-Terminal z.B. so aus:



Zeichenerklärung:

PGB: Geburtsname	TSD: sachbearbeitende Polizeidienststelle	TTO: Tatörtlichkeit
PVN: Vorname		TSS: Sachschaden
PGD: Geburtsdatum	TGM: Tatortgemeinde	TVS: Verwendung von Schußwaffen
PVL: Familienstand	TSH: Straftat	
PLD: Löschungstermin	TTZ: Tatzeit	TKA: KAN-Delikt

Die KAN-Merker bewirken zum einen, daß Erwachsene anstatt mit der 5jährigen PAD-Regelspeicherfrist mit der 10jährigen Maximalfrist, im Beispielsfall also bis 1. Febr. 2006, in der PAD erfaßt werden und zum anderen, daß jede so in der PAD gekennzeichnete Person in den bundesweiten KAN eingestellt wird.

Weil dies ein ganz gravierender Eingriff ist, sahen wir uns die Vergabe von KAN-Merkern bei den Polizeidirektionen Balingen und Offenburg näher an. Zuvor hatten wir anhand einer systematischen Auswertung der PAD vom April 1996 festgestellt, daß bei ca. 102 000 Personen ein KAN-Merker eingespeichert war. Bei ca. 58 000 Personen hatte der PAD-Computer den KAN-Merker automatisch gesetzt, weil sie wegen des Tatvorwurfs eines Verbrechens oder eines in § 100 a StPO genannten Vergehens erfaßt sind. Bei den übrigen ca. 44 000 Personen, die wegen eines sonstigen Delikts, sei es z.B. Betrug, Diebstahl, Vorenthalten und Veruntreuen von Arbeitsentgelt, Körperverletzung, Sachbeschädigung, Nötigung oder Verstoß gegen das Betäubungsmittelgesetz, gespeichert waren, hatte die Polizei den KAN-Merker im Einzelfall vergeben. Aus der PAD-Auswertung ergab sich ferner, daß die Polizeidirektion Balingen bei 1 792 von insgesamt 2 722 Personen, was einer Quote von 66 % entspricht, und die Polizeidirektion Offenburg bei 3 310 von insgesamt 5 654 Personen, was einer Quote von 59 % entspricht, wegen sonstiger Delikte per Einzelfallentscheidung einen KAN-Merker vergeben hatten. Damit lagen die beiden Polizeidirektionen weit über dem Landesdurchschnitt von 43 %. Den Ursachen gingen wir dann vor Ort anhand einer Stichprobe von jeweils mehr als 100 Fällen nach.

Um das Ergebnis vorwegzunehmen: Obwohl die Polizeidirektion Balingen bei gut einem Drittel der Stichproben die KAN-Merker noch vor dem Kontrollbesuch gelöscht hatte, zeigte sich dennoch, daß bei ihr und auch in Offenburg manches nicht in Ordnung war.

2.1.1 Mit KAN-Merkern zu schnell bei der Hand

Seit langem ist klar: Bagatelldelikte, wie Hausfriedensbruch, Beleidigung, einfache Körperverletzung und Nötigung oder Diebstahl, Unterschlagung und Betrug bis zu einer Schadenshöhe von 500 DM, darf die Polizei allenfalls für 3 Jahre, sonstige Delikte für 5 Jahre in der PAD registrieren. Abweichend davon darf sie außer bei Verbrechen und den in § 100 a StPO aufgezählten Vergehen, wo dies der PAD-Computer automatisch tut, die 10jährige PAD-Maximalfrist nur im Einzelfall bei anderen überregional bedeutsamen Straftaten vergeben, insbesondere bei Fällen gewohnheits-, gewerbs- oder bandenmäßiger Begehung, bei Triebtäterschaft, internationaler Betätigung und Tatbegehung zur Verwirklichung extremistischer Ziele. Weil eine KAN-Speicherung einen besonders einschneidenden Eingriff in die Rechte der Betroffenen darstellt, verlangt schon der Grundsatz der Verhältnismäßigkeit, daß an die Speicherung besonders strenge Anforderungen zu stellen sind, zumal es 13 Jahre nach dem Volkszählungsurteil des Bundesverfassungsgerichts noch immer keine gesetzliche Grundlage für den KAN gibt. Die Polizeidirektionen Offenburg und Balingen hätten deshalb – wie es auch die KAN-Richtlinien verlangen – nur solche Beschuldigte und Tatverdächtige im KAN erfassen dürfen, die eine schwere oder eine andere, überregional bedeutsame Straftat mutmaßlich oder tatsächlich begangen haben. Damit nahmen es die beiden Polizeidirektionen nicht allzu genau, wie schon folgende Beispiele zeigen:

– Zwei Ster Kirschbaumholz

Die Polizeidirektion Offenburg erfaßte einen 30jährigen Holzschnitzer für 10 Jahre bis 1. Nov. 2005 wegen des Tatvorwurfs einer Hehlerei in der PAD und im bundesweiten KAN, weil ein Mann, den er mit seinem Lieferwagen losgeschickt hatte, um zwei Ster Kirschbaumholz im

Wert von 100 DM abzuholen, das Holz einfach aufgeladen und nach Hause gebracht hatte. Ein solcher Tatvorwurf rechtfertigt eine so lange PAD-Speicherung und Aufnahme in den bundesweiten KAN selbst dann nicht, wenn, was nicht zu klären war, auch die kurz zuvor in der Gegend entwendeten zwei Ster Erle-/Eichebrennholz im Wert von 140 DM auf das Konto des Holzschnitzers gegangen wären. Denn bei der angeblichen Hehlerei handelte es sich nun wirklich nicht um eine allzu schwere Straftat, sondern um ein Delikt, das allenfalls drei Jahre in der PAD registriert werden darf und im bundesweiten KAN nichts zu suchen hat.

– Die Tierschützer
Die Polizeidirektion Offenburg erfaßte vier erwachsene Männer und Frauen für 10 Jahre bis 1. Jan. 2006 und zwei Jugendliche für 5 Jahre bis 1. Jan. 2001 mit dem Tatvorwurf einer Nötigung in der PAD und im bundesweiten KAN, weil sie zusammen mit anderen Tierschützern mit Transparenten und Trillerpfeifen gegen eine Treibjagd auf Niederwild protestiert und dabei die Jagd so gestört hatten, daß die 20 Jäger unverrichteter Dinge wieder nach Hause gehen mußten. Solche Nötigungen sind aber, so steht es in der Durchführungsverordnung zum Polizeigesetz, Fälle von geringer Bedeutung, die die Polizei allenfalls drei Jahre in der PAD und schon gar nicht im bundesweiten KAN erfassen darf. Daran ändert auch der Umstand nichts, daß die Tierschützer gemeinsam mit anderen Gleichgesinnten gegen die Treibjagd protestierten, denn das gemeinsame Vorgehen macht ihren Protest noch lange nicht zu einer schweren oder überregional bedeutsamen Straftat.

– Der Autofahrer
Die Polizeidirektion Offenburg erfaßte einen 62jährigen Autofahrer wegen Nötigung für 8 Jahre bis 1. März 2003 in der PAD und im bundesweiten KAN, weil ein anderer Autofahrer den 62jährigen Mann in seiner Gegenanzeige beschuldigt hatte, er habe ihn im Oktober 1995 beim Überholen auf der Autobahn behindert. Ein solcher Tatvorwurf ist, was schon die Einstellung des Verfahrens durch die Staatsanwaltschaft mangels hinreichendem Tatverdacht zeigt, nicht von so gravierender Bedeutung, daß er eine so lange Speicherung in der PAD und eine Registrierung im bundesweiten KAN rechtfertigen könnte.

– Das Tankkonto
Die Polizeidirektion Balingen erfaßte einen Mann, der einen Kurierdienst betreibt und für sein Kurierfahrzeug seit Jahren ein Tankkonto bei einer Tankstelle eingerichtet hatte, mit dem Tatvorwurf eines Betrugs für 10 Jahre bis 1. Jan. 2005 in der PAD und im bundesweiten KAN, weil er im August 1993 insgesamt 11mal getankt hatte und hinterher die Monatsabrechnung in Höhe von 590 DM nicht zahlen konnte. Hier muß die Polizeidirektion Balingen die Speicherfrist erheblich reduzieren und die KAN-Aufnahme revidieren, weil es sich nun wirklich um keine schwere Straftat handelt und der angerichtete Schaden nur knapp über der Bagatelldeliktsgrenze liegt. Zudem hatte der Kurierfahrer bis dahin jahrelang korrekt sein Tankkonto beglichen und war auch danach polizeilich nicht mehr in Erscheinung getreten, so daß er wegen der 11 Tankfüllungen auch nicht zum Serientäter gestempelt werden kann oder ihm gar kriminelle Neigungen attestiert werden können.

– Der gebremste Bauherr
Die Polizeidirektion Balingen erfaßte einen Bauherrn, der offensichtlich eine Privatfehde mit dem örtlichen Bürger-

meister führte, mit dem Tatvorwurf eines Widerstands gegen Vollstreckungsbeamte für 10 Jahre bis 1. Jan. 2004 in der PAD und im bundesweiten KAN, weil er den beiden Polizeibeamten, die ihm im Auftrag des Bürgermeisters die weitere Ausführung der Bauarbeiten untersagten, gedroht haben soll, alle umzufahren, die sich ihm in den Weg stellen. Bei allem gebotenen Respekt vor den Gefahren, die der Polizeiberuf mit sich bringt: Hier schoß die Polizeidirektion Balingen übers Ziel hinaus, zumal fraglich ist, ob der Bauherr seine „Drohung" überhaupt jemals ernst gemeint hatte.

2.1.2 Aus „nein" einfach „ja" gemacht

Seit jeher ist klar: Die Entscheidung, ob ein Fall einen KAN-Merker bekommen soll oder nicht, ist Sache des sachbearbeitenden Polizeibeamten. So bestimmen es die KAN-Richtlinien ausdrücklich. Das ist auch gut so, denn der Sachbearbeiter kennt den Fall aus dem Effeff. Je nachdem, wie er sich entscheidet, muß er in dem auf dem PAD-Formularsatz vorgedruckten KAN-Delikt-Feld „ja" oder „nein" ankreuzen. Einen Durchschlag davon leitet er nach Abschluß der Ermittlungen der Datenstation seiner Polizeidirektion zur PAD-Erfassung des Falles zu. So läuft es seit langem bei der Polizeidirektion Offenburg und seit etwa einem Jahr bei der Polizeidirektion Balingen, für die vorher die Datenstation der Polizeidirektion Tübingen die PAD-Erfassungen erledigte. Weil jemand – die beiden Polizeidirektionen tippten bei den Kontrollbesuchen auf den sog. Prüfdienst der Datenstationen – meinte, es besser zu wissen, kam es in einer ganzen Reihe von Fällen in Offenburg und Balingen zu einer Änderung der vom Sachbearbeiter getroffenen Entscheidung „KAN-Delikt, nein" in „KAN-Delikt, ja" – und dies, ohne nur mit einem Wort zu begründen, warum. Dagegen wäre nichts einzuwenden, wenn es sich bei der Entscheidung KAN-Delikt „ja" oder „nein" um eine reine Routineentscheidung handeln würde. Dem ist indes nicht so. Vielmehr kommt es auf die Umstände des Einzelfalles an. Denn Tatvorwurf ist – selbst wenn er an ein und derselben Strafvorschrift zu messen ist – nicht Tatvorwurf. Zudem kommt es entscheidend auf die Vorgehensweise des Beschuldigten an. Die Einzelheiten dazu lassen sich aber aus der oft auf wenige Sätze komprimierten Sachverhaltszusammenfassung, wie sie in den der Datenstation zugeleiteten PAD-Erfassungsbelegen steht, in aller Regel nicht ersehen. Wozu es führt, wenn man sich so eigenmächtig und zudem ohne Begründung über die Entscheidung des Sachbearbeiters hinwegsetzt, dafür ein Beispiel:

Ein Mann, der im April 1990 im Verlauf von Mietstreitigkeiten den Kellerraum einer anderen Hausbewohnerin betreten haben soll, ist mit dem Tatvorwurf eines Hausfriedensbruchs für 10 Jahre bis 1. Mai 2000 in der PAD gespeichert und im bundesweiten KAN registriert, weil die Polizeidirektion Balingen sich über die Entscheidung des Sachbearbeiters „KAN-Delikt, nein" hinweggesetzt und wegen dieses Vorfalls einen KAN-Merker vergeben hat. Ein Hausfriedensbruch ist aber, selbst wenn ihn der Mann tatsächlich begangen hätte, ein Fall von geringer Bedeutung, den die Polizei allenfalls drei Jahre in der PAD speichern und nie und nimmer im bundesweiten KAN registrieren darf. Daran ändert nichts, daß über den Mann auch noch vier PAD-Speicherungen wegen Diebstahls, die aus den Jahren 1980 bis 1985 stammen, existieren. Denn die Polizei ging selbst davon aus, daß keiner dieser Tatvorwürfe einen KAN-Merker verdient. Das ist auch nicht überraschend. Denn einem handschriftlichen Vermerk in den Polizeiakten zufolge endete ein angeblicher Diebstahl von 1981 mit Freispruch und einer von 1985 mit

einer Einstellung mangels hinreichendem Tatverdacht; bei den beiden anderen Fällen wußte die Polizeidirektion nicht, wie sie ausgegangen waren; soviel stand aber immerhin fest: beidesmal war nur ein geringer Schaden entstanden. Deshalb wäre die Polizeidirektion Balingen gut beraten gewesen, wenn sie sich auch bei dem angeblichen Hausfriedensbruch an die Entscheidung des Sachbearbeiters „KAN-Delikt, nein“ gehalten hätte.

2.1.3 Wo bleiben die Konsequenzen aus dem Ausgang des Ermittlungsverfahrens?
Die Polizei ist verpflichtet, jeweils nach Abschluß des Ermittlungsverfahrens anhand der Entscheidung der Staatsanwaltschaft oder des Gerichts zu prüfen, ob sie den eingespeicherten Tatvorwurf löschen muß. Weiter speichern darf sie ihn nur, wenn sich aus der staatsanwaltschaftlichen oder gerichtlichen Entscheidung ergibt, daß ein Verdacht übrig bleibt und tatsächliche Anhaltspunkte dafür vorliegen, daß der Betroffene künftig eine Straftat begehen wird. Um der Polizei diese Prüfung zu erleichtern, vereinbarten Innen- und Justizministerium im Jahr 1981 einen Mitteilungsdienst zwischen Staatsanwaltschaft und Polizei. Daß dieser hin und wieder nicht rund läuft, war schon Gegenstand früherer Tätigkeitsberichte. Doch nicht darum geht es hier, sondern darum, daß die Polizeidirektionen Offenburg und Balingen aus den Mitteilungen zu selten die gebotenen Konsequenzen zogen. Wohin dies führt, sei an folgenden Beispielen illustriert:

– Der Fliesenleger-Azubi
Die Polizeidirektion Offenburg erfaßte einen Fliesenleger-Azubi mit dem Tatvorwurf eines besonders schweren Falles eines Diebstahls für 10 Jahre in der PAD bis 1. Jan. 2006 und stellte ihn in den bundesweiten KAN ein, weil er zusammen mit einem Freund in das Wohnhaus eines Bauherrn, für den er „schwarz“ gearbeitet hatte und mit dem er wegen der Bezahlung über Kreuz gekommen war, eingestiegen war und angeliefertes Baumaterial im Gesamtwert von ca. 1 000 DM abgeholt hatte. Dabei beließ es die Polizeidirektion, obwohl die Staatsanwaltschaft Offenburg sie wissen ließ, daß sie das Ermittlungsverfahren mangels hinreichendem Tatverdacht mit folgender Begründung eingestellt hatte:

> „Bei der Abwicklung des Auftrags gab es zwischen dem Bauherrn und (dem Fliesenleger-Azubi) Schwierigkeiten. Beide behaupten, Eigentümer des entwendeten Baumaterials zu sein. Welche Aussage zutrifft, konnte nicht geklärt werden. Es ist dies auch nicht Aufgabe der Staatsanwaltschaft. Da deshalb nicht ausgeschlossen werden kann, daß der (Fliesenleger-Azubi) Eigentümer des mitgenommenen Baumaterials war, kann das Baumaterial auch nicht Gegenstand eines Diebstahls durch (den Fliesenleger-Azubi) gewesen sein.“

Damit war klar, daß sich der Tatverdacht eines Diebstahls gegen den Fliesenleger-Azubi nicht mehr begründen ließ. Hinzu kam, daß er belegen konnte, woher er das abgeholte Baumaterial bezogen hatte und wohin er es gegen Gutschrift wieder zurückgegeben hatte. Deshalb hätte die Polizeidirektion den Fall nach der Einstellung des Ermittlungsverfahrens löschen müssen. Zumindest hätte sie die PAD-Speicherfrist erheblich reduzieren und die KAN-Aufnahme revidieren müssen, denn bei einer so vagen Verdachtslage kann von einer schweren oder überregional bedeutsamen Straftat nicht gesprochen werden.

– Der Schüler
Die Polizeidirektion Offenburg erfaßte einen 15 ½ Jahre alten Schüler mit dem Tatvorwurf des illegalen Handelns mit Cannabis für 5 Jahre bis 1. Jan. 2001 in der PAD und stellte ihn in den bundesweiten KAN ein, weil er zwei Mitschülern, die ihm im Auftrag des Vertrauenslehrers eine Falle stellen und ihn als Haschischhändler entlarven wollten, für 10 DM ein Stückchen Haschisch besorgt hatte. Dabei beließ es die Polizeidirektion, obwohl ihr die Staatsanwaltschaft Offenburg mitgeteilt hatte, daß sie das Ermittlungsverfahren mangels hinreichendem Tatverdacht eingestellt und zur Begründung u.a. ausgeführt hat:

„Daß der Beschuldigte sich mit An- und Verkauf von Betäubungsmitteln befaßt hat, hat er gegenüber seinen Klassenkameraden offenbar eingeräumt. Dies kann aber durchaus Angabe gewesen sein. Weitere Anhaltspunkte hierfür haben sich nicht ergeben. Eine Durchsuchung förderte keinerlei Beweismittel zutage. Auch eine Urinprobe ergab keinerlei Anhaltspunkt auf Betäubungsmittelkonsum. Es ist daher nicht auszuschließen, daß der Beschuldigte durch seine Aufschneiderei dazu provoziert worden ist, das Haschisch-Stück zu besorgen."

Auch diesen Schüler hätte die Polizeidirektion Offenburg wenigstens jetzt in der PAD löschen müssen. Auf jeden Fall hätte sie seine Aufnahme in den bundesweiten KAN revidieren müssen, weil bei dem ihm zur Last gelegten Delikt nun wirklich nicht von einer schweren oder überregional bedeutsamen Straftat gesprochen werden kann.

– Nicht strafbar
Die Polizeidirektion Balingen erfaßte eine Frau mit dem Tatvorwurf eines Verstoßes gegen das Betäubungsmittelgesetz mit Cannabis für 10 Jahre bis 1. Mai 2002 in der PAD und stellte sie in den bundesweiten KAN ein, weil sie im November 1991 einmal Haschisch erworben und konsumiert haben soll. Dabei beließ es die Polizeidirektion, obwohl die Staatsanwaltschaft Hechingen das Ermittlungsverfahren mangels hinreichendem Tatverdacht eingestellt und in der Begründung ausgeführt hatte:

„Der Beschuldigten kann man allenfalls den Gebrauch einer illegalen Droge nachweisen. Der Verbrauch selbst ist jedoch nicht strafbar."

Diese PAD-Speicherfrist hätte die Polizeidirektion Balingen zumindest erheblich reduzieren und die Einstellung der Frau in den bundesweiten KAN löschen müssen. Denn nach den Feststellungen der Staatsanwaltschaft stand allenfalls noch zur Debatte, daß die Frau einmal Haschisch geraucht hatte, was jedoch nicht strafbar ist. Weil zudem die Durchsuchung ihrer Wohnung negativ verlaufen war und die Urinprobe belegte, daß sie keine Haschischkonsumentin war, hätte die Polizeidirektion die Frau keinesfalls für 10 Jahre in der PAD und auch nicht im bundesweiten KAN registrieren dürfen.

2.1.4 Nach Ablauf der Speicherfrist noch immer nicht genug
PAD-Speicherungen muß die Polizei nach Ablauf der Speicherfrist im Regelfall löschen. Nur ausnahmsweise darf sie die Speicherung verlängern – und dies nur um drei Jahre. Tut sie dies, muß sie dies schriftlich begründen. So steht es in § 38 Abs. 3 des Polizeigesetzes. Diese Regelung umging die Polizeidirektion Balingen in mehreren Fällen so: Anstatt auf die Mitteilung des Landeskriminalamts, daß die PAD-Speicherfrist abgelaufen ist, die PAD-Datensätze zu löschen, speicherte die Polizeidirektion Balingen KAN-Merker ein

und verlängerte dadurch die PAD-Speicherfrist nicht nur um 3, sondern gleich um 5 Jahre und nahm die Fälle in den bundesweiten KAN auf, obwohl der sachbearbeitende Polizeibeamte einst in die Akte „KAN-Delikt, nein“ geschrieben hatte. Wozu das führt, zeigt der Fall eines Mannes exemplarisch, der insgesamt 20 Jahre in der PAD bleiben soll:

Die Polizeidirektion Balingen hatte ihn 1981 wegen des Tatvorwurfs einer Beleidigung erstmals in der PAD erfaßt, weil er einen anderen Autofahrer, mit dem er sich an einer Tankstelle nicht einigen konnte, wer zuerst tanken darf, beleidigt haben soll. 1987 kam eine Körperverletzung hinzu, weil er vor der Scheidung seine Frau mehrmals körperlich mißhandelt hatte und deshalb zu einer Geldstrafe von 25 Tagessätzen verurteilt worden war. 1991 speicherte die Polizeidirektion mit einer 5jährigen Speicherfrist einen Betrug zu, weil der Mann 1 972,20 DM Arbeitslosengeld zu Unrecht bezogen hatte und deshalb zu einer Geldstrafe von 30 Tagessätzen verurteilt worden war; Löschtermin für den PAD-Datensatz des Mannes war demzufolge der 1. April 1996. Statt auf die Löschwarnung des Landeskriminalamts den PAD-Datensatz des Mannes zu löschen, setzte die Polizeidirektion Balingen einen KAN-Merker und verlängerte dadurch die Speicherfrist um 5 Jahre bis 1. April 2001 und erfaßte den Mann auch noch im bundesweiten KAN und vermerkte in ihrer Akte zur Begründung: „KAN-relevant, da Mehrfachtäter“. In Wirklichkeit ist dieser KAN-Merker nicht gerechtfertigt. Denn sowohl die mittlerweile mehr als 9 Jahre zurückliegende Körperverletzung als auch der schon mehr als 5 Jahre zurückliegende unrechtmäßige Bezug von Arbeitslosenentgelt sind weder für sich betrachtet noch zusammengenommen schwere oder überregional bedeutsame Straftaten, wie schon die am untersten Rand des Strafrahmens liegenden Verurteilungen zeigen. Sie waren auch nicht durch einen besonderen modus operandi geprägt, insbesondere gibt es keine Anhaltspunkte für eine gewohnheitsmäßige Begehung. Deshalb hätte die Polizeidirektion Balingen der Entscheidung des damaligen Sachbearbeiters „KAN-Merker, nein“ folgen sollen und den PAD-Datensatz des Mannes nach Ablauf der Speicherfrist (1. April 1996) löschen müssen.

2.1.5 Konsequenzen

Diese Beispiele sind keineswegs nur einzelne Ausreißer, sondern das Ergebnis fehlerhafter Vorgehensweisen, die wir vor kurzem gegenüber dem Innenministerium beanstandet haben. Deshalb ist es nicht damit getan, daß die beiden Polizeidirektionen die Speicherungen entsprechend unseren Hinweisen ändern. Notwendig ist vor allem für die Zukunft sicherzustellen, daß die Polizei bei anderen Straftaten als Verbrechen und den in § 100 a StPO genannten Vergehen eine 10jährige PAD-Speicherfrist nur dann vergibt und deren Aufnahme in den bundesweiten KAN wirklich nur dann bewirkt, wenn die Tatvorwürfe einem Verbrechen oder einem der in § 100 a StPO genannten Vergehen vergleichbar sind und eine der genannten Vorgehensweisen vorliegt.

2.2 Aus dem PAD-Alltag

Wie in den vorangegangenen Jahren wandten sich auch heuer viele Bürger wegen Datenspeicherungen im PAD-Computer rat- und hilfesuchend an unser Amt. Manchen konnten wir helfen. Hin und wieder löschte die Polizei von sich aus sofort, manchmal bedurfte es einiger Überzeugungsarbeit, bisweilen half aber auch das nichts.

– Eine Waffenbehörde hatte einem Geschäftsmann die Erteilung eines Waffenscheines verweigert. Weil sie ihm dabei auch geschrieben hatte, die örtliche Polizeidirektion habe auf Anfrage Besorgnis an seiner Zuverlässigkeit geäußert und der Geschäftsmann sich keiner Schuld bewußt war, wollte er wissen, was da-

hinter steckt. Dies ließ sich nicht mehr klären, weil die örtliche Polizeidirektion die Akten, die darüber hätten Aufschluß geben können, bereits vernichtet hatte. Von einer bei unserer Recherche festgestellten PAD-Speicherung wegen Urkundenfälschung konnten die Zuverlässigkeitsbedenken nicht herrühren, weil dieser Tatvorwurf erst nach der Anfrage der Waffenbehörde und zudem von einer ganz anderen Polizeidirektion in die PAD eingespeichert worden war. Im Zuge unserer Ermittlungen löschte diese Polizeidirektion ihre Einspeicherung, so daß der Geschäftsmann zwar nach wie vor keinen Waffenschein besitzt, jedoch jetzt wenigstens PAD-negativ ist.

– Eine Frau wollte ihre erkennungsdienstlichen Unterlagen, von deren Existenz sie wußte, vernichtet wissen und bat uns ein Auge darauf zu werfen, daß dies geschieht. Was sie nicht wußte, war, daß es über sie auch PAD-Speicherungen wegen einer weiteren erkennungsdienstlichen Behandlung und wegen der Tatvorwürfe der Förderung der Prostitution, eines Betrugs sowie eines Diebstahls gab. Auf unsere Anfrage löschte die Polizei auch diese PAD-Speicherungen und sonderte die erkennungsdienstlichen Unterlagen aus.
– Ein eingefleischter Fußballfan schrieb uns, er habe in den 80er Jahren ab und an mit der Polizei zu tun gehabt und befürchte, er sei deswegen noch immer in der PAD. Damit lag er richtig. Denn er war dort mit insgesamt sieben Tatvorwürfen registriert. Dabei wollte es die speichernde Landespolizeidirektion belassen. Bei fünf der sieben Tatvorwürfe war auch nichts dagegen einzuwenden, hatte der Fußballfan doch immerhin für seine Taten Strafbefehle erhalten oder Geldbeträge an gemeinnützige Einrichtungen zahlen müssen. In den beiden übrigen Fällen hatte die Staatsanwaltschaft das Ermittlungsverfahren einst mangels hinreichenden Tatverdachts eingestellt. Deshalb sahen wir uns diese beiden polizeilichen Akten näher an. Weil in der einen nicht mehr stand, als daß der Fußballfan am 8. Dez. 1984 im Stuttgarter Neckarstadion einem Fan des Karlsruher Sportclubs einen Fußtritt verpaßt haben soll, aber gar nicht ersichtlich war, worauf sich dieser Vorwurf stützte, und sich in der anderen Akte kein Beleg dafür fand, daß der Fußballfan bei einem Vorfall, der sich am selben Tag in Karlsruhe abgespielt hatte, einen Fan des Karlsruher Sportclubs geschlagen hat, baten wir die Landespolizeidirektion, die Tatvorwürfe einer Körperverletzung und einer gefährlichen Körperverletzung vom 8. Dez. 1984 in der PAD zu löschen. Diese revidierte ihre ursprüngliche Absicht, auch diese beiden Tatvorwürfe in der PAD zu belassen, und folgte unserer Empfehlung.
– Im Juni 1996 beantragte eine Frau bei der Polizei die Löschung ihrer PAD-Speicherungen und schickte uns eine Mehrfertigung ihres Löschungsantrags. Auf unsere Anfrage, ob die Polizei dem Antrag stattgibt, schrieb uns das Landeskriminalamt, die Antwort könnten wir der seinem Brief beiliegenden Mehrfertigung seines Bescheids entnehmen. Darin stand, daß es bis 1. Jan. 1998 bei den beiden PAD-Speicherungen wegen eines Vergehens der Ausübung der verbotenen Prostitution und eines Vergehens eines Diebstahls bleibe. Ein Widerspruch sei zwecklos, deshalb könne die Frau, wenn sie wolle, gleich beim Verwaltungsgericht Stuttgart klagen, hieß es am Ende des Bescheids.
  Die weitere PAD-Speicherung erschien uns nicht gerechtfertigt, weil schon die Ausführungen des Landeskriminalamts in seinem Bescheid nicht schlüssig waren. Denn ein Vergehen der Ausübung der verbotenen Prostitution setzt voraus, daß jemand einem durch Rechtsverordnung erlassenen Verbot, der Prostitution an bestimmten Orten überhaupt oder zu bestimmten Tageszeiten nachzugehen, aus Mißachtung oder Gleichgültigkeit immer wieder zuwider handelt oder bereit ist, dies zu tun. Anhaltspunkte dafür, daß es bei der Frau so gewesen sein könnte, ergaben sich aus dem Bescheid des Landeskriminalamts nicht; im Gegenteil: Der im Bescheid zitierte Zeuge hatte nicht einmal

sagen können, ob die Frau tatsächlich der Prostitution nachgegangen war. Deshalb hatte die Staatsanwaltschaft das Ermittlungsverfahren umgehend mangels hinreichenden Tatverdachts eingestellt. Weil das Landeskriminalamt in seinem Bescheid auch nichts dazu sagte, weshalb sein pauschaler Hinweis, im Bereich der Eigentumskriminalität bestünde Wiederholungsgefahr, gerade auf die Frau paßte, baten wir es, seinen Bescheid noch einmal zu überdenken und den PAD-Datensatz der Frau zu löschen. Das tat es dann auch.

– Diese Reaktionen hätten sich speichernde Polizeidirektion, Landeskriminalamt und Innenministerium in einem anderen PAD-Fall zum Vorbild nehmen und die von uns beanstandete Speicherung der Tatvorwürfe einer Bedrohung, eines Mißbrauchs von Notrufen und des Vortäuschens einer Straftat im PAD-Datensatz eines Mannes aus folgenden Gründen löschen sollen:
  Der Mann lebte mit seiner Frau in Scheidung. Sie war zu ihren Eltern gezogen. Um festzustellen, ob ihr Mann zuhause ist, habe sie – so die Version der Frau – abends dort einmal angerufen. Ihr Ehemann habe abgenommen. Sie habe nichts gesagt. Obwohl ihr Mann demzufolge gar nicht gewußt haben konnte, wer am Telefon ist, habe er sie bedroht. Mehr als einen Satz habe er zu ihr nicht gesagt. Ein paar Worte davon will der Vater der Frau, der den Ablauf der Dinge bei seiner Zeugenvernehmung freilich etwas anders als seine Tochter geschildert hatte, mitbekommen haben. Der Ehemann bestritt energisch, seine Frau bedroht zu haben. Er vermutete, daß die angebliche Bedrohung Teil einer gegen ihn gerichteten Kampagne sei, die zum Ziel habe, die Schenkung der Hälfte des ehelichen Hauses an ihn wegen groben Undanks rückgängig machen zu können. Weil es keine objektiven Zeugen gab und somit letztendlich Aussage gegen Aussage stand, ohne daß der einen oder anderen Seite der Vorzug der Wahrheit gegeben werden konnte, stellte die Staatsanwaltschaft das Ermittlungsverfahren umgehend ein und ließ dies die Polizeidirektion wissen. Diese hätte zur Löschung schreiten sollen, weil eine so unklare Situation sich nicht zu Lasten des Mannes in der PAD niederschlagen darf.
  Etwa ein Jahr nach der angeblichen Bedrohung ging bei der Feuerwehr ein anonymer Anruf ein, im Haus der Schwiegereltern des Mannes werde eine Frau erstochen. Die Feuerwehr alarmierte die Polizei. Diese rückte aus und stellte fest, daß es ein Fehlalarm war. Der Schwiegervater tippte sofort auf seinen Schwiegersohn. Das Amtsgericht hörte sich das Tonband an, auf dem der anonyme Anruf aufgezeichnet worden war, und sprach danach den Ehemann auf Antrag der Staatsanwaltschaft vom Vorwurf eines Mißbrauchs von Notrufen und des Vortäuschens einer Straftat frei. Trotzdem wollen speichernde Polizeidirektion, Landeskriminalamt und Innenministerium die beiden Tatvorwürfe in der PAD belassen. Weil es hier und bei dem Tatvorwurf einer Bedrohung nicht dabei bleiben kann, haben wir vor kurzem das Innenministerium gebeten, seine Haltung nochmals zu überdenken.

2.3 Aus Datenmißbrauch nichts gelernt?
Mehr Publicity als ihm lieb war hatte das Polizeipräsidium Mannheim. Einer seiner Polizeibeamten hatte bei der Datenstation, die rund um die Uhr die Personenauskunftsdatei (PAD), das auf dem Rechner des Bundeskriminalamts betriebene Informationssystem der Polizeien des Bundes und der Länder (INPOL) und über ihren Anschluß an das Zentrale Verkehrsinformationssystem (ZEVIS) das Zentrale Fahrzeugregister des Kraftfahrt-Bundesamts in Flensburg abfragen kann, angerufen und unter Vorspiegelung dienstlicher Belange mindestens sieben Personen abchecken lassen, die Mitglied in seiner Partei waren oder werden wollten. Nachdem dies bekannt geworden war, verurteilte ihn das Amtsgericht Mannheim in erster Instanz zu einer Geldbuße, weil der Polizeicomputer nicht dafür da ist, zu überprüfen, ob Parteimitglieder oder Personen, die es werden

wollen, eine weiße Weste haben. Da in dem Urteil auch stand, daß sich die Datenstation des Polizeipräsidiums nicht einmal das Codewort nennen ließ und sich nicht mit letzter Sicherheit über die Berechtigung des Anrufers vergewissert hatte, stellte sich die Frage: Was tut eigentlich das Polizeipräsidium, um solche unberechtigten Computerabfragen zu verhindern? Dazu muß man folgendes wissen:

Über die Datenstationen der Polizeipräsidien und der Polizeidirektionen laufen Tag für Tag mehrere tausend PAD-, INPOL- und ZEVIS-Abfragen, sei es, daß die Polizeibeamten dort direkt vorsprechen oder sich schriftlich, telefonisch oder per Funk – wie dies insbesondere bei Personenüberprüfungen vor Ort geschieht – an die Datenstationen wenden. Dabei fragen die Polizeibeamten beispielsweise mit Familiennamen und Geburtsdatum der zu überprüfenden Personen oder mit deren Autokennzeichen an, ob die Person von wem zu welchem Zweck gesucht wird, wegen welcher Tatvorwürfe sie in der PAD oder in INPOL erfaßt ist, ob ein personenbezogener Hinweis über sie vorhanden ist, ob sie Halter des Autos ist, mit dem sie unterwegs ist, oder ob ihr die Fahrerlaubnis entzogen worden ist. Die Datenstationen teilen den Polizeibeamten dann das Ergebnis ihrer Computerabfragen mit. Dabei erfahren die Beamten äußerst sensible Informationen, beispielsweise, daß und ggf. in welchen polizeilichen Informationssystemen die überprüfte Person wegen welcher mutmaßlich oder tatsächlich begangenen Straftaten erfaßt ist oder daß über sie ein personengebundener Hinweis, z.B. „geisteskrank", vorhanden ist. Daß Polizeibeamte sich solche Informationen nur zu dienstlichen Zwecken beschaffen und daß sie nicht in fremde Hände gelangen dürfen, ist jedem klar. Nur, wie läßt sich das sicherstellen? Keine Frage: Davor, daß ein Polizeibeamter in ordnungswidriger oder gar strafbarer Weise seine dienstliche Berechtigung zu Computerabfragen für seine privaten Belange mißbraucht, ist letztendlich niemand gefeit. Das kann aber nicht bedeuten, daß die Polizei die Hände in den Schoß legen darf. Sie muß vielmehr alles dafür tun, daß Polizeibeamte Computerabfragen nur für dienstliche Zwecke starten und nur sie und nicht auch andere Personen auf Anruf von den Datenstationen Auskünfte aus dem Polizeicomputer und ZEVIS erhalten. Dazu gibt es verschiedene Möglichkeiten: Mündliche Hinweise – wie sie das Polizeipräsidium Mannheim bei Dienstversammlungen vornimmt – sind zwar wichtig und richtig; sie haben jedoch nur Appellcharakter. Um Auskünfte an nicht abfrageberechtigte Personen zu verhindern, bestimmt deshalb die einschlägige Dienstanweisung des Landeskriminalamts, daß die Datenstationen bei telefonischen Auskunftsersuchen nach dem extra dafür ausgegebenen Codewort fragen oder durch Rückruf sicherstellen müssen, daß die Computerauskunft auch wirklich nur an Abfrageberechtigte gelangt. Zudem wird jede ZEVIS-Abfrage automatisch im Computer des Kraftfahrt-Bundesamts in Flensburg registriert, jede 50. PAD-Abfrage vom Computer des Landeskriminalamts. Schließlich müssen die Datenstationen telefonisch oder per Funk an sie herangetragene Bitten um Computerabfragen in Listen eintragen. Diese Aufzeichnungen sind durchaus geeignet, unberechtigten Abfragen entgegenzuwirken. Denn immerhin muß jeder, der eine solche über eine Datenstation veranlaßt, gewärtigen, daß er in der einen oder anderen Weise notiert wird. Der damit einhergehende Abschreckungseffekt würde aber verpuffen, wenn sich die Abfrageprotokolle nur in den Schränken stapeln und dort verstauben. Deshalb muß die Polizei anhand der Aufzeichnungen hin und wieder stichprobenartig überprüfen, ob bei solchen Computerabfragen wirklich alles so läuft, wie es sein muß. Denn nur dann kann davon gesprochen werden, daß der, der den Polizeicomputer oder ZEVIS unberechtigt oder gar für seine privaten Zwecke abfrägt, einem nennenswerten Entdeckungsrisiko ausgesetzt ist. Das wollte das Polizeipräsidium nicht so recht einsehen. Bei ihm gäbe es – außer derjenigen des verurteilten Polizeibeamten – keine unberechtigten Computerabfragen. Schon recht so, bloß wie will es das wissen, wo es doch bisher keinerlei Proben aufs Exempel anhand der Protokolle gemacht hat. Das

muß sich ändern. Dabei sollte das Polizeipräsidium auch bedenken, daß dies – wie die öffentlichen Diskussionen und Berichte um den Fall des Polizeibeamten deutlich gezeigt haben – auch in seinem eigenen Interesse liegt.

3. So nicht

3.1 Ein Strafbefehl als Anschauungsmaterial
Weil manche Zeitgenossen sich gerade bei Verstößen im Straßenverkehr ziemlich uneinsichtig zeigen, kann es ganz lehrreich sein, wenn man ihnen die Unrechtmäßigkeit ihres Verhaltens an Ort und Stelle sofort vor Augen führen kann. So mag ein Polizeibeamter des Verkehrsdienstes der Polizeidirektion Ravensburg gedacht haben, als er im Sommer 1996 bei einer Verkehrskontrolle zur Tat schritt. Daß er dabei gegen den Datenschutz verstieß, merkte er nicht. Das kam so:

Im Zuge einer allgemeinen Verkehrskontrolle fiel dem Verkehrsdienst der Polizeidirektion Ravensburg ein Motorrad aus dem Allgäu auf, dessen Kennzeichen so schräg nach oben gestellt war, daß es nicht mehr abgelesen werden konnte. Die Polizei hielt den Motorradfahrer deswegen an. Um ihn zu überzeugen, daß er damit gegen das Straßenverkehrsgesetz verstieß, händigte ein Polizeibeamter dem kontrollierten Motorradfahrer die Ausfertigung eines Strafbefehls aus, den das Amtsgericht Schwäbisch Gmünd gegen einen Motorradfahrer aus dem Ostalbkreis in einer solchen Sache erlassen hatte. Darin konnte er den Vor- und Familiennamen des Motorradfahrers, dessen Adresse und nähere Einzelheiten darüber nachlesen, daß diesen das Amtsgericht Schwäbisch Gmünd mit einer Geldstrafe in Höhe von 750 DM wegen eines Vergehens des Kennzeichenmißbrauchs belegt hatte, weil er das hintere Kennzeichen seines Motorrads so hochgebogen hatte, daß es nicht mehr voll ablesbar war. Den Strafbefehl hatte der Polizeibeamte, der einst auch schon gegen den Motorradfahrer aus dem Ostalbkreis ermittelt hatte, auf seine Bitte von der Staatsanwaltschaft Ellwangen erhalten.

Keine Frage: Strafbefehle und Strafurteile können Polizeibeamten bei ihrer täglichen Arbeit von Nutzen sein, weil sie darin nachlesen können, wie Staatsanwaltschaften und Gerichte die ermittelten Sachverhalte strafrechtlich bewerten. Sammelt ein Polizeibeamter jedoch solche Urteile und Strafbefehle für diesen Zweck, muß er darauf achten, daß er sie von vornherein nur in anonymisierter Form bei Gericht oder Staatsanwaltschaft anfordert, sie auch nur so zu seinen Handakten nimmt und bei seiner täglichen Arbeit verwendet. Denn die Personalien und die weiteren Angaben über den Verurteilten und denjenigen, gegen den ein Strafbefehl ergangen ist, sowie über all die anderen darin genannten Personen braucht er hierfür gar nicht. Weil der Polizeibeamte dies außer acht ließ und mit dem Vorzeigen der Strafbefehlsausfertigung recht sensible Informationen über den Motorradfahrer aus dem Ostalbkreis unnötigerweise weitergab, beanstandeten wir dies. Das Innenministerium teilte unsere Beurteilung. Die Polizeidirektion Ravensburg und die Landespolizeidirektion Tübingen nahmen den Vorgang zum Anlaß, ihre Beamten auf die Rechtslage hinzuweisen. Bleibt nur noch anzumerken, daß natürlich auch die Staatsanwaltschaft Ellwangen gut beraten gewesen wäre, wenn sie die Strafbefehlsausfertigung anonymisiert hätte, ehe sie sie nach Ravensburg schickte.

3.2 Weitergabe von Halterdaten mit Folgen
Ein Autofahrer aus dem Karlsruher Raum war völlig überrascht, als ihn der Pächter einer nahegelegenen Tankstelle anrief und ihm vorhielt, er habe am Vortag für 20 DM getankt und sei ohne zu zahlen weggefahren. Der Autofahrer konnte den Vorwurf rasch ausräumen. Weil er sich aber fragte, woher der Tankstellenpächter seinen Namen und seine Adresse wußte, wandte er sich an unser Amt. Rasch stellte sich heraus, wie alles abgelaufen war: Der Tankstel-

lenpächter hatte beim örtlichen Polizeiposten angerufen, das Autokennzeichen des Autofahrers genannt und erklärt, daß dieser nach dem Betanken seines Fahrzeugs ohne zu zahlen einfach davongefahren sei. Der Polizeiposten fragte über den Online-Anschluß der Polizei den Computer des Kraftfahrt-Bundesamts ab, erhielt so Name und Adresse des Autofahrers und informierte den Tankstellenpächter. Damit waren die Aktivitäten des Polizeipostens beendet. Aber schon damit hatte er des Guten zuviel getan: Denn die Weitergabe der Halterdaten an den Tankstellenpächter war nicht in Ordnung. Auf § 406 e der Strafprozeßordnung, der die Erteilung von Auskünften an den durch eine Straftat Geschädigten regelt, ließ sie sich nicht stützen, weil diese Vorschrift nur im Strafverfahren gilt und ein solches im Zeitpunkt der Information des Tankstellenpächters noch gar nicht eingeleitet worden war, und die Auskunftserteilung an den Geschädigten zudem Sache der Staatsanwaltschaft oder des Gerichts und nicht der Polizei ist. § 39 des Straßenverkehrsgesetzes war ebenfalls nicht anwendbar. Diese Vorschrift regelt zwar detailliert, wann Halterdaten zur Verfolgung von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr weitergegeben werden dürfen; Halterdatenauskünfte dürfen danach aber nur die örtlichen Zulassungsstellen und das Kraftfahrt-Bundesamt erteilen. Wer Halterdaten benötigt, um Rechtsansprüche, die aus der Teilnahme am Straßenverkehr resultieren, geltend machen zu können, muß sich also dorthin und nicht an die Polizei wenden.

Weil wir uns mit diesem Problem schon zum wiederholten Mal befassen mußten, baten wir das Innenministerium, die Rechtslage gegenüber den Polizeidienststellen klarzustellen. Dieses trug dieser Empfehlung Rechnung.

4. Versammlungsanmeldungen und Genehmigungen für Infostände zu weit gestreut

Weil die Stadt Stuttgart auf einer Genehmigung zum Aufstellen von Infoständen auch angegeben hatte, welche Stellen eine Abschrift der Genehmigung erhalten, stießen wir 1996 auf einen unzulässigen Mitteilungsdienst an den Verfassungsschutz und den polizeilichen Staatsschutz. Das kam so:

Eine Frau hatte aus Anlaß eines Kongresses des Studienzentrums Weikersheim, der in Stuttgart stattfand, bei der Stadt eine Demonstration vor dem Kongreßgebäude angemeldet und beantragt, auf der Königstraße drei Infotische aufstellen zu dürfen. Kurz darauf erhielt sie von der Stadt einen Bescheid, was sie als Leiterin der Demonstration zu beachten hat, und eine Ausnahmegenehmigung, daß sie – wie beantragt – jeweils einen Infostand für die Partei des Demokratischen Sozialismus (PDS), die Vereinigung der Verfolgten des Naziregimes – Bund der Antifaschisten (VVN-BdA) und für die Antifaschistische Jugend aufstellen darf. Jeweils eine Abschrift der beiden Bescheide schickte die Stadt dem Landesamt für Verfassungsschutz, dem Dezernat Staatsschutz der Landespolizeidirektion Stuttgart II und dem für die Stuttgarter Innenstadt zuständigen Schutzpolizeirevier. Auf die Idee, den Verfassungsschutz und den polizeilichen Staatsschutz so zu informieren, war die Stadt nicht von alleine gekommen: Bei ihrem Amt für öffentliche Ordnung hatten hin und wieder Mitarbeiter des Verfassungsschutzes mit dem aktuellen Verfassungsschutzbericht im Gepäck vorbeigeschaut und ganz allgemein darum gebeten, dem Landesamt Abschriften von versammlungsrechtlichen Bescheiden und Ausnahmegenehmigungen für Infostände zu schicken, sofern dabei eine im Verfassungsschutzbericht erwähnte Gruppierung mit von der Partie ist. Das Staatsschutzdezernat der Landespolizeidirektion Stuttgart II hatte erst im März 1996 schriftlich Klage über den ins Stottern geratenen Meldedienst geführt und das Amt für öffentliche Ordnung ganz pauschal gebeten, es bei „Ausnahmegenehmigungen für das Aufstellen von Info-Ständen deutscher und ausländischer politischer Gruppierungen/Organisationen (bei Ausländern auch Einzelpersonen) wieder in den Verteiler aufzunehmen“.

Diesen Begehrlichkeiten hätte die Stadt Stuttgart besser nicht nachgeben sollen. Denn dieser Mitteilungsdienst, den wir beanstandet haben, war, einmal abgesehen von der Unterrichtung des Schutzpolizeireviers, das für einen reibungslosen Ablauf der Demonstration sorgen und sich um die Einhaltung der Ausnahmegenehmigung für die Infostände kümmern mußte, ganz gleich von welcher Seite man ihn betrachtet nicht in Ordnung:

– Will das Landesamt für Verfassungsschutz von der Stadt Stuttgart solche Informationen wie hier, muß es sein Ersuchen so präzisieren, daß die Stadt genau erkennen kann, welche personenbezogenen Daten über wen davon umfaßt sein sollen. Anders gesagt: Das Datenübermittlungsersuchen muß konkret und einzelfallbezogen sein, nur dann entspricht es den Vorgaben des Landesverfassungsschutzgesetzes. Daß die allgemeine Bitte des Landesamts für Verfassungsschutz diesen Anforderungen nicht genügte, liegt auf der Hand. Zudem muß das Landesamt für Verfassungsschutz, wenn es von einer anderen Behörde personenbezogene Daten haben will, sein Ersuchen aktenkundig machen; auch das hatte es nicht getan. Diese Dokumentationspflicht ist kein purer Formalismus, sondern vielmehr geboten, um sicherzustellen, daß es nicht zu überflüssigen Datenübermittlungsverlangen kommt.
– Das Staatsschutzdezernat der Landespolizeidirektion Stuttgart II darf zwar zur Abwehr von konkreten Gefahren Informationen vom Stuttgarter Amt für öffentliche Ordnung einholen. Von einer solchen Gefahr ging aber das Staatsschutzdezernat hier selbst nicht aus. Es hielt sich vielmehr, anders ist sein Schreiben vom März 1996 an das Amt für öffentliche Ordnung nicht zu verstehen, für generell berechtigt, zur Lagebeurteilung bei Veranstaltungen, Demonstrationen oder Aktionen von politischen Gruppierungen vom Amt für öffentliche Ordnung jeweils eine Abschrift der Bescheide zu erhalten, mit dem es deutschen oder ausländischen politischen Gruppierungen und Organisationen das Aufstellen von Infoständen erlaubte. Ein derart pauschales Datenübermittlungsverlangen findet im Polizeigesetz jedoch keine Stütze. Im übrigen gab es keine Anhaltspunkte, daß bei der Demonstration oder an den drei Infoständen Straftaten mit staatsfeindlicher Zielrichtung zu befürchten gewesen wären, solche sind dann dort auch nicht begangen worden.
– Aus der Perspektive der Stadt Stuttgart hätte die Konsequenz aus diesen viel zu pauschalen und unbestimmten Datenübermittlungsverlangen des Verfassungsschutzes und des polizeilichen Staatsschutzes lauten müssen: Keine Daten über die Frau und auch nicht über sonst wen. Denn so wenig, wie diese beiden Stellen so pauschal anfragen durften, so wenig durfte die Stadt daraufhin aktiv werden. Auch für sie gilt nämlich: Ohne korrektes, also konkretes und einzelfallbezogenes Datenübermittlungsersuchen dürfen keine Daten fließen.

Daß ihre Vorgehensweise schon deshalb weder vom Polizeigesetz noch vom Verfassungsschutzgesetz gedeckt war, sah die Stadt Stuttgart ein. Vor kurzem schrieb sie uns, daß sie den Meldedienst schon Ende April 1996 eingestellt und ihr Amt für öffentliche Ordnung angewiesen hat, Verfassungsschutz und polizeilichem Staatsschutz im Zusammenhang mit Versammlungsanmeldungen oder Informationsständen nur noch Daten zu übermitteln, wenn im Einzelfall ein begründetes Ersuchen vorliegt. Das Innenministerium ließ uns wissen, daß das Landesamt für Verfassungsschutz unserer Beanstandung künftig Rechnung tragen wird. Bemerkenswert war dabei allerdings, daß es bei dessen bisheriger – gesetzwidriger – Praxis von einer „verantwortungsbewußten Auslegung“ des Verfassungsschutzgesetzes durch das Landesamt für Verfassungsschutz sprach, bei unserer Rechtsauffassung dagegen von einer „strengen und lediglich am Wortlaut“ orientierten Interpretation. Dabei hatten wir nur das eingefordert, was das Innenministerium 1991 selbst in die Begründung von § 9 Abs.4 des Landesverfassungsschutzgesetzes geschrieben hatte – nämlich, daß Datenübermittlungsersuchen des Verfassungsschutzes „konkret und einzelfallbezogen“ sein müssen (vgl. LT-Drs. 10/5231, S. 32). Was das Innenministerium zu dem pauschalen Datenübermittlungsersuchen des Staatsschutzdezernats sagt, wissen wir noch nicht.

3. Teil: Gesundheit

1. Datenschutz im Krankenhaus

In kaum einem Bereich fallen so viele und so sensible Daten an wie in einem Krankenhaus. Konsequenter Datenschutz tut hier not, auch und gerade in Zeiten, in denen Krankenhäuser vermehrt auf den Einsatz des Computers setzen, um die Informationsflut zu bewältigen. In der Praxis liegt freilich einiges im argen, wie ein Kontrollbesuch beim Universitätsklinikum Ulm, einem Krankenhaus mit insgesamt 13 Kliniken und etwa 37 000 stationären Patienten pro Jahr, ergab.

1.1 Das Patientenverwaltungssystem
Jeder, der personenbezogene Daten mit Hilfe der EDV verarbeitet, muß bedenken, daß er selbst in vollem Umfang für einen datenschutzgerechten Betrieb seiner EDV-Verfahren verantwortlich ist. Dazu gehört, daß er vor der beabsichtigten Einführung eines neuen EDV-Verfahrens zuerst einmal sorgfältig prüft, ob das Verfahren datenschutzrechtlichen Anforderungen genügt und welche Verbesserungen daran noch vorzunehmen sind, bevor an die Aufnahme des Echtbetriebs zu denken ist. Dieser Anforderung wurde das Klinikum jedoch bei der Einführung seines Patientenverwaltungssystems, mit dem es neben den Stammdaten seiner Patienten auch noch Diagnosen und sonstige Abrechnungsdaten verarbeitet, nicht gerecht. Die Ausgestaltung dieses von einem namhaften Softwarehaus entwickelten EDV-Systems ließ aus datenschutzrechtlicher Sicht sehr zu wünschen übrig.

1.1.1 Probleme mit den Eingabemasken
Verbesserungsbedürftig war die Gestaltung der für die Patientenaufnahme vorgesehenen Eingabemasken. Sie enthielten Eingabefelder, die gar nicht benötigt wurden und sahen Freitextfelder vor, ohne daß exakt festgelegt war, was in ihnen gespeichert werden darf. Das Klinikum sagte inzwischen Abhilfe zu.

1.1.2 Zugriffsrechte zu weitgehend
In der Theorie ist man sich einig: Jeder Mitarbeiter des Klinikums darf nur die Zugriffsrechte auf Patientendaten erhalten, die er zur Erfüllung seiner Aufgaben tatsächlich benötigt. In der Praxis sieht manches anders aus:

- Jeder Arzt des Klinikums konnte nicht nur lesend und schreibend auf die Daten der Patienten seiner eigenen Klinik zugreifen, sondern er konnte sich darüber hinaus auch jederzeit die Patientendaten der anderen Kliniken am Bildschirm anzeigen lassen. Im Regelfall benötigt ein Arzt den Zugriff auf Patientendaten der anderen Kliniken nicht. In Betracht kommen kann er lediglich in Ausnahmesituationen, beispielsweise in einem Notfall. Da das EDV-System eine spezielle Notfall-Berechtigung bislang aber nicht kennt, räumte das Klinikum seinen Ärzten diese weitreichenden Zugriffsrechte ein. Das ging zu weit. Es geht nicht an, jedem Arzt von vornherein lesenden Zugriff auf Daten aller gerade im Klinikum behandelten Patienten einzuräumen, nur weil ein solcher klinikumsweiter Zugriff in seltenen Ausnahmefällen einmal erforderlich sein kann. Auf unsere Beanstandung und die Forderung, das Klinikum möge sich beim Hersteller mit allem Nachdruck auf die Fertigstellung einer Notfall-Berechtigung einsetzen, teilte das Klinikum mit, der Mangel würde durch eine der nächsten Änderungen in der Software behoben.
- Weil jeder der sieben mit der Abwicklung der Abrechnungen betrauten Mitarbeiter des Klinikums nur für eine ganz bestimmte Patienten-Buchstabengruppe zuständig ist, bräuchte er auch nur Zugriff auf die gespeicherten, abrechnungsrelevanten Patientendaten seiner Buchstaben-

gruppe. Da das Patientenverwaltungssystem dies jedoch bislang nicht ermöglicht, räumte das Klinikum ihnen jeweils den Zugriff auf die abrechnungsrelevanten Daten sämtlicher Patienten ein. Damit wurde das Klinikum der Anforderung an eine datenschutzgerechte Organisation seiner Datenverarbeitung nicht gerecht. Auf unsere Beanstandung teilte das Klinikum mit, der Hersteller sehe eine entsprechende Verbesserung seiner Software vor.

- Die Pflegekräfte der Intensivstationen konnten nicht nur, wie das Pflegepersonal der übrigen Stationen auch, jeweils auf Daten von Patienten der eigenen Station zugreifen, sondern ihnen hatte das Klinikum darüber hinaus auch noch den Zugriff auf Daten sämtlicher, gerade im Klinikum behandelter Patienten eingeräumt. Als Grund gab das Klinikum an: Bei der Verlegung eines Patienten von einer Station auf eine andere werde häufig vergessen, die Verlegung in den Computer einzutragen. Folge sei, daß die aufnehmende Station plötzlich einen Patienten habe, dessen Daten sie im Computer nicht abrufen könne. Die aufnehmende Station muß in einem solchen Fall nachforschen, woher der Patient kommt und veranlassen, daß die Verlegung nachträglich in den Computer eingegeben wird. Da nach Ansicht des Klinikums für die Pflegekräfte der Intensivstationen eine solch zeitaufwendige Vorgehensweise nicht vertretbar ist, räumte das Klinikum ihnen dieses umfassende Zugriffsrecht ein. Auch dies ist nicht hinnehmbar: Schlechter Umgang mit der EDV darf nicht dazu führen, Mitarbeitern mehr Zugriffsrechte einzuräumen, als dies eigentlich notwendig wäre. Auf unsere Beanstandung und Forderung, das Klinikum möge auf einen korrekten Umgang mit dem EDV-System hinwirken und dann alsbald die Zugriffsrechte des Pflegepersonals der Intensivstationen auf das sonst übliche Maß beschränken, beharrte das Klinikum auf der Notwendigkeit der getroffenen Regelung. Die Erörterungen hierzu sind noch nicht abgeschlossen.
- Das Patientenverwaltungssystem ist so angelegt, daß die Patientendaten zentral auf einem Rechner gespeichert sind. Allerdings bestand auch die Möglichkeit, manche der gespeicherten Daten auf die Festplatte eines PC zu kopieren, einen sog. Download durchzuführen. Datenschutzrechtliche Probleme sind die Folge. So muß sich beispielsweise jeder, der einen Download auslöst, selbst um die fristgerechte Löschung der Daten auf seinem PC kümmern. Von der Möglichkeit des Downloads ist daher äußerst zurückhaltend Gebrauch zu machen. Sie darf nur solchen Mitarbeitern des Klinikums offenstehen, die sie auch tatsächlich benötigen. Bislang läßt sich die Download-Funktion aber nicht benutzerbezogen einschränken. Das Klinikum teilte inzwischen mit, der Hersteller werde den Mangel abstellen.
- Das Klinikum beabsichtigt, in Zukunft die komplette medizinische Dokumentation per EDV zu speichern. Bis zum Abschluß der Behandlung soll die behandelnde Klinik Zugriff auf alle im Klinikum gespeicherten Daten ihres Patienten erhalten. Eine solche Regelung ist zu pauschal. Sie hätte beispielsweise zur Folge, daß ein Zahnarzt, der eine Patientin behandelt, die früher bereits in der Frauenklinik in Behandlung war, nachsehen könnte, welche Daten dabei anfielen. Warum dies so sein muß, ist nicht einzusehen. Zu denken ist vielmehr an eine abgestufte Zugriffsregelung, bei der die behandelnde Klinik etwa sofort ermitteln kann, welche anderen Kliniken den betreffenden Patienten früher schon einmal behandelten, sie aber nicht von vornherein auf gespeicherte Befunde und Diagnosen zugreifen kann. Das Klinikum will dies bei der weiteren Planung berücksichtigen.

1.1.3 Löschprobleme
Nicht genug Augenmerk legte das Klinikum auf eine Löschung von Patientendaten:

– Fehlende Löschkonzeption
Wer personenbezogene Daten mit Hilfe der EDV verarbeitet, muß gleichzeitig regeln, wann welche Daten zu löschen oder zumindest für den Zugriff zu sperren sind. So verlangen es die Anforderungen des Datenschutzes. Eine spezielle Löschkonzeption für das eingesetzte Patientenverwaltungssystem konnte das Klinikum nicht vorlegen, sondern nur auf von ihr erstellte allgemeine Grundsätze für die Löschung von Patientendaten verweisen. Diese sehen eine Löschung von Patientendaten vor, wenn deren Qualität oder Nutzungsmöglichkeit so gering eingeschätzt wird, daß eine Speicherung über die Mindestaufbewahrungsfrist hinaus unzweckmäßig erscheint. Bei dieser Frist ging das Klinikum von einer „gesetzlichen Aufbewahrungsfrist“ von 30 Jahren aus. Datenschutzrechtlich konnte dies nicht befriedigen: Eine Rechtsvorschrift, die eine 30jährige Speicherung von Krankenakten oder elektronisch gespeicherten Patientendaten verlangt, gibt es nicht. Eine Aufbewahrung medizinischer Unterlagen über diesen langen Zeitraum läßt sich allenfalls auf die allgemeinen Verjährungsfristen für die Geltendmachung von Schadenersatzansprüchen stützen. Einen Automatismus, medizinische Unterlagen generell so lange vorzuhalten, darf es dabei jedoch nicht geben, zumal erfahrungsgemäß solche Ersatzansprüche schon wesentlich früher geltend gemacht werden. Maßgebend muß vielmehr die Dokumentationsregelung der ärztlichen Berufsordnung sein. Diese verlangt eine über 10 Jahre hinausgehende Speicherung nur, wenn dies nach ärztlicher Erfahrung geboten ist. Zudem ist bei elektronisch gespeicherten Patientendaten noch zu bedenken, daß eine direkte Zugriffsmöglichkeit auf alle gespeicherten Daten über einen Zeitraum von 30 Jahren wohl kaum notwendig ist. Bei Patienten, die schon längere Zeit nicht mehr im Klinikum waren, genügt es statt dessen, wenn ein Klinikumsmitarbeiter auf Knopfdruck lediglich einige wenige Angaben am Bildschirm angezeigt bekommt, die ausreichen, um festzustellen, wer der Patient ist und ob über ihn noch weitere Daten gespeichert sind. Das Klinikum hat zugesagt, ein spezielles Lösch- und Sperrkonzept für das Patientenverwaltungssystem zu erstellen und hierbei kürzere Aufbewahrungsfristen vorzusehen.

– Fehlende Löschfunktionen
Die beste Löschkonzeption nützt nichts, wenn das EDV-Verfahren keine Löschfunktionen bereitstellt, durch die sich gespeicherte Patientendaten auch wieder löschen lassen. Dies war bei dem eingesetzten Patientenverwaltungssystem aber der Fall. Weder kannte das Verfahren eine sog. Regellöschfunktion, bei der die zu löschenden Datensätze automatisiert zu bestimmten Stichtagen gelöscht werden, noch konnte ein Benutzer einzelne Datensätze selbst löschen. Auf unsere Forderung, das Klinikum möge dafür Sorge tragen, daß umgehend Löschfunktionen bereitstehen, teilte es mit, dies sei voraussichtlich noch im Laufe des Jahres der Fall.

1.2 Die Mikroverfilmung
Krankenakten wachsen recht schnell zu umfangreichen Papiersammlungen an, muß der Arzt doch darin den Befund, alle eingeleiteten Behandlungsmaßnahmen und veranlaßten Leistungen sowie den jeweiligen Tag der Behandlung penibel registrieren. So verwundert es nicht, daß das Klinikum nach einem kostengünstigen Weg Ausschau hielt, seine Krankenakten möglichst platzsparend vorzu-

halten und eine bequeme und schnelle Nutzung der Unterlagen zu ermöglichen. Es beauftragte dazu eine Firma mit der sukzessiven Mikroverfilmung von Patientenakten: Zu einem vereinbarten Termin holt die Firma jeweils die vom Klinikum bereitgestellten Patientenunterlagen ab, verfilmt sie und führt sie anschließend der Vernichtung zu. Ein PC-Programm mit angeschlossenem Lesegerät ermöglicht dann einem Klinikumsmitarbeiter den schnellen Zugriff auf die verfilmten Unterlagen. Dazu muß er lediglich einige Angaben zum Patienten, wie Name und Geburtsdatum, in den Computer eintippen und schon kann er sich die verfilmten Unterlagen am Bildschirm anschauen. Damit dies klappt, speichert das EDV-Programm zu den Stammdaten eines Patienten jeweils die richtige Fundstelle auf dem Mikrofilm. Die Beauftragung einer Firma und die damit verbundene Verarbeitung von Patientendaten durch eine Stelle außerhalb des Krankenhauses ist nach unserem Landeskrankenhausgesetz nicht von vornherein ausgeschlossen. Absolut inakzeptabel war freilich die Art und Weise, wie dies geschah:

- Um den Stammdaten eines Patienten die richtige Fundstelle auf dem Mikrofilm im EDV-Programm zuordnen zu können, stellte das Klinikum der Firma im Zuge des allerersten Verfilmungslaufs den kompletten Stammdatensatz aller bis dahin in der EDV gespeicherten Patienten auf Disketten zur Verfügung. Dies war entschieden zu viel. Es hätte genügt, nur die Stammdaten der Patienten weiterzugeben, deren Unterlagen tatsächlich zu verfilmen waren.
- Die ihr auf Disketten übergebenen Patientendaten kopierte die Firma auf ein eigenes Sicherungsband und behielt dieses als zusätzliche Datensicherung bei sich. Dazu bestand überhaupt keine Notwendigkeit. Nach Abschluß der Verfilmungsarbeiten gibt es keinerlei Grund, daß die Firma noch irgendwelche Patientendaten vorhält.
- Ein gravierender Mangel war ferner, daß die Firma nach Abschluß der Verfilmungsarbeiten das Filmoriginal bei sich behielt, um auf Anforderung des Klinikums einen neuen Filmabzug herstellen zu können. Damit unterhielt die Firma sozusagen ein eigenes Krankenaktenarchiv mit einer Fülle äußerst sensibler Angaben über eine Vielzahl von Patienten. Dies stellt einen gravierenden datenschutzrechtlichen Verstoß dar. Geboten ist vielmehr, daß das Klinikum selbst die Filmoriginale vorhält und allenfalls bei Bedarf der Firma für die Erstellung eines neuen Filmabzugs zur Verfügung stellt.
- Schließlich war auch die Vernichtung der Patientenakten unzureichend. Dabei ist darauf zu achten, daß die entstehenden Papierteilchen ausreichend klein sind. Wie klein sie sein müssen, hängt von der Sensibilität der zu vernichtenden Daten ab. Als Richtschnur für eine datenschutzgerechte Vorgehensweise läßt sich die entsprechende DIN-Norm heranziehen. Diese sieht bei der Vernichtung fünf Sicherheitsstufen vor, wobei die entstehenden Papierteilchen immer kleiner werden, die Wiederherstellung der vernichteten Daten also immer schwieriger wird. Für die Vernichtung sensibler medizinischer Angaben ist zumindest die Stufe drei als Maßstab anzulegen. Dies war jedoch nicht der Fall.

Auf unsere Beanstandung hin hat das Klinikum die Mängel bereits teilweise abgestellt. Die Erörterungen über die Weitergabe von Stammdaten sind noch nicht abgeschlossen.

1.3 Was sonst noch Mühe macht

Bei der Kontrolle zeigten sich aber auch noch eine ganze Reihe weiterer technischer und organisatorischer Mängel. Einige davon sind altbekannt und sollten langsam der Vergangenheit angehören. Unverständlich, daß sie dennoch immer wieder auftreten, noch dazu in einem Krankenhaus, in dem ein strenger Datenschutzmaßstab anzulegen ist.

1.3.1 Die Fernwartung

Zur Beseitigung von Störungen und Fehlern im laufenden Betrieb beauftragte das Klinikum sowohl den Hersteller der Rechner, auf denen das Patientenverwaltungssystem installiert ist, als auch den Software-Produzenten mit den notwendigen Wartungsarbeiten unter Einschluß von Fernwartung. Wenn ein Krankenhaus dies zuläßt, muß es bedenken, daß Fernwartung generell zu Risiken für die gespeicherten Patientendaten führt, da eine externe Stelle per Leitung Zugang zu Rechnern des Krankenhauses erhält. Bei der Einrichtung einer Fernwartungsmöglichkeit ist deshalb besondere Sorgfalt vonnöten. Dem trug das Klinikum nicht ausreichend Rechnung:

– Die beiden Verträge mit den Fernwartungsunternehmen enthielten lediglich ganz pauschale Hinweise auf die Einhaltung der Datenschutzbestimmungen. Durch welche Maßnahmen dies sicherzustellen ist, blieb vollkommen offen. So war zum Beispiel völlig ungeregelt, ob Fernwartungspersonal gespeicherte personenbezogene Daten des Klinikums für Zwecke der Fehlerbeseitigung auf einen eigenen Rechner übertragen darf oder nicht. Bei derart sensiblen Daten, wie sie das Klinikum speichert, ist dies jedoch von vornherein auszuschließen.
– Nicht hinnehmbar war auch, daß – wie es sich der Software-Produzent vorbehalten hatte – freie Mitarbeiter oder Mitarbeiter ganz anderer Unternehmen Fernwartungsarbeiten im Klinikum durchführen. Vielmehr müssen die Fernwartungsunternehmen dem Klinikum die Mitarbeiter mitteilen, die im Rahmen der Fernwartung tätig werden.
– Schließlich war es auch ein Mangel, daß das Klinikum die Fernwartung des Patientenverwaltungssystems zwar automatisch protokollierte, die Protokolle aber nur jeweils einen Tag vorhielt. Nach Ablauf der 24 Stunden konnte das Klinikum somit nicht mehr nachprüfen, was das Fernwartungspersonal im einzelnen gemacht und insbesondere, auf welche Daten es zugegriffen hatte. Erforderlich ist vielmehr, die Protokolle über einen wesentlich längeren Zeitraum von etwa einem Jahr aufzubewahren.

Auf unsere Beanstandung hin sicherte das Klinikum zu, die Mängel abzustellen.

1.3.2 Die Protokollierung

Im Klinikum zeigten sich bei der Protokollierung zwei Mängel:

– Damit sich auch im nachhinein noch feststellen läßt, welcher Mitarbeiter des Klinikums wann über welche Zugriffsrechte verfügte, ist es notwendig, die Aktivitäten der Benutzerverwaltung, also das Einrichten, Verändern und Löschen von Benutzern und deren Zugriffsrechten zu protokollieren. Dies geschieht im Klinikum auch. Ungeregelt war jedoch, wie lange das Klinikum die Protokolldaten vorhalten will. Eine entsprechende Festlegung durch das Klinikum steht noch aus.
– Im laufenden Betrieb erfolgte zwar eine Protokollierung, wenn jemand gespeicherte Patientendaten veränderte; eine Protokollierung lesender Zugriffe gab es dagegen nicht. Derzeit mag dies gerade noch angehen. Wenn aber – wie vorgesehen – das Klinikum vermehrt medizinische Angaben per EDV verarbeitet und die einzelnen Kliniken in gegenseitiger Abstimmung klinikübergreifende Zugriffe auf ihre Daten zulassen, ist eine solch rudimentäre Protokollierung nicht ausreichend. Unverzichtbar ist dann eine zumindest stichprobenartige Protokollierung auch der lesenden Zugriffe auf gespeicherte Patientendaten. Das Klinikum sieht dazu bislang keine Notwendigkeit. Dabei übersieht es aber, daß ein zugriffsberechtigter Mitarbeiter des Klinikums nicht automatisch berechtigt ist, von diesem

Zugriffsrecht auch tatsächlich jederzeit Gebrauch zu machen. Dies darf er nur dann tun, wenn der Zugriff zur Versorgung des Patienten auch tatsächlich notwendig oder wenn er für Forschungszwecke nach Maßgabe des Landesdatenschutzgesetzes zulässig ist. Solches nachzuprüfen ist aber nur möglich, wenn sich feststellen läßt, wer was wann am Computersystem gemacht und auf welche Daten er zugegriffen hat. Ein vollständiger Verzicht auf die stichprobenartige Protokollierung lesender Zugriffe würde das Klinikum jedenfalls von vornherein einer Kontrollmöglichkeit berauben. Die Protokollierung verfolgt ja gerade auch den Zweck, einer mißbräuchlichen Datenverarbeitung vorzubeugen, weil niemand darauf vertrauen kann, daß Verstöße unentdeckt bleiben. Die Erörterungen hierzu sind noch nicht abgeschlossen.

1.3.3 Die Benutzerverwaltung

Im Klinikum mit seinen vielen Mitarbeitern, die am Computer arbeiten, sind laufend Benutzer neu einzurichten, zu löschen oder Zugriffsrechte bereits eingerichteter Benutzer zu ändern, wenn sie eine andere Tätigkeit übernehmen. Dabei ist jeder Benutzerverwalter des Klinikums jeweils für eine bestimmte Benutzergruppe, beispielsweise für alle Ärzte einer Klinik oder alle Pflegekräfte einer bestimmten Klinikstation, zuständig. Um bei der Vielzahl der Benutzer – zum Zeitpunkt des Kontrollbesuchs waren etwa 1 850 Benutzerkennungen vergeben – und der stattlichen Zahl von bis zu 250 Benutzern, für die ein einzelner Benutzerverwalter zuständig ist, den Überblick zu behalten, ist unerläßlich, daß ein Benutzerverwalter schnell auf Knopfdruck feststellen kann, welche Benutzergruppen mit welchen Benutzern eingerichtet sind. Dies ist unverzichtbar, um beispielsweise rasch nachprüfen zu können, ob einer Benutzergruppe etwa noch Mitarbeiter angehören, die in der entsprechenden Klinik oder Station gar nicht mehr beschäftigt sind. Da dies bisher nicht möglich war, forderten wir das Klinikum auf, auf eine entsprechende Umgestaltung der Software hinzuwirken. Die Erörterungen hierüber sind noch nicht abgeschlossen.

1.3.4 Mängel beim Paßwortschutz

Die Veröffentlichungen zur richtigen Gestaltung von Paßwörtern sind Legion. So sollten gut gewählte Paßwörter mindestens sechs Zeichen lang sein, möglichst aus Groß- und Kleinbuchstaben sowie Ziffern oder Sonderzeichen bestehen und nicht für immer und ewig gelten, sondern nach einer gewissen Zeit verfallen. Umso unverständlicher, daß der Zugriff auf gespeicherte Patientendaten im Klinikum mit Paßwörtern möglich war, die lediglich drei Zeichen lang waren und nie automatisch verfielen, obwohl die EDV dies ermöglicht hätte. Auf unsere Beanstandung und die Forderung, diese Mängel abzustellen, verwies das Klinikum darauf, die allseits bekannten Regeln für die Vergabe von Paßwörtern würden nur für versierte EDV-Benutzer und solche gelten, die mit der EDV vertraut seien. Hier irrt das Klinikum: Maßgeblich für die zu treffenden technischen und organisatorischen Sicherungsmaßnahmen sind nicht die Fähigkeiten der einzelnen Benutzer, sondern ist die Schutzwürdigkeit der gespeicherten personenbezogenen Daten. Die Erörterungen in dieser Sache dauern an.

1.3.5 Zu viele Fehlversuche möglich

Potentiellen Eindringlingen in ein Computernetzwerk kann man den Spaß am Ausprobieren von Benutzerkennungen und Paßwörtern dadurch verderben, daß die Benutzerkennung nach einer bestimmten Anzahl von Fehlversuchen gesperrt wird. Das hatte das Klinikum getan, dabei allerdings die Zahl der möglichen Fehlversuche mit 12 zu großzügig

bemessen. Ob das Klinikum der Forderung, diese Zahl auf drei oder maximal fünf zu begrenzen, nachkommen will, ist noch offen.

1.3.6 Keine automatische Abmeldung bei Unterbrechungen
Unterbricht ein am Computer arbeitender Benutzer seine Tätigkeit am Bildschirm und verläßt seinen Arbeitsplatz, so sollte er sich generell abmelden oder den Bildschirm für weitere Eingaben sperren. Doch wer ist dagegen gefeit, daß er dies in der Hektik des Arbeitsalltags einmal vergißt? Deswegen ist es geboten, daß das EDV-System nach einer gewissen Zeitspanne der Untätigkeit eine automatische Abmeldung selbst vornimmt oder den Bildschirm sperrt und ihn erst wieder nach Eingabe eines geheimen Paßworts freigibt. Mit dem Patientenverwaltungssystem ist dies bislang nicht möglich. Auf unsere Beanstandung teilte das Klinikum mit, in den nächsten Monaten sei mit einer solchen Verbesserung zu rechnen.

1.3.7 Fehlende Terminalbeschränkung
Der beste Paßwortschutz nützt nichts, falls ein Paßwort doch einmal einem Unbefugten bekannt wird. Findet er dann noch die zugehörige Benutzerkennung heraus, so könnte er sich am Computer anmelden und mit der Berechtigung des eigentlichen Benutzers auf Daten zugreifen. Diese Mißbrauchsgefahr läßt sich dadurch verringern, daß eine Anmeldung mit einer bestimmten Kennung nur von ganz bestimmten Rechnern aus möglich ist. Besonders wichtig ist dies bei Kennungen, die mit sehr weitreichenden Zugriffsrechten verknüpft sind, wie beispielsweise bei System- oder Benutzerverwaltern. Hier macht es einen gewaltigen Unterschied, ob es sich der Angreifer an seinem eigenen Rechner in einer abgeschiedenen Ecke bequem machen oder ob er seinen unlauteren Absichten nur an einem im gesicherten Rechenzentrumsbereich aufgestellten PC nachgehen kann. Das Patientenverwaltungssystem bietet bislang keine Möglichkeit, eine Terminalbeschränkung einzurichten. Auf unsere Beanstandung teilte das Klinikum mit, es werde beim Hersteller einen entsprechenden Entwicklungsantrag stellen.

1.3.8 Benutzung nicht benötigter Programme möglich
Auf einem Computer dürfen nur die Programme installiert und startbar sein, die die Mitarbeiter, die mit diesem PC arbeiten, für ihre Arbeit tatsächlich benötigen. Bei den PC in der Patientenaufnahme einer Klinik waren jedoch Hilfsprogramme installiert, die beispielsweise Zugriffe auf Netzwerkrechner erlaubten und sogar ermöglichten, selbst Programme zu erstellen und auszuführen. Da diese PC nicht einmal mit einem Startpaßwort gesichert waren, hätte jeder, der Zugang zu diesen PC hat, diese Hilfsprogramme auch starten können. Da die Mitarbeiter der Patientenaufnahme diese Programme nicht für ihre Tätigkeit benötigen, darf es ihnen aber auch nicht möglich sein, sie aufzurufen. Die Erörterungen hierüber dauern noch an.

1.3.9 Fehlende Regelungen zur Datensicherheit
Wer personenbezogene Daten mit Hilfe der EDV verarbeitet, muß sich Gedanken darüber machen, wie er den mit der automatisierten Datenverarbeitung einhergehenden Gefahren für die gespeicherten Daten der Betroffenen begegnen will. Unerläßlich ist dazu, ausreichende technische und organisatorische Sicherungsmaßnahmen zu treffen und diese zu dokumentieren. Dies verlangt auch das Landesdatenschutzgesetz. Solche Regelungen waren im Klinikum Mangelware. So existierten weder schriftliche Festlegungen zur Ausgestaltung von Paßwörtern noch Vorgaben, was Mitarbeiter des Klinikums bei der Arbeit am PC zu beachten haben und welche Sicherungsmaßnahmen sie selbst ergreifen müssen.

Auch fehlten Regelungen, wie bei einer Fernwartung zu verfahren ist. Dies ist in einem Klinikum, das eine Fülle äußerst sensibler Daten speichert und verarbeitet, absolut inakzeptabel. Auf unsere Beanstandung teilte das Klinikum mit, es beabsichtige, entsprechende Regelungen zu erstellen.

2. Die Personalunion

Es gibt Funktionen, die ein und dieselbe Person nicht gleichzeitig ausüben kann, weil sie sonst in Interessenkonflikte gerät, die eine korrekte Wahrnehmung der einzelnen Aufgaben nahezu unmöglich machen. Darauf hinzuweisen, gab uns der Krankenhausdezernent eines Landratsamts Anlaß. Denn dieser war nicht nur gleichzeitig auch noch Verwaltungsleiter in den Kreiskrankenhäusern, sondern fungierte zudem als Beauftragter für den Datenschutz in eben diesen Krankenhäusern. Ein solcher multifunktionaler Einsatz einer Person ist aber nicht möglich. § 51 des Landeskrankenhausgesetzes verlangt die Bestellung eines Beauftragten für den Datenschutz, damit im Krankenhaus eine qualifizierte Eigenkontrolle der Verarbeitung der Patientendaten stattfindet. Ein Krankenhausdezernent und Verwaltungsleiter trägt demgegenüber Verantwortung für die Betriebsführung und das wirtschaftliche Ergebnis des Krankenhauses. In dieser Funktion ist es zu einem wesentlichen Teil seine Aufgabe, die Datenverarbeitung im Krankenhaus zu regeln und zu organisieren. Als Beauftragter für den Datenschutz, der den Umgang mit Patientendaten im Krankenhaus zu kontrollieren hat, müßte er deshalb etwas überprüfen, was er in seiner anderen Funktion zu einem wesentlichen Teil zu bestimmen und zu verantworten hat.

Welche Auswirkungen es im Einzelfall haben kann, wenn eine solche Personalunion praktiziert wird, zeigt gerade der Fall, der Anlaß dafür war, diese Frage aufzugreifen: Der Krankenhausdezernent und Verwaltungsleiter verlangte von den für das Krankenhaus bestellten Betriebsärzten, daß sie dann, wenn sie im Rahmen einer arbeitsmedizinischen Untersuchung eines Mitarbeiters externe Labors mit Untersuchungen beauftragen, die darüber ausgestellten Rechnungen mit dem darauf festgehaltenen Namen des untersuchten Mitarbeiters und Untersuchungsschlüssel, aus dem die Art der Laboruntersuchung ersichtlich ist, zur Auszahlung weiterleiten sollten. Er begründete diese Forderung damit, als Krankenhausdezernent seien ihm die Betriebsärzte unterstellt. Es sei seine Sache sicherzustellen, daß sie die arbeitsmedizinischen Untersuchungen entsprechend den Richtlinien der Berufsgenossenschaft durchführen. Dazu müsse er die Namen der untersuchten Mitarbeiter und die Art der Laboruntersuchung kennen. Hinzu komme, daß er die Verantwortung für die Betriebsführung des Kreiskrankenhauses trage und damit das wirtschaftliche Ergebnis gegenüber dem Krankenhausträger zu verantworten habe. In dieser Eigenschaft habe er darauf zu achten, daß nur die Ausgaben getätigt würden, die durch entsprechende Vorschriften abgedeckt seien.

Diese Argumentation mag aus der Sicht eines Krankenhausdezernenten und Verwaltungsleiters noch verständlich sein, für den Beauftragten für den Datenschutz eines Krankenhauses ist sie es jedoch nicht. Denn als solcher muß er wissen, daß die Betriebsärzte auch gegenüber dem Arbeitgeber die ärztliche Schweigepflicht zu beachten haben und deshalb der Krankenhausverwaltung persönliche Geheimnisse von untersuchten Mitarbeitern nur offenbaren dürfen, wenn entweder diese eingewilligt haben oder aber eine Rechtsvorschrift die Weitergabe erlaubt. Zu den von den Betriebsärzten geheimzuhaltenden persönlichen Geheimnissen gehört aber auch die Information, daß und welche Laboruntersuchung bei einem Mitarbeiter im Rahmen der arbeitsmedizinischen Untersuchung vorgenommen wurde. Eine Rechtsvorschrift, die die Weitergabe dieser Informationen an die Krankenhausverwaltung zuläßt, gibt es nicht. Denn ein Betriebsarzt ist bei der Anwendung seiner arbeitsmedizinischen Fachkunde weisungsfrei. Ob und welche Laboruntersuchung im Einzelfall erforderlich ist, hat deshalb allein er zu entscheiden. Ein Kontrollrecht steht insoweit weder dem Krankenhausdezernenten noch dem

Verwaltungsleiter zu. Deshalb können diese auch nicht vom Betriebsarzt für diesen Zweck Informationen anfordern, die der ärztlichen Schweigepflicht unterliegen.

Wir haben das Krankenhaus auf diese Rechtslage hingewiesen, verbunden mit der Aufforderung,
- das Auszahlungsverfahren bei Laborrechnungen so auszugestalten, daß der Krankenhausverwaltung nicht bekannt wird, bei welchen Mitarbeitern die Laboruntersuchungen durchgeführt wurden und
- dafür Sorge zu tragen, daß unverzüglich ein geeigneter Beauftragter für den Datenschutz im Krankenhaus bestellt wird.

Eine Antwort steht noch aus.

3. Die Schlafstudie

Medizinische Forschung ist sicher sehr wichtig, aber auch sie muß sich beim Umgang mit Patientendaten an die dafür maßgebenden Rechtsvorschriften halten. Darauf hinzuweisen, gab uns das Klinikum der Universität Freiburg i. Br. Anlaß. Geschehen war folgendes: Bei einer Schlafstudie, die im Rahmen der klinischen Prüfung eines Arzneimittels im Schlaflabor der Psychiatrischen Universitätsklinik durchgeführt wurde, gewann der dafür verantwortliche Leiter der Studie den Eindruck, daß ein Teilnehmer die für die Teilnahme an der Schlafstudie notwendigen Voraussetzungen nicht erfüllt. Um dies zu überprüfen, schaute er die in der Psychiatrischen Universitätsklinik geführte Sammlung von Ambulanzkarten durch und stellte dabei fest, daß sich der Teilnehmer bereits früher einmal in der Klinik hatte behandeln lassen. Daraufhin konfrontierte er den Teilnehmer mit dem Ergebnis seiner Recherche und teilte ihm mit, daß er damit nicht mehr Teilnehmer der Schlafstudie sein könne. Verärgert darüber, daß ihm Informationen seiner früheren Behandlung in der Klinik von dem an der damaligen Behandlung nicht beteiligten Leiter der Schlafstudie entgegengehalten wurden, wandte sich der Teilnehmer an uns, nachdem ihm die Klinik zuvor bedeutet hatte, daß ihr Vorgehen völlig korrekt gewesen sei. Dem konnten wir freilich nicht beipflichten. Denn Informationen, die ein Krankenhaus im Rahmen einer Behandlung eines Patienten erhebt und in seinen Unterlagen festhält, darf es Ärzten, die nicht an der Behandlung beteiligt waren, zur Durchführung einer Studie nur zugänglich machen, wenn entweder der Patient eingewilligt hat oder eine Rechtsvorschrift diese Verwendung der Daten erlaubt. Keine dieser beiden Voraussetzungen war aber gegeben. Die Einsichtnahme in die Sammlung der Ambulanzkarten war also unzulässig. Dies bedeutet durchaus nicht, daß eine Klinik in solchen Fällen die Mitwirkung von ungeeigneten Teilnehmern hinnehmen muß. Sie kann bei Zweifeln an der Eignung ohne weiteres an den Teilnehmer herantreten und um eine Klärung bitten. Gelingt es dabei nicht, die Zweifel auszuräumen, hat sie immer noch die Möglichkeit, ihn von der weiteren Teilnahme an der Studie auszuschließen.

4. Die Psychiatrie-Akte auf der Straße

Ende vergangenen Jahres erregte ein Aktenfund in Tübingen einiges Aufsehen. Ein Autofahrer entdeckte dort in einem auf dem Gehweg für die Altpapierabfuhr bereitgestellten Karton zahlreiche Kopien aus Abrechnungsunterlagen eines Psychiatrischen Landeskrankenhauses. Diese Kopien hatte ein Mitarbeiter der ehemaligen Vorprüfungsstelle beim Regierungspräsidium Tübingen, der Vorgängerin des Staatlichen Rechnungsprüfungsamts Tübingen, im Jahr 1991 bei einer örtlichen Prüfung der Abrechnung von Krankenhausleistungen des Psychiatrischen Landeskrankenhauses hergestellt und in seine Dienststelle mitgenommen. Im wesentlichen handelte es sich um einen Schriftwechsel zwischen dem Psychiatrischen Landeskrankenhaus, dem Landeswohlfahrtsverband Württemberg-Hohenzollern, einem Kreissozialamt und um eigene Aufzeichnungen des Psychiatrischen Landeskrankenhauses über die Abrechnung von Unterbringungskosten eines Patienten. Unter anderem waren

darin detailliert der Krankenhausaufenthalt des Patienten, die dabei festgestellten Diagnosen und die erbrachten Leistungen beschrieben.

Bei der Überprüfung zeigte sich, daß das Staatliche Rechnungsprüfungsamt die Aussonderung von Unterlagen mit personenbezogenen Daten durchaus sachgerecht in einer internen Dienstanweisung geregelt hatte. Nur nützt die beste Regelung recht wenig, wenn sie nicht beachtet wird. Genauso war es hier. Bei einem hausinternen Umzug gerieten die für die Vernichtung bestimmten Kopien zum normalen Altpapier mit den bekannten Folgen. Bei unserer Beanstandung des Vorgehens des Staatlichen Rechnungsprüfungsamts gegenüber dem Rechnungshof blieb uns daher nur, zu einer strikten Beachtung der für die Vernichtung von Unterlagen mit personenbezogenen Daten getroffenen Regelung aufzufordern. Wieder einmal zeigte sich in diesem Fall, wie gefährlich es ist, wenn solche Unterlagen erst dann zur Vernichtung freigegeben werden, wenn ein Umzug ansteht, denn erfahrungsgemäß wird gerade bei solchen Anlässen die gebotene Sorgfalt häufig nicht beachtet. Diese Gefahr ließe sich wesentlich verringern, wenn die Vernichtung von Akten nicht von der Zufälligkeit von Umzügen abhängig gemacht würde, sondern sie, wie von § 19 LDSG gefordert, immer schon dann vorgenommen würde, wenn die Akten tatsächlich nicht mehr benötigt werden.

5. Die Akteneinsicht im Gesundheitsamt

Wie weit muß ein Gesundheitsamt Bürgern reinen Wein darüber einschenken, was es in seinen Unterlagen über sie festhält? Die Antwort auf diese Frage bereitet Gesundheitsämtern hin und wieder Schwierigkeiten. Das zeigten uns einige Anfragen von Bürgern, die sich über das Auskunftsverhalten von Gesundheitsämtern beklagten. Klar ist, die Gesundheitsämter sind nach § 17 LDSG grundsätzlich verpflichtet, Auskunft über die Informationen zu geben, die sie über die Bürger besitzen. In welcher Form diese Auskunft erteilt wird, ist ihrem Ermessen überlassen. Sie können die Auskunft deshalb mündlich, schriftlich oder auch in der Weise erteilen, daß der Betroffene Einsicht in Akten nehmen kann oder Kopien aus Akten erhält. Eine Grenze müssen sie jedoch in jedem Fall beachten. Die Gesundheitsämter dürfen keine Auskunft geben, wenn die Informationen oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen überwiegender berechtigter Interessen eines Dritten geheimzuhalten sind. Als Dritte, deren Geheimhaltungsinteresse der Erteilung einer vollständigen Auskunft über den Akteninhalt entgegenstehen kann, kommen freilich allenfalls Angehörige, Bekannte oder sonstige Bezugspersonen des Betroffenen in Betracht, wenn sie dem Gesundheitsamt vertrauliche Informationen über diesen zur Verfügung gestellt haben. Dagegen kann, anders als dies hin und wieder geltend gemacht wird, von einem überwiegenden Geheimhaltungsinteresse des Arztes, der ein amtsärztliches Gutachten erstellt hat, nicht gesprochen werden und zwar auch dann nicht, wenn es um ein psychiatrisches Gutachten geht. Zwar haben Gerichte wiederholt entschieden, daß ein Patient, der psychiatrisch behandelt wurde, u.a. deshalb kein Recht auf Einsicht in über diese Behandlung geführte Krankenakten hat, weil ein Psychiater in der Regel seine Person in erheblichem Maße in die Behandlung einbringt, doch besteht zwischen solchen Krankenakten und psychiatrischen Gutachten des Gesundheitsamts ein entscheidender Unterschied: Anders als der Inhalt der Krankenakten ist ein Gutachten nämlich von vornherein dazu bestimmt, daß es nicht geheim bleibt, sondern außerhalb des Arzt-Patienten-Verhältnisses stehenden Personen und Stellen zugänglich gemacht wird.

Eine andere Frage ist, ob die Auskunft im wohlverstandenen Interesse des Betroffenen selbst verweigert werden darf. Dies ist jedoch nur eingeschränkt zulässig. Denn das Auskunftsrecht ist ein Ausfluß des durch Art. 2 Abs. 1 i.V. mit Art. 1 Abs. 1 des Grundgesetzes garantierten Rechts auf informationelle Selbstbestimmung. Ein Bürger, so verlangt es unsere Verfassung, muß danach wissen können, „wer was wann und bei welcher Gelegenheit über ihn weiß“. Auch verwehrt es dieses Recht dem Staat und damit auch dem Gesundheitsamt, den Bürger zu bevormunden

und ihm vorzuschreiben, was er im Interesse seines Eigenschutzes nicht zu wissen hat. Die Kehrseite der Medaille ist dann allerdings auch, daß er grundsätzlich die Risiken in Kauf nehmen muß, die ihm aus der Ausübung seines Selbstbestimmungsrechts erwachsen. Die Grenze ist jedoch dann erreicht, wenn und soweit die Gefahr besteht, daß der Betroffene durch die Auskunftserteilung zum Suizid veranlaßt wird oder zu befürchten ist, daß damit eine lebensbedrohende Verschlechterung seines Gesundheitszustands eintritt. In diesem Falle gebietet es die sich aus Art. 2 Abs. 1 des Grundgesetzes ergebende allgemeine Schutzpflicht des Staates seinen Bürgern gegenüber, die Auskunft zu verweigern.

6. Die Vorladung zum Gesundheitsamt

Anlaß, auf die begrenzten Aufgaben und Befugnisse eines Gesundheitsamts hinzuweisen, gab folgender Fall:

Ein Staatliches Gesundheitsamt im Regierungsbezirk Stuttgart forderte per Formularschreiben einen Bürger auf, auf Ersuchen des Bürgermeisteramts seiner Heimatgemeinde persönlich zu einer Rücksprache in das Gesundheitsamt zu kommen und dazu seinen Ausweis mitzubringen. Das Gesundheitsamt sah sich zu diesem Schritt veranlaßt, nachdem ihm das Bürgermeisteramt unter Beifügung von Schreiben des Bürgers mitgeteilt hatte, der Nachbar des Bürgers fühle sich durch diesen belästigt und bedroht, sein Verhalten weise nach seiner Auffassung krankhafte Züge auf. Der Bürger leistete der Aufforderung Folge und suchte zum angegebenen Zeitpunkt das Gesundheitsamt auf. Danach teilte dieses dem Bürgermeisteramt mit, es habe ihn im Gesundheitsamt amtsärztlich untersucht. Dabei habe es eine ausführliche psychiatrische Exploration durchgeführt. Diese habe ergeben, daß der Bürger unter einer psychischen Erkrankung leidet, die dringend behandelt werden sollte. Neben weiteren Informationen enthielt das Schreiben noch den Hinweis, daß die Einweisung nach dem Unterbringungsgesetz erwogen werden müsse, wenn sich in Zukunft Hinweise auf eine zunehmende Fremd- bzw. Selbstgefährdung ergäben.

Bei alledem lief einiges schief:

- Zum einen war das Gesundheitsamt nicht berechtigt, den Bürger von sich aus aufzufordern, beim Gesundheitsamt unter Vorlage seines Ausweises zu erscheinen und sich dort einer psychiatrischen Untersuchung zu unterziehen. Eine Rechtsgrundlage für ein solches Vorgehen gibt es nicht. Eine derartige Untersuchung muß ein Bürger nur hinnehmen, wenn die untere Verwaltungsbehörde sie gemäß § 5 des Unterbringungsgesetzes anordnet, weil dringende Gründe für die Annahme vorhanden sind, daß bei ihm die Voraussetzungen für eine Unterbringung vorliegen. In keinem Fall kann eine Gemeinde, die nicht untere Verwaltungsbehörde ist, eine solche Anordnung treffen. Ein Gesundheitsamt kann deshalb in solchen Fällen nur im Rahmen seiner allgemeinen Beratungsaufgabe tätig werden. Das bedeutet: Es kann dem Bürger seine Beratung anbieten. Da die Annahme eines Beratungsangebots aber freiwillig ist, muß ihn das Gesundheitsamt gemäß § 11 Abs. 2 LDSG über die Freiwilligkeit und den angestrebten Zweck informieren. Das aber hatte das Gesundheitsamt nicht getan.
- Unzulässig war aber auch, daß das Gesundheitsamt das Bürgermeisteramt über Einzelheiten des Untersuchungsergebnisses unterrichtete. Diese Unterrichtung war durch keine Rechtsvorschrift gedeckt. Sie wäre im übrigen auch dann zu weit gegangen, wenn ein rechtlich zulässiger Untersuchungsauftrag vorgelegen hätte. Denn auch in diesem Fall hätte sich das Gesundheitsamt auf das unbedingt Notwendige beschränken müssen und deshalb, nicht zuletzt wegen der gebotenen Wahrung der ärztlichen Schweigepflicht, nur mitteilen dürfen, daß die Voraussetzungen für eine Unterbringung gegenwärtig nicht gegeben sind.

Das Sozialministerium schloß sich auf unsere Beanstandung unserer rechtlichen Beurteilung an und teilte uns mit, daß es den Vorgang zum Anlaß für allgemeine Hinweise an die Gesundheitsämter nehmen werde.

Das Gesundheitsamt selbst und das Bürgermeisteramt haben inzwischen ihre Unterlagen über die unzulässige amtsärztliche Untersuchung vernichtet.

7. Telefax-Irrläufer – eine Fortsetzungsgeschichte ohne Ende?

Ein Privatmann aus Emmendingen staunte nicht schlecht: Kaum hatte er sein Telefaxgerät an dem neu geschalteten Anschluß in Betrieb genommen, spuckte es laufend Sendungen aus, die an ganz andere Empfänger gerichtet waren. Innerhalb weniger Wochen gelangten so Dutzende von Sendungen von unterschiedlichen Absendern an die falsche Adresse. Fehlgeleitet wurden unter anderem:

- Ein vom Zentrum für Psychiatrie Emmendingen (ZPE) abgesandtes ärztliches Zeugnis über eine durch Namen, Geburtsdatum und Wohnanschrift bezeichnete Person. Es bescheinigt der Person unter anderem eine „paranoide Psychose mit ausgedehntem Wahnsystem", Halluzinationen sowie „ein wechselhaftes, bisweilen ängstlich angepaßtes, dann wieder dysphorisch-drängend forderndes, untergründig angespanntes Affektverhalten".
- Eine von einem anderen Gerät des ZPE abgesandte Stellungnahme zum Behandlungsverlauf eines durch Namen und Geburtsdatum bezeichneten Patienten. Darin geht es um Vorstrafen, frühere Aufenthalte in psychiatrischer Behandlung und das Verhältnis des Patienten zur Bewährungshilfe. Ferner wird über die Entwicklung der Persönlichkeit während der mehrjährigen Unterbringungsdauer des Patienten berichtet.
- Eine von einem dritten Gerät des ZPE abgesandte Bitte um Untersuchung eines Patienten, dem eine „beginnende senile Demenz" attestiert wird. Das Schreiben zählt mehrere vermutete medizinische Befunde auf, deren tatsächliches Vorliegen im einzelnen geprüft werden soll.
- Ein von der AOK-Geschäftsstelle Emmendingen abgesandtes Schreiben, dem ein Strafbefehl angeschlossen war, der gegen zwei durch Namen, Geburtsdatum, Geburtsort, Familienstand und Wohnanschrift bezeichnete Personen wegen illegaler Beschäftigung eines namentlich genannten Ausländers ergangen war.
- Ein von einem anderen Telefaxgerät der AOK-Geschäftsstelle Emmendingen abgesandtes Protokoll einer Geschäftsstellenleiterbesprechung.
- Vom Finanzamt Emmendingen abgesandte Auszüge aus dem Steuerkonto eines durch Namen, Anschrift und Steuernummer bezeichneten Ehepaares, aus denen hervorgeht, wieviel Umsatzsteuer, Lohnsteuer, Solidaritätszuschlag und Kirchensteuer das Ehepaar zu unterschiedlichen Zeitpunkten schuldig war, wann einzelne Beträge fällig waren, wann Zahlungen in welcher Höhe eingingen sowie wann ausstehende Zahlungen gemahnt wurden.

Bei der Suche nach den Ursachen dieser Irrläufer stellten wir fest, daß die Telefaxgeräte, von denen aus die Irrläufer abgesandt wurden, jeweils an einer behördlichen Nebenstellenanlage angeschlossen waren. Will man von einem dieser Geräte ein Telefax absenden, so muß man vor der eigentlichen Telefaxnummer, nehmen wir einmal an, sie laute 01234/5678, stets noch eine zusätzliche „0", in unserem Beispielsfall also die Ziffern 0012345678, eintippen. Sie signalisiert der Nebenstellenanlage, daß diese eine Verbindung in das öffentliche Telefon- und Telefaxnetz bereitstellen soll, die gelegentlich auch als „Amtsleitung" bezeichnet wird. Wenn jemand nicht weiß, daß er eine zusätzliche „0" eingeben muß und zum Versand der Sendung lediglich die Nummer des Telefaxanschlusses, im obigen Beispiel also bloß 012345678, eintippt, hat dies fatale Folgen: In diesem Fall benutzt die Nebenstellenanlage die an führender Stelle stehende „0", um eine Verbindung ins öffentliche Netz bereitzustellen. Die „0" ist damit verbraucht und kann nicht mehr für den Aufbau der Verbindung im öffentlichen Netz benutzt werden. Sofern nun die restliche Rufnummer – im obigen Beispiel also die 12345678 – oder auch nur deren erste Ziffern mit einer Telefaxnummer im Ortsnetz

des Absenders übereinstimmt, wird die Telefaxsendung dorthin übertragen. Nach Lage der Dinge verursachte genau eine solche Fehlbedienung die Irrläufer in Emmendingen. Denn die Rufnummern der Empfänger, an die die Sendungen hätten gehen sollen, stimmten nach der führenden „0“ exakt mit der Rufnummer des Anschlusses überein, an den die Sendungen fehlgeleitet wurden. Zu diesem Massenaufgebot von Irrläufern hätte es nicht zu kommen brauchen, wenn die Stellen, die die Telefaxe abgeschickt haben, ihre Mitarbeiter und Mitarbeiterinnen ausreichend geschult und dabei gezielt auf die besonderen Datenschutzrisiken von an Nebenstellenanlagen angeschlossenen Telefaxgeräten hingewiesen hätten. Dies war indes nicht der Fall. Das ZPE hatte nicht einmal festgelegt, wer welche Daten wann per Telefax versenden darf. Auf unsere Beanstandung dieses Organisationsmangels reagierten ZPE, Finanzministerium und die AOK Baden-Württemberg sehr rasch und übernahmen unsere Empfehlungen.

Weil dieser Vorfall wieder einmal gezeigt hatte, daß der Versand von Telefaxen in der Behördenpraxis nach wie vor ein erhebliches Datenschutzrisiko darstellt, hat unser Amt die im Anhang 8 ersichtlichen Hinweise „Datensicherheit beim Telefax“ erarbeitet, die wir bei Bedarf jedem, der daran interessiert ist, zur Verfügung stellen.

4. Teil: Soziale Leistungen

1. Die Sozialversicherung

Die meisten unserer Bürger nehmen teil an den Segnungen der Sozialversicherung. Ihr Datenbedarf ist naturgemäß immens. Klar deshalb, daß der Datenschutz gerade in diesem Bereich besonders gefordert ist.

1.1 Zuviel gefragt

Wer hat nicht schon über einem amtlichen Vordruck gebrütet und sich gefragt, ob er wirklich alles angeben muß, was darin gefragt wird. Genauso erging es einem Bürger, der einen Antrag auf Rente aus der Alterssicherung der Landwirte gestellt hatte. Als Reaktion darauf hatte ihm nämlich die Landwirtschaftliche Krankenkasse Württemberg einen Meldebogen „zur Überprüfung der Kranken- und Pflegeversicherungspflicht für Antragsteller auf Rente aus der Alterssicherung der Landwirte“ ins Haus geschickt und ihn aufgefordert, den Vordruck vollständig auszufüllen. Weil er nicht einsehen wollte, wozu das alles gut sein soll, wandte er sich an uns und bat uns um Überprüfung. Nicht zu beanstanden war, daß ihn die Krankenkasse überhaupt zu einer Meldung aufgefordert hatte, denn jeder, der Rente aus der Alterssicherung der Landwirte beantragt, muß der Krankenkasse Meldung machen, damit sie überprüfen kann, ob er bei ihr versichert ist. Mängel wies jedoch der eingesetzte Meldebogen auf: Zugegeben, Vordrucke entwerfen und ausgestalten ist eine hohe Kunst. Weil sich Vordrucke meist für eine Vielzahl von Fallgestaltungen eignen sollen, besteht die Gefahr, daß Angaben, die nur bei einer bestimmten Fallgestaltung benötigt werden, auch dann erfragt werden, wenn sie für den angegebenen Zweck ohne Bedeutung sind. Genau dieser Gefahr war die Landwirtschaftliche Krankenkasse erlegen, als sie ihren Vordruck konzipierte. Weil Antragsteller auf Rente aus Alterssicherung der Landwirte in den meisten Fällen bei der Landwirtschaftlichen Kranken- und Pflegekasse pflichtversichert sind, begnügte sie sich nicht damit, zunächst einmal nur die Angaben zu erfragen, die sie für die Prüfung der Versicherungspflicht benötigt, sondern wollte auch schon Dinge wissen, die sie erst dann und nur dann wissen muß, wenn die Versicherungspflicht festgestellt ist. Insbesondere sollten die Rentenantragsteller der Krankenkasse schon zu diesem Zeitpunkt detailliert ihr für die Bemessung des Beitrags maßgebliches monatliches Einkommen offenlegen, unabhängig davon, ob eine Mitgliedschaft und damit eine Beitragspflicht besteht oder nicht. Deshalb war die Verärgerung unseres Bürgers jedenfalls insoweit durchaus berechtigt, denn bei ihm war klar, daß er nicht Mitglied ist.

Noch einen weiteren, leider sehr häufig vorkommenden Mangel mußten wir kritisieren. Die bei der Zusendung des Meldebogens gemachten Hinweise darüber, für welchen Zweck die Angaben erfragt wurden, ob eine Auskunftspflicht besteht und, wenn ja, aufgrund welcher Rechtsvorschrift, waren viel zu ungenau und teilweise auch widersprüchlich. Aber immerhin: Nach unserer Beanstandung sagte die Landwirtschaftliche Krankenkasse Remedur zu. Im Meldebogen wird sie künftig die Rentenantragsteller zunächst einmal nur nach den für die Mitgliedschaft maßgebenden Angaben fragen und ihrer Hinweispflicht nach § 67 a Abs. 3 SGB X korrekt nachkommen.

1.2 Grau ist alle Theorie

Gesetzliche Regelungen zu beschließen, ist eine Sache, eine andere, sie in die Praxis umzusetzen. Dies zeigen einmal mehr die Probleme, die bei der Umsetzung der Regelungen des Gesundheitsreformgesetzes 1989 und des Gesundheitsstrukturgesetzes 1993 auftreten, mit denen eine Kostendämpfung durch verstärkten Einsatz der automatisierten Datenverarbeitung bewirkt werden sollte. Dafür zwei Beispiele:

1.2.1 Noch einmal: Der Datenaustausch zwischen KV/KZV und den Krankenkassen

Seit 1. Jan. 1993 sind die Kassenärztlichen Vereinigungen (KVen) und die Kassenzahnärztlichen Vereinigungen (KZVen) nach § 295 Abs. 2 SGB V verpflichtet, den Krankenkassen bei der Abrechnung der Vergütung die für die vertragsärztliche Versorgung erforderlichen Angaben über die abgerechneten Leistungen nur fallbezogen, nicht versichertenbezogen, zu übermitteln. Nach der Intention des Gesetzgebers sollte diese Forderung mit Hilfe der automatisierten Datenverarbeitung realisiert werden. Die Einzelheiten dieses elektronischen Datenaustausches sollten die Spitzenverbände der Krankenkassen mit der Kassenärztlichen Bundesvereinigung bzw. der Kassenzahnärztlichen Bundesvereinigung vereinbaren. Dieser Austausch findet indes bis heute nicht statt. Ein Grund dafür war, darauf haben wir schon im 16. Tätigkeitsbericht unseres Amtes (LT-Drs. 11/6900, S. 62 ff.) hingewiesen, daß sich die Spitzenverbände der Krankenkassen und die Kassenzahnärztliche Bundesvereinigung nicht darüber einigen konnten, welche Daten die KZVen den Krankenkassen zur Verfügung stellen sollen. Zwar hatte daraufhin das Bundesschiedsamt für die Vertragszahnärztliche Versorgung eine Vereinbarung angeordnet, doch trug diese der Forderung des § 295 Abs. 2 SGB V, wonach die Krankenkasse nur die für die Abrechnung erforderlichen Daten und auch nur fallbezogen und nicht versichertenbezogen erhalten dürfen, nur schwerlich Rechnung. Deshalb ist es aus der Sicht des Datenschutzes zu begrüßen, daß sich die zunächst sehr kontroversen Standpunkte der Spitzenverbände der Krankenkassen auf der einen und der Kassenzahnärztlichen Bundesvereinigung auf der anderen Seite inzwischen nicht zuletzt auf Drängen der Datenschutzbeauftragten des Bundes und der Länder weitgehend angenähert haben. Dies läßt hoffen, daß es zu einer erheblichen Reduzierung des Datensatzes kommen wird, den die KZVen den Krankenkassen zur Verfügung stellen müssen. Würde dies erreicht, würde dies bedeuten, daß es für die Krankenkassen kaum noch möglich wäre, im Einzelfall festzustellen, welche zahnärztlichen Leistungen ein bestimmter Versicherter in Anspruch genommen hat. Genau dieses will aber § 295 Abs. 2 SGB V sicherstellen. Um etwaigen Mißverständnissen vorzubeugen: Die Möglichkeit, nach Maßgabe der Bestimmungen des SGB V Wirtschaftlichkeitsprüfungen durchzuführen und in diesem Zusammenhang auch konkrete Einzelfälle daraufhin zu überprüfen, ob eine zahnärztliche Leistung notwendig und wirtschaftlich erbracht worden ist, würde dadurch in keiner Weise eingeschränkt.

1.2.2 Der ICD-10-Schlüssel

Die Absicht des Bundesgesundheitsministeriums, mit einer ebenfalls im Gesundheitsstrukturgesetz 1993 getroffenen Festlegung im Jahr 1996 Ernst zu machen, führte zu zahlreichen Beschwerdeschreiben, Anfragen und Anrufen in unserem Amt. Danach sollten nämlich die Kassenärzte Diagnosen auf den Krankenscheinen und den für die Krankenkassen bestimmten Arbeitsunfähigkeitsbescheinigungen nach dem vierstelligen Schlüssel der Internationalen Klassifikation der Krankheiten (ICD) in der jeweils im Auftrag des Bundesgesundheitsministeriums herausgegebenen Fassung verschlüsseln und nicht mehr, wie bis dahin üblich, diese Angaben frei formulieren. Die Verschlüsselung sollte nicht etwa, wie manche Beschwerdeführer offenbar meinten, eine Geheimhaltung der Diagnosen sicherstellen; dafür wäre sie von vornherein völlig ungeeignet gewesen, weil die ICD-Schlüssel-Klassifikation ja jedermann zugänglich ist. Der Gesetzgeber wollte vielmehr damit erreichen, daß die Ärzte die von

ihnen diagnostizierten Krankheiten mit denselben Begriffen bezeichnen. Eine solche Standardisierung ist wiederum eine Grundvoraussetzung für den Einsatz automatisierter Verfahren für die Abrechnung und bei Wirtschaftlichkeitsprüfungen, bei denen die die ärztlichen Leistungen auslösenden Diagnosen einbezogen werden. Auf einen kurzen Nenner gebracht kann man sagen: Ohne Standardisierung der Diagnosen wären die Bemühungen des Gesetzgebers, in der gesetzlichen Krankenversicherung moderne Abrechnungsverfahren zu installieren sowie mit Hilfe des Computers das Leistungs- und Kostengeschehen transparent zu machen und sich so Lenkungsmöglichkeiten zu verschaffen, von vornherein weitgehend zum Scheitern verurteilt. Als das Bundesgesundheitsministerium im Jahr 1995 die vierstellige ICD-10-Klassifikation im Bundesanzeiger bekanntgab und dabei anordnete, daß diese ab 1. Jan. 1996 für die Kassenärzte maßgebend sein soll, zeigte sich sehr schnell eines: Beim Erlaß des Gesundheitsstrukturgesetzes im Jahr 1992 hatte der Gesetzgeber nicht hinreichend geprüft, ob diese Klassifikation, die von der Weltgesundheitsorganisation (WHO) für wissenschaftliche Zwecke entwickelt worden ist, auch für den ihr vom Gesetzgeber zugedachten Zweck geeignet ist. Für manche Diagnosen gibt es gar keine Schlüssel, andere sind in einem Maße differenziert, wie es für die gesetzliche Krankenversicherung überhaupt nicht erforderlich ist. Die Ärzte hätten damit den Kassenärztlichen Vereinigungen bzw. Krankenkassen in vielen Fällen präzisere und detailliertere Diagnoseangaben mitteilen müssen als bisher. Auf der anderen Seite sieht das ICD-10-Schlüsselverzeichnis keine Schlüssel für von den Ärzten bisher benutzte Zusätze wie „V“ = „Verdacht auf“ oder „A“ = „Ausschluß von“ vor. Eine buchstabengetreue Umsetzung hätte deshalb zur Speicherung unrichtiger Daten über Versicherte führen können. Mit einem Satz: Das ICD-10-Schlüsselverzeichnis war so, wie es veröffentlicht und für verbindlich erklärt worden war, nur sehr bedingt für den angestrebten Zweck geeignet und hätte zu unverhältnismäßigen Ergebnissen führen können. Nachdem die Proteste auch im politischen Raum immer stärker wurden, zogen Bundesgesundheitsministerium, Kassenärztliche Bundesvereinigung und die Spitzenverbände der Krankenkassen die Notbremse. Sie vereinbarten, das ICD-10-Schlüsselverzeichnis so zu überarbeiten, daß ein Übermaß an Regelungen vermieden wird und die Ausgestaltung so erfolgt, daß die praktische Anwendbarkeit und die Akzeptanz für alle Beteiligten sichergestellt sind. Die so überarbeitete Fassung soll in der ersten Jahreshälfte des Jahres 1997 in der Praxis erprobt und bei Bewährung ab 1. Jan. 1998 für verbindlich erklärt werden. Bis dahin bleibt es den Ärzten überlassen, wie sie die Diagnose formulieren. Auf Arbeitsunfähigkeitsbescheinigungen sollen die Ärzte in jedem Fall die Diagnose im Klartext angeben. Es bleibt abzuwarten, wie die überarbeitete Version des ICD-10-Schlüsselverzeichnisses aussehen wird und ob sie das hält, was man sich von ihr erhofft.

1.3 Die Methadon-Substitution

Bisher hat noch niemand den Stein der Weisen für den Umgang mit Drogenabhängigen gefunden. Ein Lösungsweg besteht darin, dem Abhängigen Substitutionsmittel an die Hand zu geben, um so zu versuchen, ihm das Leben wenigstens einigermaßen erträglich zu gestalten. Freilich kann dies nur nach strengen Regeln geschehen, die sicherstellen müssen, daß die mit der Substitution angestrebten Behandlungsziele tatsächlich auch erreicht werden. Dazu existieren derzeit zwei Regelungsbereiche: Zum einen muß ein Arzt, der bei einem Patienten eine Substitutionsbehandlung durchführen will, die vom Bundesausschuß der Ärzte und Krankenkassen dazu erlassenen Richtlinien über die Einführung neuer Untersuchungs- und Behand-

lungsmethoden (NUB-Richtlinien) beachten. Danach muß er Beginn und Beendigung einer Substitutionsbehandlung und beabsichtigte oder bereits eingeleitete psychologische Begleitmaßnahmen sowohl seiner Kassenärztlichen Vereinigung als auch der Krankenkasse des Patienten anzeigen. Zuvor muß der Substitutionspatient jeweils seine schriftliche Einwilligung in die Datenweitergabe geben. Unabhängig davon enthält aber auch die Betäubungsmittelverschreibungsverordnung Regelungen, an die sich ein Arzt bei der Substitution im Rahmen der Behandlung einer Betäubungsmittelabhängigkeit zu halten hat. Danach muß er u.a. jeden Substitutionspatienten und die dabei nach der Betäubungsmittelverschreibungsverordnung zu ergreifenden Maßnahmen dem jeweiligen Regierungspräsidium mitteilen. Dies bedeutet: Ein Arzt, der Substitutionsbehandlungen durchführt, muß im wesentlichen den gleichen Sachverhalt einmal seiner Kassenärztlichen Vereinigung und der Krankenkasse und zum anderen dem Regierungspräsidium teils mit, teils ohne Einwilligung des Patienten mitteilen. Diese Doppelgleisigkeit führt im Ergebnis dazu, daß sowohl bei den Kassenärztlichen Vereinigungen und den Krankenkassen als auch bei den Regierungspräsidien höchst sensible Datensammlungen entstehen und zudem der dabei entstehende bürokratische Aufwand nicht gerade geeignet ist, die Bereitschaft von Ärzten zur Durchführung solcher Behandlungen zu fördern. Aus diesem Grund haben wir schon im Jahre 1993 gegenüber dem Sozialministerium angeregt, für eine Harmonisierung zu sorgen. Die derzeit in Gang befindlichen Bestrebungen, die Substitutionsbehandlung in der Betäubungsmittelverschreibungsverordnung neu zu regeln, sollten zum Anlaß genommen werden, diese Frage erneut aufzugreifen und nach Regelungen zu suchen, die einerseits dem angestrebten Ziel, nämlich nicht gerechtfertigte und Mehrfachsubstitutionen zu verhindern, gerecht werden und auf der anderen Seite das auch Substitutionspatienten zustehende Recht auf Datenschutz besser als die bisherigen unkoordiniert nebeneinander stehenden Regelungen berücksichtigen.

1.4 Kostenerstattung beim Schwangerschaftsabbruch

Bei der Neuregelung des Schwangerschaftsabbruchs im Jahr 1995 war es dem Gesetzgeber ein wichtiges Anliegen, schwangeren Frauen den Weg zum Sozialamt zu ersparen. Deshalb bestimmte das Gesetz zur Hilfe für Frauen bei Schwangerschaftsabbrüchen in besonderen Fällen vom 21. Aug. 1995 (BGBl. I, S. 1054), daß sich die Frauen, denen die Aufbringung der Mittel für einen nicht rechtswidrigen oder nach § 218 a Abs. 1 StGB straffreien Schwangerschaftsabbruch nicht zuzumuten ist, an ihre Krankenkasse wenden und von ihr die Übernahme der Kosten verlangen können. Diese Kosten muß das Land dann der Krankenkasse erstatten. Bei diesem Verfahren ist, so verlangt es § 3 Abs. 5 dieses Gesetzes ausdrücklich, das Persönlichkeitsrecht der Frau unter Berücksichtigung der besonderen Situation der Schwangerschaft zu achten. Um dies sicherzustellen, setzten wir uns gegenüber dem Sozialministerium dafür ein, daß

- die schwangere Frau im Kostenübernahmeantrag an die Krankenkassen korrekt und verständlich über ihre Rechtsstellung informiert wird,
- die Ärzte, anders als zunächst vorgesehen, direkt und nicht über die Kassenärztliche Vereinigung mit der Krankenkasse abrechnen, weil es keine Rechtsvorschrift gibt, die die Weitergabe der Abrechnungsdaten an die Kassenärztliche Vereinigung zuläßt und für die Einschaltung dieser Stelle auch keine Notwendigkeit besteht,
- das Landesversorgungsamt, das in Baden-Württemberg den Krankenkassen die Kosten zu erstatten hat, nur Einblick in die Unterlagen nehmen und damit Kenntnis vom Namen der Schwangeren erhalten darf, wenn Anhaltspunkte für Unregelmäßigkeiten gegeben sind und
- die Krankenkassen exakte Festlegungen darüber treffen, wann die Unterlagen, die Aufschluß darüber geben können, bei welchen Frauen Schwangerschaftsabbrüche vorgenommen wurden, zu vernichten sind.

Das Sozialministerium reagierte erfreulich. Es akzeptierte unsere Vorschläge uneingeschränkt.

1.5 Steuerakten auf Abwegen

Einigermaßen überrascht war ein Bürger, der mit einer Krankenkasse einen Rechtsstreit wegen der Erhebung von Beiträgen führte, als das Sozialgericht Mannheim der Krankenkasse über ihn geführte Steuerakten des Finanzamts Mosbach zuleitete, die mit dem besten Willen nichts mit der Klärung der im Rechtsstreit strittigen Frage zu tun hatten. „Es erscheint daher schon verwunderlich, daß das Finanzamt keinerlei Bedenken hatte, diese Akten dem Gericht vollständig vorzulegen, bedenkt man den 'Eiertanz', der sonst um das Steuergeheimnis gemacht wird“, meinte unser Bürger und das mit Recht. Denn wie sich bei der Überprüfung herausstellte, hatte das Finanzamt außer acht gelassen, daß sich die ihm vom Sozialgericht mitgeteilte Einwilligungserklärung des Bürgers nur auf die Vorlage ganz bestimmter Steuerakten erstreckte und auch das Ersuchen des Sozialgerichts um Übersendung auf ganz bestimmte Akten beschränkt war. Das Finanzamt räumte die Verletzung des Steuergeheimnisses, die wir gegenüber dem Finanzministerium beanstandet haben, im wesentlichen ein. Dies sei ein durch eine Umstellung der Aktenorganisation bedingtes Versehen gewesen. Ganz überzeugte uns dieses Argument nicht. Denn mehr als die konkret vom Sozialgericht angeforderten Akten hätte es in keinem Fall weitergeben dürfen. Auf die durchaus verständliche Frage des Bürgers, ob denn das Sozialgericht von der Weiterleitung sämtlicher vom Finanzamt vorgelegten Steuerakten an die Krankenkasse hätte Abstand nehmen müssen, mußten wir uns mit dem Hinweis darauf begnügen, daß die Datenverarbeitung von Gerichten, wenn sie wie hier im Rahmen eines gerichtlichen Verfahrens stattfindet, nicht unserer Kontrolle unterliegt.

1.6 Die Unfallversicherung und der Arbeitgeber

Durchaus berechtigt war das Ansinnen, das eine Gemeinde an den Württembergischen Gemeindeunfallversicherungsverband (WGUV) richtete. Sie wollte nämlich von dem Verband, bei dem die Mitarbeiter der Kommunen in den Regierungsbezirken Tübingen und Stuttgart gegen Dienstunfälle und Berufskrankheiten versichert sind, wissen, ob die Erkrankung einer Mitarbeiterin der Gemeinde, die er als Berufskrankheit anerkannt hatte, Folge der Verwendung bestimmter Putzmittel einer Einrichtung der Gemeinde war, in der sie tätig gewesen war. Immerhin ging es dabei darum, zu klären, ob die Gemeinde zum Schutz der Kolleginnen und Kollegen der Mitarbeiterin Vorsorgemaßnahmen treffen muß, damit diese nicht auch erkranken. Wie der WGUV diese Anfrage beantwortete, ging dann allerdings um einiges zu weit. Anstatt sich darauf zu beschränken, der Gemeinde mitzuteilen, daß für solche Maßnahmen kein Anlaß besteht, gab er ihr detaillierte Auskünfte über den Gesundheitszustand der Mitarbeiterin. Dazu war der WGUV aber in keinem Fall berechtigt, denn eine Befugnis, diese Informationen, die der WGUV von Ärzten erhalten hatte und deshalb in der gleichen Weise wie ein Arzt geheimhalten muß, der Gemeinde mitzuteilen, gab es nicht. Gleichwohl wies der WGUV unsere Beanstandung zurück und zwar mit der Begründung, seine Auskünfte über die Erkrankung der Mitarbeiterin seien in der Gemeinde bereits zuvor bekannt gewesen, deshalb sei kein Datenschutzverstoß gegeben. Dies war in doppelter Hinsicht unzutreffend: Zwar lag der Gemeinde in der Tat bereits ein ärztliches Attest mit einer Diagnoseangabe vor, doch waren die Informationen im Auskunftsschreiben des WGUV wesentlich detaillierter und sagten mehr aus, als im Attest zu lesen war. Zudem hätte der WGUV nach den Bestimmungen zum Schutz des Sozialgeheimnisses auch Informationen, die der Gemeinde bereits bekannt waren, nur mitteilen dürfen, wenn dies zur Erfüllung seiner Aufgaben erforderlich gewesen wäre. Dies war jedoch nicht der Fall.

2. Sozial- und Jugendhilfe

2.1 Ohne Daten kein Geld

„Sollten Sie unserem Auskunftsersuchen nicht nachkommen, so behalten wir uns eine Überprüfung Ihres Anspruchs auf Begleichung der Heimkosten vor. Wir haben Ihnen mit Schreiben vom ... eine Frist bis zum ... gesetzt – dabei bleibt es!“

Mit solch drastischen Worten verlieh der Landeswohlfahrtsverband Württemberg-Hohenzollern seiner Forderung an ein Behindertenheim Nachdruck, ihn über den exakten Stand des Taschengeldguthabens eines behinderten Heimbewohners zu informieren. Dies obwohl das Heim ihm zuvor mitgeteilt hatte, daß das Taschengeldguthaben des behinderten Sozialhilfeempfängers unterhalb der Freigrenze des § 88 Abs. 2 Nr. 8 des Bundessozialhilfegesetzes (BSHG) von 4.500 DM liegt, ab der es bei der Leistung von Sozialhilfe einzusetzen ist. Damit nicht genug; nachdem das Behindertenheim seiner Forderung nicht innerhalb der gesetzten Frist nachgekommen war, sondern statt dessen uns um eine Überprüfung gebeten hatte, machte der Landeswohlfahrtsverband seine Drohung auch wahr und stellte die Zahlung ein.

Mit seiner ultimativen Aufforderung an das Behindertenheim, ihm die exakte Höhe des Taschengeldguthabens des Heimbewohners mitzuteilen, verstieß der Landeswohlfahrtsverband gleich mehrfach gegen den Datenschutz.

- Will, wie hier, der Landeswohlfahrtsverband in seiner Eigenschaft als überörtlicher Träger der Sozialhilfe die Angaben über die Einkommens- und Vermögensverhältnisse eines Sozialhilfeempfängers statt bei diesem selbst bei einem Dritten, in unserem Fall also beim Behindertenheim, erfragen, dann muß er dabei nach § 67 a Abs. 4 SGB X beim Bestehen einer Auskunftspflicht auf die Rechtsvorschrift, die zur Auskunft verpflichtet, sonst auf die Freiwilligkeit der Angaben hinweisen. Da eine Rechtsvorschrift, die ein Heim, in dem ein behinderter Sozialhilfeempfänger wohnt, zur Auskunft über die Vermögensverhältnisse des Heimbewohners verpflichtet, nicht existiert, hätte der Landeswohlfahrtsverband demzufolge das Heim darauf hinweisen müssen, daß die gewünschte Auskunft freiwillig ist. Statt dessen behauptete der Landeswohlfahrtsverband, das Heim sei zur Auskunft verpflichtet, ohne anzugeben, woraus sich diese Verpflichtung ergeben soll, und verlieh seiner Aufforderung sogar durch Einstellung der Sozialhilfeleistung zusätzlich Nachdruck.
- Das Vorgehen des Landeswohlfahrtsverbands stand aber auch deshalb nicht mit dem Datenschutz in Einklang, weil er zuviel wissen wollte. Denn für die Sozialhilfegewährung durch den Landeswohlfahrtsverband war nur wichtig zu wissen, ob der behinderte Heimbewohner mehr als 4 500 DM Barvermögen besitzt und, wenn ja, wieviel. Dazu hatte ihm aber das Heim schon mitgeteilt, daß das Taschengeldguthaben diese Grenze nicht übersteigt. Anhaltspunkte dafür, daß der Heimbewohner sonstiges, für die Feststellung der Freigrenze relevantes Geldvermögen besitzt, gab es nicht. Weil der Landeswohlfahrtsverband gleichwohl die exakte Höhe des Taschengeldguthabens und damit mehr, als er zur Bewilligung der Sozialhilfeleistung benötigte, wissen wollte, stand dies nicht in Einklang mit § 67 a Abs. 1 SGB X.

Auf unsere Beanstandung bedauerte der Landeswohlfahrtsverband die Behandlung des Einzelfalls gegenüber dem Heim und sagte zu, daß er die Heime in Zukunft korrekt über ihre Rechtsstellung bei der Beantwortung von Anfragen unterrichten will. Nach wie vor hält er sich aber für berechtigt, jeweils den genauen Stand des Taschengeldguthabens zu erfragen, ein Vorgehen, das jedoch nur dann gerechtfertigt ist, wenn konkrete Anhaltspunkte dafür vorliegen, daß weiteres Geldvermögen vorhanden ist.

2.2 Schlechte Karten für den Datenschutz
Auf dem Gebiet der Sozialhilfe hat der Datenschutz beim Gesetzgeber keine guten Karten:

2.2.1 Auf ein neues: Der automatisierte Datenabgleich
Angesichts der Ebbe in den öffentlichen Kassen ist es sicher legitim und notwendig, verstärkt dafür Sorge zu tragen, daß jeder nur die Sozialleistungen erhält, die ihm von Rechts wegen zustehen. Zumal wenn es um die Sozialhilfe geht, stoßen deshalb Kontrollmaßnahmen auf allgemeines Verständnis. Bei alledem sollte freilich darauf geachtet werden, daß auch Sozialhilfeempfänger Menschen sind, die Anspruch darauf haben, daß man sie als selbstverantwortliche Bürger behandelt und nicht von vornherein ihre Glaubwürdigkeit in Zweifel zieht. Darauf hatte unser Amt bereits im 14. Tätigkeitsbericht (LT-Drs. 11/2900, S. 20 ff.) hingewiesen und die mit dem Gesetz zur Umsetzung des Föderalen Konsolidierungsprogramms (FKPG) vom 23. Juni 1993 (BGBl. I, S. 944) in das Bundessozialhilfegesetz (BSHG) aufgenommenen Regelungen über automatisierte Datenabgleiche zu Kontrollzwecken kritisiert. Daß wir mit unserer damaligen Kritik an der Notwendigkeit solcher Abgleiche offensichtlich nicht so falsch lagen, zeigt sich daran, daß die damals zugelassenen automatisierten Datenabgleiche nach § 117 Abs. 1 und 2 BSHG bis heute nicht vorgenommen werden können, weil die dazu notwendigen Durchführungsverordnungen noch nicht erlassen sind und derzeit auch nicht abzusehen ist, bis wann dies der Fall sein wird. Um so verwunderlicher ist, daß der Gesetzgeber in der Sozialhilfe weiter auf die Karte automatisierter Datenabgleiche setzt. Denn neben den vielen anderen teilweise in der Öffentlichkeit sehr umstrittenen Regelungen ließ das Gesetz zur Reform des Sozialhilferechts vom 23. Juli 1996 (BGBl. I, S. 1088) einen weiteren solchen Abgleich zu. Während bisher die Sozialämter auf der Grundlage des § 117 Abs. 3 BSHG im Einzelfall, wenn es Anhaltspunkte für Unrichtigkeiten gab, bei anderen Stellen innerhalb eines Landrats- oder Bürgermeisteramts und auch bei anderen Gemeinden und wirtschaftlichen Unternehmen der Kommunen Auskunft darüber anfordern durften, seit wann ein Mietverhältnis mit dem Sozialhilfeempfänger besteht, wie hoch die Miete ist, was er an Strom, Gas, Wasser oder Fernwärme bezieht, wie er es mit der Abfallentsorgung hält und ob er Halter eines Kraftfahrzeugs ist, ist es künftig im Wege des automatisierten Abgleichs bei jedem Sozialhilfeempfänger möglich, diese Angaben abzufragen. Unsere Bitte an das Sozialministerium, im Bundesrat darauf hinzuwirken, daß diese dem Grundsatz der Verhältnismäßigkeit widersprechende Regelung nicht Gesetz wird, hatte leider keinen Erfolg.

2.2.2 Die überflüssige Aktivität
Nicht der Absicht, Mißbräuche zu verhindern, sondern eher dem Perfektionsstreben von Sozialämtern dürfte die ebenfalls im Gesetz zur Reform des Sozialhilferechts beschlossene Ausweitung der Auskunftspflichten Dritter auf dem Gebiet der Sozialhilfe zu verdanken sein. Während bis dahin § 116 BSHG nur die Unterhaltspflichtigen eines Sozialhilfeempfängers zu Auskünften über ihre Einkommens- und Vermögensverhältnisse verpflichtete, damit das Sozialamt feststellen kann, ob es von ihm geleistete Sozialhilfe vom Unterhaltspflichtigen zurückfordern kann, muß künftig auch dessen Ehegatte diese Angaben dem Sozialamt offenlegen. Damit einhergehend muß auch der Arbeitgeber des Ehegatten, wenn das Sozialamt es so will, diesem bekanntgeben, was und wie lange der Ehegatte schon bei ihm arbeitet und was er verdient. Damit korrigierte der Gesetzgeber die Rechtsprechung des Bundesverwaltungsgerichts; denn dieses

hatte zum Unwillen der Sozialämter und entgegen einer bis dahin weitverbreiteten Praxis entschieden, daß ein Sozialamt diese Angaben nur auf freiwilliger Basis vom Unterhaltspflichtigen anfordern darf. Für diese Korrektur bestand keine Notwendigkeit. Denn die Einkommens- und Vermögensverhältnisse des Ehegatten des Unterhaltspflichtigen sind für das Sozialamt nur von Bedeutung, soweit sich aus ihnen ergibt, daß auch der Ehegatte einen Unterhaltsanspruch gegen den Unterhaltspflichtigen besitzt. Ist dies der Fall, mindert sich nämlich dessen Unterhaltsverpflichtung gegenüber dem Sozialhilfeempfänger und damit auch die Möglichkeit des Sozialamts, Ersatz für die geleistete Sozialhilfe zu erhalten. Dies geltend zu machen, sollte aber dem Unterhaltspflichtigen und seinem Ehegatten überlassen bleiben. Da beide in aller Regel daran interessiert sind, dem Sozialamt so wenig wie möglich zurückzuerstatten, werden sie diesem die dazu notwendigen Angaben auch freiwillig zur Verfügung stellen, wenn sie das Sozialamt hinreichend deutlich über diese Zusammenhänge unterrichtet. Leider blieb unsere Intervention beim Sozialministerium auch in diesem Punkt ohne Erfolg.

2.3 Die Generalvollmacht für das Jugendamt

Das Datenschutzrecht erlaubt das Sammeln, Speichern, Ändern, Nutzen, Weitergeben und Löschen von persönlichen Daten in jedem Fall dann, wenn derjenige, um dessen Daten es geht, dazu seine Einwilligung gibt. Deshalb nehmen viele Behörden vorsorglich Einwilligungserklärungen in ihre Antragsvordrucke auf in der Annahme, damit im Falle eines Falles gewissermaßen auf der sicheren Seite zu stehen und sich bei Bedarf darauf berufen zu können, daß der Antragsteller mit der Unterschrift unter den Antrag ja sein Einverständnis erklärt hat. Sie verkennen dabei freilich oft, daß das Datenschutzrecht gewisse Anforderungen an das Vorliegen einer wirksamen Einwilligung stellt und beachten dies häufig nicht. Deshalb zählen Fehler bei der Einholung von Einwilligungen zu den Mängeln, die wir am häufigsten in unserer Kontrollpraxis feststellen müssen. Ein Beispiel dafür war dem Antragsvordruck zu entnehmen, den ein Kreisjugendamt für die Gewährung von Erziehungshilfe nach dem Jugendhilfegesetz (SGB VIII) einsetzte. Mit seiner Unterschrift unter den Antrag mußte der Antragsteller u.a. folgende, im Antragsvordruck aufgeführte Erklärung akzeptieren:

„Ich stimme/Wir stimmen zu, daß vom Jugendamt benötigte Auskünfte von Dritten eingeholt werden dürfen. Ich habe/Wir haben davon Kenntnis genommen, daß es als Voraussetzung für die Entscheidung für meinen/unseren Antrag auf Gewährung der Hilfe und für die Durchführung der Hilfe erforderlich ist, daß das Jugendamt personenbezogene Daten erhebt, verarbeitet (u.a. auch speichert), verwendet und weitergibt. Hiermit erkläre ich mich/erklären wir uns einverstanden. Ärzte und Psychologen entbinde ich/entbinden wir gegenüber dem Jugendamt für die Dauer der Hilfestellung von der Schweigepflicht."

Diese Erklärung war in mehrfacher Hinsicht mit dem Datenschutzrecht nicht vereinbar:

– Zu weit ging es, daß sich das Jugendamt damit pauschal die Zustimmung dazu verschaffen wollte, Auskünfte bei Dritten einzuholen. Denn nach § 62 Abs. 2 und 3 SGB VIII muß das Jugendamt sich grundsätzlich an den Betroffenen selbst wenden, wenn es über ihn Informationen erhalten will und darf nur ausnahmsweise diese Angaben bei Dritten erfragen. Diese zum Schutz des Selbstbestimmungsrechts der Betroffenen getroffene Regelung wurde durch das Vorgehen des Jugendamtes konterkariert, zumal der Vordruck so ausgestaltet war, daß ein Antragsteller gar keine Möglichkeit hatte, den Antrag zu stellen, ohne die Zustimmungserklärung abzugeben. Hinzu kam, daß die Erklärung so allgemein gehalten war, daß der Antragsteller gar nicht übersehen konnte, welche Tragweite seine Zustimmung hat. Eine

Einwilligungserklärung ist aber nur dann wirksam, wenn sie so bestimmt ist, daß der Erklärende erkennen kann, welche Folgen sich für ihn aus der Erklärung ergeben können.

– Nicht akzeptabel war, daß sich die Antragsteller mit der Stellung des Antrags damit einverstanden erklären sollten, daß das Jugendamt „personenbezogene Daten erhebt, verarbeitet (u.a. auch speichert), verwendet und weitergibt". Für die Einholung einer solchen Erklärung besteht nämlich keinerlei Notwendigkeit. Ein Jugendamt kann und muß auch ohne Einwilligung die zur Entscheidung über den Antrag und die Durchführung der Hilfe notwendige Erhebung, Nutzung und Verarbeitung von Daten nach Maßgabe der Bestimmungen des Sozialgesetzbuchs vornehmen. Wenn es gleichwohl den Antragsteller auffordert, eine Einwilligungserklärung abzugeben, kann bei ihm der irrige Eindruck entstehen, er könne darüber selbst entscheiden. Behörden sollten deshalb Einwilligungen grundsätzlich nur einholen, wenn sie diese tatsächlich benötigen.
– Nicht wirksam war auch die Erklärung über die Entbindung von Ärzten und Psychologen von ihrer Schweigepflicht. Auch sie war viel zu unbestimmt, weil aus ihr nicht hervorging, welche Ärzte oder Psychologen zur Herausgabe welcher Patientendaten berechtigt werden sollten.
– Fehlerhaft war schließlich, daß der Antragsvordruck entgegen § 67 b Abs. 2 SGB X keinen Hinweis darauf enthielt, welche Folgen es für den Antragsteller hat, wenn er die geforderte Einwilligung verweigert.

Das Kreisjugendamt sagte auf unseren Hinweis auf diese Mängel zu, daß es die von uns dargelegte Rechtslage künftig beachten will.

2.4 Der Investitionszuschlag

Welche Konsequenzen es haben kann, wenn beim Erlaß von Regelungen der Datenschutz außer acht gelassen wird, zeigt sich sehr anschaulich am Beispiel des Investitionszuschlags, den Pflegedienste nach § 15 des Landespflegegesetzes vom 22. Sept. 1995 (GBl. S. 665) erhalten sollen. Die Höhe dieses Zuschlags bemißt sich, so sieht es die Verordnung des Sozialministeriums über die Gewährung des Investitionszuschlags bei Pflegediensten vom 10. Mai 1996 (GBl. S. 381) vor, nach der Zahl der Hausbesuche. Dabei können mehr als drei Hausbesuche pro Tag berücksichtigt werden, wenn ein besonders aufwendiger Pflegebedarf nachgewiesen wird. Den Investitionszuschlag zu zahlen haben die Stadt- und Landkreise. Die Pflegedienste müssen ihren Anträgen jeweils eine Bestätigung des Hausbesuchs durch die pflegebedürftige Person oder einen Angehörigen beifügen. Das bedeutet: Wenn die Pflegedienste den ihnen zustehenden Investitionszuschlag erhalten wollen, müssen sie dem jeweils zuständigen Stadt- oder Landkreis mindestens die Namen der von ihnen gepflegten Personen, die Tage, an denen die Hausbesuche stattfanden und die Zahl der Hausbesuche an diesen Tagen sowie bei mehr als drei Hausbesuchen am Tag eine Begründung für den besonders aufwendigen Pflegebedarf angeben. Diese Angaben aber haben die Mitarbeiter der Pflegedienste, bei denen es sich in der Regel um Angehörige von Heilberufen mit staatlich geregelter Ausbildung handelt, nach § 203 Abs. 1 Nr. 1 StGB geheimzuhalten. Da, anders als für die Mitteilung der Abrechnungsdaten an die Pflegekasse, keine Rechtsvorschrift existiert, die eine Weitergabe der für die Gewährung des Investitionszuschlags erforderlichen Angaben über die pflegebedürftigen Personen erlaubt, sind die Pflegedienste deshalb dazu nur berechtigt, wenn die pflegebedürftigen Personen wirksam ihre Einwilligung gegeben haben. Dabei wird sich freilich in vielen Fällen die Frage stellen, ob die pflegebedürftige Person überhaupt noch einwilligungsfähig ist. Zudem soll der Investitionszuschlag auch rückwirkend für bereits in der Vergangenheit durchgeführte Hausbesuche gewährt werden. Für all diese Fälle noch nachträglich Einwilligungen einzuholen, dürfte erhebliche praktische Schwierigkeiten bereiten. Vor allem aber: Die für die Gewährung des Investitionszuschlags getroffene Regelung wird

dazu führen, daß bei den Stadt- und Landkreisen Datensammlungen mit Angaben über alle von den Pflegediensten ambulant betreuten pflegebedürftigen Personen entstehen. Dabei sind diese Daten bei den Stadt- und Landkreisen weniger geschützt als die Abrechnungsdaten bei den Pflegekassen und dem Medizinischen Dienst der Krankenversicherungen. Bei letzteren fallen sie nämlich unter den besonderen Schutz des Sozialgeheimnisses. Demgegenüber müssen die Stadt- und Landkreise beim Umgang mit den bei der Gewährung des Investitionszuschlags erhobenen Daten nur das Landesdatenschutzgesetz beachten, das geringeren Schutz bietet. Wir haben das Sozialministerium auf diese Problematik hingewiesen. So wie die Dinge jetzt aussehen, wird sie sich von selbst lösen: Der Investitionszuschlag soll nämlich in Bälde abgeschafft werden.

5. Teil: Rund ums Rathaus

1. Das Melderegister

Mit Fug und Recht kann man das Melderegister als wichtigen Eckpfeiler unseres Verwaltungssystems bezeichnen. Denn fast alle Behörden nutzen diese Datensammlung, in der jeweils alle Einwohner einer Stadt oder Gemeinde mit einer Fülle von Daten gespeichert sind, als wichtige Informationsquelle. Aber nicht nur sie, sondern auch private Personen und Stellen können daraus unter bestimmten, im Melderecht geregelten Voraussetzungen Informationen beziehen. Nur allzuoft ist das Register aber auch Quelle von Datenschutzärgernissen:

1.1 Der neue alte Meldeschein – Chance vertan
Das Einwohnermeldeamt muß jeden, der sich dort anmeldet, über seine Datenschutzrechte informieren. Insbesondere muß es ihm sagen, daß er einer Weitergabe seiner Daten für Zwecke der Wahlwerbung widersprechen und auch verlangen kann, daß sie nicht in Einwohneradreßbüchern veröffentlicht werden. Die Art und Weise, wie dies in der Praxis geschieht, mag zwar formal gerade noch in Ordnung sein, bürgerfreundlich ist sie jedoch keinesfalls. Denn in aller Regel sehen die Einwohnermeldeämter ihre Hinweispflicht mit der Aushändigung des Anmeldevordrucks als erfüllt an, weil auf dessen Rückseite die Hinweise zusammen mit umfangreichen Erläuterungen für das Ausfüllen abgedruckt sind. Wie wir aus zahlreichen Bürgereingaben wissen, werden sie dort aber kaum zur Kenntnis genommen, denn wer macht sich schon die Mühe, bei der ohnehin lästigen Anmeldeprozedur das umfangreiche Kleingedruckte auf der Rückseite des Vordrucks durchzulesen. Wir schlugen dem Innenministerium deshalb vor, den in der Meldeverordnung verbindlich vorgeschriebenen Anmeldevordruck, der ohnehin verändert werden mußte, umzugestalten und die Hinweise auf die Datenschutzrechte schon auf der Vorderseite abzudrucken. Leider ohne Erfolg. Das Innenministerium fand sich lediglich dazu bereit, auf der Vorderseite einen dezenten Hinweis auf die auf der Rückseite abgedruckte Unterrichtung über das Widerspruchsrecht anzubringen. Eine gute Chance, die für den Bürger so wichtige Information über seine Datenschutzrechte „herüberzubringen“, wurde so ohne Not vertan.

1.2 Die unerwünschten Wählerbriefe
Man mag sich durchaus fragen, ob es gerechtfertigt ist, daß Parteien vor Wahlen Adressen von nach Altersgruppen ausgewählten Wählergruppen aus dem Melderegister erhalten dürfen. Viele Bürger, das wissen wir aus zahlreichen Anrufen und Briefen, haben dafür jedenfalls kein Verständnis. Wenigstens hat aber jeder im Land seit 1990 die Möglichkeit, der Herausgabe seiner Adreßdaten zu widersprechen. Zunächst nur im Erlaßwege vom Innenministerium geregelt, ist dieses Widerspruchsrecht seit 3. Jan. 1996 ausdrücklich im Meldegesetz verankert. Damit die Bürger auch von diesem Recht erfahren können, muß das Einwohnermeldeamt vor jeder Wahl durch öffentliche Bekanntmachung auf das Widerspruchsrecht hinweisen. Eine klare Sache, sollte man meinen, nur: Als wir den zahlreichen Beschwerden verärgerter Bürger nachgingen, die vor der Landtagswahl im März 1996 persönlich adressierte Wahlbriefe erhalten hatten, stellten wir fest, daß 10 Städte und Gemeinden Adreßdaten an Parteien herausgegeben hatten, obwohl sie ihre Einwohner zuvor nicht durch öffentliche Bekanntmachung auf ihr Widerspruchsrecht hingewiesen hatten. Diese konnten deshalb auch nicht darüber entscheiden, ob sie die Weitergabe ihrer Daten für Wahlwerbungszwecke hinnehmen wollen oder nicht. Einige dieser Kommunen rechtfertigten dieses Unterlassen damit, die am 3. Jan. 1996 im Meldegesetz neu eingeführte Frist für die öffentliche Bekanntmachung – 6 bis 8 Monate vor der Wahl – habe für die Landtagswahl am 24. März 1996 ja ohnehin nicht mehr eingehalten werden können. Wie wir meinen zu Unrecht: Denn das Innenministerium hatte die Mel-

debehörden bereits früher im Vorgriff auf die schon damals vorgesehene gesetzliche Regelung angewiesen, daß sie die Bürger rechtzeitig vor der Wahl auf das Widerspruchsrecht hinweisen müssen. Teils war dies offensichtlich in Vergessenheit geraten, teils so verstanden worden, als ob sich diese Anweisung nur auf die seinerzeit gerade anstehenden Wahlen bezogen habe. Solchen Rechtfertigungsversuchen wäre freilich von vornherein der Boden entzogen gewesen, wenn das Innenministerium rechtzeitig vor der Landtagswahl 1996 die Einwohnermeldeämter nochmals an ihre Bekanntmachungspflicht erinnert hätte.

1.3 Einwohnerbücher auf CD-ROM?
Zugegeben, der Gedanke liegt nahe. Warum sollten Einwohnerbücher nicht auch auf einer CD-ROM erfaßt und vertrieben werden? Die Frage ist jedoch, ob die Städte und Gemeinden Verlagen die Adreßdaten auch dafür zur Verfügung stellen dürfen. Wir meinen nein. Das Meldegesetz erlaubt die Weitergabe von Adreßdaten für die Herausgabe von „Einwohnerbüchern und ähnlichen Nachschlagewerken“. Schon der Wortlaut dieser Regelung spricht dafür, daß sie nur die Weitergabe von Einwohnerdaten zur Veröffentlichung in einem Werk in Buchform zulassen will. Vor allem aber ist zu bedenken: Eine Speicherung von Daten auf einer CD-ROM ist wegen der mit diesem Speichermedium verbundenen vielfältigen Auswertungs- und Verknüpfungsmöglichkeiten qualitativ etwas anderes als die Veröffentlichung in einem Buch. Hätte der Gesetzgeber auch dies zulassen wollen, hätte er dies unmißverständlich zum Ausdruck bringen müssen. Auf unsere Bitte, die Einwohnermeldeämter so zu instruieren, wies sie das Innenministerium auf die CD-ROM-Problematik hin, freilich nicht ohne sich noch eine Hintertür offenzuhalten: Es hält lediglich „derzeit für sachgerecht“, die Herausgabe von Einwohnerdaten zur Veröffentlichung auf CD-ROM zu verweigern.

1.4 Auskunftssperren
Will ein Einwohner nicht, daß sein Einwohnermeldeamt über ihn eine Melderegisterauskunft an einzelne Personen oder private Stellen erteilt, so hat er nur die Möglichkeit, eine Auskunftssperre zu beantragen. Diese wird freilich nicht jedermann bewilligt, sondern nur dem, der ein berechtigtes Interesse daran glaubhaft macht. Aber auch wenn eine Auskunftssperre im Melderegister eingetragen ist, verhindert dies nicht etwa automatisch eine Auskunftserteilung, sondern verpflichtet lediglich das Einwohnermeldeamt, im Falle eines Auskunftsersuchens den Einwohner anzuhören und seine Interessen mit denen des Antragstellers abzuwägen, bevor es über die Auskunftserteilung entscheidet. Selbst diese eingeschränkte Schutzwirkung der Auskunftssperre wird unterlaufen, wenn ein Einwohnermeldeamt so verfährt, wie die Stadt Radolfzell dies in folgendem Fall getan hat:

Als ein Rechtsanwalt die neue Anschrift einer Einwohnerin erfragte, für die eine Auskunftssperre eingetragen war, teilte das Einwohnermeldeamt dieser mit, daß ein Auskunftsantrag des Rechtsanwalts eingegangen sei; sie möge sich innerhalb einer kurz bemessenen Frist dazu äußern. Wen der Rechtsanwalt vertrat und in welcher Sache er die Auskunft haben wollte, behielt das Amt zunächst einmal für sich. Das erfuhr die Einwohnerin erst zwei Wochen später auf hartnäckiges Nachhaken. Zu diesem Zeitpunkt hatte das Einwohnermeldeamt die neue Anschrift aber schon weitergegeben, nachdem die von ihm gesetzte Äußerungsfrist abgelaufen war. Unabhängig davon, ob die Bekanntgabe der neuen Adresse letztlich zulässig war oder nicht, so darf ein Einwohnermeldeamt nicht vorgehen. Wenn in einem solchen Fall ein Auskunftsantrag gestellt wird, muß es dem betroffenen Einwohner schon sagen, wer weshalb die Anschrift wissen will und ihm eine angemessene Äußerungsfrist einräumen, damit er zu diesem Antrag sachgerecht Stellung nehmen kann. Auf unsere Beanstandung hin sagte die Stadt zu, es künftig richtig zu machen.

1.5 Personenverwechslung
Erteilt ein Einwohnermeldeamt eine Melderegisterauskunft, dann muß es sich zuvor darüber vergewissern, daß die Person, über die Auskunft gewünscht wird, identisch ist mit der Person, über die es die Auskunft geben will. Denn Personenverwechslungen bereiten den beteiligten Personen nicht nur Scherereien, sondern führen auch dazu, daß Unbeteiligte Informationen über Einwohner erhalten, die sie nichts angehen. Erneut lieferte die Stadt Esslingen a. N. dafür ein unrühmliches Beispiel. Beim dortigen Einwohnermeldeamt fragte ein Amtsgericht nach der neuen Anschrift einer Person an; dabei nannte es außer deren Namen die letzte ihm bekannte Anschrift in Esslingen. Das Einwohnermeldeamt fand in seinem Melderegister nur eine Person mit dem gesuchten Namen. Obwohl diese in Esslingen immer unter einer anderen Adresse gewohnt hatte, als in dem Auskunftsersuchen angegeben war, schloß das Einwohnermeldeamt, es müsse sich um die angefragte Person handeln, und teilte dem Amtsgericht deren Adresse mit. Tatsächlich war aber der gemeldete Einwohner nicht identisch mit der Person, nach der das Amtsgericht suchte. Der „verwechselte“ Einwohner fiel wenig später aus allen Wolken, als er vom Amtsgericht eine Ladung zum Strafantritt erhielt, der das zugrundeliegende Strafurteil angeschlossen war. Die Verwechslung ließ sich aufklären; nicht rückgängig zu machen war jedoch, daß der „verwechselte“ Einwohner aus dem Strafurteil all die vielen Einzelheiten aus dem Privatbereich der eigentlich gesuchten Person erfuhr. Die Stadt hätte allen Grund zu mehr Sorgfalt gehabt, denn vor Jahresfrist war ihr ein fast gleicher Fehlschluß mit ähnlich fatalen Folgen unterlaufen, den wir beanstandet hatten (vgl. 16. Tätigkeitsbericht, LT-Drs. 11/6900, S. 71 f.). Auf unsere erneute Beanstandung hin teilte die Stadt mit, sie habe jetzt angeordnet, daß Anfragen nur noch dann beantwortet werden dürfen, wenn zweifelsfrei feststeht, nach welcher Person angefragt wird. Das sollte doch wohl selbstverständlich sein!

1.6 Der begehrte Direktzugriff
Was Polizei und Landratsämter schon lange angestrebt haben, ist jetzt erreicht. Die neue Meldeverordnung des Innenministeriums läßt zu, daß sowohl die Polizeidienststellen, angefangen beim Landeskriminalamt bis hin zu den Polizeidirektionen und der Wasserschutzpolizei, als auch die Kfz-Zulassungsstellen und Abfallgebührenämter der Landratsämter direkt auf die automatisiert geführten Melderegister der Städte und Gemeinden zugreifen und dort die Daten abrufen können, die sie für ihre Aufgaben benötigen. Dieser direkte Weg ist nicht nur für die Polizei und die Landratsämter, sondern auch für die Einwohnermeldeämter bequem, weil diesen damit die manchmal lästige Erteilung von Einzelauskünften erspart bleibt. Soweit so gut. Darüber darf jedoch nicht die Kehrseite der Medaille außer acht gelassen werden, nämlich das erhöhte Mißbrauchsrisiko, dem die Bürgerdaten künftig ausgesetzt sind. Denn ist einmal ein solches Abrufverfahren eingerichtet, muß sich die abrufberechtigte Stelle nicht mehr wie bisher an das Einwohnermeldeamt wenden, ihr Anliegen erklären und warten, bis die gewünschte Auskunft erteilt wird. Weil dieses zeitraubende Verfahren entfällt, wird in Zukunft die Versuchung größer als bisher sein, es mit der Prüfung der Erforderlichkeit der Auskunft nicht so genau zu nehmen oder aber Abrufe auch für Zwecke zu tätigen, für die sie nicht zugelassen sind. Wegen dieser, Direktabrufverfahren immanenten Risiken empfahlen wir dem Innenministerium, u.a. folgende Regelungen in die Meldeverordnung aufzunehmen:

– Die abrufenden Stellen sollten die zum Abruf zugelassenen Daten nicht nach Belieben, sondern nur anhand von in der Meldeverordnung festgelegten Suchkriterien suchen und auswerten dürfen. Auch sollten die Polizeidienststellen jeweils nur auf die Melderegister der Einwohnermeldeämter ihres Dienstbezirks zugreifen können. Beiden Empfehlungen trug das Innenministerium nicht Rechnung.

– Zur Kontrolle der Zulässigkeit der Abrufe sollte ein Stichprobenverfahren vorgesehen werden, bei dem der Abrufende ständig damit rechnen muß, daß seine Abfrage protokolliert wird. Dazu müssen die zu protokollierenden Abrufe nach einem Zufallsverfahren ausgewählt werden. Auch muß sichergestellt sein, daß dem Abrufenden nicht vor dem Ende des Dialogs signalisiert wird, daß der Abruf protokolliert wurde. Auch diese Empfehlung blieb unberücksichtigt. Die Verordnung legt nur fest, daß jeder 50. Abruf zu protokollieren ist. Ein, wie wir meinen, zu starres Protokollierungssystem.

Bei dieser Sach- und Rechtslage bleibt nur zu hoffen, daß wenigstens die Meldebehörden, Landratsämter und die Polizei in der Praxis von der in der Meldeverordnung eingeräumten Möglichkeit mit Augenmaß Gebrauch machen und beim Datenschutz von sich aus mehr tun, als die Meldeverordnung verlangt.

2. Wenn es ums Geld geht

Städte und Gemeinden müssen ihre Steuern und Abgaben gleichmäßig erheben, also auch dafür sorgen, daß alle abgabepflichtigen Personen erfaßt und herangezogen werden. Nicht alles, was ihnen dazu einfällt, darf auch so realisiert werden.

2.1 Hundesteuerkontrolle
Darf eine Stadt Beauftragte von Haus zu Haus schicken und jeden einzelnen Haushalt befragen lassen, ob er einen Hund hält? So oder ähnlich fragten uns gleich mehrere Städte sowie eine Firma, die dazu ihre Dienste anbietet. Die Antwort konnte nur „nein“ lauten, nicht anders als bei ähnlichen Varianten, mit denen wir uns schon früher zu befassen hatten (vgl. 11. Tätigkeitsbericht, LT-Drs. 10/4540, S. 105 und 12. Tätigkeitsbericht, LT-Drs. 10/6470, S. 68). Denn auch wenn sich auf diesem Weg tatsächlich bislang nicht angemeldete Hunde aufspüren lassen, so macht der mögliche Erfolg diese Art von Hundesteuerfahndung nicht rechtmäßig. Selbstverständlich darf eine Stadt konkreten Anhaltspunkten, daß ein bestimmter Einwohner einen nicht angemeldeten Hund hält, nachgehen und aufklären, ob dem so ist. Dagegen ist es einer Stadt nicht erlaubt, ohne irgendwelche Verdachtsmomente gegen bestimmte Personen möglichst lückenlos alle Haushalte vor Ort zu befragen, mithin also eine flächendeckende Totalerhebung durchzuführen, von der ganz überwiegend solche Personen betroffen werden, die gar keinen Hund halten oder ihren Hund ordnungsgemäß angemeldet haben. Ein derartiges Vorgehen steht außer Verhältnis zu dem damit verfolgten Ziel, einige Steuersünder aufzuspüren. Daran ändert sich auch nichts, wenn die Befragung als freiwillig deklariert wird. Denn abgesehen davon, daß es mit der Freiwilligkeit in einem solchen Fall so eine Sache ist, bleibt entscheidend: Bürger, die sich in puncto Hundesteuer nichts zuschulden kommen lassen, können erwarten, daß sie an ihrer eigenen Wohnungstür nicht mit steuerlichen Ermittlungen behelligt werden.

2.2 Gästekontrolle
Muß man wirklich Familienbesucher, die über Nacht bleiben, der Kurverwaltung melden? fragte ein Einwohner eines Kurorts im Schwarzwald, als die Kurverwaltung im gemeindlichen Amtsblatt gegen die immer mehr abnehmende Meldemoral wetterte. Tatsächlich ergab sich aus der Kurtaxesatzung dieser Gemeinde, daß solche Familienbesucher zwar keine Kurtaxe zahlen müssen, wenn sie keine Kureinrichtungen in Anspruch nehmen, daß sie sich aber gleichwohl innerhalb von drei Tagen nach Ankunft anmelden und spätestens am letzten Aufenthaltstag abmelden müssen. Auf unsere Frage nach dem Sinn dieser Regelung verwies die Gemeinde darauf, auch Familienbesucher seien nach dem Kommunalabgabengesetz und der Kurtaxesatzung „an sich“ kurtaxepflichtig und lediglich von der Kurtaxepflicht befreit; ob aber tatsächlich ein Befrei-

ungstatbestand vorliege, könne letztlich nur die Gemeinde entscheiden und müsse deshalb auch von den „befreiten Abgabetatbeständen“ Kenntnis erlangen. Freilich räumte die Gemeinde gleichzeitig ein, daß sie faktisch kaum Kontrollmöglichkeiten hat. In Wirklichkeit ging es ihr vorrangig darum, dem Land gegenüber eine möglichst hohe Übernachtungszahl vorweisen zu können, weil nämlich das Land seine Zuweisungen an Fremdenverkehrsgemeinden nach dem Verhältnis der kurtaxepflichtigen Übernachtungen verteilt und dabei auch solche Übernachtungen einbezieht, die nur „an sich“ kurtaxepflichtig, aber von der Kurtaxe befreit sind. Macht die Meldepflicht für Familiengäste aber für die Kurtaxeerhebung selbst keinen rechten Sinn, so wäre es an der Zeit, sie zu überdenken, und zwar in allen Kurorten und Fremdenverkehrsgemeinden, die eine solche Meldepflicht eingeführt haben.

3. Ausforschung statt Forschung

Als sich beim Standesamt einer Kleinstadt am Telefon ein freundlicher Mann meldete, seinen Namen nannte und um die Vornamen aller in einem bestimmten Monatszeitraum geborenen Kinder bat, die er als Mitarbeiter eines Instituts für eine Namensforschungsarbeit benötige, dachte sich das Standesamt nichts Böses dabei und nannte dem Anrufer bereitwillig die Vornamen der in dem gewünschten Zeitraum geborenen 34 Kinder. Wer der Anrufer tatsächlich war, steht nicht sicher fest; vieles spricht dafür, daß es ein Angehöriger der rechtsradikalen Szene war, der auf diese linke Tour einen Verdeckten Ermittler zu enttarnen versuchte, dessen Geburtstag in den fraglichen Zeitraum fiel. Wie dem auch sei, so hätte das Standesamt nicht verfahren dürfen. Auf eine telefonische Anfrage hin hätte es überhaupt keine Auskunft erteilen dürfen, weil es sich so der Identität des Anrufenden nicht vergewissern und damit auch nicht überprüfen konnte, ob die im Personenstandsgesetz festgelegten Voraussetzungen für eine Auskunft gegeben sind. Das Standesamt hatte sich nicht einmal vergewissert, ob das angebliche Forschungsinstitut, dem anzugehören der Anrufer vorgab, ein öffentliches oder privates sein sollte; an ein privates Institut hätte es die Auskunft schon deshalb nicht erteilen dürfen, weil das Personenstandsgesetz dies gar nicht zuläßt. Die Stadt sah den Fehler ein und sicherte auf unsere Beanstandung hin zu, Auskünfte aus den Unterlagen des Standesamts nur noch auf schriftliche Anforderung zu erteilen.

4. Schach den Müllsündern – aber nicht so

Die Sammelplätze, an denen Container für Altglas, Altpapier oder andere Wertstoffe aufgestellt sind, scheinen vielerorts geradezu magisch Zeitgenossen anzuziehen, die dort ihren Müll los werden wollen. Sie verschandeln dabei nicht nur die Umwelt, sondern verursachen zusätzliche Kosten für Reinigung und Abfuhr – alles andere als ein Kavaliersdelikt. Deshalb ist verständlich, daß die Landkreise und Städte solchen Müllsündern den Kampf ansagen. Nicht in Ordnung war freilich, wie die Stadt Konstanz das Problem anging: Sie postierte an besonders gefährdeten Containerstandplätzen, in einem Pkw versteckt, eine Videokamera und zeichnete mit ihr alles auf, was sich auf dem Platz abspielte. Neben vielen Personen, die sich korrekt verhielten, wurden so auch einige entdeckt, die ihren Müll ordnungswidrig ablagerten. Die letzteren stellte die Stadt schriftlich ob ihres Verhaltens zur Rede und ermahnte sie, ihren Abfall künftig ordnungsgemäß zu entsorgen. Weil die Stadt die Bürger nicht deutlich auf die Videoaufzeichnungen hingewiesen hatte, sondern diese heimlich durchführte, und weil die Stadt zudem die Bänder mit den Aufzeichnungen zu lange aufbewahrte, griff sie stärker als notwendig in das Recht auf Datenschutz der aufgezeichneten Personen ein. Auf unsere Beanstandung hin stellte sie dieses Verfahren ein und machte alle Unterlagen unkenntlich. Künftig will sie Containerstandplätze durch Aufsichtspersonen überwachen lassen, die Bürger deutlich auf die Überwachung hinweisen und nur noch Angaben über solche Personen festhalten, gegen die sie eine Ordnungswidrigkeitenanzeige erstattet.

5. Tue Gutes und rede darüber

In der Landeshauptstadt wollte eine Gemeinderatsfraktion, auf deren Antrag hin der Gemeinderat eine Erhöhung der Aufwandsentschädigung der freiwilligen Feuerwehrleute sowie andere Verbesserungen für die Feuerwehren beschlossen hatte, diese wissen lassen, wem sie dies zu verdanken haben. Zu diesem Zweck erbat die Fraktion von der städtischen Branddirektion die Namen und Anschriften der 900 freiwilligen Feuerwehrleute – und erhielt diese anstandslos. Die Adressen verwandte die Fraktion dazu, jedem einzelnen ihren im Gemeinderat eingebrachten Antrag zuzusenden und gleich auch noch eine Broschüre beizulegen, in der sie ihre Mitglieder vorstellte und ihre Ziele darstellte. Die Datenschutzfrage bei diesem Vorgang war, ob die Branddirektion die Daten der freiwilligen Feuerwehrleute an die Fraktion weitergeben durfte. Unsere Antwort konnte nur „nein“ lauten. Die Fraktion war auf die Daten gar nicht angewiesen, weil sie die Feuerwehrleute auch ohne eine persönlich adressierte Zusendung über ihre Wohltäter hätte informieren können, beispielsweise durch Aushang oder Auslegen von Informationsmaterial in den Diensträumen der Feuerwehren. Die Feuerwehrleute dagegen, die sich freiwillig und ehrenamtlich zum Dienst an der Gemeinschaft zur Verfügung gestellt haben, müssen darauf vertrauen können, daß die Stadt ihre Daten grundsätzlich nur so verwendet, wie es für die Wahrnehmung dieses Dienstes erforderlich ist, und sie nicht für einen ganz anderen Zweck weitergibt.

6. Endlich!

In schöner Regelmäßigkeit beschwerten sich immer wieder verärgerte Bauherren bei uns darüber, daß im Amtsblatt ihrer Gemeinde über die Behandlung ihres Bauvorhabens im Gemeinderat berichtet wurde, obwohl sie ihr Einverständnis mit der Veröffentlichung im Amtsblatt in dem Bauantrag ausdrücklich verweigert hatten. Dieser Ärger war gewissermaßen vorprogrammiert, denn die in dem amtlichen Vordruck vorgedruckte Erklärung konnte durchaus falsche Vorstellungen erwecken. Ihr war nicht zu entnehmen, daß sich die Erklärung nur auf die Veröffentlichung von Bauvorhaben in einer eigenen Rubrik des Amtsblatts bezieht, daß aber die gesetzliche Pflicht der Gemeinde, ein im Gemeinderat zu behandelndes Bauvorhaben in die Tagesordnung aufzunehmen und diese öffentlich bekanntzugeben, und ihr Recht, über die öffentlichen Beratungen des Gemeinderats im Amtsblatt zu berichten, unberührt bleibt. Deshalb forderten wir schon 1991, in den Antragsvordruck einen Hinweis aufzunehmen, der diese Rechtslage deutlich klarstellt. Jetzt trug das Wirtschaftsministerium mit den neu eingeführten Bauantragsvordrucken diesem Vorschlag Rechnung.

6. Teil: Weitere Schwerpunkte

1. Abschnitt: Die Justiz

1. Datenschutz bei der Gerichtshilfe und der Bewährungshilfe

Gericht und Staatsanwaltschaft müssen sich häufig ein Bild über die Persönlichkeit von Angeklagten oder Verurteilten und deren Umfeld machen, etwa wenn es darum geht, ob einem mittellosen Verurteilten gestattet werden soll, Arbeitsleistungen zu erbringen, um ihm die Ersatzfreiheitsstrafe zu ersparen oder wenn ein sog. Täter-Opfer-Ausgleich vermittelt und überwacht werden muß. Unterstützung erfahren sie dabei von der bei der Staatsanwaltschaft angesiedelten Gerichtshilfe.

Hat ein Gericht die Strafe zur Bewährung ausgesetzt, stellt es dem Verurteilten einen der dem Landgericht zugeordneten Bewährungshelfer zur Seite, wenn es das als notwendig ansieht, um ihn von weiteren Straftaten abzuhalten. Weil Gerichtshilfe und Bewährungshilfe nicht nur in diesen Fällen, sondern auch bei ihren vielfältigen weiteren Aufgaben recht sensible Daten sammeln, speichern und weitergeben, sahen wir uns die Praxis bei der Gerichtshilfe und der Bewährungshilfe in Ulm näher an.

1.1 Probleme mit der Einwilligung
Gerichtshelfer und Bewährungshelfer können ihre Arbeit nur erledigen, wenn sie über den Probanden Bescheid wissen. Die dazu nötigen Informationen können sie aber nicht alle von diesem selbst erfahren, sondern brauchen mitunter auch Auskünfte von Personen und Stellen, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. Das kann z.B. ein Arzt sein, bei dem der Proband gerade in Behandlung ist, oder ein Sozialamt. Klar ist: Ohne Einwilligung des Probanden erhalten Gerichts- oder Bewährungshilfe von diesen keine Auskunft. Um sich dessen Einverständnis geben zu lassen, hielten Gerichts- und Bewährungshilfe Formulare vor, die freilich den Anforderungen an eine wirksame Einwilligung nicht entsprachen. Deshalb rieten wir beiden Stellen, ihre Einwilligungsformulare so zu ändern, daß die Probanden klar ersehen können, welche Auskünfte über sie eingeholt werden sollen und für welchen Zweck dies geschieht. Auch sollten die Formulare, wie es Landesdatenschutzgesetz und Sozialgesetzbuch vorschreiben, einen Hinweis auf die Konsequenzen der Verweigerung der Einwilligung enthalten. Unsere Empfehlung setzte das Landgericht sofort in die Tat um und zog die unzureichenden Einwilligungsformulare aus dem Verkehr. Die Staatsanwaltschaft dagegen hofft, daß das Problem im Zuge der anstehenden Überarbeitung der Verwaltungsvorschriften für die Sozialarbeiter in der Justiz aus der Welt geschafft wird.

1.2 Altakten
Weil in den Unterlagen der Gerichtshilfe oft recht sensible Informationen über Probanden und andere Personen stehen, ist es besonders wichtig, daß die nicht mehr benötigten Akten möglichst schnell ausgesondert werden. Dem trug die Gerichtshilfe nicht hinreichend Rechnung. Anstatt sich ihrer Altakten – wie es eine Verwaltungsvorschrift vorsieht – pünktlich nach 5 Jahren zu entledigen, bewahrte sie diese 10 Jahre lang auf. Inzwischen schafft sie in ihren Regalen schneller Platz.

1.3 Technisch-organisatorische Mängel
Bei der Gerichtshilfe nutzen drei Gerichtshelfer und eine Verwaltungsangestellte einen nichtvernetzten PC, auf dem unter anderem ein sog. integriertes Programm installiert ist, mit dem sie Texte und Tabellen erstellen und auswerten können. Die Gerichtshilfe führt u.a. eine Falldatei, in der alle Personen erfaßt sind, mit denen sie zu tun hat. Die Bewährungshilfe nutzt vier nicht vernetzte PC, um Probandendaten zu erfassen und die dienstliche Korrespondenz abzuwickeln. Vor allem folgende Mängel traten dabei zutage:
- Seit es PC in der Verwaltung des Landes gibt, müssen wir immer wieder feststellen, daß es vor allem beim Zugriffsschutz

und bei den Löschfunktionen hapert. Unsere Hinweise auf diese Mängel gleichen einer Sisyphusarbeit. Auch in Ulm mußten wir praktisch von vorne anfangen. Die gravierendsten Fehler waren:

* Obwohl die PC von Gerichts- und Bewährungshilfe jeweils von mehreren Personen genutzt wurden, mußten sich diese nicht mit einer individuellen Kennung anmelden, sondern alle Nutzer arbeiteten mit demselben Gerätepaßwort. Das Gerätepaßwort der Gerichtshilfe bestand zudem lediglich aus zwei Buchstaben, stammte noch von einem früheren Mitarbeiter und war seither noch nie geändert worden. Die Gerätepaßwörter der Bewährungshilfe wurden zwar alle 4 bis 6 Monate geändert, aber nicht von den PC-Nutzern selbst, sondern vom Geschäftsstellenleiter des Landgerichts.
* Nach Eingabe des Gerätepaßworts konnte sowohl bei der Gerichts- als auch bei der Bewährungshilfe jeder Nutzer auf die Betriebssystemebene eines PC gelangen und dort beliebige Kommandos ausführen.
* An dem PC der Bewährungshilfe gab es keine Bildschirmsperre, die den Bildschirm automatisch abschaltet, wenn eine gewisse Zeit am PC nicht gearbeitet wird.
* Zum Löschen nicht mehr benötigter Daten nutzte die Bewährungshilfe die Löschfunktion des Betriebssystems, die lediglich den Namen der zu löschenden Datei, nicht aber die gespeicherten Daten unkenntlich macht.

Man muß nun wirklich kein Experte für einen datenschutzgerechten Betrieb von PC sein, um zu wissen, daß es so nicht geht. Denn zum Standard gehört schon längst, daß

* jeder Benutzer ein individuelles Paßwort haben muß, das nur er kennt, das aus mindestens 6 Zeichen besteht und von ihm selbst von Zeit zu Zeit geändert werden muß,
* PC-Nutzer in aller Regel auf der Betriebssystemebene nichts zu suchen haben,
* PC eine automatische Bildschirmabschaltung haben müssen und eine Löschung nur dann ihrem Namen gerecht wird, wenn die gespeicherten Daten tatsächlich unkenntlich gemacht werden.

Die Bewährungs- und die Gerichtshilfe stellten inzwischen weitgehend Abhilfe in Aussicht. Beide hoffen dabei auf die Hilfe der gemeinsamen DV-Stelle der Justiz.

– Wer erst einmal in der Falldatei der Gerichtshilfe erfaßt war, konnte bislang nicht mit einer fristgerechten Löschung seiner Daten rechnen. Denn die Gerichtshilfe hatte es versäumt, allen ihren Mitarbeitern mitzuteilen, wie sie eine Löschung bewerkstelligen können. Die Folge davon war, daß selbst Datensätze aus dem Jahr 1985 noch in der Falldatei zu finden waren, obwohl die dazugehörigen Akten bereits vernichtet waren. Um sicherzustellen, daß mit der Aussonderung von Akten auch Zug um Zug die dazugehörigen Daten in der Falldatei gelöscht werden, muß die Gerichtshilfe allen PC-Nutzern sagen, wie die Löschung funktioniert. Dies will sie jetzt tun.
– Die Gerichtshilfe und die Bewährungshilfe sind im selben Gebäude untergebracht. Teilweise sitzen Gerichts- und Bewährungshelfer Tür an Tür. Das mag bisweilen ganz praktisch sein. Trotzdem muß aber gewährleistet sein, daß jede Stelle Herr ihrer Daten bleibt. Dies war in Ulm problematisch, weil für alle Dienstzimmer der Bewährungshilfe und der Gerichtshilfe ein- und derselbe Schlüssel paßte, weil die Altakten der Gerichtshilfe und der Bewährungshilfe sich in ein- und demselben Raum befanden, der von allen Mitarbeitern beider Dienststellen ohne weiteres betreten werden konnte und die Altakten der Bewährungshilfe zudem in offenen Regalen lagen, und weil die Gerichtshilfe das Telefaxgerät der Bewährungshilfe mitbenutzte, ohne daß es schriftliche Regelungen gab, wie dabei zu verfahren ist. Weil auch der Gerichts- und der Bewährungshilfe klare Verhältnisse lieber sind, versprachen sie Abhilfe.

2. Die Zentrale Stelle der Landesjustizverwaltungen zur Aufklärung nationalsozialistischer Verbrechen

Vor nunmehr 38 Jahren richteten die Landesjustizverwaltungen der Bundesländer auf der Grundlage einer Verwaltungsvereinbarung die Zentrale Stelle in Ludwigsburg ein. Seit dieser Zeit sammeln dort Staatsanwälte das über nationalsozialistische Verbrechen im In- und Ausland erreichbare Material, sichten es und werten es aus. Dabei ging und geht es insbesondere darum, nach Ort, Zeit und Täterkreis abgegrenzte Tatkomplexe herauszuarbeiten und festzustellen, welche daran beteiligten Personen wegen ihrer Verbrechen noch verfolgt werden können. Manches strafrechtliche Ermittlungsverfahren wegen nationalsozialistischer Verbrechen hat so begonnen. Von den Staatsanwaltschaften wiederum erhält die Zentrale Stelle Abschlußverfügungen und gerichtliche Entscheidungen in strafrechtlichen Ermittlungsverfahren wegen nationalsozialistischer Verbrechen und, wenn sie will, die kompletten Ermittlungsakten. Auf diese Art und Weise sammelte sich bei der Zentralen Stelle im Laufe der Zeit ein enormer Fundus an Akten, Unterlagen und sonstigen Dokumenten über die nationalsozialistische Zeit und damals verübte Verbrechen an, der für die zeitgeschichtliche Forschung von kaum zu überschätzender Bedeutung ist und – wie man z.B. aus der öffentlichen Diskussion um das 1996 erschienene Buch eines jungen amerikanischen Historikers weiß – Wissenschaftler aus aller Welt anzieht, die auf dem Gebiet der NS-Vergangenheit forschen. Kurzum: Die Zentrale Stelle erhebt, speichert, nutzt und übermittelt – um es mit den Worten des Datenschutzes zu sagen – personenbezogene Daten, die – nicht so sehr wegen der Täter, wohl aber wegen der Opfer und der anderen Personen – gemeinhin als besonders sensibel gelten. Damit liegt die Frage auf der Hand: Wie steht es eigentlich mit dem Grundrecht auf Datenschutz der in dem Fundus der Zentralen Stelle erwähnten Personen? Denn spätestens seit dem Volkszählungsurteil des Bundesverfassungsgerichts vom Dezember 1983 steht fest, daß jede Verarbeitung personenbezogener Daten einen Eingriff in das Grundrecht auf Datenschutz darstellt und ein solcher nur aufgrund einer verfassungsmäßigen gesetzlichen Grundlage erfolgen darf, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben müssen. Solche gesetzlichen Regelungen gibt es aber bisher für die Datenverarbeitung der Zentralen Stelle nicht. Die Verwaltungsvereinbarung über die Errichtung der Zentralen Stelle vom November 1958 stellt keine solche Regelung dar. Die von den Landesjustizverwaltungen erlassenen Richtlinien über das Straf- und Bußgeldverfahren helfen auch nicht weiter, weil sie lediglich Verwaltungsvorschriften sind und zudem gar keine Regelungen zu den Fragen enthalten, um die es hier geht. Die Anwendung der Landesdatenschutzgesetze der Bundesländer, deren Staatsanwaltschaften personenbezogene Daten an die Zentrale Stelle weitergegeben haben, ist schon rechtlich mehr als problematisch. Sie würde auf jeden Fall aber auch der Sache nicht gerecht.

Um in dieser Situation den Besonderheiten der Ludwigsburger Sammlung und ihrer historischen Bedeutung einerseits und dem Grundrecht auf Datenschutz bzw. dem Persönlichkeitsrecht der vielen darin erwähnten Personen andererseits besser Rechnung zu tragen als bisher, regten wir im Februar 1996 beim Justizministerium an, alles in einem Staatsvertrag zu regeln. Darin wäre insbesondere auch festzulegen, was mit den Akten und Unterlagen passiert, wenn sie die Zentrale Stelle für ihre strafrechtliche Ermittlungstätigkeit, deren Ende langsam aber sicher näher kommt, nicht mehr braucht. Dazu gaben wir zu erwägen, die Zentrale Stelle insoweit als besonderes Archiv zu betreiben. Das Justizministerium sah die Dinge ähnlich und verwies darauf, daß sich die Justizministerkonferenz im November mit der Zentralen Stelle befassen werde. Zeitungsberichten zufolge standen bei dieser Konferenz vor allem die Frage, ob aus dem Aktenfundus der Zentralen Stelle ein eigenes Archiv oder eine Außenstelle des Bundesarchivs wird, und die Standortfrage auf der Tagesordnung. So wichtig diese Probleme sind, so wenig darf aber die Schaffung einer gesetzlichen Grundlage für die Zentrale Stelle weiter auf die lange Bank geschoben werden.

3. Lascher Umgang mit Registerauszügen

Kommt es nach einem Verkehrsunfall zu einem Ordnungswidrigkeitenverfahren, ist es gang und gäbe, daß Versicherungen, Krankenkassen oder Rechtsanwälte von Geschädigten, die Regreß- oder Schadenersatzansprüche geltend machen wollen, Akteneinsicht beantragen und auch erhalten. Das ist problematisch genug. Denn nahezu 13 Jahre nach dem Volkszählungsurteil des Bundesverfassungsgerichts gibt es noch immer keine Regelung im Ordnungswidrigkeitengesetz oder einem anderen Gesetz, die so etwas erlaubt und regelt, wie dabei zu verfahren ist. Das Justizministerium, das wir auf dieses Manko aufmerksam gemacht haben, hofft darauf, daß der Gesetzgeber in Bonn endlich vorankommt und die überfälligen gesetzlichen Regelungen schafft. Ginge es allein darum, wäre hier kein weiteres Wort zu verlieren. Zu berichten ist jedoch von der weit verbreiteten unzulässigen Praxis, Bundeszentralregister- und Verkehrszentralregisterauszüge einfach in den Akten zu belassen. Auf sie sind wir so gestoßen:

Die Staatsanwaltschaft Mosbach führte gegen eine junge Frau, die einen Verkehrsunfall verursacht hatte, ein Ermittlungsverfahren wegen fahrlässiger Körperverletzung. Im Zuge ihrer Ermittlungen holte sie eine unbeschränkte Bundeszentralregisterauskunft über die Frau ein. Darin stand, daß diese vor nicht allzu langer Zeit einmal wegen eines Verstoßes gegen das Betäubungsmittelgesetz und wegen Fahrens mit einem nicht versicherten Fahrzeug zu Geldstrafen verurteilt worden war. Diese Auskunft nahm die Staatsanwaltschaft zu ihrer Ermittlungsakte. Bald darauf stellte sie das Verfahren mangels hinreichendem Tatverdacht ein und übersandte ihre Ermittlungsakte samt der Bundeszentralregisterauskunft an die zuständige Bußgeldbehörde, nämlich die Stadt Mosbach, weil sie davon ausging, die Frau habe zwar keine fahrlässige Körperverletzung, wohl aber eine Verkehrsordnungswidrigkeit begangen. Die Stadt ging dem nach und holte dazu eine Auskunft aus dem Verkehrszentralregister in Flensburg ein. Darin stand neben der auch im Bundeszentralregister eingetragenen Verurteilung wegen des Verfahrens mit einem nicht versicherten Fahrzeug, daß sie vor ein paar Jahren einmal mit abgefahrenen Reifen Auto gefahren war und deshalb 150 DM Bußgeld zahlen mußte. Die komplette Akte, also samt Bundeszentralregister- und Verkehrszentralregisterauskunft, sandte die Stadt, nachdem sie darum gebeten worden war, sowohl den Rechtsanwälten des Unfallgegners, die gegen die Frau wegen des Unfalls zivilrechtlich vorgehen wollten, als auch der AOK, die sich überlegte, ob sie für ihre Leistungen Regreß nehmen kann, ins Haus.

Dieses Vorgehen war in mehreren Punkten nicht in Ordnung: Zum einen hätte die Staatsanwaltschaft die unbeschränkte Auskunft aus dem Bundeszentralregister nicht mit ihrer Akte an die Stadt weitergeben dürfen. Denn § 41 des Bundeszentralregistergesetzes sagt klipp und klar, daß die Staatsanwaltschaft die im Zuge eines strafrechtlichen Ermittlungsverfahrens eingeholte Bundeszentralregisterauskunft nur für diesen Zweck verwenden darf und verbietet zugleich ihre Weitergabe an eine andere Behörde für ein ganz anderes Verfahren und damit auch für ein Ordnungswidrigkeitenverfahren. Zum anderen hätte die Stadt die unbeschränkte Bundeszentralregisterauskunft nicht einfach in ihren Ordnungswidrigkeitenakten belassen dürfen. Denn Daten, die einer Behörde rechtswidrig zugegangen sind, darf sie nicht in ihren Unterlagen festhalten. Dies widerspricht dem Grundsatz der Gesetzmäßigkeit in der Verwaltung. Zum dritten hätte die Stadt die unbeschränkte Verkehrszentralregisterauskunft und die Auskunft aus dem Bundeszentralregister über die junge Frau weder dem Rechtsanwalt des Unfallgegners noch der AOK zugänglich machen dürfen. Dies gebieten das Bundeszentralregistergesetz und das Straßenverkehrsgesetz. So steht es im übrigen auch in den Richtlinien über das Straf- und Bußgeldverfahren, was Staatsanwaltschaft und Stadt offenbar ebenfalls übersehen hatten. Weil Staatsanwaltschaft und Stadt mit dieser von uns beanstandeten Vorgehensweise nicht etwa Mosbacher Landrecht praktizierten, sondern nur das taten, was offenbar landauf landab weitverbreitete Übung war, baten wir Justizministerium und Verkehrsministerium, Abhilfe zu schaffen. Dem entsprachen die beiden Ministerien im Juni 1996.

4. Geteiltes Leid, halbes Leid?

Ende Dezember 1995 bekamen elf Arbeitskollegen Post von der Staatsanwaltschaft. Sie trauten ihren Augen nicht, weil sie darin nicht nur auf Punkt und Komma lesen konnten, was die Staatsanwaltschaft ihnen selbst, sondern auch das, was sie den Kollegen zur Last legte. Das kam so:

Die Staatsanwaltschaft hatte gegen die elf Arbeitskollegen wegen des Verdachts der Steuerhinterziehung und der Beihilfe zum Vorenthalten von Arbeitsentgelt ein Ermittlungsverfahren eingeleitet. Sie hätten sich – so lautete der Vorwurf – über Jahre hinweg einen Teil ihrer Überstundenvergütungen „schwarz“ auszahlen lassen und diese Zahlungen in ihren Steuererklärungen verschwiegen. Durch die Entgegennahme des Schwarzgeldes hätten sie ihrem Arbeitgeber zugleich ermöglicht, die für die Überstundenvergütungen eigentlich fälligen Beitragsanteile zur Sozialversicherung und zur Arbeitslosenversicherung für sich zu behalten. Die Ermittlungsverfahren faßte die Staatsanwaltschaft zu zwei Verfahren zusammen; eines richtete sich gegen fünf, das andere gegen die übrigen sechs Arbeitskollegen. Den Fünfen teilte die Staatsanwaltschaft Ende Dezember 1995 dann mit, sie beabsichtige, gegen sie Anklage wegen Steuerhinterziehung zu erheben. Weil sich die Staatsanwaltschaft in ihren Schreiben nicht darauf beschränkte, anzugeben, in welcher Höhe der Adressat des Schreibens in welchem Jahr Überstundenvergütungen „schwarz“ eingestrichen haben soll, sondern zugleich immer auch auflistete, wie dies jeweils bei den anderen vier Arbeitskollegen war, konnte jeder von ihnen schwarz auf weiß nachlesen, welcher seiner Kollegen in welchem Jahr in welcher Höhe Überstundenvergütungen „schwarz“ kassiert und dem Finanzamt verschwiegen haben soll. Genauso verfuhr die Staatsanwaltschaft auch in dem Ermittlungsverfahren gegen die übrigen sechs Arbeitskollegen.

Damit ging die Staatsanwaltschaft zu weit. Zwar durfte sie die Ermittlungsverfahren zu den beiden Verfahren zusammenfassen. Dies sieht die Strafprozeßordnung vor, wenn – wie hier – ein sachlicher Zusammenhang besteht. Das heißt aber noch lange nicht, daß die Staatsanwaltschaft den Elfen zu diesem Zeitpunkt mitteilen durfte, welcher ihrer Kollegen welches Schwarzgeld eingesteckt und dem Finanzamt verschwiegen haben soll. Denn mit den Briefen von Ende Dezember 1995 wollte die Staatsanwaltschaft nur den elf Arbeitskollegen vor dem Abschluß ihrer Ermittlungen noch einmal Gelegenheit geben, sich zur Sache zu äußern. Dazu hätte es aber vollkommen ausgereicht, wenn sie jedem der elf Arbeitskollegen jeweils allein das Schwarzgeld, das an ihn geflossen sein soll, vor Augen geführt hätte. Darauf wiesen wir die Staatsanwaltschaft hin. Zu ihrem Einwand, die Arbeitskollegen hätten bei der Anklageerhebung ohnehin Kenntnis vom Schwarzgeldbezug der mitangeklagten Kollegen erlangt, gaben wir zu bedenken, daß es auf die Einlassung der Beschuldigten durchaus in dem ein oder anderen Fall noch zu einer Einstellung des Verfahrens, sei es z.B. mangels öffentlichem Interesse an der weiteren Verfolgung oder gegen Zahlung eines Geldbetrags an die Staatskasse oder eine gemeinnützige Einrichtung, hätte kommen können. Dann wäre der Beschuldigte aber bei der Vorgehensweise, die die Staatsanwaltschaft an den Tag gelegt hatte, unnötigerweise vor den anderen bloßgestellt.

2. Abschnitt: Die Mitarbeiter

1. Der polizeiärztliche Dienst

In kaum einem anderen Bereich sorgt sich das Land so um die Gesundheit seiner Beamten, wie bei der Polizei. Das zeigt sich u.a. daran, daß sowohl die Bereitschaftspolizei als auch die Landespolizeidirektionen eigene, beamtete Ärzte beschäftigen. Gleich zweimal gaben uns diese polizeiärztlichen Dienste Anlaß zu Beanstandungen:

1.1 Was für alle Arbeitgeber gilt, soll für die Bereitschaftspolizei noch lange nicht gelten

Zweifellos muß ein Polizeibeamter physisch und psychisch hundertprozentig fit sein, damit er den hohen Anforderungen seines Dienstes gerecht werden kann. Deshalb ist durchaus zu verstehen, daß sich die Bereitschaftspolizeidirektion ein genaues Bild über den Gesundheitszustand von Bewerbern für den Polizeidienst machen will. Bereits in unserem 13. Tätigkeitsbericht (LT-Drs. 11/1060, S. 36) mußten wir jedoch kritisieren, daß sie bei diesem Bemühen über das Ziel hinausschießt, wenn sie von den Bewerbern, noch bevor der Polizeiarzt sie überhaupt zu Gesicht bekommen hat, verlangt, daß sie eine Krankenkassenauskunft vorlegen, aus der sämtliche dort bekannten Arbeitsunfähigkeitszeiten mit Diagnosen sowie alle Krankenhausaufenthalte mit Diagnosen und Versicherungszeiten ersichtlich sein müssen. Denn damit zwingt die Bereitschaftspolizeidirektion die Bewerber, ihr Informationen über ihre gesundheitlichen Verhältnisse zur Verfügung zu stellen, die für die Beurteilung der Polizeitauglichkeit meist völlig irrelevant sind und die sie deshalb auch nicht erheben darf. Das wollte die Bereitschaftspolizeidirektion allerdings nicht einsehen und bat deshalb das Innenministerium um Unterstützung ihrer Position. Seitdem bemühen sich beide darum, die bisherige Praxis zu rechtfertigen. Dazu wiesen sie wiederholt auf die besonderen geistigen und körperlichen Anforderungen des Polizeidienstes hin und machten auf die „Verpflichtung zum sparsamen Einsatz der Haushaltsmittel“ aufmerksam. Zu guter Letzt durfte natürlich auch das bei solchen Auseinandersetzungen beliebte Argument nicht fehlen, die bisherige Praxis habe sich bewährt. Dagegen gingen beide Stellen mit keinem Wort darauf ein, daß die Bereitschaftspolizeidirektion mit der Anforderung pauschaler Krankenkassenauskünfte Informationen verlangt, die in den allermeisten Fällen für die Frage der Polizeitauglichkeit nicht relevant sind. Ebensowenig wollten sie sich zu der Tatsache äußern, daß andere Bundesländer, wie z.B. Bayern, Mecklenburg-Vorpommern, Rheinland-Pfalz, Sachsen und Sachsen-Anhalt, gänzlich auf solche Bescheinigungen verzichten und Niedersachsen eine Krankenkassenauskunft nur anfordert, wenn die polizeiärztliche Auswahluntersuchung Anlaß dazu gegeben hat. Dabei ist dies doch ein deutliches Indiz dafür, daß solche Auskünfte gerade nicht erforderlich sind. Da nützte auch unser Hinweis nichts mehr, daß es das Innenministerium in seinen Hinweisen zum Bundesdatenschutzgesetz für die private Wirtschaft selbst für unzulässig erklärt, wenn private Arbeitgeber von Stellenbewerbern die Beibringung einer Krankenkassenauskunft verlangen. Angesichts dieser starren Haltung blieb uns nur, diese datenschutzwidrige Praxis zu beanstanden. Auf die schon lange überfällige Stellungnahme warten wir noch.

1.2 Die polizeiärztliche Rundumfürsorge

Auch wenn der Polizeibeamte nach seiner Ausbildung irgendwo im Land seinen Dienst verrichtet, ist sein Dienstherr sehr an seiner gesundheitlichen Verfassung interessiert. In allen fünf Landespolizeidirektionen gibt es eine Abteilung „Ärztliche Betreuung“, die in der Regel von einem beamteten Polizeiarzt geleitet wird. Ihm sind im wesentlichen folgende Aufgaben übertragen:

- Er hat festzustellen, ob der Polizeibeamte allgemein oder für eine bestimmte Verwendung (noch) dienstfähig ist.
- Er ist gleichzeitig auch Betriebsarzt und führt u.a. arbeitsmedizinische Vorsorgeuntersuchungen durch.
- Er wirkt bei der Gewährung der Heilfürsorge mit. Diese stellt sicher, daß der einzelne Polizeibeamte im Krankheitsfall im wesentlichen die gleichen Leistungen erhält wie ein Versicherter der gesetzlichen Krankenversicherung.

Um uns ein Bild darüber zu machen, wie der polizeiärztliche Dienst diese unterschiedlichen Aufgaben wahrnimmt, besuchten wir den Polizeiarzt der Landespolizeidirektion (LPD) Stuttgart II. Dabei stellten wir folgendes fest:

Begibt sich ein Polizeibeamter in ärztliche Behandlung oder sucht er ein Krankenhaus auf, landen alle Abrechnungsunterlagen, also Krankenscheine, Rezepte und Krankenhausrechnungen beim Polizeiarzt, damit dieser prüfen kann, ob dies alles von der Heilfürsorge gedeckt ist. Hat er Zweifel, ob ein Krankenhausaufenthalt gerechtfertigt ist, fordert er dafür eine Begründung des Krankenhauses an. Damit nicht genug: Zum Polizeiarzt gelangen im Rahmen des Heilfürsorgeverfahrens auch die Verschreibungen und Rechnungen für Heil- und Hilfsmittel. Dazu gehören u.a. Brillen und Massagen. Darüber hinaus hat er alle Anträge auf Gewährung von genehmigungspflichtigen Heilfürsorgeleistungen, wie z.B. Kuren oder Zahnersatz, zu beurteilen. Bis auf die Krankenscheine, Rezepte und Abrechnungen über Heil- und Hilfsmittel, die der polizeiärztliche Dienst der LPD Stuttgart II separat 10 Jahre aufbewahrt, kommen alle diese Unterlagen in die sog. Krankenakte. Diese begleitet den Polizeibeamten während seiner ganzen Dienstzeit und wandert auch mit, wenn er in den Bezirk einer anderen Landespolizeidirektion versetzt wird. Die Krankenakte verwendet der Polizeiarzt nicht nur für Zwecke der Heilfürsorge. Er greift auf sie auch dann zurück, wenn es darum geht, Fragen zu klären, die in Zusammenhang mit Berufsunfällen und -krankheiten stehen, oder wenn die Dienstfähigkeit zu beurteilen ist. Soweit er für diese Zwecke Gutachten erstellt und Stellungnahmen abgibt, nimmt er diese ebenfalls in die Krankenakte.

Konkret bedeutet dies: Jeder Polizeibeamte muß, wenn er einen Arzt aufsuchen, sich einer Behandlung bei einem Psychotherapeuten unterziehen oder ins Krankenhaus begeben will, damit rechnen, daß der Polizeiarzt dies zum Anlaß nimmt, die Frage nach der Dienstfähigkeit zu stellen. Keine besonders beruhigende Situation, wie wir aus Kontakten mit Polizeibeamten wissen, sondern eher Anlaß, im Zweifel eine an sich gebotene Behandlung zu unterlassen oder sich zumindest ständig bevormundet zu fühlen. Letzteres empfand z.B. ein Polizeibeamter, der sich bei uns darüber beklagte, daß sich der Polizeiarzt nach einem Krankenhausaufenthalt, ohne ihn zu fragen, mit seinem Vorgesetzten in Verbindung gesetzt hatte, um mit diesem zu erörtern, ob die Belastung an seinem Arbeitsplatz noch in Einklang mit seiner gesundheitlichen Leistungsfähigkeit steht.

All dies müßte freilich nicht sein, wenn die LPD Stuttgart II die für den Umgang mit Heilfürsorgeunterlagen getroffenen gesetzlichen Regelungen beachten würde. Diese verlangen nämlich folgendes:

- Unterlagen über die Heilfürsorge dürfen für andere Zwecke nur verwendet werden, wenn der Polizeibeamte im Einzelfall einwilligt oder soweit es zur Abwehr erheblicher Nachteile für das Gemeinwohl, einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit oder einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist. Dies verlangt § 113 a des Landesbeamtengesetzes (LBG).
- Um diese Zweckbindung der Heilfürsorgedaten sicherzustellen, sind die Heilfürsorgeakten getrennt von anderen Unterlagen zu führen. Auch sollen mit der Gewährung der Heilfürsorge nur solche Personen betraut werden, die nicht zugleich für Personalmaßnahmen zuständig sind oder – wie der Polizeiarzt – an Personalmaßnahmen mitwirken. Auch dies ist unmißverständlich in § 113 a LBG nachzulesen.
- Schließlich sind nach § 113 f LBG Heilfürsorgeunterlagen ebenso wie Unterlagen über Beihilfe und Heilverfahren im Zusammenhang mit Berufsunfällen und -krankheiten drei Jahre nach Ablauf des Jahres, in dem die Bearbeitung des einzelnen Vorgangs abgeschlossen wurde, zu vernichten.

Warum die LPD Stuttgart II und, soweit uns bekannt, auch die anderen Landespolizeidirektionen diese so im wesentlichen seit 1. Jan. 1987 geltende Rechtslage bisher völlig negiert haben, ist schlechthin unverständlich. Erst recht nicht nachvollziehbar war für uns die

erste Reaktion des Innenministeriums auf unsere im August 1996 ausgesprochene Beanstandung. Kurz vor Ablauf der von uns gesetzten Äußerungsfrist teilte dieses nämlich mit, es benötige für die Stellungnahme noch Zeit bis 30. Juni 1997. Dabei kann es nicht bleiben, denn dem gravierend rechtswidrigen Zustand muß das Innenministerium im Interesse der betroffenen ca. 21 000 Polizeibeamten schleunigst ein Ende bereiten. Jetzt will es die Angelegenheit zunächst einmal mit uns besprechen.

2. Der mißverstandene Dienstweg

Auch in anderen Bereichen hat die Personalverwaltung mitunter ihre liebe Not, mit Informationen zum Gesundheitszustand eines Bediensteten datenschutzgerecht umzugehen. Beim Oberschulamt Stuttgart zeigte sich das gleich zweimal. Im ersten Fall schrieb das Oberschulamt einem Lehrer, der sich einer amtsärztlichen Überprüfung seiner Dienstfähigkeit zu unterziehen hatte:

> „Das Staatliche Gesundheitsamt ... hat mit o.g. Gutachten mitgeteilt, daß von Seiten der psychischen Problematik sich nicht viel geändert habe, die innerfamiliären Probleme nach wie vor gravierend seien, daß Sie weiterhin große Mengen Alkohol trinken ..., bisher keine Entgiftungsbehandlung gemacht haben und somit weiterhin dienstunfähig sind."

Eine Mehrfertigung dieses Schreibens schickte es dem zuständigen Staatlichen Schulamt. Damit war der Lehrer gar nicht einverstanden. Zu Recht, denn die höchst sensiblen Angaben über die gesundheitlichen Verhältnisse und die familiäre Situation des Lehrers gehen das Staatliche Schulamt nichts an. Dieses muß nur wissen, ob, ab wann und ggf. mit welchen Einschränkungen der Lehrer seinen Dienst verrichten kann. Mehr darf es wegen des Personaldatengeheimnisses nicht erfahren. Zur Rechtfertigung seines Tuns berief sich das Oberschulamt auf das „Dienstwegprinzip". Nach diesem Prinzip müsse es alle Schreiben an den Lehrer über das Staatliche Schulamt leiten, das eine Mehrfertigung zu den bei ihm geführten Nebenpersonalakten des Lehrers zu nehmen habe. Dabei übersah es aber, daß nach dem Beamtenrecht nur Beamte bei Anträgen und Beschwerden den Dienstweg einzuhalten haben und nicht die Behörde. Für Beamte ist dieser Dienstweg vorgeschrieben, um sicherzustellen, daß sie nicht an den zur Entscheidung berufenen Stellen vorbei Anträge und Beschwerden vorbringen. Weil aber das Oberschulamt allein und nicht auch das Staatliche Schulamt oder die Schulleitung die Prüfung der Dienstfähigkeit eines Lehrers zu veranlassen und die Konsequenzen aus dem Ergebnis der Prüfung zu ziehen hat, muß sich das Oberschulamt über alle die Dienstfähigkeit betreffenden Fragen und Maßnahmen unmittelbar mit dem Lehrer auseinandersetzen und das Staatliche Schulamt außen vor lassen. Von unserem Amt mit dieser Rechtslage konfrontiert, veranlaßte das Oberschulamt das Staatliche Schulamt, sein Schreiben wieder aus der Nebenpersonalakte des Lehrers zu entfernen. Unsere Erwartung, daß damit das Oberschulamt auf den rechten Weg gebracht war, erwies sich freilich als Irrtum. Einige Zeit später leitete dasselbe Referat des Oberschulamts die Ablehnung eines Antrags einer Lehrerin auf Zurruhesetzung wieder auf dem Dienstweg, also über das Staatliche Schulamt und die Schule der Lehrerin zu, die diesen Bescheid dann vom Sekretariat der Schule in einem offenen Umschlag ausgehändigt bekam. Das Oberschulamt ging so vor, obwohl im Bescheid zur Begründung der Ablehnung ausgeführt war, daß „weder aufgrund der orthopädischen Beschwerden noch aufgrund der psychosomatischen Probleme Dienstunfähigkeit konstatiert werden" könne und sich zudem die Frage nach einer psychotherapeutischen Behandlung stelle. Auch diesmal fiel dem Oberschulamt zur Rechtfertigung seines Vorgehens zunächst einmal das „Dienstwegprinzip" ein. Dabei hätte es genügt, wenn das Oberschulamt das Staatliche Schulamt und die Schule von der Ablehnung des Antrags in Kenntnis gesetzt und den Bescheid selbst mit Begründung unmittelbar der Lehrerin zugeschickt hätte. Diesmal sahen wir uns zu einer Beanstandung dieses Verstoßes gegen das

Personaldatengeheimnis gegenüber dem Kultusministerium veranlaßt. Dessen abschließende Stellungnahme steht noch aus.

3. Die Personalakten

Seit 13. Jan. 1996 besitzt auch das Land Baden-Württemberg ein Personalaktenrecht, das diesen Namen verdient. Hoffentlich trägt diese Aktivität des Gesetzgebers bald Früchte, denn die Kette der bei uns eingehenden Eingaben zum Personaldatenschutz reißt nicht ab.

3.1 Die Personalakten und die Personalvertretung

In der Vergangenheit waren Dienststelle und Personalvertretung häufig gleichermaßen ratlos, ob und welche Beschäftigtendaten die Personalvertretung ohne besonderen Anlaß von der Dienststelle anfordern und vorhalten darf. Diese Unsicherheit hat der Gesetzgeber jetzt beendet und im Landespersonalvertretungsgesetz diese Frage abschließend geregelt. Schon lange, nämlich seit dem Jahr 1958, ist dagegen im Landespersonalvertretungsgesetz klipp und klar bestimmt, daß der Personalrat in die Personalakte von Beschäftigten nur mit deren ausdrücklicher Erlaubnis Einblick nehmen darf. Entweder hat sich das immer noch nicht überall herumgesprochen oder wird diese Vorschrift hin und wieder „übersehen“, wenn einer Dienststelle daran gelegen ist, den Personalrat für ihre Sicht der Dinge zu gewinnen. Zwei Fälle belegen das:

- Eine Gemeinde wollte das Dienstverhältnis mit einer Mitarbeiterin lösen. Um die Zustimmung des Personalrats zu erhalten, erörterte ein Mitarbeiter der Gemeindeverwaltung die Angelegenheit mit den Mitgliedern des Personalrats und ließ, „um dem Vorwurf der Beeinflussung zu begegnen“, diese dann mit der Personalakte der Kollegin allein, damit sie unbehelligt in diese Akten Einblick nehmen konnten. Einen solch klaren Datenschutzverstoß mußten wir beanstanden.
- Eine Stadt im Schwarzwald machte es nicht besser. Um Vorhaltungen des Personalrats zu entkräften, drängte die Stadtverwaltung dessen Vorsitzenden geradezu, in die Personalakte einer Mitarbeiterin Einsicht zu nehmen. Weil der sich jedoch nicht aufs Glatteis führen ließ und das rechtswidrige Angebot nicht annahm, ersparte er der Stadt eine Beanstandung.

3.2 Probleme bei der Personalaktenführung

Wer seinem Dienstherrn über viele Jahre die Treue hält, bringt es oft zu einer stattlichen Personalakte. Dort sammeln sich Prüfungszeugnisse, dienstliche Beurteilungen, Besoldungs- und Beförderungsunterlagen, Disziplinarvorgänge, Gesundheitszeugnisse und vieles mehr. Die Personalakte gibt Aufschluß über die Befähigung und den Werdegang des Beschäftigten und ist deshalb eine wesentliche Grundlage für viele dienstrechtliche Entscheidungen. Folglich hat jeder Bedienstete großes Interesse daran, daß der Dienstherr seine Personalakte ordentlich führt und nicht, womöglich hinter seinem Rücken, über Gebühr aufbläht. Einen Beweis dafür, daß dies nicht immer so geschieht, lieferte die Personalakte der Mitarbeiterin einer Stadtverwaltung:

- Bei der Durchsicht dieser Akte fanden wir z.B. eine Liste aller Mitbewerber, Schriftverkehr zwischen dem Bürgermeister und der Mitarbeiterin wegen der Erledigung bestimmter Aufgaben, Schriftverkehr mit Stellen außerhalb der Stadt über Stellenbewertungs- und Haftungsfragen und Organisationsregelungen. All dies hat in einer Personalakte nichts zu suchen, denn zur Personalakte gehören nur Unterlagen und Informationen, die in einem unmittelbaren inneren Zusammenhang mit dem Dienstverhältnis des Beschäftigten stehen.
- Damit die Personalakte nicht heimlich zu einem Schwarzbuch über den Betroffenen wird, gibt es seit jeher eine weitere wichtige Hürde. Vor der Aufnahme von Unterlagen über Beschwerden, Behauptungen und Bewertungen, die für den Beschäftigten ungünstig sind oder ihm nachteilig werden können, ist dieser zu

hören und seine Äußerung zur Personalakte zu nehmen. Sei es aus Unkenntnis, sei es aus Bequemlichkeit, jedenfalls fanden wir in der Personalakte der Mitarbeiterin auch einige Unterlagen mit für sie wenig schmeichelhaftem Inhalt, ohne daß sie zuvor angehört worden wäre.

Auf unsere Beanstandung der datenschutzwidrigen Führung der Personalakte bereinigte die Stadt diese umgehend und versprach, das gleiche auch bei den Personalakten der übrigen Mitarbeiter zu tun. Zudem will sie unserem Vorschlag folgen und die Personalakten durchnumerieren, wie dies für alle Akten der Landesverwaltung vorgeschrieben ist.

3.3 Das aufschlußreiche Schwarze Brett

Nicht wegzudenken ist in einer Behörde das Schwarze Brett, ein wichtiger Umschlagplatz für allerlei Informationen. Dort sind Stellenausschreibungen, Einladungen zum Behördensport, Notizen über Fundsachen, Gewerkschaftsmitteilungen und vieles mehr zu finden, manchmal sogar zuviel:

- Was der Chef des Eigenbetriebs Abfallwirtschaft eines Landkreises praktizierte, geschieht auch andernorts: Auf einer auch für Besucher zugänglichen Tafel im Flur sollten alle Mitarbeiter nicht nur ihre Abwesenheit, sondern auch den Grund für ihr Fernbleiben vom Dienst, also z.B. „Urlaub“, „krank“, „Arztbesuch“ oder „Gerichtstermin“ eintragen.
- Gleichsam als Pranger nutzte der Rektor einer Schule das Schwarze Brett im Lehrerzimmer. Er hängte dort eine Liste aus, der das Kollegium entnehmen konnte, welche Lehrer sich erdreistet hatten, welche seiner Anweisungen wie oft nicht zu befolgen.

Keine Frage, mit dem Personaldatengeheimnis läßt sich ein solches Vorgehen nicht vereinbaren. Selbstverständlich ist es zur Abwicklung des Dienstbetriebs häufig notwendig zu wissen, welcher Kollege wie lange nicht an seinem Arbeitsplatz anzutreffen ist. Deswegen darf dies die Leitung der Dienststelle den Mitarbeitern durch Aushang bekanntgeben. Der genaue Grund der Abwesenheit geht die Mitarbeiter dagegen nichts an. Erst recht darf das Schwarze Brett nicht als moderner Pranger dienen. Und noch etwas: Ein Schwarzes Brett, dem Informationen über einzelne Mitarbeiter zu entnehmen sind, muß an einer Stelle angebracht sein, die für Fremde nicht zugänglich ist.

4. Theorie und Praxis

Solange das monatliche Salär jeden Monat pünktlich auf das Konto kommt, kann lange verborgen bleiben, daß auch bei dessen Berechnung nicht alles seine datenschutzrechtliche Ordnung hat, wie folgendes Beispiel zeigt:

Aufgabe des Landesamts für Besoldung und Versorgung (LBV) ist es, die Bezüge aller Beamten und Richter des Landes festzusetzen und auszuzahlen. Bei den Angestellten und Arbeitern ist das teilweise anders. Die Universitäten sind z.B. selbst verantwortlich dafür, daß ihre nichtbeamteten Beschäftigten ihre Vergütung bekommen. Doch keine Regel ohne Ausnahme – für die nach Tarif bezahlten Mitarbeiter der Universitäten Ulm und Konstanz ist das LBV zuständig. Soweit die Theorie – die Praxis sieht, wie wir vom Personalrat der Universität Stuttgart erfuhren, ganz anders aus: Auch alle anderen Universitäten lassen die Vergütungen ihrer Arbeiter und Angestellten vom LBV berechnen und die Auszahlung in die Wege leiten, die Universität Stuttgart z.B. seit 1. Jan. 1980. Die dazu nötigen Daten gibt die Universität Stuttgart per Diskette an das LBV und erhält von dort die Gehaltsmitteilungen und andere Unterlagen wie z.B. die Meldenachweise für die Sozialversicherung zurück. Dagegen wäre grundsätzlich auch nichts einzuwenden, wenn es einen schriftlichen Auftrag gäbe, durch den eindeutig geregelt ist, welche Berechnungen das LBV durchzuführen, welche Bescheide und Mitteilun-

gen es zu erstellen und wie es mit diesen umzugehen hat. Einem solchen Auftrag spürt man freilich vergeblich nach. Die Universität Stuttgart meldete Fehlanzeige und verwies an das Wissenschaftsministerium. Dieses hatte zwar auch keinen Auftrag erteilt, berief sich aber auf ein Schreiben des Finanzministeriums, in dem dieses sein Einverständnis dazu erklärte, daß die Universität Stuttgart für die Berechnung und Auszahlung der von ihr zu zahlenden Löhne und Gehälter das LBV und das von diesem beauftragte Rechenzentrum der Finanzverwaltung heranziehen darf. Ein Auftrag im Sinne des Landesdatenschutzgesetzes ist darin aber beim besten Willen nicht zu sehen. Das meint inzwischen wohl auch das Wissenschaftsministerium und überlegt, wie es die Dinge wieder ins Lot bringen kann.

7. Teil: Sorgen der Bürger

1. Diskretion – ein Fremdwort bei der Zwangsvollstreckung?

Immer wieder erstaunt, wie wenig Gespür für den Datenschutz amtliche Stellen an den Tag legen, wenn sie Geldforderungen beitreiben wollen. Dafür drei Beispiele:

- Als ein Gerichtsvollzieher einen Pfarrer wegen eines ihn persönlich betreffenden Vollstreckungstitels aufsuchen wollte und ihn weder in seiner Wohnung noch im Pfarramt antraf, übergab er kurzerhand das Schreiben zur Leistungsaufforderung in Kopie zusammen mit einem vorgedruckten Zahlschein offen der Pfarramtssekretärin mit der Bitte um Weiterleitung an den Pfarrer. Die Sekretärin erhielt somit genaue Kenntnis von dem Vollstreckungsersuchen gegen ihren Vorgesetzten. So hätte der Gerichtsvollzieher nicht vorgehen dürfen. Denn abgesehen davon, daß die Pfarramtssekretärin überhaupt nicht zu dem Personenkreis gehört, dem ersatzweise eine Leistungsaufforderung ausgehändigt werden darf, hätte der Gerichtsvollzieher das Schreiben auf jeden Fall nur in einem an den Schuldner adressierten verschlossenen Umschlag übergeben dürfen.
- Als der Vollstreckungsbeamte einer Großen Kreisstadt eine Geldforderung bei einem Schuldner einziehen wollte und vor verschlossener Tür stand, erbot sich dessen Wohnungsnachbar, den Betrag auszulegen. Der Vollstreckungsbeamte nahm dankbar an und händigte dem Nachbarn eine Quittung aus, aus der sich Art und Höhe der Forderung ergab. So nicht, kann man da nur sagen. Denn der Vollstreckungsbeamte konnte nicht vom Einverständnis des Schuldners ausgehen, zumal dieser die Forderung grundsätzlich bestritten hatte.
- Als das Bürgermeisteramt einer Gemeinde mit knapp 5 000 Einwohnern eine Einwohnerin von der eingeleiteten Kontenpfändung unterrichten wollte, gab es dem Amtsboten, der das Schriftstück zustellen sollte, ein vorbereitetes Empfangsbekenntnis mit, auf dem nicht nur Datum und Aktenzeichen des Schreibens, sondern auch der Zusatz „Kontenpfändung“ eingetragen war. So erfuhr der Amtsbote, um was es in dem zuzustellenden Schreiben ging, obwohl er dies nicht zu wissen brauchte. Nicht auszuschließen ist, daß auch andere Mitarbeiter auf dem Rathaus, die mit der Sache nichts zu tun haben, das Empfangsbekenntnis auf dem „Rücklauf“ zu Gesicht bekamen. Das Bürgermeisteramt hätte das zuzustellende Schreiben auf dem Empfangsbekenntnis nur mit Datum und Aktenzeichen bezeichnen dürfen, also ohne weitere inhaltliche Angaben.

Zwar sind dies nur Einzelfälle, symptomatisch und bedenklich zugleich war jedoch: In allen drei Fällen hatten die Behörden zunächst zu erkennen gegeben, daß sie ihr Vorgehen für rechtmäßig halten. Hoffentlich konnten wir sie vom Gegenteil überzeugen!

2. Was Post und Telekom unter Service verstehen

Ihren Ärger über zwei mißglückte Aktionen der Deutschen Telekom AG und der Deutschen Post AG luden viele Bürger bei unserem Amt ab, nicht wissend, daß diese Erben der früheren Bundespost der Datenschutzkontrolle des Bundesbeauftragten für den Datenschutz unterliegen.

Die Telekom kam ihrer Rechtspflicht, ihre Kunden über ihr Widerspruchsrecht bei der Komfortauskunft und bei den Kundenverzeichnissen zu informieren, so nach: Sie verpackte die Informationen auf die inneren Seiten eines Faltblattes, das durch seine ganze Aufmachung den Eindruck von Werbung erwecken konnte und daher von vielen Telefonkunden ungelesen beiseite gelegt wurde. Aber auch wer das Faltblatt aufmerksam durchlas, erfuhr beispielsweise nicht, daß er einen Widerspruch jederzeit und nicht nur innerhalb einer Vier-Wochen-Frist einlegen kann. Wer schließlich von seinem Widerspruchsrecht Gebrauch machen wollte, fand in dem Faltblatt eine Antwortkarte für die Erklärung des Widerspruchs nur hinsichtlich der Komfortauskunft und nicht auch hinsichtlich

der Kundenverzeichnisse, so daß er in letzterem Fall selbst zur Feder oder zum Telefonhörer greifen mußte. Alles in allem eine wenig kunden- und bürgerfreundliche Aktion, die zu Recht auch in den Medien auf Kritik stieß. In einem weiteren Faltblatt besserte die Telekom ihre Information schließlich nach.

Kaum war die Aufregung über diese Aktion der Telekom abgeklungen, verursachte die Post neuen Wirbel. Mit einer Postwurfsendung bat sie die „lieben Postkunden", sie möchten doch bitte Name und Anschrift und zudem die Namen aller anderen Personen eintragen, die unter derselben Anschrift Post erhalten sollen; diese Angaben dienten ausschließlich der prompten Zustellung der Postsendungen, die an den Haushalt gerichtet sind. Sofern man nicht widerspreche, könne die Post die Anschriften auch weitergeben, damit zukünftige Postsendungen eine richtige Anschrift erhalten. Dieser letztere Hinweis war viel zu vage, als daß den Postkunden hätte klar werden können, was genau mit ihren Daten geschehen soll. Und weil die Postkarte keinerlei Unterschrift vorsah, war nicht sichergestellt, daß die Personen, die auf einer an die Post zurückgesandten Postkarte eingetragen sind, davon wissen und damit einverstanden sind. So konnte es nicht gehen. Deshalb stellte die Post nach einer Intervention des Bundesbeauftragten für den Datenschutz ihre Aktion dann rasch ein.

3. Das ärztliche Gutachten auf dem Rathaus

Zu Recht war ein Bürger verärgert darüber, wie die Landesversicherungsanstalt Baden (LVA) auf seine Bitte reagierte, ihm zur Begründung seines Widerspruchs das ärztliche Gutachten zuzusenden, das der Ablehnung seines Rentenantrags zugrunde lag. Denn als Antwort teilte ihm die Landesversicherungsanstalt mit, die komplette Akte sei seinem Bürgermeisteramt übersandt worden, damit er dort Einsicht nehmen könne. Klar, daß ein solches Vorgehen nicht angeht. Die LVA hätte dem Bürger ohne weiteres gegen Kostenersatz eine Kopie des Rentengutachtens zugehen lassen können. Zumindest hätte sie vorher den Bürger fragen müssen, ob er mit der Übersendung der Akte an das Bürgermeisteramt einverstanden ist. Auf unsere Beanstandung räumte die LVA ihr Fehlverhalten mit dem Hinweis darauf ein, daß es sich dabei um einen bedauerlichen Einzelvorgang gehandelt habe, den sie gegenüber dem Bürger zu entschuldigen bitte. In der Regel übersende sie in solchen Fällen die Kopie des Gutachtens direkt an den Versicherten. Eine Akteneinsicht im Bürgermeisteramt werde nur ermöglicht, wenn dieser sich damit einverstanden erklärt habe. In diesem Falle werde die LVA künftig, unserer Empfehlung Rechnung tragend, die Akte in einem gesonderten Umschlag verschlossen übersenden und das Bürgermeisteramt in einem beigefügten Anschreiben auffordern, den Umschlag nur in Anwesenheit des die Akteneinsicht Begehrenden zu öffnen und die Akte nach erfolgter Einsichtnahme in seiner Gegenwart wieder in einem Umschlag zu verschließen und an die LVA zurückzusenden.

4. Die Routine und ihre Folgen

„Das haben wir schon immer so gemacht!" Dieser ungeschriebene Verwaltungsgrundsatz kam uns in den Sinn, als wir im Sommer 1996 der Frage eines Bürgers nachgingen, ob denn das örtliche Amtsgericht berechtigt sei, dem ansässigen Notariat laufend Abdrucke aus dem Schuldnerverzeichnis zu übersenden. Rasch stellte sich nämlich heraus, daß das Amtsgericht die Neuregelung des Gesetzgebers über den laufenden Bezug von Abdrucken aus dem Schuldnerverzeichnis vom 15. Dez. 1994 nicht beachtet hatte, als es die monatlichen Abdrucke des Schuldnerverzeichnisses dem Notariat übersandte. Denn nach der gesetzlichen Neuregelung hätte es dies nur tun dürfen, wenn dies der hierfür zuständige Präsident des Landgerichts bewilligt hätte. Eine solche Bewilligung lag jedoch nicht vor; was auch schlechterdings nicht möglich war, da das Notariat noch nicht einmal einen entsprechenden Antrag gestellt hatte. Das

Amtsgericht räumte dies ein und stoppte unverzüglich den weiteren Versand. Es versäumte jedoch nicht darauf hinzuweisen, daß bereits vor der gesetzlichen Neuregelung dem Notariat die monatlichen Abdrucke aus dem Schuldnerverzeichnis übersandt wurden. Womit wir wieder am Anfang der Geschichte wären.

5. Überzogener Diensteifer

Sage nur einer, es gebe keine diensteifrigen Beamten mehr. Hin und wieder tun sie sogar des Guten zuviel. Diese Erfahrung mußte eine Angestellte einer Polizeidirektion machen. Sie hatte ein gegen sie in ihrer Abwesenheit ergangenes ausländisches Strafurteil von einer Dolmetscherin übersetzen lassen. Deren Ehemann wollte ihr Original und Übersetzung an ihrem Arbeitsplatz aushändigen und traf dort auf einen hilfsbereiten Polizeibeamten, der versprach, der Angestellten die unverschlossenen Unterlagen zu geben. Als der Beamte bemerkte, daß er ein gegen die Kollegin ergangenes Strafurteil in Händen hielt, erwachte sein Diensteifer. Vielleicht, so dachte er, könnte man auf das Urteil auch eine dienstrechtliche Sanktion stützen und gab deshalb die Unterlagen seinem Vorgesetzten. Der merkte wohl, daß ihn die Unterlagen nichts angingen und ließ sie der Angestellten zugehen, versäumte es jedoch nicht, auch den Leiter der Polizeidirektion über das Urteil zu unterrichten. Darüber war die Angestellte zu Recht verärgert. Die privaten Unterlagen ihrer Mitarbeiterin hätten beide nämlich nur mit ihrem Einverständnis für dienstliche Zwecke verwenden dürfen oder wenn eine Rechtsvorschrift ihnen dies erlaubt hätte. Weil beides nicht der Fall war, haben wir die Polizeidirektion auf ihr Fehlverhalten hingewiesen.

6. Wider Willen im Rampenlicht

Was an vielen Gymnasien Usus ist, hat auch an einem oberschwäbischen Wirtschaftsgymnasium Tradition: Die Abiturienten erhalten nicht etwa sang- und klanglos ihr Abiturszeugnis ausgehändigt, sondern werden im Rahmen eines Abiturballes, zu dem die Abiturienten, ihre Eltern und die Schüler der Klassenstufe 12 eingeladen sind, feierlich verabschiedet. Dabei kommen die Abiturienten klassenweise auf die Bühne und nehmen ihr Reifezeugnis entgegen. Den Besten wird noch eine besondere Ehre zuteil. Ihr guter Notendurchschnitt wird ausdrücklich hervorgehoben und sie erhalten für ihre Leistungen einen Preis oder eine Belobigung. Bei der letztjährigen Feier war die Zeremonie damit aber noch nicht zu Ende. Der Fachabteilungsleiter der Oberstufe stellte bei einigen Abiturienten die Durchschnittsnote im Abschlußzeugnis dem Zeugnis des Vorjahres gegenüber, um den Zwölftklässlern zu zeigen, daß sie ihre Leistungen im Abschlußjahr noch verbessern können, und sie dadurch zusätzlich anzuspornen. Das war nun allerdings des Guten zuviel. Denn während es bei einer Auszeichnung dazugehört, sie nicht im stillen Kämmerlein, sondern coram publico zu überreichen, gibt es keinen Grund, Noten und Leistungsverbesserungen von Schülern ohne deren Einwilligung öffentlich bekanntzugeben. Um die Schüler der 12. Klassen zu motivieren, hätte es genügt, jeweils die Noten des Klassendurchschnitts gegenüberzustellen oder einige Beispielsfälle ohne Namensangabe darzustellen. Das Wirtschaftsgymnasium versprach, unserer Beanstandung Rechnung zu tragen und auf die namentliche Nennung von Notendurchschnitten beim Schuljahresvergleich künftig zu verzichten.

7. Voreingenommene Gutachter?

Wer wegen Alkohol am Steuer seinen Führerschein verloren hat, muß sich, wenn sein Blutalkoholgehalt über 2 Promille lag oder ihm schon einmal die Fahrerlaubnis wegen Alkoholkonsums entzogen war, einer medizinisch-psychologischen Untersuchung (MPU) unterziehen, bevor ihm die Führerscheinstelle wieder eine Fahrerlaubnis erteilt. Dagegen ist auch nichts einzuwenden, denn die Sicherheit des Straßenverkehrs ist ein

hohes Gut. Deshalb muß sich die Führerscheinstelle in einem solchen Fall vergewissern, daß der Antragsteller geeignet ist, ein Kraftfahrzeug sicher zu führen. Außer dem Institut für gerichtliche Medizin der Universität Heidelberg darf in Baden-Württemberg nur das Medizinisch-Psychologische Institut des Technischen Überwachungs-Vereins Südwestdeutschland e.V. (TÜV), das in verschiedenen Städten Untersuchungsstellen unterhält, eine MPU durchführen. Im einzelnen läuft die Prozedur folgendermaßen ab: Die Führerscheinstelle fordert den Alkoholsünder auf, innerhalb einer bestimmten Frist das Gutachten einer amtlich anerkannten medizinisch-psychologischen Untersuchungsstelle beizubringen und sein Einverständnis zur Übersendung der Führerscheinakte an die gewünschte Untersuchungsstelle, im Regelfall also eine solche des TÜV, zu erteilen. Hat der Proband dieser den Gutachterauftrag erteilt, die Kosten von mindestens 621 DM bezahlt und liegen der Untersuchungsstelle die Führerscheinakten vor, steht der Untersuchung nichts mehr im Wege. Das daraufhin erstellte Gutachten erhält der Proband, eine Zweitfertigung bleibt bei der Untersuchungsstelle und die Führerscheinakte geht an die Führerscheinstelle mit dem Vermerk zurück, daß die Akte nicht mehr benötigt wird.

Ein für ihn günstiges Gutachten wird der Führerscheinanwärter natürlich der Führerscheinstelle vorlegen. Was aber kann er tun, wenn er das Gutachten für falsch hält? Auch Gutachter sind nicht unfehlbar. Kein Problem für den, der bereit ist, noch einmal zu zahlen. Er kann sich nochmals von einer anderen Untersuchungsstelle begutachten lassen und hoffen, daß das zweite Gutachten günstiger ausfällt. In diesem Fall geht alles wieder von vorne los, mit einem Unterschied allerdings: In der Führerscheinakte, die der neuen Untersuchungsstelle zugeht, befindet sich jetzt auch noch der Untersuchungsauftrag an die erste Untersuchungsstelle und deren Vermerk, daß sie die Akte nicht mehr benötigt. Daraus ersieht die Untersuchungsstelle, welche andere Untersuchungsstelle gerade erst den Probanden, allerdings offenkundig nicht zu dessen Zufriedenheit, beurteilt hat. Dieses Wissen machten sich Gutachter in einigen Fällen zunutze, forderten dort die Erstgutachten an und bezogen sie in ihre Beurteilung ein. Daß diese Praxis des TÜV nicht nur das Interesse des Probanden völlig ignoriert, auch beim zweiten Mal von unvoreingenommenen Gutachtern auf die Fahreignung untersucht zu werden, sondern auch nicht mit dem Datenschutz in den Einklang zu bringen ist, war dem Innenministerium, das die datenschutzrechtliche Aufsicht über den TÜV führt, dem Regierungspräsidium Freiburg, dem Landratsamt Schwarzwald-Baar-Kreis und uns sofort klar. Nur das Verkehrsministerium hatte an dem Vorgehen des TÜV zunächst nichts auszusetzen, im Gegenteil: Es hielt die Beiziehung des ersten erstellten Gutachtens durch die zweite Untersuchungsstelle des TÜV sogar für notwendig. Ein halbes Jahr später machte es allerdings dann doch einen Rückzieher und ließ den TÜV wissen, daß die Gutachtenanforderung unzulässig sei. Unserer Forderung, dafür zu sorgen, daß die Führerscheinstellen künftig schon den Gutachtenauftrag an die erste Untersuchungsstelle und deren Schreiben, mit dem es die Akte der Führerscheinstelle zurückgibt, vor der Aktenübersendung an die zweite Untersuchungsstelle der Führerscheinakte entnimmt, wollte das Verkehrsministerium bisher nicht nachkommen, ohne dafür allerdings eine nachvollziehbare Begründung zu geben. Die Zukunft wird weisen, ob das jetzt zuständige Ministerium für Umwelt und Verkehr auch in dieser Frage noch einsichtig wird.

Inhaltsverzeichnis des Anhangs

Anhang 1

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 9./10. Nov. 1995

Datenschutzrechtliche Anforderungen an den Einsatz von Chipkarten im Gesundheitswesen

Die Datenschutzbeauftragten des Bundes und der Länder haben auf ihrer 47. Konferenz am 9./10. März 1994 kritisch zum Einsatz von Chipkarten im Gesundheitswesen Stellung genommen. In dem Beschluß wird die Nutzung von Patientenkarten von mehreren Voraussetzungen zur Sicherung des Persönlichkeitsrechts abhängig gemacht.
Seitdem werden in mehreren Ländern Modellversuche und Pilotprojekte durchgeführt. Die Bandbreite reicht

- von allgemeinen Patientenkarten, die an möglichst viele Patienten/Versicherte ausgegeben werden, eine Vielzahl von Krankheitsdaten enthalten und von einem unbestimmten Kreis von Personen und Institutionen des Gesundheitswesens zu vielfältigen Zwecken verwendet werden können (z.B. VitalCard der AOK Leipzig, Persönliche Patientenkarte Neuwied, BKK-Patientenkarte Berlin)
- bis zu krankheitsspezifischen Karten für bestimmte Patientengruppen mit reduziertem Datensatz und einer Definition der Verwendung (z.B. Dialyse-Card, Diab-Card, Krebsnachsorgekarte, Defi-Card).

Datenschutzrechtlich stellen sich vor allem folgende Probleme:

- Die massenhafte Einführung der Karten erzeugt einen sozialen Druck auf die Betroffenen, sie mitzuführen und vorzuzeigen. Diesen Erwartungen wird sich der Betroffene vielfach nur unter Befremden des Arztes oder sogar der Gefahr, daß dieser die Behandlung ablehnt, verweigern können.
- Die Verwendung von allgemeinen Patientenkarten bringt die Gefahr einer pauschalen Offenbarung von medizinischen Daten mit sich.
- Dem Patienten wird die Last aufgebürdet, für die Sicherheit seiner medizinischen Daten selbst zu sorgen.

Die Datenschutzbeauftragten fordern alle für Kartenprojekte im Gesundheitswesen Verantwortlichen in Politik, Industrie, Ärzteschaft, Wissenschaft und in den Krankenversicherungen auf, das Recht auf informationelle Selbstbestimmung der betroffenen Patienten bzw. Versicherten zu gewährleisten. Die 50. Konferenz hält folgende Voraussetzungen für elementar:

1. Besondere Schutzwürdigkeit medizinischer Daten
   Medizinische Daten sind besonders schutzwürdig, unabhängig davon, welche Technologien eingesetzt werden, ob die Patientendaten beim Arzt gespeichert und versandt oder über ein Netz abgerufen werden oder ob der Patient die Daten auf einer Chipkarte bei sich hat. Es handelt sich oftmals um belastende, schicksalhafte Daten. Zudem geht es nicht nur um Daten des Patienten, sondern auch um fremde Einblicke in die ärztliche Tätigkeit.

2. Wirksame Entscheidung der Betroffenen über die Verwendung einer Karte
   Die freie Entscheidung der Betroffenen (Patienten/Versicherten), eine Chipkarte zu verwenden, muß gewährleistet sein. Dies umfaßt die Entscheidung,
   - ob Daten auf einer Chipkarte gespeichert werden,
   - welche der Gesundheitsdaten auf die Karte aufgenommen werden,
   - welche Daten auf der Karte wieder gelöscht werden,
   - ob die Karte bei einem Arztbesuch bzw. einem Apothekenbesuch vorgelegt wird und
   - welche Daten im Einzelfall zugänglich gemacht werden.

   Ein Widerruf der Entscheidung muß ohne Nachteile für die Betroffenen möglich sein. Die gleiche Freiheit der Entscheidung für oder gegen die Verwendung der Chipkarte muß für Ärzte und Apotheker gewährleistet sein. Eine wirksame Entscheidung für oder gegen die Verwendung einer Chipkarte setzt eine schriftliche, objektive, vollständige und nachvollziehbare Information über Zweck, Art, Umfang und Beteiligte der Chipkarten-Kommunikation voraus. Das Gesamtkonzept des Chipkarteneinsatzes und der damit

verbundenen Datenverarbeitung muß für die Betroffenen überschaubar sein. Auf der Karte darf nicht der Datensatz der Krankenversichertenkarte nach § 291 Abs. 2 SGB V, insbesondere nicht die Krankenversicherung und die Krankenversicherungsnummer, gespeichert werden, da andernfalls – zumal bei allgemeinen Patientenkarten mit hohem Verbreitungsgrad – die Krankenversichertenkarte verdrängt und deren Nutzungsbeschränkungen umgangen werden.

3. Freiheit der Entscheidung
Die uneingeschränkte Freiheit der Entscheidung der Betroffenen für oder gegen die Verwendung einer Chipkarte muß gewährleistet sein, denn der Einsatz von Chipkarten im Gesundheitswesen führt keineswegs zwangsläufig zu größerer Autonomie der Patienten. Neue Technologien können sich auch als Verführung erweisen, deren Preis erst langfristig erkennbar wird. Die individuelle Entscheidung des Bürgers über die Verarbeitung seiner Daten war und bleibt ein zentrales Recht gegenüber Eingriffen in seine Freiheitssphäre. Mit der Chipkarte können sich jedoch Situationen ergeben, in denen wirkliche Freiheit, tatsächliche Wahlmöglichkeit der Betroffenen nicht mehr gewährleistet sind und durch technische und organisatorische, rechtliche und soziale Rahmenbedingungen wiederhergestellt werden müssen.
Dem Staat kommt hier eine veränderte Rolle zu: Freiheitsrechte nicht einzuschränken, sondern sie zu sichern, wo Entwicklungen des Marktes und der Technologien sowie Gruppeninteressen die Entscheidungsfreiheit des Bürgers bedrohen. Die Technologie selbst kann für die Sicherung der Freiheitsrechte ein wertvolles Hilfsmittel sein. Darüber hinaus kommt der Informiertheit der Betroffenen ein zentraler Stellenwert zu. Ihre Kompetenz zur Entscheidung und zum praktischen Umgang mit der Karte muß gestärkt werden, damit sie auch langfristig die größtmöglichen Chancen haben, ihre Interessen durchzusetzen.
Mit der Ausstellung der Karte dürfen nur die Vorteile verknüpft werden, die sich unmittelbar aus den Nutzungspraktiken der Karte selbst ergeben. Die freie Entscheidung der Betroffenen, eine Karte zu nutzen oder dies abzulehnen, darf nicht durch einen Nutzungszwang oder eine Bevorzugung von Karten-Nutzern (z.B. durch Bonuspunkte) bzw. von Karten-Verweigerern eingeschränkt werden.

4. Keine Verschlechterung der Situation der Betroffenen
Durch die Einführung von Kommunikationssystemen mit Chipkarten dürfen die Betroffenen nicht schlechter gestellt werden als im konventionellen Verfahren. Die medizinische Versorgung, der Schutz der Gesundheitsdaten und die Mitentscheidungsrechte der Betroffenen müssen in Umfang und Qualität erhalten bleiben.
Das therapeutische Verhältnis Arzt/Patient darf sich durch den Einsatz von Chipkarten nicht verschlechtern. Freiheit und Vertrauen innerhalb des Arzt-Patienten-Verhältnisses sowie der Grundsatz der Abschottung der dem Arzt anvertrauten Informationen und der ärztlichen Erkenntnisse nach außen, gegen die Kenntnisnahme durch Dritte, müssen erhalten bleiben. Insbesondere muß der Gesetzgeber sicherstellen, daß die auf der beim Patienten befindlichen Chipkarte gespeicherten medizinischen Daten ebenso gegen Beschlagnahme und unbefugte Kenntnisnahme geschützt sind wie die beim Arzt gespeicherten Daten. Eine Kommunikation unter Vorlage der Karte mit Personen oder Stellen außerhalb des Arzt-Patienten-Verhältnisses, z.B. Arbeitgebern oder Versicherungen, muß vom Gesetzgeber untersagt werden.
Das sich im Gespräch entwickelte Vertrauensverhältnis zwischen Arzt und Patient darf nicht durch eine Chipkarten-vermittelte Kommunikation verdrängt werden. Verkürzte Darstellungen medizinischer Sachverhalte auf der Chipkarte – z.B. mit Hilfe von Schlüsselbegriffen – dürfen nicht zu einer Minderung der Qualität des therapeutischen Verhältnisses führen; das liegt auch im Interesse des Arztes. Der Patient muß auch weiterhin die Möglichkeit des individuellen Dialogs wählen können. Dies schließt insbesondere die Freiheit des Betroffenen ein, eine Chipkarte im Einzelfall nicht vorzulegen, auf der Chipkarte nur einen begrenzten Datensatz speichern zu lassen oder zu entscheiden, welchem Arzt welche Informationen oder Informationsbereiche offenbart werden. Der Patient darf durch die Ausgestaltung und den Verwendungszusammenhang der Chipkarte nicht zur pauschalen Offenbarung seiner Daten gezwungen sein. So sind Daten auf der Chipkarte so zu ordnen, daß z.B. beim Zahnarzt die gynäkologische Behandlung geheim bleiben kann.

Es darf keine „Einwilligung“ in Chipkarten und Chipkartensysteme mit verminderter Datensicherheit geben. Der Gesetzgeber muß die Patientenkarten vor „billigen Gesundheitskarten“ ohne ausreichende Sicherung vor einer Nutzung durch Dritte schützen.

5. Sicherstellung der Integrität und Authentizität der Daten
Zur Sicherstellung der Vertraulichkeit, Integrität und Authentizität der Daten auf Chipkarten im Gesundheitswesen und zur Differenzierung der Zugriffsmöglichkeiten nach dem Grundsatz der Erforderlichkeit in unterschiedlichen Situationen sind kryptographische Verfahren sowie geeignete Betriebssysteme zur Abschottung unterschiedlicher Anwendungsbereiche nach dem Stand der Technik in Chipkarten und Schreib-/Lese-Terminals zu implementieren. Eine Protokollierung der Lösch- und Schreibvorgänge auf der Karte ist unverzichtbar.

   Darüber hinaus ist für das infrastrukturelle Kartenumfeld (Herstellung, Verteilung, Personalisierung, ..., Rücknahme) sicherzustellen, daß ausreichende technische und organisatorische Maßnahmen Berücksichtigung finden. Für die zur Erstellung und Personalisierung von Gesundheits-Chipkarten dienenden Systeme sowie die informationstechnischen Systeme und Verfahren, mit denen Daten auf der Chipkarte gelesen, eingetragen, verändert, gelöscht oder verarbeitet werden, muß der gleiche hohe Sicherheitsstandard erreicht werden.

6. Keine neuen zentralen medizinischen Datensammlungen
Der Einsatz von Chipkarten im Gesundheitswesen darf nicht zur Entstehung neuer zentraler Dateien von Patientendaten bei Kassenärztlicher Vereinigung, Krankenkassen, Kartenherstellern oder sonstigen Stellen führen. Dies gilt auch für das Hinterlegen von Sicherungskopien der auf der Karte gespeicherten medizinischen Daten. Es steht in der freien Entscheidung der Betroffenen, ob sie dem Arzt ihres Vertrauens eine umfassende Pflege aller Chipkarten-Daten – einschließlich der Sicherungskopien – übertragen oder nicht.

7. Leserecht des Karteninhabers
Der Karteninhaber muß das Recht und die Möglichkeit haben, seine auf der Chipkarte gespeicherten Daten vollständig zu lesen.

8. Suche nach datenschutzfreundlichen Alternativen
Angesichts der aufgezeigten Gefährdungen der informationellen Selbstbestimmung im Gesundheitswesen muß die Suche nach datenschutzfreundlichen Alternativen zur Chipkarte fortgesetzt werden.

Vorstehende Kriterien sind der Maßstab für die datenschutzrechtliche Bewertung von Projekten für die Einführung von Chipkarten im Gesundheitswesen.

Die Datenschutzbeauftragten von Bund und Ländern fordern die Gesetzgeber auf, die dringend notwendigen Regelungen zur Sicherung der Rechte von Patienten und Ärzten zu schaffen. Ebenso ist durch die Gesetzgeber den Besonderheiten der Datenverarbeitung auf Chipkarten durch bereichsspezifische Regelungen Rechnung zu tragen.

Anhang 2

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 14./15. März 1996

Transplantationsgesetz

Bei der anstehenden gesetzlichen Regelung, unter welchen Voraussetzungen die Entnahme von Organen zur Transplantation zulässig sein soll, werden untrennbar mit der Ausformung des Rechts auf Selbstbestimmung auch Bedingungen des Rechts auf informationelle Selbstbestimmung festgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont hierzu, daß von den im Gesetzgebungsverfahren diskutierten Modellen die „enge Zustimmungslösung“ – also eine ausdrückliche Zustimmung des Organspenders – den geringsten Eingriff in das Recht auf informationelle Selbstbestimmung beinhaltet. Sie zwingt niemanden, eine Ablehnung zu dokumentieren. Sie setzt auch kein Organspenderegister voraus.

Mit einer engen Zustimmungslösung ist auch vereinbar, daß der Organspender seine Entscheidung z.B. einem nahen Angehörigen überträgt.

Anhang 3

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 14./15. März 1996

Modernisierung und europäische Harmonisierung des Datenschutzrechts

Die Datenschutzrichtlinie der Europäischen Union vom Oktober 1995 verpflichtet alle Mitgliedstaaten, ihr Datenschutzrecht binnen drei Jahren auf europäischer Ebene zu harmonisieren. Die Richtlinie geht zu Recht von einem hohen Datenschutzniveau aus und stellt fest: „Die Datenverarbeitungssysteme stehen im Dienste des Menschen".

Die Datenschutzbeauftragten begrüßen diesen wichtigen Schritt zu einem auch international wirksamen Datenschutz. Sie appellieren an den Gesetzgeber in Bund und Ländern, die Umsetzung der Richtlinie nicht nur als Beitrag zur europäischen Integration zu verstehen, sondern als Aufforderung und Chance, den Datenschutz fortzuentwickeln. Die Datenschutzbeauftragten sprechen sich für eine umfassende Modernisierung des deutschen Datenschutzrechts aus, damit der einzelne in der sich rapide verändernden Welt der Datenverarbeitung, der Medien und der Telekommunikation über den Umlauf und die Verwendung seiner persönlichen Daten soweit wie möglich selbst bestimmen kann.

Die wichtigsten Ziele sind:

1. Weitgehende Vereinheitlichung der Vorschriften für den öffentlichen und privaten Bereich mit dem Ziel eines hohen, gleichwertigen Schutzes der Betroffenen, beispielsweise bei der Datenerhebung und bei der Zweckbindung bis hin zur Verarbeitung in Akten.
2. Erweiterung der Rechte der Betroffenen auf Information durch die datenverarbeitenden Stellen über die Verwendung der Daten, auf Auskunft, auf Widerspruch und im Bereich der Einwilligung.
3. Verpflichtung zu Risikoanalyse, Vorabkontrolle, Technikfolgenabschätzung und zur Beteiligung der Datenschutzbeauftragten bei der Vorbereitung von Regelungen mit Auswirkungen auf den Datenschutz.
4. Verbesserung der Organisation und Stärkung der Befugnisse der Datenschutzkontrolle unter den Gesichtspunkten der Unabhängigkeit und der Effektivität.
5. Einrichtung und effiziente Ausgestaltung des Amtes eines internen Datenschutzbeauftragten in öffentlichen Stellen.
6. Weiterentwicklung der Vorschriften zur Datensicherheit, insbesondere im Hinblick auf Miniaturisierung und Vernetzung.

Darüber hinaus machen die Datenschutzbeauftragten folgende Vorschläge:

7. Erweiterung des Schutzbereichs bei Bild- und Tonaufzeichnungen und Regelung der Video-Überwachung.
8. Stärkere Einbeziehung von Presse und Rundfunk in den Datenschutz, Aufrechterhaltung von Sonderregelungen nur, soweit dies für die Sicherung der Meinungsfreiheit notwendig ist.
9. Sonderregelungen für besonders empfindliche Bereiche, wie den Umgang mit Arbeitnehmerdaten, Gesundheitsdaten und Informationen aus gerichtlichen Verfahren.
10. Sicherstellung der informationellen Selbstbestimmung bei Multimedia-Diensten und anderen elektronischen Dienstleistungen durch die Pflicht, auch anonyme Nutzungs- und Zahlungsformen anzubieten, durch den Schutz vor übereilter Einwilligung, z.B. durch ein Widerrufsrecht, und durch strenge Zweckbindung für die bei Verbindung, Aufbau und Nutzung anfallenden Daten.
11. Besondere Regelungen für Chipkarten-Anwendungen, um die datenschutzrechtliche Verantwortung aller Beteiligten festzulegen und den einzelnen vor unfreiwilliger Preisgabe seiner Daten zu schützen.

12. Schutz bei Persönlichkeitsbewertungen durch den Computer, insbesondere durch Beteiligung des Betroffenen und Nachvollziehbarkeit der Computerentscheidung.
13. Verstärkung des Schutzes gegenüber Adressenhandel und Direktmarketing.
14. Verbesserung des Datenschutzes bei grenzüberschreitender Datenverarbeitung; Datenübermittlung ins Ausland nur bei angemessenem Datenschutzniveau.

Anhang 4

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 29. April 1996

Eckpunkte für die datenschutzrechtliche Regelung von Mediendiensten

In letzter Zeit finden Online-Dienste und Multimedia-Anwendungen zunehmend Verbreitung. Mit den – häufig multimedialen – Angeboten, auf die interaktiv über Telekommunikationsnetze zugegriffen werden kann, sind besondere Risiken für das Recht auf informationelle Selbstbestimmung der Teilnehmer verbunden; hinzuweisen ist insbesondere auf die Gefahr, daß das Nutzerverhalten unbemerkt registriert und zu Verhaltensprofilen zusammengeführt wird. Das allgemeine Datenschutzrecht reicht nicht aus, die mit den neuen technischen Möglichkeiten und Nutzungsformen verbundenen Risiken wirkungsvoll zu beherrschen.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für dringend erforderlich, durch bereichsspezifische Regelungen technische und rechtliche Gestaltungsanforderungen für die elektronischen Dienste zu formulieren, die den Datenschutz sicherstellen. Leitlinie sollte hierbei der Grundsatz der Datenvermeidung bzw. -minimierung sein. Die Datenschutzbeauftragten haben dazu in einer Entschließung vom 14./15. März 1996 zur Modernisierung und zur europäischen Harmonisierung des Datenschutzrechts vorgeschlagen, daß die informationelle Selbstbestimmung bei Multimediadiensten und anderen elektronischen Dienstleistungen durch die Pflicht, auch anonyme Nutzungs- und Zahlungsverfahren anzubieten, durch den Schutz vor übereilter Einwilligung, z.B. durch ein Widerspruchsrecht, und durch strenge Zweckbindung für die bei der Verbindung, Nutzung und Abrechnung anfallenden Daten sichergestellt wird.

Die Datenschutzbeauftragten weisen darauf hin, daß auch mit Inhalten, die durch Mediendienste verbreitet werden, datenschutzrechtliche Probleme verbunden sein können. Auf diese Probleme wird im folgenden jedoch – ebenso wie auf die Datenschutzaspekte der Telekommunikation – nicht näher eingegangen. Bei den datenschutzrechtlichen Eckpunkten wird ferner bewußt darauf verzichtet, den Regelungsort – etwa einen Länder-Staatsvertrag oder ein Bundesgesetz – anzugeben. Die Datenschutzbeauftragten appellieren an die Gesetzgeber in Bund und Ländern, eine angemessene datenschutzgerechte Regulierung der neuen Dienste nicht an Kompetenzstreitigkeiten scheitern zu lassen.

1. *Anonyme bzw. datensparsame Nutzung:* Die Dienste und Multimedia-Einrichtungen sollten so gestaltet werden, daß keine oder möglichst wenige personenbezogene Daten erhoben, verarbeitet und genutzt werden; deshalb sind auch anonyme Nutzungs- und Zahlungsformen anzubieten. Auch zur Aufrechterhaltung und zur bedarfsgerechten Gestaltung von Diensten und Dienstleistungen (Systempflege) sind soweit wie möglich anonymisierte Daten zu verwenden. Soweit eine vollständig anonyme Nutzung nicht realisiert werden kann, muß jeweils geprüft werden, ob durch andere Verfahren, z.B. die Verwendung von Pseudonymen, ein unmittelbarer Personenbezug vermieden werden kann. Die Herstellung des Personenbezugs sollte bei diesen Nutzungsformen nur dann erfolgen, wenn hieran ein begründetes rechtliches Interesse besteht.

2. *Bestandsdaten:* Bestandsdaten dürfen nur in dem Maße erhoben, verarbeitet und genutzt werden, soweit sie für die Begründung und Abwicklung eines Vertragsverhältnisses sowie für die Systempflege erforderlich sind. Die Bestandsdaten dürfen zur bedarfsgerechten Gestaltung von Diensten und Dienstleistungen sowie zur Werbung und Marktforschung genutzt werden, soweit der Betroffene dem nicht widersprochen hat. Für die Werbung und Marktforschung durch Dritte dürfen Bestandsdaten nur mit der ausdrücklichen Einwilligung des Betroffenen verarbeitet werden.

3. *Verbindungs- und Abrechnungsdaten:* Verbindungs- und Abrechnungsdaten dürfen nur für Zwecke der Vermittlung von Angeboten und für Abrechnungszwecke erhoben, gespeichert und genutzt werden. Sie sind zu löschen, wenn sie für die Erbringung der Dienstleistung oder für Abrechnungszwecke nicht mehr erforderlich sind. Soweit Verbindungsdaten ausschließlich zur

Vermittlung einer Dienstleistung gespeichert werden, sind sie spätestens nach Beendigung der Verbindung zu löschen. Die Speicherung der Abrechnungsdaten darf den Zeitpunkt, die Dauer, die Art, den Inhalt und die Häufigkeit bestimmter von den einzelnen Teilnehmern in Anspruch genommener Angebote nicht erkennen lassen, es sei denn, der Teilnehmer beantragt eine dahin gehende Speicherung. Verbindungs- und Abrechnungsdaten sind einer strikten Zweckbindung zu unterwerfen. Sie dürfen über den hier genannten Umfang hinaus nur mit der ausdrücklichen Einwilligung des Betroffenen erhoben, verarbeitet und genutzt werden. Unberührt hiervon bleibt die Speicherung von Daten von Verantwortlichen für Angebote im Zusammenhang mit Impressumspflichten.

4. *Interaktionsdaten:* Werden im Rahmen von interaktiven Dienstleistungen darüber hinaus personenbezogene Daten erhoben, die nachweisen, welche Eingaben der Teilnehmer während der Nutzung des Angebots zur Beeinflussung des Ablaufs vorgenommen hat (Interaktionsdaten; hierzu gehören z.B. Daten, die bei lexikalischen Abfragen, in interaktive Suchsysteme – etwa elektronische Fahrpläne und Telefonverzeichnisse – und bei Online-Spielen eingegeben werden), darf dies nur in Kenntnis und mit ausdrücklicher Einwilligung des Betroffenen geschehen. Interaktionsdaten dürfen nur unter Beachtung einer strikten Zweckbindung verarbeitet und genutzt werden. Sie sind grundsätzlich zu löschen, wenn der Zweck, zu dem sie erhoben wurden, erreicht wurde (so müssen Daten über die interaktive Suche von Angeboten unmittelbar nach Beendigung des Suchprozesses gelöscht werden). Eine weitergehende Verarbeitung dieser Daten ist nur auf Grundlage einer ausdrücklichen Einwilligung des Betroffenen zulässig.

5. *Einwilligung:* Der Abschluß oder die Erfüllung eines Vertragsverhältnisses dürfen nicht davon abhängig gemacht werden, daß der Betroffene in die Verarbeitung oder Nutzung seiner Daten außerhalb der zulässigen Zweckbestimmung eingewilligt hat. Soweit Daten aufgrund einer Einwilligung erhoben werden, muß diese jederzeit widerrufen werden können. Für die Form und Dokumentation elektronisch abgegebener Einwilligungen und sonstiger Willenserklärungen ist ein Mindeststandard zu definieren, der einen fälschungssicheren Nachweis über die Tatsache, den Zeitpunkt und den Gegenstand gewährleistet. Dabei ist sicherzustellen, daß der Teilnehmer bereits vor der Einwilligung soweit wie möglich über den Inhalt und die Folgen seiner Einwilligung und über sein Widerrufsrecht informiert ist. Deshalb müssen die Betroffenen sowohl vor als auch nach Eingabe der Erklärung die Möglichkeit haben, auf Einwilligungen, Verträge und sonstige Informationen über die Bedingungen der Nutzung von Diensten, Multimedia-Einrichtungen und Dienstleistungen zuzugreifen und diese auch in schriftlicher Form zu erhalten. Da Verträge oder andere rechtswirksame Erklärungen, die in einer Fremdsprache verfaßt sind, unter Umständen juristische Fachbegriffe enthalten, die nur vor dem Hintergrund der jeweiligen Rechtsordnung zu verstehen sind, sollten zumindest diejenigen Dienste, die eine deutschsprachige Benutzeroberfläche anbieten, derartige Unterlagen auch in deutscher Sprache bereitstellen.

6. *Transparenz der Dienste und Steuerung der Datenübertragung durch die Teilnehmer:* Die automatische Übermittlung von Daten durch die beim Betroffenen eingesetzte Datenverarbeitungsanlage ist auf das technisch für die Vertragsabwicklung notwendige Maß zu beschränken. Eine darüber hinausgehende Übermittlung ist nur aufgrund einer besonderen Einwilligung zulässig. Im Hinblick darauf, daß die Teilnehmer bei der eingesetzten Technik nicht erkennen können, in welchem Dienst sie sich befinden und welche Daten bei der Nutzung von elektronischen Diensten bzw. bei der Erbringung von Dienstleistungen automatisiert übertragen und gespeichert werden, ist sicherzustellen, daß die Teilnehmer vor Beginn der Datenübertragung hierüber informiert werden und die Möglichkeit haben, den Prozeß jederzeit abzubrechen. Die zur Nutzung vom Anbieter oder Netzbetreiber bereitgestellte Software muß eine vom Nutzer aktivierbare Möglichkeit enthalten, den gesamten Strom der ein- und ausgehenden Daten vollständig zu protokollieren. Bei einer Durchschaltung zu einem anderen Dienst bzw. zu einer anderen Multimedia-Einrichtung müssen die Teilnehmer über die Durchschaltung und damit mögliche Datenübertragungen informiert werden. Diensteanbieter haben zu gewährleisten, daß sie keine erkennbar unsicheren Netze für die

Übertragung personenbezogener Daten nutzen bzw. den Schutz dieser Daten durch angemessene Maßnahmen sicherstellen. Entsprechend dem Stand der Technik sind geeignete (z.B. kryptographische) Verfahren anzuwenden, um die Vertraulichkeit und Integrität der übertragenen Daten sowie eine sichere Identifizierung und Authentifikation zwischen Teilnehmern und Anbietern zu gewährleisten.

7. *Rechte von Betroffenen:* Die Rechte von Betroffenen auf Auskunft, Sperrung, Berichtigung und Löschung sind auch bei multimedialen und sonstigen elektronischen Diensten zu gewährleisten. Soweit personenbezogene Daten im Rahmen eines elektronischen Dienstes veröffentlicht wurden, der dem Medienprivileg unterliegt, ist das Gegendarstellungsrecht der von der Veröffentlichung Betroffenen sicherzustellen.

8. *Datenschutzkontrolle:* Eine effektive, unabhängige und nicht anlaßgebundene Datenschutzaufsicht ist zu gewährleisten. Den für die Kontrolle des Datenschutzes zuständigen Behörden ist ein jederzeitiger kostenfreier elektronischer Zugriff auf die Dienste und Dienstleistungen und der Zugang zu den eingesetzten technischen Einrichtungen zu ermöglichen. Bei elektronischen Diensten, für die das Medienprivileg gilt, ist die externe Datenschutzkontrolle entsprechend zu beschränken.

9. *Geltungsbereich:* Der Geltungsbereich der jeweiligen Regelungen ist eindeutig festzulegen. Es ist sicherzustellen, daß die Datenschutzbestimmungen auch gelten, sofern personenbezogene Daten nicht in Dateien verarbeitet werden.

10. *Internationale Datenschutzregelung:* Im Hinblick auf die zunehmende Bedeutung grenzüberschreitender elektronischer Dienste und Dienstleistungen ist eine Fortentwicklung der europäischen und internationalen Rechtsordnung dringend erforderlich, die auch bei ausländischen Diensten, Dienstleistungen und Multimedia-Angeboten ein angemessenes Datenschutzniveau gewährleistet. Die Verabschiedung der sog. ISDN-Datenschutzrichtlinie mit einem europaweiten hohen Schutzstandard ist überfällig. Kurzfristig ist es notwendig, den Betroffenen angemessene Mittel zur Durchsetzung ihrer Datenschutzrechte gegenüber ausländischen Betreibern und Dienstleistern in die Hand zu geben. Die in Deutschland aktiven Dienste aus Nicht-EG-Staaten haben im Sinne der EG-Datenschutzrichtlinie (95/46/EG) vom 24.10.1995 einen verantwortlichen inländischen Vertreter zu benennen.

Anhang 5

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 9. Mai 1996

Forderungen zur sicheren Übertragung
elektronisch gespeicherter personenbezogener Daten

Der Schutz personenbezogener Daten ist während der Übertragung oder anderer Formen des Transports nicht immer gewährleistet. Elektronisch gespeicherte, personenbezogene Daten können sowohl auf leitungsgebundenen oder drahtlosen Übertragungswegen als auch auf maschinell lesbaren Datenträgern weitergegeben werden. Oft sind die Eigenschaften des Transportweges dem Absender und dem Empfänger weder bekannt noch durch sie beeinflußbar. Vor allem die Vertraulichkeit, die Integrität (Unversehrtheit) und die Zurechenbarkeit der Daten (Authentizität) sind nicht sichergestellt, solange Manipulationen, unbefugte Kenntnisnahme und Fehler während des Transportes nicht ausgeschlossen werden können. Die Verletzung der Vertraulichkeit ist möglich, ohne daß Spuren hinterlassen werden.

Zahlreiche Rechtsvorschriften gebieten, das Grundrecht auf informationelle Selbstbestimmung auch während der automatisierten Verarbeitung personenbezogener Daten zu sichern (z.B. § 78 a SGB X mit Anlage, § 10 Abs. 8 Btx-Staatsvertrag, § 9 BDSG nebst Anlage und entsprechende landesgesetzliche Regelungen).

Kryptographische Verfahren (z.B. symmetrische und asymmetrische Verschlüsselung, digitale Signatur) sind besonders geeignet, um Verletzungen des Datenschutzes beim Transport schutzwürdiger elektronisch gespeicherter Daten zu verhindern. Mit ihrer Hilfe lassen sich Manipulationen und Übertragungsfehler nachweisen und die unberechtigte Kenntnisnahme verhindern. Derartige Verfahren sind heute Stand der Technik und können in vielen Anwendungsfällen mit vertretbarem Aufwand eingesetzt werden.

Angesichts der beschriebenen Situation und der vorhandenen technischen Möglichkeiten fordern die Datenschutzbeauftragten des Bundes und der Länder, geeignete, sichere kryptographische Verfahren beim Transport elektronisch gespeicherter personenbezogener Daten unter Berücksichtigung ihrer Schutzwürdigkeit anzuwenden.

Anhang 6

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 22./23. Oktober 1996

Datenschutz bei der Vermittlung und Abrechnung digitaler Fernsehsendungen

Mit der Markteinführung des digitalen Fernsehens eröffnen sich für die Anbieter – neben einem deutlich ausgeweiteten Programmvolumen – neue Möglichkeiten für die Vermittlung und Abrechnung von Sendungen. Hinzuweisen ist in erster Linie auf Systeme, bei denen die Kunden für die einzelnen empfangenen Sendungen bezahlen müssen. Dort entsteht die Gefahr, daß die individuelle Vorliebe, Interessen und Sehgewohnheiten registriert und damit Mediennutzungsprofile einzelner Zuschauer erstellt werden. Die zur Vermittlung und zur Abrechnung verfügbaren technischen Verfahren können die Privatsphäre des Zuschauers in unterschiedlicher Weise beeinträchtigen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Anbieter und Programmlieferanten auf, den Nutzern zumindest alternativ auch solche Lösungen anzubieten, bei denen die Nutzung der einzelnen Programmangebote nicht personenbezogen registriert werden kann, wie es der Entwurf des Mediendienste-Staatsvertrags bereits vorsieht. Die technischen Voraussetzungen für derartige Lösungen sind gegeben.

Die technischen Verfahren sind so zu gestalten, daß möglichst keine personenbezogenen Daten erhoben, gespeichert und verarbeitet werden (Prinzip der Datensparsamkeit). Verfahren, die im voraus bezahlte Wertkarten – Chipkarten – nutzen, um die mit entsprechenden Entgeltinformationen ausgestrahlten Sendungen zu empfangen und zu entschlüsseln, entsprechen weitgehend dieser Forderung. Allerdings setzt eine anonyme Nutzung voraus, daß beim Zuschauer gespeicherte Informationen über die gesehenen Sendungen nicht durch den Anbieter abgerufen werden können.

Die Datenschutzbeauftragten sprechen sich außerdem dafür aus, daß für die Verfahren auf europäischer Ebene Vorgaben für eine einheitliche Architektur mit gleichwertigen Datenschutzvorkehrungen entwickelt werden.

Anhang 7

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 22./23. Oktober 1996

Eingriffsbefugnisse zur Strafverfolgung im Informations- und Telekommunikationsbereich

Die Entwicklung moderner Informations- und Telekommunikationstechniken führt zu einem grundlegend veränderten Kommunikationsverhalten der Bürger.

Die Privatisierung der Netze und die weite Verbreitung des Mobilfunks geht einher mit einer weitreichenden Digitalisierung der Kommunikation. Mailboxen und das Internet prägen die Informationsgewinnung und -verbreitung von Privatleuten, von Unternehmen und öffentlichen Institutionen gleichermaßen.

Neue Dienste wie Tele-Working, Tele-Banking, Tele-Shopping, digitale Videodienste und Rundfunk im Internet sind einfach überwachbar, weil personenbezogene Daten der Nutzer in digitaler Form vorliegen. Die herkömmlichen Befugnisse zur Überwachung des Fernmeldeverkehrs erhalten eine neue Dimension; weil immer mehr personenbezogene Daten elektronisch übertragen und gespeichert werden, können sie mit geringem Aufwand kontrolliert und ausgewertet werden. Demgegenüber stehen jedoch auch Gefahren durch die Nutzung der neuen Technik zu kriminellen Zwecken. Die Datenschutzbeauftragten erkennen an, daß die Strafverfolgungsbehörden in die Lage versetzt werden müssen, solchen mißbräuchlichen Nutzungen der neuen Techniken zu kriminellen Zwecken wirksam zu begegnen.

Sie betonen jedoch, daß die herkömmlichen weitreichenden Eingriffsbefugnisse auch unter wesentlich veränderten Bedingungen nicht einfach auf die neuen Formen der Individual- und Massenkommunikation übertragen werden können. Die zum Schutz der Persönlichkeitsrechte des einzelnen gezogenen Grenzen müssen auch unter den geänderten tatsächlichen Bedingungen der Verwendung der modernen Informationstechnologien aufrechterhalten und gewährleistet werden. Eine Wahrheitsfindung um jeden Preis darf es auch insoweit nicht geben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher Thesen zur Bewältigung dieses Spannungsverhältnisses entwickelt.

Sie hebt insbesondere den Grundsatz der spurenlosen Kommunikation hervor. Kommunikationssysteme müssen mit personenbezogenen Daten möglichst sparsam umgehen. Daher verdienen solche Systeme und Technologien Vorrang, die keine oder möglichst wenige Daten zum Betrieb benötigen. Ein positives Beispiel ist die Telefonkarte, deren Nutzung keine personenbezogenen Daten hinterläßt und die deshalb für andere Bereiche als Vorbild angesehen werden kann. Daten allein zu dem Zweck einer künftig denkbaren Strafverfolgung bereitzuhalten ist unzulässig.

Bei digitalen Kommunikationsformen läßt sich anhand der Bestands- und Verbindungsdaten nachvollziehen, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und damit wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen und Neigungen nachgeht. Eine staatliche Überwachung dieser Vorgänge greift tief in das Persönlichkeitsrecht der Betroffenen ein und berührt auf empfindliche Weise die Informationsfreiheit und den Schutz besonderer Vertrauensverhältnisse (z.B. Arztgeheimnis, anwaltliches Vertrauensverhältnis). Die Datenschutzbeauftragten fordern daher, daß der Gesetzgeber diesen Gesichtspunkten Rechnung trägt.

Die Datenschutzbeauftragten wenden sich nachhaltig dagegen, daß den Nutzern die Verschlüsselung des Inhalts ihrer Nachrichten verboten wird. Die Möglichkeit für den Bürger, seine Kommunikation durch geeignete Maßnahmen vor unberechtigten Zugriffen zu schützen, ist ein traditionelles verfassungsrechtlich verbürgtes Recht.

Aus Sicht des Datenschutzes besteht andererseits durchaus Verständnis für das Interesse der Sicherheits- und Strafverfolgungsbehörden, sich rechtlich zulässige Zugriffsmöglichkeiten nicht dadurch versperren zu lassen, daß Verschlüsselungen verwandt werden, zu denen sie keinen Zugriff haben. Eine Reglementierung der

Verschlüsselung, z.B. durch Schlüsselhinterlegung, erscheint aber aus derzeitiger technischer Sicht kaum durchsetzbar, da entsprechende staatliche Maßnahmen – insbesondere im weltweiten Datenverkehr – ohnehin leicht zu umgehen und kaum kontrollierbar wären.

Anhang 8

Hinweise zur Datensicherheit beim Telefax

Immer mehr Behörden, Unternehmen und auch Privatpersonen nutzen den Telefaxdienst, um schriftliche Nachrichten zu übertragen. Die Telefaxübertragung ist im Vergleich zum herkömmlichen Brief schneller und oft auch preiswerter. Zudem ist es scheinbar kinderleicht, Telefaxe zu versenden. Aber die Telefax-Technik birgt auch – im Vergleich zu herkömmlichen Briefen und Telefongesprächen – neue Risiken: Während man beim Telefon eine falsche Verbindung sehr schnell erkennt und sich entsprechend verhalten kann, wird ein Telefax im Fall einer falschen Verbindung oft vollständig übertragen, bevor der Absender den Fehler bemerkt. Ein wesentlicher Unterschied zum Brief besteht darin, daß Telefaxe beim Empfänger unverschlossen ankommen. Jeder, der sich in der Nähe des Telefaxgerätes aufhält, kann die ankommenden Telefaxe lesen.
Leider kommt es nur zu oft zu Telefax-Irrläufern, die in den meisten Fällen auf vermeidbare organisatorische Mängel oder Bedienungsfehler zurückzuführen sind. Soweit personenbezogene Informationen betroffen sind, stellt eine Telefax-Fehlleitung einen Verstoß gegen den Datenschutz dar, denn dabei gelangen die Daten in die Hände von Personen, für die sie nicht bestimmt sind. Um dem vorzubeugen, sollten alle Dienststellen – so wie dies die „zehn Gebote“ des Datenschutzes (vgl. z.B. § 9 LDSG) verlangen – im Umgang mit Telefaxgeräten ausreichende technische und organisatorische Sicherungsmaßnahmen ergreifen.

Was ist bei der Anschaffung eines Telefaxgeräts zu beachten?
Wer beabsichtigt, ein neues Telefaxgerät zu erwerben, sollte beim Kauf nicht nur auf den Preis, sondern auch auf folgende Eigenschaften achten, die später einen datenschutzgerechten Betrieb des Telefaxgeräts erleichtern:

- Bedienungsanleitung
  Bei der Anschaffung eines neuen Geräts ist darauf zu achten, daß eine ausführliche und gut verständliche Bedienungsanleitung mitgeliefert wird. Dies ist eine wichtige Voraussetzung, um die Anzahl der Telefax-Irrläufer, die auf Bedienungsfehler zurückzuführen sind, möglichst gering zu halten.
- Verschlüsselung
  Nach Möglichkeit sollte die Wahl auf ein Gerät fallen, das Telefax-Sendungen verschlüsselt absenden und empfangen kann. Sofern sowohl Absender als auch Empfänger über ein entsprechendes Gerät verfügen, kann durch die verschlüsselte Übertragung verhindert werden, daß Unbefugte die übertragenen Daten beispielsweise durch Anzapfen einer Übertragungsleitung mitlesen oder unbemerkt ändern können.

Datenschutzgerechte Inbetriebnahme
Wer ein Telefaxgerät neu erworben hat, sollte folgendes berücksichtigen, bevor er das Gerät zur Benutzung freigibt:

- Aufstellung
  Das Telefaxgerät ist so aufzustellen, daß Unbefugte keine Kenntnis vom Inhalt eingehender Telefax-Sendungen erhalten können. Insbesondere sollte ein Telefaxgerät nicht in einem Flur oder einem anderen Raum aufgestellt werden, in dem viele Mitarbeiter oder Besucher ungehindert in die Nähe des Telefaxgeräts kommen und empfangene Sendungen lesen können.
- Gerätekennung
  Es ist darauf zu achten, daß sich das eigene Telefaxgerät, wenn es von einem anderen Gerät angewählt wird, mit seiner aktuell gültigen Rufnummer meldet. Diese Nummer muß vor der Inbetriebnahme manuell eingegeben werden und ist entsprechend anzupassen, wenn das Gerät später eine andere Rufnummer erhält.
- Einweisung der Mitarbeiter
  Mitarbeiter der Dienststelle dürfen das Telefaxgerät nur nach vorheriger Einweisung bedienen.
- Dienstanweisung
  Alles was die Mitarbeiter bei der Bedienung des Telefaxgeräts zu beachten haben, sollte in einer Dienstanweisung schriftlich festgelegt sein. Alle Mitarbeiter, die das Telefaxgerät bedienen, müssen diese Dienstanweisung kennen.
- Bedienungshinweise in Kurzform
  Die Dienststelle sollte die wichtigsten Bedienungshinweise gut sichtbar in der Nähe des Telefaxgeräts anbringen.

Was bei der Inbetriebnahme eines an einer Nebenstellenanlage angeschlossenen Telefaxgeräts zu beachten ist

Bei Telefaxgeräten, die an einer Nebenstellenanlage angeschlossen sind, ist das Risiko einer falschen Verbindung größer als bei Geräten, die einen eigenen Hauptanschluß an das öffentliche Netz haben. Daher ist beim Umgang mit derartigen Geräten besondere Sorgfalt geboten. Neben der Telefaxnummer muß ein Absender bei solchen Geräten in der Regel weitere Ziffern oder Zeichen zur Steuerung der Nebenstellenanlage eingeben. Bei Verbindungen in das öffentliche Netz ist es beispielsweise oft erforderlich, eine zusätzliche „0“ einzugeben und zwischen der „0“ und der gewünschten Telefaxnummer die Pausentaste zu betätigen. Welche Eingaben jeweils erforderlich sind, hängt von der Art der Nebenstellenanlage ab. Diese Informationen sind der Bedienungsanleitung des jeweiligen Telefaxgeräts nicht zu entnehmen. Da es durch falsche Verwendung der Steuerzeichen leicht zu Irrläufern kommen kann, sollte der Betreiber des Telefaxgeräts die entsprechenden Bedienungshinweise schriftlich formulieren, allen Benutzern mitteilen und – wie bereits angesprochen – gut sichtbar in der Nähe des Telefaxgeräts aushängen. Sofern technisch möglich, sollte die Nebenstellenanlage so eingerichtet werden, daß sie eine Verbindung ins öffentliche Netz nicht nach Eingabe einer „0“, sondern nach Eingabe eines Zeichens oder einer Zeichenfolge bereitstellt, die nicht auch in normalen Telefaxnummern vorkommen können (z. B. „*“ oder „#“).

Sorgfaltsregeln beim täglichen Umgang mit dem Telefax

Beim Versand von Telefaxen gilt der allgemeine Grundsatz, daß der Absender die Verantwortung für die vertrauliche Übertragung und den Empfang trägt. Er muß einkalkulieren, daß jemand, für den das Telefax nicht bestimmt ist, dieses, sei es aufgrund eines gezielten Angriffs oder eines Bedienungs- oder eines technischen Fehlers, erhält und liest. Folgendes ist deshalb zu beachten:

– Anschlußnummer des Empfängers überprüfen
  Der Absender sollte überprüfen, ob er (noch) die richtige Telefaxnummer des Empfängers besitzt. Dies ist vor allem deshalb empfehlenswert, weil die Telekom die Nummer eines abgemeldeten Telefaxanschlusses oft schon nach kurzer Zeit wieder an einen anderen Teilnehmer vergibt.
– Kein zeitversetztes Senden
  Das von manchen Geräten ermöglichte zeitversetzte Absenden von Telefaxen, mit dem es beispielsweise möglich ist, die am Tag vorbereiteten Sendungen in der Nacht zu übertragen, sollte möglichst nicht genutzt werden, da der Absender bei einer erkennbaren Fehlleitung die Übertragung nicht rechtzeitig abbrechen kann und da der persönliche Empfang hierbei in der Regel nicht gewährleistet werden kann.
– Eingaben überprüfen
  Sofern der Absender die gewünschte Rufnummer über die Tastatur eintippt, sollte er die Nummer zunächst am Display überprüfen, bevor er durch einen Druck auf die Start-Taste dafür sorgt, daß das Telefaxgerät die eingetippte Nummer wählt.
– Nummer des erreichten Geräts überprüfen
  Wenn das Telefaxgerät nach erfolgreicher Wahl eine Verbindung aufgebaut hat, so zeigt es am Display die Rufnummer an, mit der sich das angerufene Gerät meldet. Wenn diese Nummer von der eingegebenen Nummer abweicht, so ist Vorsicht geboten. Der Absender sollte dann den Übertragungsvorgang sofort abbrechen. Falls das Telefaxgerät bei mehrmaligen Versuchen immer die gleiche falsche Rufnummer anzeigt, so sollte man den vorgesehenen Empfänger anrufen, um zu erfahren, ob sein Gerät eine falsche Gerätekennung aussendet oder ob bei ihm eine Rufumleitung auf eine andere als die gewählte Nummer erfolgt.
– Sendebericht prüfen
  Nach dem Absenden eines Telefaxes sollte der Absender einen Blick auf den Sendebericht werfen und kontrollieren, ob die richtige Verbindung zustande kam.
– Was tun bei einem Irrläufer?
  Im Falle einer Fehlübertragung ist der Empfänger aufzufordern, den Telefax-Irrläufer sofort zu vernichten.
– Aufbewahrung der Sendeberichte und Kommunikationsjournale
  Der Absender sollte den unmittelbar nach der Sendung ausgedruckten Sendebericht mit der gesendeten Unterlage zu den Akten nehmen oder, sofern es keine eigene Akte gibt, in einem Sammelordner für Sendeberichte abheften.

Ferner sind die von Zeit zu Zeit ausgedruckten Kommunikationsjournale daraufhin zu überprüfen, ob sie Anhaltspunkte für Unregelmäßigkeiten enthalten. Anschließend sind sie ca. drei bis sechs Monate aufzubewahren, um eventuelle spätere Überprüfungen zu ermöglichen.

Besonderheiten bei der Übertragung sensibler Daten
Besonders sensible Daten, z.B. Sozial-, Steuer-, Personal- und medizinische Daten, sind grundsätzlich nur verschlüsselt zu übertragen. Dabei sollte der Absender die Telefaxübertragung in jedem Fall telefonisch ankündigen, damit der Empfänger das Telefax persönlich entgegennehmen kann; dieser Anruf bietet dem Absender gleichzeitig die Gelegenheit, zu überprüfen, ob er noch über die aktuelle Telefaxnummer des Empfängers verfügt.

Dokumentation des laufenden Betriebs
Die Kommunikationsjournale, in denen das Telefaxgerät automatisch alle Übertragungsvorgänge (ein- und ausgehende Telefaxe) protokolliert, sind – sofern das nicht automatisch geschieht – regelmäßig auszudrucken und für eine gewisse Zeit vor unbefugtem Zugriff gesichert aufzubewahren, um früheren Übertragungsfehlern nachgehen zu können. Der Betreiber des Telefaxgeräts sollte die Journale von Zeit zu Zeit stichprobenhaft daraufhin überprüfen, ob sie Anhaltspunkte für frühere Fehlleitungen enthalten und die Journale anschließend vernichten.

Aussonderung und Reparatur benutzter Geräte
Wird ein gebrauchtes Telefaxgerät verkauft, entsorgt oder zur Reparatur außer Haus gegeben, so sind alle noch im Gerät gespeicherten Daten (z.B. Zielrufnummern, Daten des Kommunikationsjournals) zuvor zu löschen.

Anhang 9

Hinweise zur Datensicherheit beim Einsatz von Personal Computern

Mehr und mehr setzen auch Behörden und sonstige öffentliche Stellen die in den letzten Jahren immer leistungsfähiger gewordenen Personal Computer (PC) zur Verarbeitung personenbezogener Daten ein. Die Erfahrungen der Praxis zeigen dabei allerdings, daß sie sich häufig schwer damit tun, den im Landesdatenschutzgesetz und im Sozialgesetzbuch (SGB X) enthaltenen „zehn Geboten" des Datenschutzes Rechnung zu tragen und die danach notwendigen technischen und organisatorischen Sicherungsmaßnahmen zu treffen. Die folgenden Hinweise wollen deswegen eine Hilfestellung für die Verarbeitung personenbezogener Daten auf unvernetzten PC geben.

Was ist bei der Anschaffung eines PC zu beachten?
Wer personenbezogene Daten auf einem PC verarbeiten will, sollte sich bereits vor dem Kauf überlegen, welche Daten dies sein werden. Denn davon hängen maßgeblich die Sicherungsmaßnahmen ab, die zum Schutz der Daten zu treffen sind. Bieten Computer und Standardbetriebssystem nicht die notwendige Sicherheit – dies ist bei gängigen Betriebssystemen für Einzelplatz-PC in der Regel nach wie vor der Fall –, ist ein zusätzliches Sicherheitsprodukt (Software und/oder Hardware) zu beschaffen. Sollen besonders sensible Daten, wie Sozial-, Steuer-, Personal- und medizinische Daten, auf dem PC verarbeitet werden, sollte die Möglichkeit bestehen, die Daten sowohl auf der Festplatte des PC als auch auf Disketten verschlüsselt zu speichern. Eine Verschlüsselungsmöglichkeit sollte ferner bei der Verarbeitung personenbezogener Daten auf portablen Computern, wie Laptops oder Notebooks, gegeben sein, da bei diesen Geräten die erhöhte Gefahr besteht, daß sie durch Diebstahl oder Unachtsamkeit in falsche Hände geraten.

Was ist vor Aufnahme des regulären Betriebs zu beachten?
Wer personenbezogene Daten auf einem PC verarbeiten möchte, muß zuvor ein Sicherheitskonzept entwickeln. Daraus muß hervorgehen, aufgrund welcher Rechtsgrundlage welche Daten gespeichert werden sollen, wer auf welche Daten zugreifen darf, ob und, wenn ja, an wen Daten regelmäßig zu übermitteln, wann die Daten zu löschen und welche Sicherungsmaßnahmen zum Schutz der gespeicherten Daten zu treffen sind. Diese Maßnahmen sollen insbesondere sicherstellen, daß die Mitarbeiter, die den PC nutzen sollen, die personenbezogenen Daten nur in dem Umfang verarbeiten können, wie dies zu ihrer Aufgabenerfüllung notwendig ist. Außerdem soll eine Nutzung des PC durch Unbefugte möglichst verhindert werden. Im einzelnen sollte folgendes beachtet werden:

– Verantwortlichkeiten
  Spätestens mit Beginn der Verarbeitung personenbezogener Daten auf dem PC sollten die Verantwortlichkeiten beim Umgang mit dem PC klar geregelt sein: Während es unter anderem zu den Aufgaben des Systemverwalters gehört, Benutzer einzurichten, Programme zu installieren sowie Störungen und Probleme im Alltagsbetrieb zu beheben, arbeiten alle anderen Benutzer nur mit den ihnen zur Verfügung gestellten Anwendungsprogrammen.
– Aufstellung
  An einem PC angeschlossene Bildschirme und Drucker sind so aufzustellen bzw. durch Sichtblenden so abzuschirmen, daß nicht mit der Bedienung dieser Geräte betraute Personen weder den Bildschirminhalt noch Druckausgaben einsehen können. Besonders wichtig ist dies in Arbeitsräumen mit Publikumsverkehr.
– Gehäuse abschließen
  Wird das Gehäuse des PC abgeschlossen, so bietet dies zwar keinen perfekten, aber doch einen leidlichen Schutz gegen das unbefugte Öffnen des Geräts und Manipulationen an der Hardware. Der Gehäuseschlüssel ist dann freilich an einem sicheren Ort aufzubewahren.
– Starten des PC
  Der Systemverwalter sollte den PC so einrichten, daß niemand außer ihm in der Lage ist, ihn, anstatt über die Festplatte, über das Diskettenlaufwerk zu starten. Ansonsten könnte ein findiger PC-Nutzer Sicherheitsfunktionen leicht umgehen.
– Paßwortschutz
  Wer mit einem PC arbeiten möchte, soll dies nur tun können, wenn er sich

zuvor mit seiner Benutzerkennung und dem zugehörigen geheimen, nur ihm bekannten Paßwort anmeldet und als berechtigt ausweist. Paßwörter sollten eine Mindestlänge von sechs Zeichen haben, bei der Eingabe nicht am Bildschirm angezeigt werden, möglichst aus Groß- und Kleinbuchstaben sowie Ziffern bestehen und in regelmäßigen Zeitabständen geändert werden, möglichst dadurch, daß sie automatisch verfallen. Ferner sind Paßwörter stets verschlüsselt zu speichern. Arbeiten verschiedene Benutzer an einem PC, so sollten individuelle Benutzerkennungen und Paßwörter verwendet werden.

– Sperren des PC
  Nach wenigen fehlerhaften Anmeldeversuchen sollte der PC für die weitere Benutzung gesperrt werden.
– Differenzierte Zugriffsbefugnisse
  Es ist darauf zu achten, daß die Dienststelle jedem ihrer Mitarbeiter nur die Zugriffsrechte auf Programme und Daten einräumt, die dieser für die Erfüllung seiner dienstlichen Aufgaben tatsächlich benötigt. Auf Anweisung der Dienststelle richtet der Systemverwalter dann die entsprechenden differenzierten Zugriffsrechte für die einzelnen Benutzer ein.
– Betriebssystemebene
  Benutzer – ausgenommen der Systemverwalter – sollten weder die Möglichkeit haben, bereits installierte Betriebs- oder Anwendungsprogramme zu ändern noch neue zu installieren. Deswegen sollten sie auch nicht direkt auf die Betriebssystemebene gelangen können, von der aus sie uneingeschränkt alle Kommandos aufrufen könnten, die der Computer zur Verfügung stellt, ob sie diese nun zur Erfüllung ihrer Aufgaben brauchen oder nicht.
– Diskettenlaufwerke
  Der Systemverwalter sollte Diskettenlaufwerke für Benutzer sperren, sofern diese Maßnahme die Arbeitsabläufe nicht wesentlich beeinträchtigt. Dies bietet sowohl einen Schutz gegen das unbefugte Kopieren personenbezogener Daten auf eine Diskette und der Weitergabe an Dritte als auch gegen das Einschleusen von Computerviren.
– Protokollierung
  Der PC sollte die Aktivitäten der einzelnen Benutzer sowie des Systemverwalters automatisch protokollieren. Die Protokolldaten sollten zumindest Aufschluß darüber geben, wer von wann bis wann am Computer arbeitete. Ferner ist es hilfreich, wenn darüber hinaus auch Zugriffe auf Programme und Dateien protokolliert werden. Die Protokolldatei sollte nachträglich nicht geändert werden können.
– Freigabe von Programmen
  Die Verarbeitung personenbezogener Daten darf nur mit Hilfe sorgfältig getesteter, dokumentierter und von der jeweils zuständigen Stelle schriftlich für den Echteinsatz freigegebener PC-Programme erfolgen.
– Dienstanweisung
  Die getroffenen Sicherheitsmaßnahmen sollten in einer Dienstanweisung für den ordnungsgemäßen PC-Einsatz schriftlich festgehalten werden.
– Geräte- und Verfahrensverzeichnis
  Die Behörden und sonstigen öffentlichen Stellen haben das nach § 10 des Landesdatenschutzgesetzes zu führende Geräte- und Verfahrensverzeichnis zu aktualisieren.

Sorgfaltsregeln für den Betrieb

Beim Betrieb des PC muß der an ihm arbeitende Mitarbeiter insbesondere folgendes beachten:

– Verlassen des Arbeitsplatzes
  Verläßt der Benutzer während des laufenden Betriebs den PC, so sollte er den Computer ausschalten oder aber den Bildschirm sperren. Eine Bildschirmsperre ist allerdings nur dann sinnvoll, wenn sie sich ausschließlich durch Eingabe eines geheimen Paßworts und nicht durch einfachen Druck auf eine beliebige Taste wieder aufheben läßt.
– Störungen nachgehen
  Treten beim Betrieb Störungen auf, beispielsweise nicht erklärbare Fehlermeldungen, sollte der Benutzer dies sofort dem für Sicherheitsfragen zuständigen Mitarbeiter melden. Dieser sollte der Sache möglichst unverzüglich nachgehen. Besteht der Verdacht, ein Unbefugter könnte Kenntnis von einem Paßwort erhalten haben, so ist das Paßwort unverzüglich zu ändern.

– Umgang mit Disketten
  Gerade nicht eingesetzte Disketten, auf denen personenbezogene Daten gespeichert sind, sollten verschlossen aufbewahrt werden.
  Systembetreuung
– Der Systemverwalter richtet neue Benutzer ein und löscht diejenigen, die nicht mehr mit dem Computer arbeiten müssen. Ferner aktualisiert er die Zugriffsbefugnisse, so daß die einzelnen Benutzer immer nur die Zugriffsrechte haben, die sie zur Erfüllung ihrer Aufgaben brauchen.
  Virengefahr begegnen
– Um der Virengefahr vorzubeugen, sollten nur Programme aus einwandfreien Quellen zum Einsatz kommen, z.B. eigenerstellte Programme oder lizenzierte Originalprogramme. Zu denken ist aber auch an die Verwendung leistungsfähiger Virenerkennungsprogramme, die Hauptspeicher und Festplatte des PC sowie Disketten nach Viren durchsuchen, sie anzeigen und beseitigen können. Hilfreich ist außerdem der Einsatz von Prüfsummenprogrammen, durch die sich (durch Viren ausgelöste) Veränderungen bei installierten Programmen feststellen lassen. Die Gefahr eines Virenbefalls besteht insbesondere beim Laden des Betriebssystems von einer virenbefallenen Diskette sowie beim Einsatz infizierter Programme. Neuerdings kann aber sogar das Lesen einer sonstigen Datei, z.B. eines Textdokuments, einen Virus aktivieren.
– Auswertung der Protokolldatei
  In regelmäßigen Zeitabständen sollte die Protokolldatei zumindest stichprobenartig ausgewertet werden, um nachzuprüfen, wer wann was am Computer gemacht hat. Systemverwaltung und Auswertung der Protokolle sollten dabei möglichst nicht in einer Hand liegen.
– Sicherungsmaßnahmen überprüfen
  In regelmäßigen Zeitabständen sollten die getroffenen Sicherungsmaßnahmen dahin gehend überprüft werden, ob sie noch ausreichen. Eine solche Überprüfung ist zumindest immer dann erforderlich, wenn sich die Programme, mit deren Hilfe personenbezogene Daten auf dem PC verarbeitet werden, ändern.

Aussonderung und Reparatur benutzter Geräte
Wird ein zuvor benutzter PC verkauft, entsorgt oder zur Reparatur außer Haus gegeben, so sind zuvor alle noch auf der Festplatte des Geräts gespeicherten Daten zu löschen. Diese Löschung darf nicht nur eine logische sein, wie bei dem Löschbefehl mancher PC-Betriebssysteme, sondern muß physikalisch erfolgen. Nur so kann verhindert werden, daß durch Einsatz spezieller Hilfsprogramme die Daten wiederhergestellt werden können.