Landtag von Sachsen-Anhalt **Drucksache 4/839**
Vierte Wahlperiode **18.06.2003**

Unterrichtung

Präsident des Landtages von Sachsen-Anhalt

Magdeburg, 17. Juni 2003

Sechster Tätigkeitsbericht des Landesbeauftragten für den Datenschutz für die Zeit vom 1. April 2001 bis 31. März 2003

Sehr geehrte Damen und Herren,

mit Schreiben vom 5. Juni 2003, hier eingegangen am 10. Juni 2003, hat der Landesbeauftragte für den Datenschutz Sachsen-Anhalts gemäß § 22 Abs. 4 Satz 3 des Gesetzes zum Schutz personenbezogener Daten der Bürger (DSG-LSA) dem Landtag seinen sechsten Tätigkeitsbericht übermittelt. Er schließt an den fünften Tätigkeitsbericht an, der als Drucksache 3/4565 vorliegt und in den Ausschüssen für Inneres und für Recht und Verfassung beraten wurde.

Die Unterrichtung des Landtages erfolgt gemäß § 54 Abs. 1 Satz 2 der Geschäftsordnung des Landtages von Sachsen-Anhalt (GO.LT).

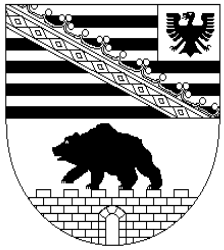
Gemäß § 40 Abs. 1 i. V. m. § 54 Abs. 1 Satz 3 GO.LT überweise ich den Tätigkeitsbericht zur Beratung und zur Berichterstattung an die Ausschüsse für Inneres (federführend) sowie für Recht und Verfassung.

Mit freundlichen Grüßen

Prof. Dr. Adolf Spotka

(Ausgegeben am 18.06.2003)

Landesbeauftragter
für den Datenschutz
Sachsen-Anhalt



VI. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

**für die Zeit
vom
1. April 2001 bis 31. März 2003**

VI. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

Landesbeauftragter für den Datenschutz - Postfach 1947 - 39009 Magdeburg

Telefon	(0391) 8 18 03 - 0
Bürgertelefon	(0800) 9 15 31 90
Fax	(0391) 8 18 03 33
Internet	
http://www.datenschutz.sachsen-anhalt.de	

Dienstgebäude: Berliner Chaussee 9 - 39114 Magdeburg

Inhaltsverzeichnis

Anlagenverzeichnis

1. Entwicklung des Datenschutzes

Wer die jeweils zweijährigen Überblicke in den letzten Tätigkeitsberichten verfolgt hat, kennt die sich immer klarer abzeichnende Entwicklung längst: Die Bürgerinnen und Bürger des Landes leben und arbeiten schon lange nicht mehr abgeschirmt in ihrem ländlichen oder städtischen Umfeld - sie sind vielmehr Teil einer über Deutschland und Europa hinausreichenden Gesellschaft aufgeregter Weltbürger. Dementsprechend spüren sie jetzt auch die Auswirkungen spektakulärer Ereignisse bis in ihren persönlichen Lebensbereich. Stichworte dieses Berichtszeitraumes sind Amerika seit dem 11. September 2001 und der terroristische Anschlag auf der Insel Djerba im Jahre 2002, der vor allem deutsche Bürger traf.
Die Innenpolitiker im Bund und auch in unserem Land versprechen hastig Sicherheit (Beispiel: bundesweite Rasterfahndung), errichten vorrangig aber nur immer neue Einschränkungen und verkleinern die unbeobachteten Bewegungsräume der "freien Bürger". Leider gibt es keine absolute Sicherheit und die relative Sicherheit ist schwer zu belegen. Dafür muss der Bürger künftig in Ausweis und Pass mit der Aufnahme seiner biometrischen Daten rechnen, sein Telefon kann schon längst - ohne dass er es weiß - in eine der inzwischen pro Jahr über 21.000 amtlich angeordneten Telefonüberwachungen geraten sein. Auch seine Reisepläne, seine Bank- und Sparkonten, seine Kreditkarten werden ohne sein Wissen abgefragt, analysiert und aufgezeichnet, seine Fahrten mit dem Auto über Streckenbeobachtungen und Mobilfunkauswertungen begleitet - wohlgemerkt, alles legal und ohne dass etwa ein Straftatverdacht gegen ihn vorliegen muss! Nur "liebevolle" Vorsorge des schützenden Staates.
Auch bei ihm oder ihr zu Hause und im unmittelbaren Wohnumfeld wird die Überwachung dichter: Die Datenschutzbeauftragten des Bundes und der Länder konnten bisher nur mit Mühe verhindern, dass nicht jede Bewegung der Bürger im Internet aufgezeichnet und für Monate zur Auswertung vorgehalten wird - ganz gleich, ob nur ein Buch über das Internet bestellt oder eine Information zum Hobby der Aquariumshaltung ausgetauscht wurde. Die tägliche Rasterung zu geheimdienstlichen Zwecken, zur Wirtschaftsspionage und für die Werbung blüht - keine E-Mail und keine Geldüberweisung bleibt mehr unbeobachtet.
Auch im kleinen Umfeld bleibt etwas hängen:
Wenn er oder sie morgens über den Marktplatz oder die große Kreuzung geht, werden sich künftig auch in diesem Land ein halbes Dutzend Videoauswerter darüber amüsieren können, dass er oder sie zwei verschiedenfarbige Socken trägt und immer in der Nase bohrt, ehe man in die (überwachte) Straßenbahn einsteigt.
Die automatisierte Datenverarbeitung, die einerseits für schnelle und bürgerfreundliche Verwaltungsabläufe sorgen kann (Beispiel: Bürgerbüro), wird auch gegen den Bürger eingesetzt (keine Anmeldung bei der Müllabfuhr, nicht bezahlte Abgaben und Steuern). Für ganz normale Sozialleistungen muss der betreffende Bürger immer mehr Angaben zu seinen persönlichen Verhältnissen machen, weil die EDV-Technik größere Speicher-

kapazitäten erlaubt und weite Querschnittskontrollen ermöglicht. Beispiele dafür sind die Verteilung der Gelder an die Flutgeschädigten des letzten Jahres und die geänderte Kinderbetreuung im Land. Auch bei der medizinischen Versorgung wird die "fürsorgliche" Erfassung des Gesundheitszustandes und der Behandlung (einschließlich der Medikamente) der Bürger immer genauer.
Die Bürger werden also täglich transparenter. Selbst Fachleute haben heute keine Kontrolle mehr darüber, wo wir eine elektronische Spur hinterlassen.
Eine gute Nachricht und eine Empfehlung zum Schluss:
Der Umgang mit den Daten des Bürgers in den Hunderten von öffentlichen Stellen des Landes ist bezüglich dessen, was erlaubt ist, und in punkto Datensicherheit professioneller geworden. Der Bürger sollte vielleicht gerade deswegen kritisch darauf achten, wem er was, in welchem Umfang, zu welchem Zweck und wie lange über sich selbst an Informationen zur Verfügung stellt. In Zweifelsfällen sollte er besser den Landesbeauftragten befragen - kostenlos.

2. Der Landesbeauftragte

2.1 Tätigkeit im Berichtszeitraum

Ein wesentlicher Schwerpunkt der Tätigkeiten des Landesbeauftragten und seiner Mitarbeiter war auch in diesem Zeitraum wieder die Prüfung, Bewertung und Erledigung der schriftlichen Geschäftseingänge, die der überwiegend telefonisch vorgebrachten Anliegen der Bürgerinnen und Bürger und die Bitten um Beratungen und Informationen durch die Bediensteten in den weit über 1.000 öffentlichen Stellen des Landes. 2001 gab es 3.145 registrierte schriftliche Eingänge, im Jahr 2002 waren es 3.173. 2001 sind dazu 594 und 2002 671 schriftliche Stellungnahmen erarbeitet worden. Nicht besonders registriert, aber datenschutzrechtlich ausgewertet und ggf. bearbeitet wurden im Berichtszeitraum alle Landtagsdrucksachen. Die Zahl der telefonischen Anfragen hat sich erhöht und liegt derzeit zwischen 950 und 1.000 pro Jahr. Zu beobachten war, vor allem im letzten Berichtsjahr, ein erhöhtes Geschäftsaufkommen durch die moderne Kommunikation per E-Mail. Leider führt dieser oft spielerisch genutzte Verbindungsweg zwar zur Erhöhung des quantitativen, aber nicht zur Erhöhung des qualitativen Arbeitsaufkommens. Circa 20 bis 25 % der eingehenden E-Mails sind fehlerhaft, unvollständig oder überflüssig. Diese Quote kann noch vergleichsweise niedrig gehalten werden, weil die E-Mail-Adresse der Geschäftsstelle nur eingeschränkt bekannt gegeben ist. Rückläufig waren die persönlichen Anfragen und Vorsprachen der Bürger in der Behörde des Landesbeauftragten. Gleich geblieben ist in etwa die Zahl der Bürgereingaben (ca. 150 bis 160 pro Jahr).

Von formellen Beanstandungen nach § 24 DSG-LSA konnte abgesehen werden. Es gab aber in den beiden Jahren jeweils ca. 30 bis 35 Fälle mit erheblichen Rechtsverstößen. Aufgrund der zunehmend verbesserten

Aus- und Fortbildung der Bediensteten in den öffentlichen Stellen des Landes ist aber der Umgang mit den personenbezogenen Daten durch die Mitarbeiter öffentlicher Stellen sicherer geworden.

Unverändert hoch ist der Bedarf an Beratungen vor Ort bei den öffentlichen Stellen des Landes. Dabei hat sich der Schwerpunkt in den technisch-organisatorischen Beratungsbereich verschoben. Der Beratungsbedarf im materiell-rechtlichen Bereich wird überwiegend durch die telefonische Beratung und in schwierigeren Fällen auch durch Besprechungen abgewickelt.
Auf längere Sicht ist zu hoffen, dass dieser Beratungsbedarf rückläufig sein wird, denn mit der obligatorischen Einführung eines Beauftragten für den Datenschutz nach § 14a DSG-LSA durch die Gesetzesänderung vom August 2001 für die meisten öffentlichen Stellen im Lande steht diesen künftig ein unmittelbarer Ansprechpartner zur Verfügung. Für diesen Personenkreis besteht noch der Bedarf an einer qualifizierten Fortbildung, welche aber von öffentlichen und privaten Fortbildungseinrichtungen ausreichend angeboten wird.

Der unveränderte Schwerpunkt der automatisierten Datenverarbeitung und die damit verbundenen besonderen Probleme der Datensicherheit sind unter den Ziffern 7 und 12 dargestellt. Die vom Landesbeauftragten anlassunabhängig angeordneten Querschnittskontrollen wurden im Berichtszeitraum bei den Ausländer- und Meldebehörden, bei den Gesundheitsämtern, den personalaktenführenden Stellen und bei einer Justizvollzugsanstalt fortgesetzt. Erstmals stichprobenartig geprüft wurden die beiden rechtsmedizinischen Institute im Lande und die Verwaltungstätigkeiten zweier Gerichte. Leider konnten aufgrund der im Folgenden erörterten personellen Veränderungen in der Geschäftsstelle des Landesbeauftragten die Querschnittskontrollen nicht im vorgesehenen Umfang durchgeführt werden.

Auch in diesem Berichtszeitraum haben die Mitarbeiterinnen und Mitarbeiter neben dem Landesbeauftragten als Dozenten oder Vortragende beim Fortbildungsprogramm für die allgemeine Verwaltung des Ministeriums des Innern, im Bereich der Aus- und Fortbildung der Polizei und bei mehreren Einzelveranstaltungen mitgewirkt und sich selbst fortgebildet.
Abschließend muss auf ein besonderes personelles Problem in der Geschäftsstelle hingewiesen werden. Seit ca. drei Jahren zeichnet sich vor allem in der bundesweiten Zusammenarbeit, aber auch im europäischen Rechtsbereich (vgl. § 22 Abs. 7 DSG-LSA), der Bedarf einer intensiveren rechtlichen Aufbereitung bestimmter Problembereiche ab. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder versucht, dies in den eingerichteten Arbeitskreisen zu bewerkstelligen. Eine fundierte praxisorientierte Erarbeitung von Vorschlägen setzt aber auch die Beteiligung qualifizierter juristischer Mitarbeiter der Datenschutzbeauftragten der Länder voraus. Dies war seitens Sachsen-Anhalts im Berichtszeitraum

nur einmal möglich und wird im Kreise der Kollegen mit Recht als unzureichend empfunden. Der Bundesbeauftragte für den Datenschutz und (mit Ausnahme des Saarlandes) alle Datenschutzbeauftragte der Länder haben in den letzten fünf Jahren auch deshalb die Zahl der Mitarbeiter erhöht. Der Landesbeauftragte hat darauf aus Gründen der Sparsamkeit bisher verzichtet und auch für das Haushaltsjahr 2004 keine Stellenvermehrung beantragt. Er hofft aber darauf - und wird sich bei der Landesregierung dafür einsetzen -, im Zuge der Auflösung und Konzentration der allgemeinen Verwaltungsbehörden für seine Geschäftsstelle eine rechtlich qualifizierte Beamtin oder einen Beamten des höheren Dienstes für seine Geschäftsstelle übernehmen zu können.

Nicht einfach zu verkraften war ein Personalwechsel auf vier Stellen in der Geschäftsstelle des Landesbeauftragten. Die Gründe lagen je zur Hälfte im altersbedingten Ausscheiden und in Veränderungen im beruflichen und im persönlichen Lebensbereich der Mitarbeiterinnen und Mitarbeiter. Zu den Ausgeschiedenen gehört leider auch der sehr erfahrene langjährige Leiter der Geschäftsstelle. Zwischenzeitlich ist es gelungen, alle Stellen wieder qualifiziert und aus dem Lande heraus neu zu besetzen. Dabei war die gute und vertrauensvolle Zusammenarbeit mit den oberen und obersten Behörden des Landes hilfreich.

Im Zuge der Neubesetzungen ist auch die Aufgabenzuweisung in den Referaten geändert worden. Die aktuelle Aufgabenzuweisung in der Geschäftsstelle kann dem anliegenden Organigramm **(Anlage 1)** entnommen werden.

2.2 Zusammenarbeit mit anderen Aufsichts- und Kontrollinstitutionen

Keinerlei Probleme haben sich in der notwendigen engen Zusammenarbeit mit dem Landtag im parlamentarischen Bereich ergeben. Nicht nur bei Anhörungen zu Gesetzentwürfen des Landtages, sondern auch bei aufkommenden komplexen datenschutzrechtlichen Fragen während der Ausschussberatungen wird über kurze Querwege der sachverständige Rat des Landesbeauftragten angefordert, wenn dieser nicht bereits selbst sein Erscheinen im Ausschuss vorgesehen oder angekündigt hat.
Sehr persönlich, offen und vertrauensvoll ist auch die Zusammenarbeit mit dem neuen Landtagspräsidenten Professor Spotka. Die konstruktive Zusammenarbeit mit der Landtagsverwaltung wird durch die Bereitschaft des Landesbeauftragten unterstrichen, eine Mitarbeiterin seiner Geschäftsstelle auch als behördliche Datenschutzbeauftragte für die Landtagsverwaltung einzusetzen und damit Kosten zu sparen.

Eine unverändert wichtige und verlässliche Brücke zur Exekutive ist die Zusammenarbeit mit dem für den Datenschutz zuständigen Ministerium des Innern. Die zwischenzeitlich im August 2001 durch den Landtag verabschiedete grundlegende Überarbeitung des DSG-LSA war mit diesem

Haus sach- und praxisorientiert vorbereitet worden und stellt eine deutliche Verbesserung der datenschutzrechtlichen Grundlagen im Lande dar. Eine problemlose Zusammenarbeit gibt es auch mit den übrigen Obersten Landesbehörden, unbeschadet sachlicher Meinungsunterschiede.

Die wichtigste Stütze im innerdeutschen Bereich ist und bleibt die Zusammenarbeit in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und in den von ihr eingerichteten Arbeitskreisen. Darüber hinaus verlangt die globale Vernetzung im Bereich der automatisierten Verarbeitung und die immer engere rechtliche Verzahnung über die Länder- und Staatengrenzen in Europa hinweg nicht nur eine enge und konstruktive Abstimmung auf Bund-Länder-Ebene, sondern auch eine erfahrungsorientierte neue Zusammenarbeit mit den in Europa und international eingesetzten unabhängigen Kolleginnen und Kollegen. Die global auftretenden neuen Rechtsfragen können und müssen - auch unter den finanziell begründeten Rationalisierungszwängen - auf einer breiten Zusammenarbeitsebene gelöst werden.
Der Landesbeauftragte hat deshalb auch im Berichtszeitraum wieder an zwei europäischen und zwei internationalen Datenschutzkonferenzen teilgenommen. Er ist weiterhin im Nebenamt für den Bundesrat der zweite unabhängige deutsche Vertreter in der Gemeinsamen Kontrollinstanz für Europol. Seit Oktober 2002 ist er Vorsitzender dieses Gremiums.

2.3 Die Homepage des Landesbeauftragten: Ein Angebot für Verwaltung, Bürgerinnen und Bürger und alle Interessierten

Wie bereits in seinem V. Tätigkeitsbericht (Ziff. 2.3.1) berichtet, pflegt der Landesbeauftragte seit dem 14.12.2000 zur Ausübung seines gesetzlichen Beratungsauftrages auch eine Homepage.
Unter **www.datenschutz.sachsen-anhalt.de** können sich die Beschäftigten der Landesverwaltung unter der Voraussetzung eines Zuganges zum Landesverwaltungsnetz (Intranet) schnell und bequem über die aktuellen Entwicklungen in datenschutzrechtlichen Fragen informieren. Den Landkreisen und Gemeinden ist der Zugang bisher nur über das Internet möglich.
Zukünftig sollen nach den Planungen des Ministeriums des Innern auch die Landkreise und Gemeinden Zugang zum Landesverwaltungsnetz und damit kostenfrei zum Informationsangebot des Landesbeauftragten erhalten.

Der Landesbeauftragte hat sein Angebot unter der Rubrik "Rechtsvorschriften" mit den einschlägigen Gesetzestexten und den Verwaltungsvorschriften zum DSG-LSA **neu** gestaltet.
Nach der Novellierung des DSG-LSA vom 21.08.2001 (GVBl. LSA S. 348) und der Bekanntmachung der Neufassung vom 18.02.2002 (GVBl. LSA S. 54) sowie der Veröffentlichung der Verwaltungsvorschriften zum DSG-LSA vom 31.08.2002 (MBl. LSA S. 1091) wurden auf der Homepage die

nichtamtlichen Texte des DSG-LSA und der VV-DSG-LSA so verlinkt, dass von den einzelnen Paragraphen des DSG-LSA sofort zu den dazugehörigen Passagen der VV-DSG-LSA gewechselt werden kann und umgekehrt.
Der Landesbeauftragte hofft, damit insbesondere den neu bestellten Beauftragten für den Datenschutz die Einarbeitung in die komplexe Materie "Datenschutz" zu erleichtern. Dieses Angebot ersetzt natürlich keine umfassende Fortbildung, trägt aber zumindest den vorhandenen aktuellen Informationsmöglichkeiten an einem vernetzten PC-Arbeitsplatz Rechnung.
Unter der Rubrik "DSB-Konferenz" sind die Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ab dem Jahr 1997 zu finden.
Ein Schlagwortverzeichnis von A-Z erleichtert die Suche zu bestimmten Themen.

Alle Tätigkeitsberichte des Landesbeauftragten an das Parlament und ausgewählte Mitteilungen in den Bekanntmachungsblättern sowie an die Presse sind unter der Rubrik "Veröffentlichungen" abrufbar und stehen auch zum Download im pdf-Format bereit.
In der Rubrik "Service" der Homepage gibt es weitere Hinweise und Orientierungshilfen zu speziellen Problemen des Datenschutzes und der Datensicherheit sowie externe weiterführende Links zum Thema Datenschutz, u.a. auf Fortbildungsveranstaltungen.

Über eine viertel Million mal wurden im Jahre 2002 Seiten aus dem Informationsangebot des Landesbeauftragten genutzt, davon waren fast 15.000 Zugriffe allein auf die Paragraphen des DSG-LSA zu verzeichnen. Das zeigt, dass sich die Mühe bei der Gestaltung seiner umfangreichen bestehenden Web-Präsenz gelohnt hat.
Für die Unterstützung und problemlose Zusammenarbeit bei der Gestaltung seiner Homepage bedankt sich der Landesbeauftragte bei den Mitarbeitern des Landesrechenzentrums in Halle.

Das Angebot wird weiter ausgebaut, wobei der Landesbeauftragte gern Änderungsvorschläge bzw. -wünsche und auch Kritiken der Nutzer entgegen nimmt, um sein Informationsangebot anzupassen.

Selbstverständlich steht dieses Informationsangebot des Landesbeauftragten allen Interessierten auch über das Internet unter der gleichen Adresse zur Verfügung.

Der Landesbeauftragte hat mit Befriedigung zur Kenntnis genommen, dass das neue Landesportal Sachsen-Anhalt eine Verlinkung mit seiner Homepage enthält. Dies war notwendig, denn für Interessierte ist das Landesportal Sachsen-Anhalt der Einstieg in Informationen über das

ganze Bundesland. Der Landesbeauftragte war bisher - trotz der besonderen verfassungsrechtlichen Stellung - über das Landesportal für die Bürgerinnen und Bürger nur auf Umwegen erreichbar.

3. Archivwesen

3.1 Entschädigungsansprüche aus der NS-Zeit

Mit dem Gesetz zur Errichtung einer Stiftung "Erinnerung, Verantwortung und Zukunft" vom 02.08.2000 (BGBl. I, 1263), zuletzt geändert durch Gesetz vom 21.08.2002 (BGBl. I, 3347), ist ein Abkommen betreffend die Versicherungsansprüche aus der NS-Zeit zwischen der vorgenannten Stiftung, dem Gesamtverband der deutschen Versicherungswirtschaft (GDV) und der International Commission on Holocaust Era Insurance Claims (ICHEIC) abgeschlossen worden. Um Berechtigte auf die Möglichkeit eines Entschädigungsanspruchs aufmerksam machen zu können, soll eine Liste von jüdischen Policeninhabern aus dem Zeitraum 1933 - 1945 zusammengestellt werden. Voraussetzung dafür ist jedoch eine Liste der damaligen jüdischen Einwohner Deutschlands, die der Versicherungswirtschaft zum Abgleich zur Verfügung gestellt werden soll.

Das (Landes-)Ministerium der Justiz verwies dazu auf die Auswertung des Archivgutes gemäß Landesarchivgesetz und wies darauf hin, dass z.Zt. eine hierfür notwendige Novellierung des ArchG-LSA vorbereitet werde; das Gesetzgebungsverfahren soll im ersten Halbjahr 2003 abgeschlossen werden. Der Landesbeauftragte wurde hierzu um Stellungnahme gebeten.

In seiner Stellungnahme wies der Landesbeauftragte darauf hin, dass eine Nutzung personenbezogener Informationen ohne Änderung des Gesetzes zur Zeit erst 80 Jahre nach ihrer Entstehung möglich ist. Gerade in schwierigen Fällen einer solchen "politischen Abwägung" muss der Gesetzgeber selbst vorher tätig werden. Im übrigen ist es - schon wegen möglicher weniger wünschenswerter Nachahmungsfälle - im Hinblick auf die gebotene Verlässlichkeit rechtsstaatlichen Handelns nicht empfehlenswert, seitens der Regierung geltendes Recht zu missachten.

3.2 Archivgut aus der Behörde des Landesbeauftragten

Abgeschlossene Vorgänge aus der Behörde des Landesbeauftragten, die nicht mehr zur Erfüllung der öffentlichen Aufgaben benötigt werden, hat der Landesbeauftragte dem Landesarchiv zur Übernahme angeboten. Das Landesarchiv hat gem. § 8 ArchG-LSA nach Übernahme das Verfügungsrecht und ist verpflichtet, die Unterlagen nach archivwissenschaftlichen Erkenntnissen zu bearbeiten und der Benutzung zugänglich zu machen. Die Benutzung des Archivgutes richtet sich nach § 10 ArchG-LSA.

4. Ausländerangelegenheiten

4.1 Datenübermittlungen im Kostenabrechnungsverfahren

Schon in seinem IV. Tätigkeitsbericht (Ziff. 4.1) hatte der Landesbeauftragte aufgrund der Beschwerden gleich mehrerer Landkreise darauf hingewiesen, dass die generelle automatische Übermittlung personenbezogener Daten der von der Kostenerstattung betroffenen Ausländer an die Regierungspräsidien nicht zulässig ist; denn § 11 Abs. 1 DSG-LSA lässt die Übermittlung nur zu, soweit sie im Einzelfall zur Erfüllung der in der Zuständigkeit des Empfängers liegenden Aufgaben erforderlich ist.

Daraufhin hatte das Ministerium des Innern zwar das Verfahren geändert, doch im Berichtszeitraum wandte sich erneut ein Landkreis an den Landesbeauftragten und monierte, die Regierungspräsidien würden noch immer "umfangreiche Kopien aus den bei den Landkreisen zu führenden Leistungsakten" abfordern. Außerdem habe im Rahmen des Abrechnungsverfahrens auch "eine monatliche Aufstellung unter Nennung aller Namen und Geburtsdaten" durch die leistungsgewährenden Stellen an die Regierungspräsidien zu erfolgen.

Der Landesbeauftragte verdeutlichte gegenüber dem Ministerium noch einmal seine Rechtsauffassung und geht davon aus, dass das Kostenabrechnungsverfahren jetzt eindeutig im Sinne des Datenschutzes geregelt wird.

4.2 Prüfung von Ausländerbehörden

Auch die Prüfung von Ausländerbehörden ging im Berichtszeitraum weiter. Mittlerweile hat der Landesbeauftragte den Eindruck gewonnen, dass in den Ausländerbehörden im Land insgesamt gute und datenschutzbewußte Arbeit geleistet wird.

4.3 Umgang mit Asylanträgen beim Bundesamt für die Anerkennung ausländischer Flüchtlinge

Bei einer Außenstelle des Bundesamtes für die Anerkennung ausländischer Flüchtlinge im Land war es gängige Praxis, Ausfertigungen von Niederschriften zu Asylanträgen ungefragt und ohne Rechtsgrundlage an die örtliche Polizeidienststelle weiterzuleiten. Dies fiel dem Landesbeauftragten bei der Prüfung einer Polizeidirektion auf. Er informierte den für die Bundesbehörde zuständigen Bundesbeauftragten für den Datenschutz, und der sorgte dafür, dass diese unzulässige Praxis eingestellt wurde.

5. Ausweis- und Meldewesen

5.1 Biometrische Merkmale in Ausweisen und Pässen

Im Zusammenhang mit den Regelungen im Gesetz zur Bekämpfung des internationalen Terrorismus vom 09.01.2002 nahm auch die öffentliche Diskussion zu biometrischen Merkmalen in Personalausweisen und Pässen breiten Raum ein. Die von der Bundesregierung vorgesehene Erhöhung der inneren Sicherheit ist dabei mit den individuellen Freiheitsrechten der betroffenen Bürgerinnen und Bürger abzuwägen. Einschränkungen dürfen nur in dem Maße zugemutet werden, wie dies im Rahmen eines überwiegenden Allgemeininteresses zur Terrorismusbekämpfung tatsächlich erforderlich ist.
Nach der Rechtsprechung des Bundesverfassungsgerichts sind Regelungen jedenfalls dann als Verstoß gegen das Menschenbild des Grundgesetzes anzusehen, wenn sie zu einer umfassenden Katalogisierung und Registrierung der Bürger führen. Deshalb ist bis heute die Einführung eines Personenkennzeichens unterblieben. Das in der ehemaligen DDR verwendete Zeichen wurde bei der Wiedervereinigung mit dem Einigungsvertrag verboten.

Auch die Einrichtung zentraler (Referenz-)Dateien ist wegen ihres hohen Gefährdungspotentials für den freiheitlich demokratischen Rechtsstaat und seine Bürger nicht akzeptabel.
Problematisch bleibt außerdem die tatsächliche und praktische Geeignetheit dieser Merkmale.
So konnte bis heute die praktische Eignung der Vermessung des Gesichts, der Papillarmuster der Finger, der Handgeometrie und Handlinien und der Iris und Retinastruktur als zuverlässiges und schnelles Mittel nicht belegt werden.
Da sich die Vorschriften des Passgesetzes und des Ausweisgesetzes (nur) an Deutsche richten, die Mitglieder der bis dato relevanten Terrorgruppierungen jedoch fast ausschließlich ausländische Staatsangehörige sind, ist auch die Eignung als Schutzmaßnahme ohne ihre zumindest europaweite Abstimmung und Einführung höchst zweifelhaft.
Der "brave Bürger" würde von Kopf bis Fuß vermessen und erfasst - die tatsächlich gefährlichen Täter blieben beweglich und unerkannt.

Der Gesetzgeber hat die rechtlichen Bedenken - auch zur Zweckbindung solcher Daten - teilweise aufgegriffen und zunächst lediglich die Möglichkeit vorgesehen, in Pässen und Personalausweisen weitere biometrische Merkmale von Fingern, Händen oder Gesicht des Inhabers aufzunehmen; z.Zt. wird die technische Verwendbarkeit der Merkmale bei einem flächendeckenden Einsatz überprüft.

Zu biometrischen Merkmalen in Personalausweisen und Pässen finden sich weitere Hinweise in der Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. bis 26. Oktober

2001 **(Anlage 9)** und der Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07. bis 08. März 2002 **(Anlage 12).**

5.2 Übermittlung von Einwohnermeldedaten für Mikrozensus 2002

Im Rahmen des Mikrozensus 2002 wandte sich ein ehrenamtlicher Erhebungsbeauftragter des Statistischen Landesamtes an das Einwohnermeldeamt einer Stadt, um Namen und Vornamen von Personen dieser Stadt für die Erfüllung von Mikrozensusbefragungen zu erhalten. Dazu legitimierte er sich gegenüber der Behörde mit einem Ausweis des Landesamtes.

Von der für das Einwohnermeldeamt der Stadtverwaltung zuständigen Sachgebietsleiterin wurden datenschutzrechtliche Bedenken dahingehend geäußert, dass nach ihrer Auffassung eine Rechtsgrundlage im Einwohnermeldegesetz für die Übermittlung von Einwohnermeldedaten an den Mikrozensusbeauftragten nicht vorhanden ist.

Gemäß § 11 Abs. 1 Mikrozensusgesetz dürfen Einwohnermeldebehörden für die Durchführung und Erhebung, einschließlich ihrer methodischen Auswertung, den Statistischen Ämtern der Länder auf Verlangen die Daten gem. § 11 Abs. 1 Nrn. 1 bis 6 Mikrozensusgesetz übermitteln.
Der Erhebungsbeauftragte nimmt auf gesetzlicher Grundlage ein öffentliches Amt für das Statistische Landesamt wahr. Somit ist die Übermittlung von personenbezogenen Daten an ihn zulässig, wenn diese Vorgehensweise durch das Statistische Landesamt so vorgegeben ist.

6. Europäischer Datenschutz

6.1 Eurojust

Mit Beschluss des Rates der Europäischen Union vom 28.02.2002 ist EUROJUST als eine neue europäische Ermittlungsbehörde zur Verstärkung der Bekämpfung der schweren Kriminalität errichtet worden. Sie soll die justizielle Zusammenarbeit zwischen den Mitgliedsstaaten verbessern. Das Verhältnis zur europäischen Polizeibehörde EUROPOL (siehe Ziff. 6.2), insbesondere hinsichtlich einer Kontrollfunktion, ist bisher eher unscharf geregelt und bleibt hinter den Erwartungen zurück.

Die Datenschutzbeauftragten des Bundes und der Länder haben dazu schon auf ihrer 62. Konferenz (2001) eine Entschließung **(Anlage 4)** verfasst, in der sie darauf hinweisen, dass mit Blick auf die sensiblen personenbezogenen Daten, die von Eurojust erhoben, verarbeitet und genutzt werden sollen, umfassende Datenschutzvorschriften erforderlich sind.

Diese müssen sowohl Regelungen zur Verarbeitung, Speicherung, Nutzung, Berichtigung, Löschung als auch zum Auskunftsausspruch des Betroffenen enthalten.
Für die Datenschutzbeauftragten steht außerdem die Erforderlichkeit einer gemeinsamen Kontrollinstanz für Eurojust außer Frage. Die Unabhängigkeit dieser gemeinsamen Kontrollinstanz ist bereits durch die personelle Zusammensetzung zu gewährleisten. Sowohl für die Eurojust-Mitglieder als auch das Kollegium müssen die Entscheidungen der Gemeinsamen Kontrollinstanz bindenden Charakter haben.

Der Landesbeauftragte begrüßt, dass der Beschluss des Rates vom 28.02.2002 in Art. 23 die Schaffung einer solchen Kontrollinstanz vorsieht (an die sich nach Art. 17 Abs. 4 des Beschlusses auch der Eurojust-Datenschutzbeauftragte wenden kann). Als deutsches Mitglied der Kontrollinstanz ist ein Bundesrichter benannt worden.

EUROJUST soll noch im Frühjahr 2003 seine Arbeit im vollen Umfang aufnehmen.
Wie sich die Arbeitsteilung und die Zusammenarbeit mit Europol in der Praxis bewährt, bleibt abzuwarten.

6.2 Europol

Im Anschluss an die Berichterstattung im V. Tätigkeitsbericht (Ziff. 5.3) kann zur weiteren Entwicklung der europäischen Polizeibehörde festgestellt werden, dass diese mit inzwischen über 400 Mitarbeitern ihren Arbeitsschwerpunkt im Bereich der Analysedateien ausgebaut hat. Zwischenzeitlich sind über 40 Analyseverfahren mit unterschiedlicher Zielstellung aufgelegt worden. Demgegenüber ist das als "personeller Grundfundus" für die Auswertung und Zusammenarbeit vorgesehene Informationssystem noch immer nicht voll arbeitsfähig. Die Lücke muss unverändert über eine intensive Zusammenarbeit der bei Europol akkreditierten Verbindungsbeamten aus den Mitgliedsländern geschlossen werden.
Ein weiter ausgedehnter Bereich ist die Zusammenarbeit Europols mit Drittstaaten und -stellen. Inzwischen gibt es 18 bereits abgeschlossene bzw. in der Verhandlung befindliche Abkommen. Darunter ist das im Dezember 2002 abgeschlossene und bei den Verhandlungen in mehreren Punkten schwierige Abkommen mit den USA. Hauptstreitpunkte waren die Zweckbindung, Korrektur- und Löschungsregelungen und die unabhängige datenschutzrechtliche Kontrolle der über 20.000 beteiligten amerikanischen öffentlichen Stellen. Letztere ist, verglichen mit europäischen Maßstäben, unzulänglich.
Während der dänischen EU-Präsidentschaft im zweiten Halbjahr 2002 wurde auch ein erster Entwurf zur Änderung bzw. Erweiterung der Europol-Konvention vorgelegt. Die Vorschläge zielen im wesentlichen auf eine Verschlankung und Rationalisierung der Arbeitsabläufe bei Europol. Dazu

wird auch - nicht ungefährlich - eine erst nachträgliche Kontrolle datenschutzrechtlicher Standards durch den Verwaltungsrat und die Gemeinsamen Kontrollinstanz (GKI) vorgeschlagen.
Die Vergabe von Exekutivrechten an Europol ist bisher nicht vorgesehen.

Von der GKI ist im Februar 2003 eine zweite datenschutzrechtliche Kontrolle bei Europol durchgeführt worden. Die Ergebnisse werden z.Zt. mit Europol diskutiert und ausgewertet.
Weitere Einzelheiten - auch zur Arbeit der GKI für Europol - können deren Ende 2002 erstelltem ersten Tätigkeitsbericht entnommen werden, der in allen Sprachfassungen im Juli dieses Jahres ins Internet zur Information eingestellt werden soll.

7. Entwicklung der automatisierten Datenverarbeitung

7.1 Automatisierte Datenverarbeitung in der Landesverwaltung

Über den Stand der Entwicklung des Einsatzes der Informations- und Kommunikationstechnik (IuK) in der Landesverwaltung aus datenschutzrechtlicher Sicht hat der Landesbeauftragte zuletzt in seinem V. Tätigkeitsbericht (Ziff. 6) ausführlich informiert.
Das Land verfügt über eine moderne Kommunikationsinfrastruktur, die sich auf der Basis des ITN-LSA entwickelt hat und die gegenwärtig für die Landesverwaltung Kommunikationsmöglichkeiten sowohl im internen Landesverwaltungsnetz (Intranet), im TESTA-Deutschland-Netz als auch im Internet bietet. Das Ministerium des Innern als Netzbetreiber des ITN-LSA benutzt deshalb auch die Bezeichnung "Corporate Network der Polizei und der Verwaltung des Landes Sachsen-Anhalt" (CNPV LSA).
Beim Einsatz moderner IuK durch die Landesverwaltung, bei dem in vielfältiger Weise personenbezogene Daten automatisiert erhoben, verarbeitet oder genutzt werden, sind die Rechte der Bürgerinnen und Bürger wirksam zu schützen (§ 1 DSG-LSA).

Mit der Novellierung des DSG-LSA vom 21.08.2001 (GVBl. LSA S. 384) ist der Zweck des Gesetzes in § 1 Abs. 2 dahin gehend präzisiert worden, dass öffentliche Stellen Verfahren zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten an dem Ziel auszurichten haben, so wenig wie möglich personenbezogener Daten zu erheben, zu verarbeiten oder zu nutzen. Damit wird den datenschutzrechtlichen Prinzipien der Datenvermeidung bzw. Datensparsamkeit Rechnung getragen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen.
Der Landesgesetzgeber hat damit rechtliche Rahmenbedingungen geschaffen, die die Anwendung datenschutzfreundlicher Technologien unterstützen. Der Landesbeauftragte hatte diese Thematik bereits in seinem IV. Tätigkeitsbericht (Ziff. 8.2.3) dargestellt und erläutert.

Der Landesbeauftragte weist in diesem Zusammenhang erneut auf die Rechtsverantwortung der Obersten Landesbehörden nach § 14 Abs. 1 DSG-LSA, gerade bei der Umsetzung komplexer Strategien zur umfassenden Vernetzung bzw. zur Schaffung landes- und weltweiter Kommunikationsbeziehungen, hin. Bei komplexen Verfahren wie u.a. dem **eGovernment-Konzept Sachsen-Anhalt** oder dem **Landesportal Sachsen-Anhalt** müssen künftig Datenschutzbelange, d.h. die bereichsspezifischen Datenschutzvorschriften, wie z.B. im Telekommunikations- und Medienrecht, bereits bei der Planung bzw. Einrichtung noch stärker Beachtung finden.

Dieser Verantwortung müssen auch die anderen in § 14 DSG-LSA genannten öffentlichen Stellen, insbesondere die Kommunen und die öffentlich-rechtlichen Körperschaften, genügen.

In diesem Zusammenhang ist wegen festgestellter Defizite nachdrücklich auf die gesetzliche Verpflichtung hinzuweisen, den Landesbeauftragten **rechtzeitig** über Planungen des Landes beim Aufbau automatisierter Informationssysteme zu unterrichten (§ 22 Abs. 4 Satz 2 DSG-LSA).

Mit dem neu geschaffenen Institut eines **"Beauftragten für den Datenschutz"** in den Behörden (§ 14a DSG-LSA) hat der Landesgesetzgeber die Selbstkontrolle der Verwaltung gestärkt und dem Beauftragten gleichzeitig besondere Pflichten übertragen, so z.B. die Vorabkontrolle bei automatisierten Verfahren nach § 14a Abs. 4 DSG-LSA.
Die rechtzeitige Einbindung der neuen Beauftragten für den Datenschutz in die Planungen der Behörden kann somit ein wesentlicher Beitrag zum datenschutzgerechten Umgang mit den personenbezogenen Daten der Bürgerinnen und Bürger des Landes sein.

Der aktuelle 8. IT-Gesamtplan der Informationstechnik (2002) gibt einen Überblick zur neuen IT-Organisationsstruktur der Landesverwaltung, zur eingesetzten Standardsoftware und zu den Betriebssystemen, zum Stand beim Ausbau des ITN-LSA als ressortübergreifender Infrastruktur, zum Ausstattungs- und Vernetzungsgrad der Landesverwaltung mit IuK sowie zum eGovernment-Konzept der Landesverwaltung.
Demnach hat sich z.B. die Anzahl der an das ITN-LSA angeschlossenen Behörden und Dienststellen von ca. 400 im Jahr 2000 bis Ende 2002 auf 582 erhöht. Die Anzahl der Arbeitsplatz-PC in den Ressorts und deren nachgeordneten Einrichtungen hat sich im gleichen Zeitraum von 20.552 auf 24.600 erhöht. Damit ist die Ausstattung der Obersten Landesbehörden mit PC-Technik und ihre ausreichende Vernetzung im wesentlichen abgeschlossen. Nur in den nachgeordneten Bereichen des Ministeriums für Bau und Verkehr, des Ministeriums des Innern, des Ministeriums der Justiz und des Kultusministeriums besteht noch ein gewisser Nachholbedarf.

Hinsichtlich des Einsatzes von Betriebssystemen überwiegen die Microsoft-Betriebssysteme mit einen Anteil von ca. 91 % (davon Win9.X 20 %; WinNT 71 %), gefolgt von UNIX-Betriebssystemen mit 7 % (dabei LINUX unter 1 %) und den Novell-Betriebssystemen mit 2 %.
Eine ähnliche Dominanz ist beim Einsatz von Microsoft-Office-Produkten (Textverarbeitung, Tabellenkalkulation, Datenbank) in der Landesverwaltung zu verzeichnen.
Die spezifischen Fachanwendungen der Ressorts, wie z.B. in den Bereichen der Steuer- und Finanzverwaltung, der Katasterverwaltung, der Polizei oder der Justizverwaltung, bleiben dabei unberücksichtigt.

Das Ministerium des Innern ist derzeit im Auftrag der Staatskanzlei mit der Ausarbeitung eines **eGovernment-Konzepts** für die öffentliche Verwaltung des Landes Sachsen-Anhalt befasst. Bis zum Jahr 2005 sollen die wichtigsten Dienstleistungen des Landes online im Internet angeboten und die internen Verwaltungsprozesse optimiert und rationalisiert sein.

Seine grundsätzliche Position zum eGovernment hat der Landesbeauftragte bereits im V. Tätigkeitsbericht (Ziff. 6.1) dargelegt.
Abschließend sei auf die aktuellen Handlungsempfehlungen "Datenschutzgerechtes eGovernment" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 30. November 2002 hingewiesen.

Diese Handlungsempfehlungen wurden als Druckauflage seitens des Landesbeauftragten an alle Ressorts verteilt. Es gibt weiter eine rege Nachfrage, auch aus dem Kommunalbereich. Die Broschüre ist auch über seine Homepage als pdf-Datei herunterzuladen.

7.2 Neuordnung der IT-Organisation des Landes

In seinem V. Tätigkeitsbericht (Ziff. 6.2) hatte der Landesbeauftragte über das neue IT-Leitbild der damaligen Landesregierung informiert.
Mit ihrem Kabinettsbeschluss "Übergreifende IT-Organisationsstruktur der Landesverwaltung" vom 19.03.2002 (MBl. LSA S. 363) wurden weitere grundlegende Entscheidungen getroffen. Zu den wesentlichen Punkten dieses Kabinettsbeschlusses gehören:

- die Einrichtung der **Landesleitstelle IT (LIT)** zum 01.07.2002 als Referat 45 im Ministerium des Innern, ehemals Zentrale Stelle IT (ZIT, Ref. 34),
- die Bildung des **IT-Koordinierungsausschusses (IT-KA)**, der der LIT zugeordnet ist und diese bei ihrer ressortübergreifenden Koordinierungsarbeit unterstützen soll und der aus den IT-Verantwortlichen der Ressorts besteht
  sowie
- die Bildung eines **Landesinformationszentrums Sachsen-Anhalt (LIZ)** durch Herauslösung des ehemaligen Landesrechenzentrums aus dem Landesamt für Landesvermessung und Datenverarbeitung

als wirtschaftlich eigenständigem Landes-Betrieb nach § 26 LHO - mit der Funktion eines zentralen landesinternen Dienstleisters - sowie der Schaffung eines IT-Kompetenz-Centers im LIZ, sowohl für die Landes- als auch für die Kommunalverwaltung (ohne Nutzungszwang).

Gleichzeitig mit der Einrichtung des IT-KA wurde der seit 1993 existierende Interministerielle Arbeitskreis Informationstechnik (IMA-IT) aufgelöst.

Als Folge dieser Entscheidungen der Landesregierung sieht der Landesbeauftragte gute Voraussetzungen, dass seine wiederholt geübte Kritik in den Tätigkeitsberichten der zurückliegenden Jahre hinsichtlich noch bestehender Defizite bei der Datensicherheit im Rahmen der strategischen Entscheidungen der LIT und des IT-KA verstärkt Berücksichtigung finden wird.

Der Landesbeauftragte regte die Befassung des IT-KA mit nachfolgenden Themenschwerpunkten an:

- dem Sicherheitskonzept für das Landesnetz (ITN-LSA) und seiner Fortschreibung und der Zertifizierung nach den Common Criteria (CC),
- dem Projekt TESTA-Deutschland bezüglich der Anbindung an das ITN-LSA,
- der Neufassung der IT-Grundsätze für die Landesverwaltung mit Festlegung von Sicherheitsstandards bezüglich Datensicherheit (§ 6 DSG-LSA),
- der Schaffung einer einheitlichen Regelung zur Nutzung des E-Mail-Dienstes auf der Grundlage der Musterdienstanweisung zur Nutzung von Internet und E-Mail unter Beachtung sich abzeichnender Änderungen im Telekommunikationsrecht,
- der Installation der Public Key Infrastruktur (PKI) des Landes und der Lösung der Trust-Center-Problematik sowie
- den zukünftigen Anwendungen beim eGovernment und beim Landesportal Sachsen-Anhalt.

An den Beratungen des IT-KA nimmt der Landesbeauftragte als Gastmitglied teil. Er bietet diesem Gremium seine Unterstützung an und sieht darin zugleich eine gute Voraussetzung, seinem gesetzlichen Beratungsauftrag gem. § 22 Abs. 4 Satz 1 DSG-LSA nachzukommen.

7.3 Fortschritte beim Sicherheitskonzept für das Landesnetz (ITN-LSA)

Seit 1995 (III. Tätigkeitsbericht, Ziff. 8.2.2) hat sich der Landesbeauftragte wiederholt kritisch zum fehlenden Gesamtsicherheitskonzept für das bereits am 14. Oktober 1993 eingerichtete ITN-LSA geäußert.

Noch im März 2001 musste der Landesbeauftragte in seinem V. Tätigkeitsbericht (Ziff. 6.3) berichten, dass ihm kein prüffähiges Gesamtsicherheitskonzept für das ITN-LSA zur Stellungnahme vorlag, obwohl seit der Inbetriebnahme fast 8 Jahre vergangen waren.

Das Erstaudit einer Sicherheitsuntersuchung erfolgte am 09.05.2001 und hatte eine Gültigkeit bis zum 31.07.2002. Die in Auftrag gegebene Sicherheitsuntersuchung des Landesnetzes wurde mit der Übergabe des Erst-Zertifikates am 29.11.2001 erfolgreich abgeschlossen.
Gegenstand der Zertifizierung waren zwei wesentliche Sicherheitsziele:
- Bereitstellung zentraler Kommunikationsdienste
- sehr hohe Verfügbarkeit der Transportfunktionalität des Netzes.

Im Januar 2003 informierte das Ministerium des Innern den Landesbeauftragten über das erfolgreich durchgeführte Folgeaudit vom 28.11.2002. Dieses Zertifikat ist bis zum 31.12.2003 gültig. Der vollständige Auditbericht liegt dem Landesbeauftragten vor. Er geht davon aus, dass die im aktuellen Auditbericht noch aufgezeigten Mängel zeitnah beseitigt werden und er entsprechend unterrichtet wird.

Allerdings ist festzuhalten, dass die Erteilung des Zertifikats auf der Grundlage der Überprüfung nach der **internen** Richtlinie DOT-07 ("Zertifizierung von Organisation und Technik") der T-Systems ISS GmbH Bonn erfolgte.
Deshalb regt der Landesbeauftragte an, die Möglichkeiten der zukünftigen Zertifizierung des Landesnetzes bzw. einzelner ausgewählter Komponenten zur Abgrenzung des Evaluationsgegenstandes gemäß den international gültigen Common Criteria durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) prüfen zu lassen, auch wenn damit wesentlich höhere Kosten verbunden sein könnten.
Die Sicherheit beim Einsatz modernster Informations- und Kommunikationstechnik darf nicht aus Kostengründen vernachlässigt werden. Nur durch einen hohen Sicherheitsstandard und dessen regelmäßiger Überprüfung durch gesetzlich dafür bestimmte Institutionen wie das BSI wird dem Auftrag in § 1 Abs. 1 DSG-LSA langfristig Rechnung getragen, eine Beeinträchtigung des Persönlichkeitsrechts der Bürgerinnen und Bürger durch den Umgang öffentlicher Stellen mit ihren personenbezogenen Daten zu verhindern.

Die bereits vorhandenen einzelnen Dokumente zur Sicherheitspolitik des ITN-LSA sollten in ein Gesamtsicherheitskonzept einfließen, welches auch die besonderen Anforderungen der Datensicherheit für die Verarbeitung personenbezogener Daten nach § 6 Abs. 2 DSG-LSA berücksichtigt. Ein solches Gesamtkonzept sollte ein zentrales Thema für die zukünftige Arbeit im IT-KA zur Ausarbeitung von IT-Standards sein.

Mit der Festlegung einer verbindlichen Sicherheitspolitik und den entsprechend einzuhaltenden Sicherheitsstandards für alle Teilnehmer im ITN-LSA muss die längst fällige Überarbeitung der IT-Grundsätze vom 01.06. 1992 (MBl. LSA S. 805) sowie des sog. Netz-Erlasses zum ITN-LSA vom 07.02.1994 (MBl. LSA S. 1251) erfolgen.

Die Ressorts haben im Rahmen ihrer Rechtsverantwortung nach §§ 14 Abs. 1 i.V.m. 6 Abs. 2 DSG-LSA für sich und ihren nachgeordneten Bereich weitere Schutzvorkehrungen bei der Verarbeitung personenbezogener Daten zu treffen, wenn dies die besondere Qualität der personenbezogenen Daten erfordert, wie z.B. bei personenbezogenen Daten, die besonderen gesetzlichen Geheimhaltungsbestimmungen unterliegen (Sozialdaten, medizinische Daten, Steuerdaten) sowie anderen personenbezogenen Daten besonderer Art (§ 2 Abs. 1 Satz 2 DSG-LSA).
Das ITN-LSA stellt insofern "nur" ein Transportsystem mit einem definierten Sicherheitsstandard dar.

7.4 Zentraler Verzeichnisdienst im ITN-LSA

Verzeichnisdienste sind für die reibungslose Kommunikation im Landesnetz, im TESTA-Deutschland-Netz sowie im Internet eine unabdingbare Voraussetzung.
Aus diesem Grund hatte der frühere IMA-IT mit Beschluss vom 10.04. 2001 die Bildung einer **Arbeitsgruppe Verzeichnisdienste** zur Erarbeitung eines Konzeptes für einen zentralen Verzeichnisdienst der Landesverwaltung unter Federführung des Landesrechenzentrums eingesetzt. Der Landesbeauftragte wurde dabei beteiligt.

Im V. Tätigkeitsbericht (Ziff. 6.5) ist bereits über den aktuellen in der Praxis verwendeten Standard (X.509v3 von 1996) für Verzeichnisdienste ausführlich informiert und dabei auf die datenschutzrechlichen Probleme beim Einsatz solcher Verzeichnisdienste hingewiesen worden.
Problematisch sind insbesondere die Handhabung des administrativen Zugriffs auf diesen Verzeichnisdienst, seine Abschottung sowie die Veröffentlichungspraxis der Mitarbeiterdaten.

Dabei ist aus datenschutzrechtlicher Sicht wichtig, in welche Netze die Einstellung dieser personenbezogenen Daten erfolgt.
Bei der Einstellung ins **Landesnetz** (ITN-LSA) unter Beachtung des Grundsatzes der Erforderlichkeit - nicht jeder Mitarbeiter einer Behörde muss im Verzeichnisdienst geführt werden - ist die Zustimmung der Mitarbeiter nicht erforderlich. Eine Information durch die Behördenleitung kann aber für Transparenz und Vertrauen bei den Bediensteten sorgen.
Eine Einstellung dieser Daten für den Abruf im **TESTA-Deutschland-Netz** bedarf, da hierbei Daten außerhalb der Landesverwaltung genutzt werden können, stets der Einwilligung der betroffenen Bediensteten.
Bei einer Einstellung dieser Daten im zentralen Verzeichnisdienst für einen Abruf über das **Internet** ist vorab zu prüfen, ob dabei die gesetzlichen Voraussetzungen für die Übermittlung dieser personenbezogenen Daten ins Ausland vorliegen.

Diese grundlegenden Hinweise hat das Ministerium des Innern berücksichtigt.

Das Landesinformationszentrum führt die Anbindung des zentralen Verzeichnisses des Landes über die Verwaltungs-PKI im TESTA-Deutschland-Netz durch. Über das HTTP/LDAP-Gateway im TESTA-Deutschland-Netz wird das zentrale Verzeichnis des Landes mit den Verzeichnisdiensten der anderen Bundesländer verbunden.
Mit der Differenzierung durch Ziffern beim Attribut "Veröffentlichungshinweis" in

0 – keine Veröffentlichung
1 – Veröffentlichung im Intranet (Landesnetz)
2 – Veröffentlichung im TESTA-Deutschland-Netz und
3 – Veröffentlichung im Internet,

wobei der Standard-Wert auf "1" gesetzt wurde, ist den datenschutzrechtlichen Belangen Rechnung getragen worden.

In einem Gemeinsamen Runderlass vom 01.01.2003 (MBl. LSA S. 35) hat das Ministerium des Innern im Einvernehmen mit der Staatskanzlei, den übrigen Ministerien, dem Landesrechnungshof und der Landtagsverwaltung die Richtlinie zum Verzeichnisdienst der Landesverwaltung bekannt gemacht und darin entsprechende datenschutzrechtliche Hinweise für eine über das Landesnetz hinausgehende Veröffentlichung gegeben.

Bei seinen Kontrollen wird der Landesbeauftragte ein besonders Augenmerk auf die Erforderlichkeit der Personaleinträge in den Verzeichnissen der Ressorts und die Einhaltung der technischen und organisatorischen Maßnahmen nach § 6 Abs. 2 DSG-LSA legen, insbesondere was die Authentifizierungsmechanismen und die Nutzung der Zugriffskontrollmechanismen betrifft.

7.5 Neues IP- und Routingkonzept im ITN-LSA

Der Landesbeauftragte erinnert in diesem Zusammenhang an seine grundlegenden Ausführungen im III. Tätigkeitsbericht (Ziff. 8.1 f) zum Thema Vernetzung bzw. Herstellung neuer Kommunikationsbeziehungen. In seinem V. Tätigkeitsbericht (Ziff. 6.1) hatte der Landesbeauftragte über die Erneuerung der Netzknotentechnik (Ablösung der ASCOM-Knotentechnik) in Verbindung mit dem Konzept zur Umstellung auf ein **dynamisches Routing** im Backbone-Bereich des ITN-LSA informiert. Die Erneuerung der Netzknotentechnik (Einsatz von DATUS-Knotentechnik) ist nun im Wesentlichen abgeschlossen.

Das z.Zt. noch praktizierte IP-Konzept entstand 1992 im Zusammenhang mit dem Aufbau des ursprünglichen ITN-LSA auf Basis der ASCOM-Knotentechnik. Durch die Verwendung vorwiegend **statischer** Routen wurde die Administration im Zusammenhang mit dem Anwachsen der Verwaltung, des Internetverkehrs und der zunehmenden Routerzahl extrem komplex und aufwendig.

Das Land Sachsen-Anhalt hatte damals im Zuge des Aufbaus des ITN-LSA vom DENIC, der Deutschen Vergabestelle für IP-Adressen, die international gültige **Class B** Adresse 164.133.0.0 zugewiesen bekommen.
Die Adresse wurde durch den Betreiber des ITN-LSA, das Technische Polizeiamt Magdeburg (TPA), in Subnetze (Class C) aufgeteilt und an die Teilnehmer des Netzes auf Antrag vergeben.
Zum gegenwärtigen Zeitpunkt sind fast alle Class C Netze (ca. 250 insgesamt) im Netzwerk 164.133.0.0 vergeben.
Daher mussten seitens des Netzbetreibers Maßnahmen ergriffen werden, um weiterhin IP-Adressen zur Verfügung stellen zu können.

Neues IP-Konzept
Zur Lösung des Problems hat sich das TPA in Abstimmung mit dem Ministerium des Innern für die Verwendung (Routing) von nicht offiziellen IP-Adressen im ITN-LSA in Verbindung mit der Umsetzung eines sog. Core-Router-Konzeptes entschieden.
Diese Lösung bietet neben der Erlangung ausreichender IP-Adressen die Möglichkeit für eine sukzessive systematische IP-mäßige Neustrukturierung des ITN-LSA. Derzeitig ist das ITN-LSA nach außen gegenüber dem Internet nur mit zwei IP-Netzen bekannt. Dies soll aus Sicherheitsgründen so bleiben.
Innerhalb des ITN-LSA ist es gleichgültig, welche IP Adressen verwendet werden. Wichtig ist dabei, dass an allen Übergängen zu anderen Fremdnetzen nur die Netzadresse 164.133.xxx.xxx des ITN-LSA sichtbar ist.

Einsatz von sog. Core-Routern
Mit Aufstellung der **Core-Router** und Einführung des dynamischen Routings über das dynamische Routingprotokoll **OSPF** (Open Shortest Path First – "kürzester Weg zuerst") werden neue IP Nummernkreise eingeführt. Dazu werden im Land Sachsen-Anhalt entsprechende OSPF-Sektoren eingerichtet. Jeder Sektor gehört zu einer sog. OSPF-Area.
Damit wird es möglich, ein "Sammelrouting" einzuführen. Vorteile dieser Methode liegen in der Verringerung der Anzahl der zu verwaltenden Routen, in der Vereinfachung der Fehlersuche und somit der schnelleren Fehlererkennung und Beseitigung. Insgesamt entsteht für das ITN-LSA eine übersichtliche IP-Struktur.
Ein Router einer Lokation braucht dann nur noch eine Defaultroute zum nächstgelegenem Core-Router zu kennen.
Der Administrationsaufwand in den einzelnen Lokationen und Ressorts wird ebenfalls erheblich verringert. Veränderungen bei Netzadressen werden automatisch bekannt gemacht.

Datenschutzrechtliches Fazit
Die vorgenannten Veränderungen unterstützen in gewissem Umfang auch die in § 6 Abs. 2 DSG-LSA genannten Ziele der Datensicherheit (Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz).

Aus datenschutzrechtlicher Sicht bringt aber die Einführung des **dynamischen Routings** (OSPF) auch Probleme mit sich. So führt die Einführung dazu, dass **alle** Netze im gesamten ITN-LSA bekannt werden. Damit wäre theoretisch die Kommunikation "jeder mit jedem" bei automatischer Routenwahl möglich.
Unter Berücksichtigung der Rechtsverantwortung nach § 14 Abs. 1 DSG-LSA sind aber im Sinne eines vorgelagerten Grundrechtsschutzes nach den Anforderungen des Bundesverfassungsgerichtes (BVerfGE 65,1) insbesondere die Grundsätze der **Verhältnismäßigkeit** und der **Zweckbindung** bei der Herstellung von Kommunikationsbeziehungen zu beachten. Daraus folgt, die Herstellung neuer Kommunikationsbeziehungen (z.B. durch Routing) ist nur zulässig, wenn sie zur Erfüllung konkreter Verwaltungsaufgaben **erforderlich** ist. Auch sind die Zweckbindung bei der Erhebung und Verarbeitung personenbezogener Daten und der Grundsatz der informationellen Gewaltenteilung zu berücksichtigen. Deshalb müssen die Erforderlichkeit und das Risiko einer Zusammenführung personenbezogener Daten aus verschiedenen Quellen, auch bei der Einführung neuer Technologien wie dem dynamisches Routing, rechtzeitig abgewogen werden.

Deshalb regt der Landesbeauftragte an, die IT-Verantwortlichen in allen Bereichen über die Folgen zu informieren und hinsichtlich der aufgezeigten datenschutzrechtlichen Problematik zu sensibilisieren.
Das betrifft insbesondere die Abschottung der lokalen Netze der Ressorts und der übrigen öffentlichen Stellen als Teilnehmer am Landesnetz (ITN-LSA), wenn darin die automatisierte Verarbeitung personenbezogener Daten stattfindet.

Es ist nicht nur davon auszugehen, dass "Außentäter" über das Internet versuchen, Zugang zum ITN-LSA zu erlangen, sondern es muss auch die Problematik der "Innentäter" gesehen und durch entsprechende Schutzmaßnahmen deren unbefugtes Eindringen in fremde Behördennetze verhindert werden.
In diesem Zusammenhang sind entsprechend umgesetzte Passwortrichtlinien schon ein guter Schutz. Passwörter sollten auch Ziffern und Sonderzeichen enthalten und eine entsprechende Mindestlänge von 6 bis 8 Zeichen besitzen, bei mehrmaliger Fehleingabe muss die Kennung gesperrt werden. Keine Verwendung vordefinierter Nutzerkennungen, wie z.B. "Gast" oder "Admin", keine Verwendung von Trivialpasswörtern.

Den genannten Gefährdungen soll durch den Einsatz von virtuellen privaten Netzen (**VPN - Virtual Private Network**) auf Basis von **IPSec** (IPSecurity) begegnet werden. So wird sichergestellt, dass nur die füreinander bestimmten Partner mit einander in Verbindung treten können. Daten werden über diese Verbindungen nur verschlüsselt gesendet.
Die Verschlüsselung erfolgt über das sog. ESP-Protokoll (Encapsulation Security Payload).

Für die Verschlüsselung kennt IPSec zwei Betriebsmodi: Transportmodus und Tunnelmodus.
Im **Transportmodus** wird ausschließlich der Datenteil (Nutzungsdaten) des IP-Pakets verschlüsselt. Die anderen Teile der Nachricht (IP-Header) bleiben unverändert.
Im **Tunnelmodus** hingegen wird das gesamte IP-Paket **vor** der Übertragung verschlüsselt und mit einem neuen IP-Header versehen, der die Daten für den Zielknoten enthält. Diese Variante wird dann auch als **VPN** bezeichnet.

Der Landesbeauftragte hält, sichere Verschlüsselungsalgorithmen und ausreichende Schlüssellängen vorausgesetzt (symmetrisch; 128 Bit), den Einsatz von VPN für eine geeignete Maßnahme der Datensicherheit zur Übermittlung personenbezogener Daten im ITN-LSA.

8. Finanzwesen

8.1 Änderung der Abgabenordnung

Der Landesbeauftragte hat zuletzt in seinem V. Tätigkeitsbericht (Ziff. 7.1) auf die Fortschritte hingewiesen, die die Datenschutzbeauftragten des Bundes und der Länder bei den Verhandlungen mit der Finanzverwaltung zu datenschutzrechtlichen Verbesserungen in der Abgabenordnung erzielen konnten. Nach den Beratungen mit der Finanzverwaltung hat der Bundesbeauftragte für den Datenschutz eine Bund-Länder-Arbeitsgruppe einberufen, die detaillierte Vorschläge für datenschutzrechtlich erforderliche bzw. wünschenswerte Änderungen und Ergänzungen der Abgabenordnung erarbeitet hat.

Hierbei sind insbesondere folgende Punkte zu nennen:
- Regelung des Akteneinsichts- bzw. Auskunftsrechts
- Regelung der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag (Outsourcing)
- Regelung von Aufbewahrungsfristen, Löschung und Sperrung von Daten.

Die Novellierung der Abgabenordnung hinsichtlich einer Ergänzung um weitere notwendige datenschutzrechtliche Vorschriften sollte im Interesse der Bürgerinnen und Bürger Sachsen-Anhalts auch von der Landesregierung entsprechend unterstützt werden.

8.2 Prüfung der Finanzämter

Der Landesbeauftragte hat im Berichtszeitraum die im Kalenderjahr 1997 (vgl. IV. Tätigkeitsbericht, Ziff. 9.5) begonnene Prüfung der Finanzämter bei zwei weiteren Ämtern fortgesetzt.

Auch bei diesen Prüfungen zeigte sich ein Schwerpunkt bei Mängeln im technisch-organisatorischen Bereich.
Dies betraf insbesondere:

- die fehlende Einsetzung eines behördlichen Datenschutzbeauftragten gem. § 14a Abs. 1 DSG-LSA,
- die fehlende Führung des Verfahrensverzeichnisses gem. § 14 Abs. 3 DSG-LSA sowie
- die Reinigung der Finanzämter durch Fremdfirmen ohne Aufsicht im Zusammenhang mit unverschlossenen Aktenräumen und offener Aktenhaltung.

Obwohl die öffentlichen Stellen seit der Novellierung des DSG-LSA vom 21.08.2001 (GVBl. LSA S. 348) verpflichtet waren, einen behördlichen Datenschutzbeauftragten gem. § 32 Abs. 2 DSG-LSA bis spätestens 31. Januar 2002 einzusetzen, war dies in beiden Finanzämtern unterblieben.

Auch ein Verfahrensverzeichnis gem. § 14 Abs. 3 DSG-LSA bzw. nach bisherigem Recht zu erstellende Dateifestlegungen konnten nicht vorgelegt werden. Da in den Finanzämtern nur zentrale Verfahren eingesetzt werden, die von der OFD Magdeburg festgelegt und im Finanzrechenzentrum Magdeburg administriert werden, bietet sich die Führung eines zentralen Verfahrensverzeichnisses an. Allerdings sollte jedes Finanzamt für Einsichtszwecke (vgl. § 14 Abs. 5 DSG-LSA) eine Duplikat dieses Verfahrensverzeichnisses vorhalten.

Die Reinigung der beiden Finanzämter erfolgte durch Fremdfirmen außerhalb der Dienstzeiten, ohne eine Kontrolle durch Mitarbeiter. Dazu waren die Reinigungsfirmen im Besitz mehrerer Schlüssel. Im Zusammenhang mit der Aufbewahrung der Steuerakten in offenen Aktenregalen bzw. unverschlossenen zentralen Aktenräumen und Arbeitsräumen ist diese Verfahrensweise nicht mit dem Steuergeheimnis § 30 AO und den Anforderungen des § 6 Abs. 3 DSG-LSA vereinbar, auch wenn die Reinigungskräfte zur Verschwiegenheit belehrt und verpflichtet wurden.

Eine dem Steuergeheimnis und den datenschutzrechtlichen Vorschriften gerechte Vorgehensweise ist nur durch eine Reinigung unter Aufsicht oder eine konsequente und sichere Aufbewahrung der Steuerakten und des Schriftgutes mit personenbezogenen Daten Steuerpflichtiger in verschlossenen Aktenschränken bzw. Aktenräumen zu erreichen.
Im Übrigen ist es nicht nachvollziehbar, wieso die technisch-organisatorischen Maßnahmen bei der **automatisierten** Verarbeitung der Steuerdaten - insbesondere durch die restriktive Vergabe von Zugriffsrechten - den Zugriff Unbefugter nahezu vorbildlich ausschließen, während bei der **nicht-automatisierten** Verarbeitung in Akten dagegen praktisch jeder Unbefugte (z.B. Besucher des Finanzamtes, aber auch unbefugte Mitarbeiter des Finanzamtes selbst) Zugang zu den dort gespeicherten personenbezogenen Daten erhalten kann.

Die Antwort der OFD Magdeburg lässt erkennen, dass Konsequenzen aus den Überprüfungen der beiden Finanzämter gezogen worden sind.
So soll dem Landesbeauftragten in Kürze die überarbeitete **Dienstanweisung Datenschutz** vorgelegt werden, in welche die Feststellungen des Landesbeauftragten aus den beiden Kontrollen einfließen werden.

Wegen der noch nicht abgeschlossenen Einführung und Pilotierung neuer Verfahren in den Finanzämtern (UNIFA) wird die OFD Magdeburg von der Regelung des § 14a Abs. 1 Satz 2 DSG-LSA Gebrauch machen und als Dienstaufsichtsbehörde einen zentralen Beauftragten für den Datenschutz für sich selbst und die Finanzämter kurzfristig ernennen.
In den Finanzämtern selbst wird ebenfalls ein Mitarbeiter mit datenschutzrechtlichen Aufgaben als Ansprechpartner für die OFD Magdeburg betraut.

8.3 Änderung des Kraftfahrzeugsteuergesetzes

Mit der Änderung des Kraftfahrzeugsteuergesetzes zum 01.08.2002 haben die Länder die Möglichkeit, durch Erlass einer entsprechenden Rechtsverordnung die Aushändigung des Kfz-Scheines von der Erteilung einer Einzugsermächtigung für die zu entrichtende Kfz-Steuer abhängig zu machen. Als weitere Möglichkeit soll der Nachweis verlangt werden können, dass keine Kfz-Steuer-Rückstände bestehen.

Aus datenschutzrechtlicher Sicht ist der **Zwang** für **alle** Kfz-Halter zur Erteilung einer generellen Einzugsermächtigung bei Kraftfahrzeugzulassungen - nicht nur beschränkt auf den ersten Entrichtungszeitraum wie bisher - ein rechtlich nicht verhältnismäßiges und auch praktisch nicht geeignetes Mittel zur Eindämmung der Kfz-Steuerrückstände.
Der Zwang, bei jeder Kraftfahrzeugzulassung eine Bankverbindung bekannt geben zu müssen, stellt einen nicht unerheblichen Eingriff in das Grundrecht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger dar, der ohnehin nur die steuerehrlichen Bürger trifft.
Erleichterungen für die Verwaltung ergeben nach der Rechtsprechung des Bundesverfassungsgerichts für sich noch keine Begründung zum Eingriff in Grundrechte der Bürger. Es ist Sache der beteiligten öffentlichen Stellen - nicht der Steuerpflichtigen -, das Besteuerungsverfahren bürgerfreundlich und effizient abzuwickeln. Dabei sind - wie beim Beispiel "Bürgerbüro“ - neue Wege zu beschreiten, ehe in ein Grundrecht eingegriffen wird. Grundsätzlich muss es deshalb dem mündigen Bürger überlassen bleiben, auf welchem Wege er seine Steuerschuld begleichen will.

Bei den Steuerpflichtigen mit Kfz-Steuerrückständen handelt es sich im übrigen um eine Minderheit. Sie trifft man mit der Einzugsermächtigung kaum, denn die "schwarzen Schafe" geben ohnehin ein nicht existierendes oder kurz darauf aufgelöstes Bankkonto an, und bei den Insolventen ist das Konto leer.

Mit der neuen Gesetzesvorschrift besteht für die Länder zudem die Möglichkeit zu bestimmen, dass über das Nichtbestehen von Kfz-Steuerrückständen ein Nachweis erbracht werden soll. Dies hält der Landesbeauftragte nur in den Fällen für akzeptabel, wenn solche Steuerpflichtige Kraftfahrzeuge erneut anmelden wollen, deren letzte Fahrzeuge auf Veranlassung der Finanzbehörde wegen ausstehender Kfz-Steuer zwangsabgemeldet worden waren. Diese sog. "faulen Kunden" sind den Zulassungsstellen vor Ort im Regelfall bekannt.

Bei der Zulassung von Kraftfahrzeugen durch Dritte (z.B. Autohändler) soll es künftig möglich sein, dem Dritten das Ergebnis der Prüfung bei Kfz-Steuerrückständen mitteilen zu dürfen. Das führt zu unverhältnismäßigen Datenübermittlungen an Dritte und hat mit den Schutzinteressen des Staates gegen Steuersünder nichts mehr zu tun.

Der Landesbeauftragte hofft, dass das Land auf den Erlass einer solchen Verordnung unter Berücksichtigung der datenschutzrechtlichen Bedenken verzichten wird.

8.4 Steuerabzug bei Bauleistungen

Im Rahmen des Gesetzes zur Eindämmung illegaler Betätigung im Baugewerbe vom 30.08.2001 hat der Gesetzgeber u.a. ein Steuerabzugsverfahren bei Bauleistungen eingeführt. Durch das Steuerverkürzungsbekämpfungsgesetz vom 19.12.2001 wurde u.a. der Umfang der auf einer Rechnung des Unternehmers aufzuführenden Angaben erweitert.

Die gesetzliche Neuregelung zum Steuerabzug bei Bauleistungen verpflichtet grundsätzlich den Empfänger der Bauleistung, von der Gegenleistung an den Auftragnehmer einen Steuerabzug von 15 v.H. vorzunehmen und diesen Betrag an die Steuerverwaltung abzuführen (§ 48 ff EStG). Als Besonderheit haftet der Auftraggeber ausdrücklich für einen nicht oder zu niedrig abgeführten Abzugsbetrag. Der Auftragnehmer kann den Steuerabzug allerdings vermeiden, indem er dem Auftraggeber eine vom Finanzamt ausgestellte Freistellungsbescheinigung vorlegt, deren Inhalt durch § 48b Abs. 3 EStG bestimmt wird. Neben den dort geforderten Angaben (Name, Anschrift und Steuernummer) enthält der amtlich vorgeschriebene Vordruck der Finanzverwaltung auch das Geburtsdatum des Unternehmers bei Einzelfirmen.

Auf Grund zahlreicher Beschwerden von Steuerbürgern wegen der ihrer Auffassung nach nicht erforderlichen Erhebung des Geburtsdatums will das Bundesfinanzministerium künftig auf die Angabe des Geburtsdatums verzichten.

8.5 Computerausdruck zu privaten Zwecken

Höchst verwundert war ein Bürger des Landes, als er eines Tages eine anonyme Zuschrift erhielt, die einen Computerausdruck mit einem Begleitzettel mit Steuernummern und seine an- und abgemeldeten Pkw der letzten Jahre, ergänzt um handschriftliche Hinweise über bestehende Kfz-Steuerrückstände, enthielt.

Der anonyme Absender behauptete, dass er den Computerausdruck mit Begleitzettel vor dem Finanzamt gefunden habe und benannte sogar den Ehemann einer Mitarbeiterin des Finanzamtes als Verlierer der Dokumente. Der betroffene Bürger wandte sich deshalb an den Landesbeauftragten und bat um Aufklärung dieses Vorgangs.

Nach umfangreichen Ermittlungen konnte der Landesbeauftragte feststellen, dass die Ehefrau des angeblichen Verlierers als Mitarbeiterin des Finanzamtes den Computerausdruck und die Feststellung der Rückstände an Kfz-Steuer zu privaten Zwecken angefertigt hatte.

Durch ihr Verhalten hatte die Mitarbeiterin als Amtsträgerin gegen die Vorschrift über das Steuergeheimnis (§ 30 AO) verstoßen. Denn ein Computerausdruck zu privaten Zwecken war und ist unzulässig. Zusätzlich lag ein Verstoß gegen § 16 Abs. 2 Nr. 1 DSG-LSA vor, weil entgegen der gesetzlichen Löschungspflicht alte personenbezogene Daten weiter von ihr gespeichert worden waren.

Das betreffende Finanzamt leitete arbeitsrechtliche Schritte gegen die Mitarbeiterin ein.

8.6 Auskunftsersuchen der Steuerfahndung an eine Wohnungsbauförderungsstelle

Eine Wohnungsbauförderungsstelle hatte sich nach einem dort eingegangenen Auskunftsersuchen der Steuerfahndung an den Landesbeauftragten gewandt, um zu erfahren, ob es rechtlich zulässig sei, der Steuerfahndung **alle** Zahlungsempfänger von Wohnungsbauförderungsmitteln zu benennen. Der Kreis der zu ermittelnden Zuschussempfänger war in dem Auskunftsersuchen nicht auf bestimmte Personenkreise oder Objekte beschränkt.
Die Steuerfahndung berief sich als "(Steuer-)Strafverfolgungsbehörde" auf die Vorschriften der §§ 93 Abs. 1, dritter Satz i.V.m. § 208 Abs. 1 Satz 3 AO.

Der Landesbeauftragte war bei seiner datenschutzrechtlichen Beurteilung zu folgendem Ergebnis gekommen:

Wenn die Steuerfahndungsstelle als (Steuer-)Strafverfolgungsbehörde tätig wird, dann hat sie sich an den Regeln der §§ 160 und 161 Abs. 1 StPO zu orientieren. Diese Vorschriften verbieten eine allgemeine Ausforschung ohne tatsächliche Anhaltspunkte auf Straftaten im Einzelfall.
Wird die Steuerfahndung aber als Steuerbehörde tätig, die eine umfassende, gleichmäßige Erfassung aller Steuerpflichtigen garantieren will, dann hat sie sich auf Steuerpflichtige zu konzentrieren.
Nicht alle in dem Auskunftsersuchen aufgeführten Zahlungsempfänger waren aber Steuerpflichtige.
Unter Beachtung der Rechtsprechung des Bundesfinanzhofes hatte sich das Auskunftsersuchen auf die steuerrelevanten Objekte und Zuschussempfänger zu beschränken. Diese waren der Wohnungsbauförderungsstelle bekannt.

Das generelle Auskunftsersuchen war weder erforderlich noch verhältnismäßig und damit unzulässig.

9. Forschung

In seinem V. Tätigkeitsbericht (Ziff. 8) hatte der Landesbeauftragte noch berichtet, dass weiterhin rechtliche Defizite bei der Erhebung personenbezogener Daten im Rahmen von Forschungsvorhaben bestehen.

Durch die intensivierte und gute Zusammenarbeit mit den Forschungseinrichtungen wird der Landesbeauftragte inzwischen frühzeitig an geplanten Forschungsvorhaben beteiligt. Die von den Forschungseinrichtungen entwickelten Anschreiben mit Erläuterungen an Betroffene, deren Daten in Forschungsvorhaben Verwendung finden sollen, sowie die vorgelegten Einwilligungserklärungen entsprechen jetzt in der Regel den gesetzlichen Vorgaben.

Im Berichtszeitraum wurden 22 Forschungsprojekte datenschutzrechtlich beraten. Kleinere datenschutzrechtliche Korrekturen wurden einvernehmlich mit den Forschern eingearbeitet.

10. Gesundheitswesen

10.1 Anforderungen an einen Arzneimittelpass

Auf Grund der Diskussionen um die Unverträglichkeit eines Cholesterin senkenden Arzneimittels hat das Bundesministerium für Gesundheit geplant, eine Medikamentenchipkarte einzuführen, auf der möglichst sämtliche Arzneien eines Patienten gespeichert werden. Die elektronische Kommunikation und Transparenz soll der Verbesserung der Qualität der

medizinischen Versorgung und der Arzneimittelsicherheit, patientenorientierten Dienstleistungen und der Wirtschaftlichkeit im Gesundheitswesen dienen.

Bei der Umsetzung der politischen Vorstellungen über strukturelle Verbesserungen im Gesundheitswesen sind die Grundrechte der Patienten, insbesondere das Recht auf informationelle Selbstbestimmung, im Umgang mit den Daten zu berücksichtigen. Neue Gestaltungskonzepte müssen deshalb das Patientengeheimnis sowie die freie Verfügung des Patienten über seine persönlichen Daten berücksichtigen. Die Teilnahme am Verfahren allgemein und insbesondere die Freigabe der einzelnen Informationen bei der konkreten Anwendung muss der freien Entscheidung des mündigen Bürgers überlassen bleiben.
Die Diskussionen dauern, auch angesichts der Überlegungen zur Verknüpfung mit einer umfassenderen Gesundheitskarte, weiter an.

Die 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. - 26. Oktober 2001 hat zu den datenschutzrechtlichen Anforderungen an den "Arzneimittelpass“ eine eigene Entschließung gefasst **(Anlage 7).**

10.2 Dekubitusfragebogen einer Pflegekasse

Ein Pflegehilfsmittelhersteller wandte sich an den Landesbeauftragten mit der Frage, ob es zulässig sei, dass eine Pflegekasse bei ihm medizinische Daten über einen Versicherten erheben dürfe, der ein Pflegehilfsmittel bestellt habe.

Der Landesbeauftragte wies darauf hin, dass die Pflegekasse berechtigt ist zu überprüfen, ob das angeforderte Pflegehilfsmittel erforderlich ist, wenn sich dieses nicht aus dem Antrag oder aus den der Pflegekasse vorliegenden Unterlagen ergibt.
Doch ist der Lieferant des Pflegehilfsmittels weder gesetzlich verpflichtet noch berechtigt - auch wenn der Versicherte eine entsprechende Einwilligungserklärung abgibt -, diese personenbezogenen und medizinischen Daten der Pflegekasse zu übermitteln. Der Gesetzgeber hat in § 40 Abs. 1 SGB XI einen Verfahrensweg vorgegeben, der weder durch die Pflegekasse noch durch den Versicherten geändert werden kann.

Die Pflegekasse hat die Verwendung des Fragebogens eingestellt und die ohne Rechtsgrundlage erhobenen Daten entsprechend § 84 Abs. 2 SGB X gelöscht.

10.3 Auskunftsbegehren aus berufsständischen Registern

Im Berichtszeitraum häuften sich Fälle, in denen öffentliche Stellen versuchten, Auskünfte aus den Mitgliederverzeichnissen von berufsständi-

schen Vereinigungen zu erlangen. Solche Anfragen gab es auch an die Ärztekammer.

Aus diesem Anlass weist der Landesbeauftragte darauf hin, dass Verzeichnisse von berufsständischen Vereinigungen keine öffentlichen Auskunftsregister darstellen.
Register sind nur dann als öffentlich zu betrachten, wenn Interessierte tatsächlich und rechtlich weitgehend uneingeschränkt auf die dort vorhandenen Daten zugreifen können. Beispiele hierfür sind Telefonverzeichnisse, Adressbücher, Bibliotheken sowie das Handels- und das Vereinsregister. Gerade dies trifft auf die Register der berufsständischen Vereinigungen jedoch nicht zu. Die dort vorliegenden Daten sind zweckgebunden für berufsständische Zwecke erhoben und gespeichert worden.
Das bedeutet, dass für das Auskunftsbegehren eine gesetzliche Übermittlungsbefugnis der registerführenden Stelle und bei der anfragenden Stelle eine Erhebungsbefugnis vorliegen müssen. Der allgemeine Amtshilfegrundsatz reicht dafür nicht aus. Ohne spezielle Rechtsgrundlage dürfen Auskünfte nur mit Einwilligung des Betroffenen erteilt werden.

10.4 Genetische Untersuchungen

Die fortschreitenden Möglichkeiten zu genetischen Untersuchungen berühren in vielfältiger Weise auch den Schutz der Persönlichkeit (Art. 2 Abs. 1 GG). Das mögliche Untersuchungsspektrum umfasst medizinische Zwecke ebenso wie Identitätsklärungen, Forschungszwecke oder Arbeits- und Versicherungsverhältnisse. Bundes- und Landesgesetzgeber sind deshalb aufgefordert, dem Persönlichkeitsschutz, insbesondere dem Informations- und Entscheidungsrecht der Betroffenen, Rechnung zu tragen.

Mit diesem datenschutzrechtlichen Kernanliegen befasst sich die Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24.-26. Oktober 2001 **(Anlage 5)**.

11. Gewerbe, Handwerk und Wirtschaft

11.1 Beitragsfestsetzung durch eine Handwerksinnung

Handwerksinnungen sind nach § 53 HandwO Körperschaften des öffentlichen Rechts. Die ihnen aus ihren umfangreichen Aufgaben erwachsenden Kosten sind gem. § 73 Abs. 1 HandwO bei fehlender Deckung durch Beiträge der Innungsmitglieder aufzubringen. Das Verfahren der Beitragsermittlung hat die Innung in ihrer Satzung genau zu bestimmen. Dazu zählt auch die Angabe einer Beitragsbemessungsgrundlage, z.B. eines bestimmten Prozentsatzes des Gewinnes aus dem Gewerbebetrieb.

Auf der Basis einer solchen Satzung war ein Klempner- und Installateurmeister zur Angabe der Bruttolohnsumme seiner gewerblichen Arbeitnehmer gebeten worden, um die Höhe seines Innungsmitgliedsbeitrages ermitteln zu können. Dies hielt er für nicht datenschutzgerecht und wandte sich entrüstet an den Landesbeauftragten.

Der prüfte die Rechtslage, die sich im Ergebnis als nicht einfach darstellt: Durch Gesetzesänderungen im Dezember 1997 und im März 1998 ergibt sich aus § 73 Abs. 3 HandwO i.V.m. der Neufassung des § 113 Abs. 3 HandwO, dass die Beitragsfestsetzung auf Basis der Bruttolohnsumme seit dem 1. Januar 1998 nicht mehr zulässig ist.
Das (Landes-)Ministerium für Wirtschaft und Arbeit hält diese Rechtslage allerdings für vom Bundesgesetzgeber nicht gewollt, sondern für einen typischen redaktionellen Fehler bei der Verweisung durch die Gesetzesänderungen.

Der Landesbeauftragte hat deshalb den Bundesbeauftragten für den Datenschutz gebeten, beim Bundesministerium für Wirtschaft und Technologie zu klären, wie die jetzt entstandene Rechtslage entsprechend der tatsächlichen Absicht des Bundesgesetzgebers geändert werden kann. Eine Antwort lag bis zum Redaktionsschluss leider noch nicht vor.

11.2 Aufbewahrungsfristen von Gewerbeanzeigen nach § 14 GewO

Erhebt oder verarbeitet eine öffentliche Stelle personenbezogene Daten oder nutzt sie diese, so ist dies nur zulässig, wenn das DSG-LSA oder eine andere Rechtsvorschrift es erlaubt oder anordnet, oder soweit der Betroffene eingewilligt hat. Dabei ist die Erhebung, Verarbeitung oder Nutzung in der Regel an einen konkreten Zweck gebunden.

So dient z.B. die Anzeige eines stehenden Gewerbes (Gewerbeanzeige) gem. § 14 Abs. 1 Satz 3 GewO ausschließlich dem Zweck, der zuständigen Behörde die Überwachung der Gewerbeausübung zu ermöglichen.

Daraus folgt, dass eine Gewerbeanzeige durch die verantwortliche Stelle nur solange aufbewahrt werden darf bzw. muss, wie die Überwachung der Gewerbeausübung währt. Danach ist die Anzeige aufgrund des weggefallenen Erfordernisses zu vernichten, die gespeicherten Daten sind zu löschen.
Der Landesbeauftragte war nun mit der Frage befasst, ob auch noch nach einer Gewerbeabmeldung**,** z.B. wegen Aufgabe des Gewerbebetriebes, die Gewerbeüberwachung andauert und, soweit dies bejaht wird, in welchen zeitlichen Grenzen.

Unter Abwägung aller Gesichtspunkte wird man auch datenschutzrechtlich einbeziehen müssen, dass bei den für die Gewerbeaufsicht zuständigen Behörden auch nach Ende der Gewerbeausübung ein befristet nachwirkender Kontroll- und Belegbedarf besteht. Dies kann ohne inhaltliche

Überdehnung unter dem Zweck "Gewerbeüberwachung" subsumiert werden und gewährleistet zudem den von der höchstrichterlichen Rechtsprechung auch nach Abschluss einer amtlichen Tätigkeit noch geforderten Nachweis eines ordnungsgemäßen Verwaltungshandelns. Die (spätere) erneute Erhebung der erforderlichen personenbezogenen Daten im Bedarfsfall stellt keine wirkliche Alternative dazu dar.

Daraus folgt, dass bei der in § 14 Abs. 11 GewO vorgesehenen Löschungsentscheidung ein begrenzter weiterer Aufbewahrungsbedarf nach § 16 Abs. 2 Nr. 2 DSG-LSA als erforderlich vertretbar erscheint. Dafür sieht § 18 Abs. 1 lit. b) der Aktenordnung aufgrund langjähriger Verwaltungserfahrung einen Zeitraum von bis zu 5 Jahren für Einzelakten vor. Der in § 14 Abs. 1 Satz 4 GewO vorgesehenen Zweckbindung wird in diesem Zeitraum dadurch Rechnung getragen, dass nach der Gewerbeabmeldung bis zu Löschung gem. § 16 Abs. 3 Nr. 1 DSG-LSA eine Sperrung der Gewerbemeldedaten eintritt.

12. Hinweise zum technischen und organisatorischen Datenschutz

12.1 Beauftragter für den Datenschutz nach § 14a DSG-LSA

Mit der Novellierung des DSG-LSA vom 21.08.2001 hat sich der Landesgesetzgeber auch dazu entschlossen, den öffentlichen Stellen beim Einsatz automatisierter Verfahren zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten in § 14a DSG-LSA verbindlich die **schriftliche** Einsetzung eines Beauftragten für den Datenschutz vorzuschreiben. Damit folgt er einem allgemein zu beobachtenden Trend, zur Gewährleistung des Datenschutzes die Selbstkontrolle in der öffentlichen Stelle der Fremdkontrolle durch den Landesbeauftragten vorzuschalten.

Der Beauftragte für den Datenschutz hat die für eine kompetente Aufgabenerfüllung erforderliche Fachkunde und Zuverlässigkeit zu besitzen. Allerdings hat sich der Gesetzgeber nicht dazu entschließen können, in § 14a DSG-LSA auch explizite Regelungen in Bezug auf die Unvereinbarkeit des Amtes des Beauftragten für den Datenschutz mit anderen Funktionen und zu Auswahlkriterien hinsichtlich seiner persönlichen und fachlichen Eignung zu erlassen. Aber gerade hierzu erhielt der Landesbeauftragte im Berichtszeitraum eine Vielzahl von Anfragen.

Es gibt weder im DSG-LSA noch in bereichsspezifischen Vorschriften spezielle Ausschließungsgründe. Eine direkte Anwendbarkeit verwaltungsverfahrensrechtlicher Interessenkollisionsregelungen ist ebenfalls nicht möglich. Es bleibt daher immer eine Einzelfallabwägung. Allerdings ist es nach allgemeinen rechtsstaatlichen Verfahrensgründen geboten, Interessenkonflikte, z.B. durch die nachträgliche Kontrolle eigener datenschutzrelevanter dienstlicher Handlungen, zu vermeiden. Folglich sollte

die Bestellung von Beschäftigten zu Beauftragten für den Datenschutz dann nicht vorgenommen werden, wenn bei diesen Personen von vornherein Interessenkonflikte zu erwarten sind.

Die gesetzlichen Aufgaben des Beauftragten für den Datenschutz sind in § 14a Abs. 4 DSG-LSA aufgezählt. Allerdings sind die öffentlichen Stellen nicht daran gehindert, ihrem Beauftragten für den Datenschutz zur umfassenden Aufgabenerfüllung weitere Aufgaben zu übertragen, die mit dem DSG-LSA und den anknüpfenden datenschutzrechtlichen Fragen im Zusammenhang stehen. Der Landesbeauftragte regt aufgrund seiner in langjähriger Kontrollpraxis gesammelten Erfahrungen an, dem Beauftragten für den Datenschutz insbesondere folgende Aufgaben zu übertragen:

- Beratung der Leitung der öffentlichen Stellen, der Mitarbeiterinnen und Mitarbeiter und des Personalrates
- Kontrolle der Datenverarbeitungsprozesse
- Kontrolle der Einhaltung des Datenschutzes bei der Verarbeitung oder Nutzung personenbezogener Daten bei Auftragnehmern
- Mitarbeit am Erlass von Richtlinien und anderen verwaltungsinternen Regelungen
- Mitarbeit bei der Erstellung datenschutzgerechter Verwaltungsunterlagen (Vordrucke und Merkblätter)
- Mitarbeit bei der Gewährleistung der Rechte Betroffener, Mitbearbeitung von Bürgereingaben
- Beteiligung bei der Konzeption und Auswertung von Protokolldateien, insbesondere unter Beachtung des § 1 Abs. 2 DSG-LSA
- Zusammenarbeit mit der oder dem IT-Sicherheitsbeauftragten
- Vorabunterrichtung des Landesbeauftragten über Planungen des Landes zum Aufbau automatisierter Informationssysteme nach § 22 Abs. 4 Satz 2 DSG-LSA
- Unterrichtung des Landesbeauftragten **vor** der Einrichtung automatisierter Abrufverfahren nach § 7 Abs. 3 DSG-LSA
- Unterrichtung des Landesbeauftragten über erteilte Aufträge zur Verarbeitung personenbezogener Daten durch nicht-öffentliche Stellen nach § 8 Abs. 6 DSG-LSA.

Eine ausführliche Beschreibung der Auswahlkriterien und der Bestellung des Beauftragten für den Datenschutz sowie der vorgenannten Aufgaben befindet sich in der **Anlage 20** und auf der Homepage des Landesbeauftragten unter der im Intranet und im Internet gleichlautenden Adresse: www.datenschutz.sachsen-anhalt.de.

12.2 Vom Dateienregister zum Verfahrensverzeichnis

Mit der Novellierung des DSG-LSA durch Artikel 1 des Gesetzes zur Änderung datenschutzrechtlicher Vorschriften vom 21.08.2001 (GVBl. LSA S. 348) wurde der bisherige § 25 DSG-LSA (Dateienregister) ersatzlos

gestrichen. Darauf hatte der Landesbeauftragte auch in seiner Bekanntmachung vom 31.08.2001 (MBl. LSA S. 842) hingewiesen.
Dennoch gehen weiterhin Meldungen zu automatisierten Dateien von öffentlichen Stellen beim Landesbeauftragten ein.
Allerdings besteht nunmehr gem. § 14 Abs. 3 Satz 1 DSG-LSA die Verpflichtung für öffentliche Stellen zur eigenen Führung eines Verfahrensverzeichnisses für automatisierte Verfahren.
Nach den Übergangsvorschriften des § 32 Abs. 1 DSG-LSA gelten zwar die nach bisherigem Recht erstellten Dateifestlegungen als Verfahrensverzeichnis fort, der Landesbeauftragte empfiehlt jedoch, das Verfahrensverzeichnis auf der Basis der alten Dateifestlegungen schnellstmöglich auf einen neuen Stand zu bringen, da sich gerade bei den technisch-organisatorischen Maßnahmen nach § 6 DSG-LSA wesentliche Änderungen ergeben haben, welche im Verfahrensverzeichnis unter § 14 Abs. 3 Ziffer 9. DSG-LSA Berücksichtigung finden müssen.

Erläuterungen hierzu finden sich in den VV-DSG-LSA, insbesondere der dortigen Anlage 3 (Muster für ein Verfahrensverzeichnis).

Die Beauftragten für den Datenschutz sollten ein besonderes Augenmerk auf die Aktualität und die Vollständigkeit der von ihnen zu führenden Verfahrensverzeichnisse gem. § 14a Abs. 4 Satz 1 DSG-LSA legen.
Bei zukünftigen Kontrollen des Landesbeauftragten kann dieses Verfahrensverzeichnis vorab von der jeweiligen öffentlichen Stelle zur Vorbereitung der Kontrolle abgefordert werden. Liegt es nicht vor, kann dies zu einer Beanstandung durch den Landesbeauftragten führen.

12.3 Gefahren durch einen Computervirus

Über Vorteile, aber auch die Gefahren der E-Mail-Benutzung berichtet der Landesbeauftragte in seinen Tätigkeitsberichten regelmäßig, zuletzt im V. Tätigkeitsbericht (Ziff. 11.3.2). Außerdem warnt er bei Beratungen, Fortbildungsveranstaltungen und Vorträgen vor den mit der Zulassung des E-Mail-Verkehrs einhergehenden vielfältigen Sicherheitsproblemen.
Ein solches Problem sind E-Mail-Computerviren.
Ein Kreiskrankenhaus hat dies bei der automatisierten Verarbeitung der Patientendaten nicht so recht ernst genommen. So erhielt der Landesbeauftragte von einer Firma in Hamburg die Mitteilung, dass das Kreiskrankenhaus offenbar von dem Internetwurm SIRCAM infiziert sei. SIRCAM versendet sich selbst an alle Einträge im Outlook-Adressbuch und an alle E-Mail-Adressen, die im Web-Browser-Cache (Temporary Internet Files) gefunden werden. Besonders unangenehm an SIRCAM ist, dass das Virus auf einen Wirt, ein Microsoft Word-Dokument aus dem Verzeichnis "Eigene Dateien", angewiesen ist, von dem es bei seiner Vermehrung Kopien mitnimmt.
So kam es, dass die genannte Firma in Hamburg und viele andere Empfänger in der ganzen Welt neben dem Virus auch eine interessante Krankengeschichte übermittelt bekamen.

Der Landesbeauftragte hatte bei seiner Kontrolle vor Ort aufgrund erheblicher Lücken beim Computervirenschutz einen Verstoß gegen § 6 Abs. 2 Ziffn. 1 und 2 DSG-LSA (Vertraulichkeit und Integrität) zu konstatieren. Das Krankenhaus hatte zwar den Server seines Datennetzes durch veraltete Virenschutzsoftware zu sichern versucht, die 20 PC mit Internet-Anschluss und Mail-Client aber völlig schutzlos gelassen. Die ankommende Virus-Mail konnte sich dadurch verbreiten, ohne von der veralteten Antivirensoftware erkannt zu werden. Ein weiterer Fehler lag darin, die Office-Dokumente mit den Patientendaten nicht in einem Serververzeichnis zu speichern, wo sie u.a. von der regelmäßigen Datensicherung erfasst worden wären.
Schließlich wurde auch noch festgestellt, dass die Office-Makrosicherheit, z.B. in Outlook 2000 unter "Extras - Makro - Sicherheit", die zumindest ein gewisses Schutzniveau vor Makroviren bietet, nur auf niedrigem Niveau eingestellt war.

Der Landesbeauftragte hat das Krankenhaus aufgefordert,
- den Servervirenschutz in kurzen Intervallen (nicht länger als eine Woche) zu aktualisieren,
- auf den Workstations mit Internetanschluß für ebenso aktuellen Virenschutz zu sorgen,
- alle Sicherheitsmechanismen des Betriebssystems und der Office-Software auszuschöpfen,
- den Speicherort für patienten- und anderen personenbezogenen Daten auf den Server zu verlegen und die lokale Speicherung generell auszuschließen und
- vor allem die Mitarbeiter bezüglich der Computervirenproblematik zu sensibilisieren und zu schulen.

Der oberflächliche Umgang mit besonderen Daten kann eine Strafverfolgung wegen Verletzung von Privatgeheimnissen gem. § 203 Abs. 1 StGB und hinsichtlich der Versendung eines Virus wegen Computersabotage gem. § 303a StGB nach sich ziehen.

12.4 Unsicherheiten in Bürosoftware

In seinem IV. Tätigkeitsbericht (Ziff. 13.5) hatte der Landesbeauftragte davon berichtet, dass durch die Benutzung simpler Menüfunktionen, wie "Datei, Speichern unter", Office-Software Dateien, die wegen ihrer besonderen Sensibilität nur im Hochsicherheitsbereich des Servers gespeichert werden sollten, plötzlich auf einem angeschlossenen, weniger geschützten Client-PC zu finden waren. Er hatte deshalb empfohlen, in die Sicherheitsbetrachtungen für das Netzwerk auch die Client-PC einzuschließen. Bei dem beschriebenen Datentransfer aus einer besonders sicheren Domäne heraus spielt der Mensch als Software-User eine Schlüsselrolle. Die entscheidende Aktivität geht von ihm aus. Ein Verbot, solche sensiblen

Daten lokal zu speichern und dies auch regelmäßig zu kontrollieren, reicht oft nicht aus.
Das Problem wird u.a. durch eine jedem rechnerabsturzgeplagten Nutzer lieb gewordene Funktion z.B. von Textverarbeitungsprogrammen hervorgerufen. Es ist die Funktion der automatischen Speicherung während der Bearbeitung. Mit dem Ziel, nach Rechnerabsturz - z.B. wegen Stromausfalls - die Änderungen der zuletzt bearbeiteten Datei restaurieren zu können, legen verschiedene Programme, wie z.B. Microsoft Word, in einstellbarem Zyklus **unbemerkt** Sicherheitskopien im Verzeichnis für die temporären Dateien ab. Dieses Verzeichnis befindet sich, wenn die Einstellung nicht geändert wird, auf der lokalen Festplatte.

Dies gilt aber auch für Anlagen von E-Mails. Wird z.B. ein Word-Dokument als Anlage einer E-Mail geöffnet, ist in der Regel schon die erste unbemerkte Speicherung auf der lokalen Festplatte erfolgt.
Obgleich alle die genannten Hilfsdateien nach Beendigung der Bearbeitung automatisch zumindest logisch, nicht jedoch physikalisch gelöscht werden, bedarf es nur eines kleinen Aufwandes, um die Informationen wieder lesbar zu machen, sofern der Angreifer Zugriff auf den PC erhält.

Sicherheitsmaßnahmen sollten also das gesamte Computernetzwerk inklusive der Client-PC umfassen und nicht an der Tür des Serverraumes enden.
An das mögliche Vorhandensein o.g. Dateien sollte man sich im übrigen auch erinnern, bevor ein PC zu Wartungs- oder Reparaturzwecken einem externen Dienstleister überantwortet wird. Hier können umfangreiche Vorarbeiten zur Datenlöschung erforderlich sein, bevor der PC das Haus verlässt.

12.5 Sichere Kommunikation im Internet

Der Landesbeauftragte ist nach wie vor darüber erstaunt, mit welcher Nonchalance der Einsatz des Internets durch öffentliche Stellen gefördert und von diesen betrieben wird. Dies betrifft sowohl das Einstellen personenbezogener Informationen in dem jeweiligen Internetangebot wie auch die Nutzung spezieller Kommunikationswege. Die festzustellende "Leichtigkeit" im Umgang mit diesem Medium mag im privaten Lebensbereich akzeptabel sein. Für die Datenverarbeitung öffentlicher Stellen kommt aufgrund der unveränderten tatsächlichen und rechtlichen Unsicherheit ein Einsatz des Internets nur unter besonderen und engen Voraussetzungen in Betracht.
Erklärbar ist dieser "lockere" Umgang nur damit, dass im Wege einer unzutreffenden Parallelwertung eine Internet"seite" nach wie vor mit der Seite eines Druckwerkes gedanklich bzw. "gefühlsmäßig" gleichgesetzt wird. In der Praxis oft ein gefährlicher und folgenschwerer Irrtum.

Eine Firma informierte den Landesbeauftragten über einen neuen interessanten Sicherheitsstandard, der für den Aufbau einer sicheren Kommuni-

kationsplattform entwickelt wurde. Es handelt sich dabei um einen Meta-Standard, der verschiedene technische und organisatorische Sicherheitsstandards zusammenfasst und Mindestanforderungen an eine vertrauliche Kommunikation im Internet beschreibt.
Grundaussage ist, dass Beratungseinrichtungen, gleich ob öffentliche oder private, die über das Internet mit Klienten, Bürgern und Kunden kommunizieren wollen, die Frage der Sicherheit nicht dem jeweiligen Nutzer überlassen, sondern von vornherein sichere Kommunikationswege zur Verfügung stellen sollten.

Unter anderem hat die Telefonseelsorge Deutschland aufgrund der bekannten Sicherheitsrisiken bei der E-Mail-Beratung eine Alternative gesucht und eine webbasierte Beratung nach dem neuen Sicherheitsstandard realisiert. Auf das Versenden von E-Mails wird jetzt völlig verzichtet. Der Ratsuchende meldet sich bei der Telefonseelsorge mit einem beliebigen Nutzernamen und einem Kennwort an. Danach kann er sein Problem schildern und bekommt nach ca. 48 Stunden "Antwort" in der Form, dass er sich wiederum anmeldet und die Antwort des Beraters abrufen kann. Der gesamte Beratungskontakt verbleibt auf dem Server der Telefonseelsorge, der u.a. durch eine Firewall und eine Viruswall gegen Zugriffe und Angriffe von außen gesichert ist.
Zum einen wird auf diese Weise die Anonymität gewahrt, da der Nutzer keine E-Mail-Adresse angeben muss, die personenbeziehbar ist und zum anderen wird die Übertragung der Daten im Internet automatisch durch eine SSL-Verschlüsselung gesichert.
Durch das SSL-Zertifikat, das vom Trust-Center der Deutschen Telekom AG (TeleSec) ausgestellt wurde, kann der Nutzer außerdem regelmäßig davon ausgehen, dass es sich bei dem Anbieter tatsächlich um die Telefonseelsorge handelt.
Die Deutsche Telekom AG als privates Unternehmen unterliegt zugleich der Datenschutzkontrolle des Bundesbeauftragten für den Datenschutz. Damit ist sichergestellt, dass eine Kontrolle der einzuhaltenden datenschutzrechtlichen Bestimmungen erfolgt. Bei einem Zertifikatsanbieter außerhalb des Geltungsbereiches des Grundgesetzes wäre dies nicht so einfach.

Die beschriebene Lösung ist jedoch nicht nur für Einrichtungen zu empfehlen, die anonyme Beratung gewährleisten müssen oder wollen, sondern generell für öffentliche Stellen, die den Bürgerinnen und Bürgern eine sichere Kommunikationsmöglichkeit ohne vorherige Installation einer Verschlüsselungssoftware und aufwendige Schlüsselverwaltung zur Verfügung stellen wollen.
Allerdings ist in diesem Fall nur die Identität des Empfängers, nicht jedoch die des Absenders als sicher anzusehen. Sicherheit über den Absender erhielte man bei einer E-Mail nur über das aufwendige Verfahren mit einer digitalen Signatur.

Da der Landesbeauftragte selbst aufgrund der bekannten Sicherheitsprobleme seine E-Mail-Adresse nur für den dienstlichen Gebrauch zur Verfügung stellt, um zu verhindern, dass Bürger und öffentliche Stellen aus Unwissenheit sensible Informationen per E-Mail offen und durch Dritte verfälschbar verschicken, prüft er zur Zeit, ob eine solche webbasierte Lösung auch eine Alternative für die datenschutzrechtliche Beratung per Internet darstellen kann.

13. Hochschulen

13.1 Aushang von Prüfungsdaten

Der Landesbeauftragte erhielt einen Hinweis auf den Aushang von Prüfungsdaten in einer Hochschule des Landes. In einem öffentlich zugänglichen Schaukasten einer Hochschuleinrichtung waren unter dem Fettdruck "Ergebnisse der Semesterabschlussklausur ..... 2. Semester (SS 2002)" u.a. unter den Rubriken "Gut", "Befriedigend" und "Bestanden" die Namen, Vornamen und zum Teil die Semesterangabe der Studenten ausgehängt.

Die Benotung einer akademischen Prüfung sowie die Tatsache des Bestehens bzw. Nichtbestehens einer akademischen Prüfung stellen im Zusammenhang mit dem Namen des betroffenen Prüflings personenbezogene Daten dar. Das Bereithalten zur Einsicht in einem öffentlich zugänglichen Schaukasten ist ein Übermitteln dieser Daten an Dritte. Für diese Verarbeitung personenbezogener Daten hätte die Hochschule eine Rechtsgrundlage bzw. die Einwilligung des jeweiligen Betroffenen benötigt (§ 4 Abs. 1 DSG-LSA). Andernfalls ist die Übermittlung ein unzulässiger Eingriff in das Grundrecht auf informationelle Selbstbestimmung des jeweils betroffenen Prüflings.

Eine Rechtsgrundlage konnte die Hochschule nicht benennen. Auch der lediglich mittelbare Hinweis, die Studenten hätten ihr Einverständnis erklärt, vermochte den Anforderungen an eine informierte, grundsätzlich schriftliche Einwilligung im Sinne des § 4 Abs. 2 DSG-LSA nicht zu genügen.

Der Direktor der betroffenen Hochschuleinrichtung teilte mit, dass er diese lange, frühere Übung zur Veröffentlichung von Ergebnissen akademischer Prüfungen bereits seit längerem beendet habe. Aufgrund des Einzelfalles habe er umgehend erneut ein Verbot ausgesprochen.
Infolge der Gesamtumstände, insbesondere der dienstlichen Anordnungen zur Vermeidung entsprechender Rechtsverletzungen, konnte der Landesbeauftragte von einer an sich gebotenen Beanstandung gem. § 24 Abs. 3 DSG-LSA absehen.

Im Hinblick auf ehemalige Verfahrensweisen hat der Landesbeauftragte angeregt, durch entsprechende Anweisungen den Persönlichkeitsschutz im Prüfungswesen für die gesamte Hochschule sicherzustellen.

13.2 Amtsärztliches Zeugnis bei Prüfungskandidaten

Bereits im II. Tätigkeitsbericht (Ziff. 14.1) hatte sich der Landesbeauftragte mit der Problematik der Angabe medizinischer Daten auf dem Attest, mit dem der Kandidat seine Prüfungsunfähigkeit nachweisen soll, auseinandergesetzt. Daraufhin hatte die Landesregierung festgestellt, dass ein Prüfungsausschuss von der Diagnose in diesem Zusammenhang keine Kenntnis haben muss.
Trotz Kenntnis dieser Sachlage wurde von einem Prüfungsamt ohne nähere Begründung weiterhin die Angabe der Krankheitsbezeichnung und darüber hinaus die Angabe des medizinischen Befundes und die Angabe der Krankheitssymptome gefordert. Zusätzlich wurde - entgegen der Approbationsordnung - ohne Angabe von Gründen ausnahmslos die Beibringung eines amtsärztlichen Attestes verlangt. Damit nicht genug, forderte man von den Prüflingen dann auch noch die Entbindung von der ärztlichen Schweigepflicht, ohne die nach § 4 Abs. 2 Satz 1 DSG-LSA erforderliche Belehrung über die Freiwilligkeit dieser Einwilligung und die Folgen bei deren Verweigerung vorzunehmen.

Der Landesbeauftragte wies das Prüfungsamt darauf hin, dass Gesundheitsdaten nicht nur nach internationalen Schutzvorschriften (Art. 8 Abs. 1 Richtlinie 95/46/EG (Datenschutz) und Art. 8 EMRK), sondern auch nach deutschem Recht (§ 3 Abs. 9 BDSG, § 67 Abs. 12 SGB X) besonderem Schutz unterliegen. Das Amt aber kannte diese Vorschriften nicht und leugnete schlicht deren Existenz. Seine Praxis ändern wollte es auch nicht.

Das Fachministerium hatte dann die dankbare Aufgabe, die Behörde zu belehren und zur Beachtung der gesetzlichen Vorschriften anzuhalten.

14. Kommunalverwaltung

14.1 Datenschutz im Standesamt

Ein Landkreis wandte sich an den Landesbeauftragten mit folgendem Sachverhalt:
Eine Antragstellerin hatte erst nach dem Tod ihrer Mutter von einer Verwandten erfahren, wer ihr leiblicher Vater war. Seitdem versuchte sie, dessen Aufenthaltsort ausfindig zu machen. Erschwert wurde die Suche dadurch, dass ihr weder der vollständige Name, das Geburtsdatum, der Geburtsort noch dessen damaliger Wohnort bekannt war. Alle Angaben beruhten auf Auskünften Dritter vom Hörensagen. Einziger Anhaltspunkt

war der Hinweis, dass der Betroffene 1945 (damals ca. 20 Jahre alt) bei der Deutschen Wehrmacht gewesen war und aus der Stadt "X" oder deren Umgebung stammen sollte.
Die Antragstellerin wandte sich mit diesen Angaben an die Deutsche Dienststelle für die Benachrichtigung der nächsten Angehörigen von Gefallenen der ehemaligen Wehrmacht in Berlin und das Bundesarchiv in Aachen. Sie erhielt aber jeweils die Auskunft, dass ohne Geburtsdatum die Suche nicht möglich sei.
Daraufhin wandte sich die Antragstellerin an das Standesamt der Stadt "X". Die Auskunft verlief ebenfalls negativ. Zwischenzeitlich hatte die Antragstellerin verschiedene Standesämter der Umgebung angeschrieben und um Auskunft gebeten. Ein Standesamt gab den Hinweis, dass unter dem möglichen Namen in dem angenommenen Zeitraum der Geburt (1920 bis 1926) sechs Eintragungen vorlägen, eine detaillierte Auskunft aus datenschutzrechtlichen Gründen aber nicht möglich sei. Die Antragstellerin wandte sich nun an das Amtsgericht. Das Amtsgericht wies den Standesbeamten mit Beschluss an, der Antragstellerin über das Geburtsdatum alle Auskünfte zu den betroffenen Personen zu erteilen.

Der zuständige Landkreis legte gegen diesen Beschluss zunächst sofortige Beschwerde ein und bat für deren Begründung den Landesbeauftragten um gutachtliche Stellungnahme. In dieser wies der Landesbeauftragte auf drei Punkte hin:

1. Nach § 61 PStG besteht (nur) für Personen ein Auskunftsanspruch, auf die sich der Eintrag bezieht, sowie deren Ehegatten, Vorfahren und Abkömmlinge. Für Ausforschungsanträge "ins Blaue" enthält das Personenstandsgesetz keine rechtliche Grundlage.

2. Die Antragstellerin hatte nicht vorgetragen und belegt, dass sie alle ihr zur Verfügung stehenden Nachforschungsmöglichkeiten ausgeschöpft hatte. So wäre zum einen eine Anfrage an das Militärarchiv in Freiburg (Breisgau), das Auskünfte zu Einheiten der Deutschen Wehrmacht und deren Bediensteten geben kann, möglich gewesen. Zum anderen hatte sie sich weder an die zuständigen Meldebehörden gewandt noch bei dem seinerzeit nach ihrer Geburt zuständigen Jugendamt Nachforschungen angestellt.

3. Die vom Amtsgericht angeordnete Auskunftserteilung stellt einen Eingriff in das grundrechtlich geschützte Recht auf informationelle Selbstbestimmung der Betroffenen dar, der nach der ständigen Rechtsprechung des Bundesverfassungsgerichts nur auf gesetzlicher Grundlage erfolgen darf. Diese lag nicht vor. Zudem wäre die Rechtsprechung des Bundesverfassungsgerichts (zuletzt BVerfGE 96, 56) zu berücksichtigen gewesen, wonach die Antragstellerin schon keinen absoluten Anspruch auf Bekanntgabe des Vaters durch ihre Mutter gehabt hätte.

Insgesamt erschien daher der mit der Auskunft einhergehende Grundrechtseingriff in die Rechte von einer wenigstens zweistelligen Zahl von Männern mit Allerweltsnamen aus der Umgebung der Stadt "X" (20, 50 oder 100 Kilometer Umkreis?) unverhältnismäßig.

Das für die Beschwerde zuständige Landgericht hat den Beschluss des Amtsgerichts aufgehoben und den Auskunftsantrag zurückgewiesen. Die Urteilsbegründung entspricht weitgehend den Ausführungen des Landesbeauftragten.

14.2 Datenverarbeitung im Rahmen der Flutkatastrophenhilfe

Den Opfern der Flutkatastrophe in Sachsen-Anhalt steht ein umfängliches und vielfältiges Programm an Hilfen zur Verfügung. Die betroffenen kommunalen Gebietskörperschaften tragen aus unterschiedlichen Gründen die Hauptlast der administrativ-organisatorischen Tätigkeit (Koordination der sachgerechten Verteilung).

Zur Sicherung der Einzelfallgerechtigkeit und zur Beachtung haushaltsrechtlicher Grundregelungen wurde eine längerfristigere Speicherung und Übermittlung von personenbezogenen Informationen über Hilfsleistungen erforderlich.
Hierzu hat der Landesbeauftragte auf folgendes hingewiesen:

1. Bei der Vermittlung von nicht-öffentlichen Fluthilfeleistungen (z.B. der Verteilung der von den Medien gesammelten Spendengelder) nehmen die staatlichen Dienststellen keine unmittelbar hoheitlichen Aufgaben wahr. Sie handeln aber als öffentliche Stellen im Rahmen ihrer Zuständigkeiten für die Angelegenheiten der örtlichen Gemeinschaft. Bereichsspezifische Regelungen, die Inhalt und Umfang der dabei erforderlichen Informationen, das Verfahren bzw. den Umgang mit den personenbezogenen Informationen vorgeben, gibt es nicht.
   Mangels bereichsspezifischer Regelungen gelten daher allgemeine datenschutzrechtliche Regelungen. Danach war zu empfehlen, die Datenerhebungen, die Speicherung in Leistungsauflistungen und insbesondere die Datenübermittlungen an Dritte (z.B. Versicherungen und gemeinnützige Organisationen), strikt von einer Einwilligung der Antragsteller bzw. der Betroffenen abhängig zu machen (§ 4 DSG-LSA). Dabei ist selbstverständlich zu berücksichtigen, dass die Einwilligung den besonderen Umständen angemessen ist.
   Auch bei Vorliegen der Einwilligung des jeweils Betroffenen ist die öffentliche Stelle bezüglich des Umfangs der Erhebung und Verarbeitung von Informationen an den allgemeinen verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit gebunden. So sind Maßnahmen zur Sicherheit der Daten zu beachten (§ 6 DSG-LSA). Zu denken ist auch an die Löschung nicht mehr erforderlicher Daten (§ 16 DSG-LSA).

2. Werden bei den Fluthilfeleistungen (auch) staatliche Zuschüsse (Haushaltsmittel von Bund und Ländern) ausgezahlt, gelten zusätzlich die besonderen haushaltsrechtlichen Regelungen zum Umgang mit personenbezogenen Daten beim Empfang staatlicher Leistungen.

14.3 Daten von Stadtratsmitgliedern und Schiedsleuten auf der Homepage einer Stadt

Im Zuge der Prüfung einer kreisangehörigen Stadt stellte der Landesbeauftragte fest, dass alle Mitglieder des Stadtrats namentlich auf der Internetseite der Stadt aufgelistet waren. Diese Auflistung war zudem im Textformat erfolgt, was bedeutet, dass sie über Suchmaschinen auswertbar war. Mit Hilfe einer Internet-Suchmaschine sowie des Namens einzelner Mandatsträger konnte z.B. deren berufliche vita zum Teil nachvollzogen werden.
Diese Feststellung erstaunte um so mehr, weil hinsichtlich der Bediensteten - datenschutzrechtlich insoweit vorbildlich - auf eine Benennung verzichtet worden war und stattdessen detailliert die Aufgabenbereiche der Kernverwaltung unter Angabe der telekommunikationstechnischen Erreichbarkeit aus dem Internetangebot ersichtlich waren.
Wie die Mandatsträger wurden auch die Schiedsleute namentlich benannt, zudem mit Privatanschrift. Wie bei der Kernverwaltung hätte auch hier die Beschreibung von Zuständigkeitsbereich und Erreichbarkeit als Serviceangebot im Internet für den gewünschten einfachen Zugang zu den Schiedsleuten ausgereicht.

Das Einstellen von personenbezogenen oder personenbeziehbaren Daten in das Internet führt zu einer Datenübermittlung an Dritte weltweit. So ermöglicht es die vorgefundene Verfahrensweise - und hierauf weist der Landesbeauftragte immer wieder hin - u.a. Vertriebsunternehmen auf der ganzen Welt mit vergleichsweise geringem Aufwand, Adresssammlungen zu erstellen und spezifisch ausgewertet zu nutzen.

Eine rechtliche Grundlage für eine solche Veröffentlichung lag nicht vor. Der Internetauftritt hätte also allenfalls auf Einwilligungserklärungen gem. § 4 Abs. 2 DSG-LSA gegründet werden können; die gab es nicht.
Im Zusammenhang mit Mandatsträgern erscheint es auch vertretbar, einen einstimmigen Beschluss **aller** Stadtratsmitglieder, nachdem sie über Umstand und Folgen der weltweiten Verfügbarkeit von Internetinformationen aufgeklärt wurden, als Einwilligung gelten zu lassen. Solch ein Beschluss fehlte ebenfalls.

Selbst wenn die Betroffenen eine adäquate Einwilligung erklären sollten, ist damit die öffentliche Stelle nicht jeglicher Pflicht enthoben, unter den dann gegebenen Alternativen der Veröffentlichung die datenschutzfreundlichste zu wählen (§ 1 Abs. 2 DSG-LSA).

Da es sich bei einer kommunalen Homepage, zumindest hinsichtlich des kritisierten Teils, um ein Angebot zur Information des örtlichen Publikums und über örtliche Belange handelt (örtlicher Wirkungskreis!), ist die Auffindbarkeit dort eingestellter personenbezogener Daten auf eine unmittelbare Einsichtnahmemöglichkeit auf der Homepage zu begrenzen. Dort wäre das Auflisten der Daten auf einer Seite dann datenschutzgerecht, wenn diese Seite in einem Bilddateiformat eingestellt würde. Dann sind die Namen mit Hilfe von Suchmaschinen nicht auswertbar.
Die Möglichkeiten der Einwohner, durch das Medium Internet an Information über ihre Stadt zu gelangen, wird dadurch nicht eingeschränkt.

14.4 Zwangsvollstreckung gegen die falsche Person

Bei jedem Verwaltungshandeln, insbesondere bei der Erhebung und Verarbeitung personenbezogener Daten, haben öffentliche Stellen größtmögliche Sorgfalt walten zu lassen. Das gilt zum einen, um die Betroffenen nicht unzulässig in ihren Persönlichkeitsrechten zu beeinträchtigen, aber auch, um nicht berechtigte Schadenersatzansprüche (§ 18 DSG-LSA) auszulösen. Dies alles ignorierend, brachte eine Stadtverwaltung erst einen unbeteiligten Bürger und schließlich sich selbst in große Schwierigkeiten.

Ein aufgebrachter Vater hatte sich mit folgendem abstrusen Sachverhalt an den Landesbeauftragten gewandt:
Er hatte Post von dieser Stadtverwaltung erhalten. Inhalt des Umschlages war zwar ein an seinen volljährigen Sohn mit Name und Vorname gerichtetes Schreiben, adressiert aber an eine völlig **fremde** Adresse. Dieses Schreiben hatte es in sich! Es handelte sich um nicht weniger als die Ankündigung einer Zwangsvollstreckung. Gepfändet werden sollte in das bewegliche Vermögen, wenn nicht innerhalb einer Woche eine Forderung von über 1.500 DM befriedigt würde. Die insgesamt 25 Einzelforderungen bestanden fast ausschließlich aus Verwarngeldforderungen im Zusammenhang mit der Teilnahme am Straßenverkehr.

Der Landesbeauftragte musste in der betreffenden Stadtverwaltung neben einer wirren Führung der amtlichen Unterlagen vor allem erhebliche Mängel im Verwaltungshandeln feststellen. So stellte sich folgendes heraus:
Der zentrale Ermittlungsdienst der Stadt erhielt von der Stadtkasse einen Antrag auf Aufenthaltsermittlung des (Verwarngeld-)Schuldners. Die zunächst geführten Ermittlungen vor Ort, nämlich dort, wo dieser nach den vorliegenden Unterlagen und einer aktuellen Melderegisterauskunft tatsächlich wohnen sollte, ergaben keinen Hinweis darauf, dass er dort wirklich seinen Wohnsitz hatte.
Daraufhin kam der Ermittlungsdienst auf die Idee, über die erweiterte Melderegisterauskunft die Eltern des Schuldners zu ermitteln. Er bemerkte dabei nicht, dass es **zwei Bürger gleichen Namens** wie den Schuldner

gibt, die jedoch unterschiedliche Geburtsdaten hatten. So wurde erstmals der Verkehrsrowdy mit dem Petenten verwechselt und mit dessen Eltern in Zusammenhang gebracht.
Um festzustellen, ob man den Schuldner unter der Adresse seiner Eltern postalisch erreichen könne, rief der Ermittlungsdienst kurzerhand dort an. Ein Familienmitglied versicherte ehrlich, dass eine entsprechende Person mit dem Namen des Schuldners dort wohne und selbstredend ein an die Eltern adressiertes Schreiben an ihn weitergegeben werden könne. Natürlich wurde bei dem Gespräch das Geburtsdatum nicht verglichen. So nahm das Unheil schließlich seinen Lauf.

Der um Hilfe angerufene Landesbeauftragte konnte das Durcheinander der Verwaltung nur aufgrund des guten Gedächtnisses der Mitarbeiterin des Ermittlungsdienstes entwirren, denn die einzelnen Ermittlungsschritte wurden dort nicht dokumentiert. Lediglich die Tatsache, dass der Schuldner über die angegebene (falsche) Adresse seiner Eltern postalisch erreichbar sei, wurde der Stadtkasse mitgeteilt.
Von einer rechtlich vorgegebenen und nachvollziehbaren Dokumentation des Verwaltungshandelns konnte also keine Rede sein.

Der Landesbeauftragte sorgte in der Stadtkasse dafür, dass die den vermeintlichen "Schuldner" betreffenden personenbezogenen Daten des Petenten und seiner Eltern als falsch gekennzeichnet und nach § 16 Abs. 3 DSG-LSA gesperrt wurden, da eine spurlose Entfernung aus den Akten (Datenlöschung) nicht in Frage kam. Auch eine Entschuldigung gegenüber dem Petenten wurde angeregt.
Dem Ermittlungsdienst wurde aufgegeben, zukünftig ordentlicher zu arbeiten und sein Verwaltungshandeln rechtskonform zu dokumentieren.

14.5 Übertragung von Ratssitzungen und anderen Veranstaltungen in das Internet

Aufgrund der Anfrage einer Stadt hatte der Landesbeauftragte zu prüfen, inwieweit es zulässig ist, die Sitzungen des Stadtrates, Trauungen von Brautleuten und andere Veranstaltungen der Stadt in das Internet zu übertragen.

Soweit über die Kameraeinstellung (insbesondere Bildausschnitt, -schärfe) ein Personenbezug besteht oder herstellbar wäre, sind die Erhebung und Verarbeitung - dazu zählt auch die Übermittlung der Bilddaten in das Internet - personenbezogener Daten sowie deren Nutzung nur zulässig, wenn das DSG-LSA oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene informiert eingewilligt hat.
Nach den Vorschriften der Gemeindeordnung des Landes finden zwar die Sitzungen des Gemeinderates öffentlich statt (Grundsatz der Transparenz der Kommunalpolitik), damit die Entscheidungsfindung für den Bürger erkennbar und nachvollziehbar wird. Dennoch enthält die Gemeindeordnung

keine spezielle Rechtsgrundlage für die Übermittlung personenbezogener Daten über das Internet an einen unbestimmten Personenkreis in aller Welt.
Deshalb beurteilt sich eine personenbezogene Datenübermittlung über das Internet ausschließlich nach den Voraussetzungen des § 13 i.V.m. § 12 DSG-LSA, da nicht nur die meisten Daten über Knoten in den USA gesendet werden, sondern die Daten im Internet auch aus der ganzen Welt abgefragt und beliebig dupliziert werden können. Folglich ist auch eine spätere Löschung der einmal per Internet übermittelten Daten tatsächlich unmöglich.

Die in § 13 DSG-LSA genannten Voraussetzungen für eine Übermittlung solcher personenbezogener Daten über das Internet sind nicht gegeben. Auch steht eine globale Verfügbarkeit im krassen Gegensatz zu der lokalen Begrenzung des Aufgaben- und Wirkungskreises der Kommunen und ihrer Mandatsträger.
Weder ist es Aufgabe der Kommunen, den Internetnutzern auf der ganzen Welt frei Haus Informationen über die Mitglieder ihrer Gremien, Mitarbeiter und Besucher zu liefern, noch kann den Internetnutzern außerhalb des lokalen Raumes und ohne Beziehung zur Kommune ein generelles berechtigtes Interesse an solchen Informationen zuerkannt werden. Das gleiche gilt auch für die übrigen Zwecke.

14.6 Fehlerhafte Satzung zur Erhebung einer Kurtaxe

Von einem ortsansässigen Hotelunternehmer einer Stadt, der sich auf Gästebeschwerden berief, wurde der Landesbeauftragte darüber informiert, dass die Satzung zur Erhebung einer Kurtaxe der Stadt eine Regelung enthielt, nach der die bei der Erhebung der Kurtaxe erhobenen personenbezogenen Daten auch bei der Verwaltung anderer Kommunalabgaben verwertet werden dürfen.
Als Rechtsgrundlage für diese mögliche Zweckänderung berief sich die Stadt in der Satzung auf § 13 Abs. 1 Ziff. 1c des KAG-LSA i.V.m. § 30 AO. Die Stadt hatte dabei aber übersehen, dass sich diese Rechtsvorschrift nur auf kommunale Steuern bezieht.
Da es sich bei der Kurtaxe aber nicht um eine Steuer, sondern nur um eine beitragsähnliche Abgabe handelt, wurde die Stadt vom Landesbeauftragten aufgefordert, diese fehlerhafte Vorschrift aus der genannten Abgabensatzung zu entfernen. Dieser Aufforderung ist die Stadt - wenn auch mit erheblicher Zeitverzögerung - nachgekommen.
Da die Stadt versicherte, dass die bisher erhobenen Daten trotz bestehender Satzungsermächtigung nicht anderweitig verwertet wurden, bestand für den Landesbeauftragten kein Anlass für ein weitergehendes Tätigwerden.

14.7 Aufgabenübertragung bei Abwasserzweckverbänden

Ein aufmerksamer Bürger informierte den Landesbeauftragten darüber, dass der für seine Gemeinde zuständige Abwasserzweckverband für die geplante künftige Erhebung von Kanalbenutzungsgebühren für befestigte Flächen von Grundstücken, von denen Niederschlagswasser in die Kanalisation gelangt, eine private Gesellschaft mit der Erfassung dieser Flächen beauftragt hatte. Der Bürger wurde von dieser privaten Gesellschaft mit einem Erfassungsbogen aufgefordert, entsprechende Angaben zu den Verhältnissen auf seinem Grundstück zu machen. An der rechtlichen Zulässigkeit dieser Erfassungsmaßnahme hatte der Bürger erhebliche Zweifel.

Wie vom Landesbeauftragten festgestellt wurde, war die Eingabe berechtigt, denn der Abwasserzweckverband hatte die Grundstücksdaten durch die private Gesellschaft ohne eine entsprechende Rechtsgrundlage erheben wollen.
Nach dem KAG-LSA ist der Abwasserzweckverband zwar berechtigt, selbst oder durch Dritte Berechnungsgrundlagen zu ermitteln. Soweit hierfür aber Dritte beauftragt werden - wie im vorliegenden Fall geschehen -, hat der Abwasserzweckverband diesen Vorgang gem. § 10 Abs. 1 KAG-LSA in die entsprechende Abwasserabgabensatzung mit aufzunehmen und zu beschreiben, damit die Betroffenen informiert sind.
Da die Abwasserabgabensatzung des Abwasserzweckverbandes diese erforderliche Regelung nicht enthielt, wurde der Abwasserzweckverband zur Beseitigung dieses Rechtsmangels aufgefordert. Die Abwasserabgabensatzung wurde von dem Verband entsprechend ergänzt.

15. Landtag

Veröffentlichung auf der Internetseite des Landtags

Der Landesbeauftragte hatte sich in den früheren Tätigkeitsberichten (z.B. III. Tätigkeitsbericht, Ziff. 12.2, und IV. Tätigkeitsbericht, Ziff. 12,2, 13.3*)* schon mehrfach mit Problemen des Datenschutzes im Zusammenhang mit der Nutzung des Internets durch öffentliche Stellen auseinandergesetzt. Anfang 2003 tauchte das Problem erneut auf, diesmal bei der Landtagsverwaltung.

Ein Beschwerdeführer hatte festgestellt, dass er namentlich auf einer Seite des Internetangebots des Landtags genannt wurde.
Dabei handelte es sich um eine von der Landtagsverwaltung eingestellte Antwort auf eine Kleine Anfrage an die Landesregierung zum Verein "Miteinander e.V.". Die Antwort des Ministeriums für Gesundheit und Soziales enthielt in der Anlage die Kopie der Teilnehmerliste zur Gründungsversammlung dieses Vereins. Aus dieser Liste waren die Gründungsmitglieder nicht nur namentlich, sondern auch mit den Privatadressen und der jeweiligen eigenhändigen Unterschrift zu ersehen.

Die Landtagsverwaltung sah die datenschutzrechtlichen Bedenken hinsichtlich der sensiblen personenbezogenen Daten in der Anlage und fragte bei der Landesregierung zurück. Diese hielt die Einstellung ins Internet aber für unbedenklich.

Der Landesbeauftragte gab dem betroffenen Bürger Recht. Die Landesregierung hat bei Antworten nach Art. 53 LVerf auch die Schutzvorschriften im dortigen Absatz 4 zu berücksichtigen. Die detaillierten personenbezogenen Angaben zu den Vereinsmitgliedern in der Anlage zur Antwort auf die Kleine Anfrage durften nicht ohne Rechtsgrundlage ins weltweit zugängliche Internet eingestellt werden. Unstreitig erlaubt oder erfordert Art. 53 LVerf eine solche Einstellung nicht, die allgemeinen Vorschriften des DSG-LSA ebenso wenig.

Personenbezogene Daten sind über das Internet weltweit einsehbar und ihre leichte Auffindbarkeit durch Suchmaschinen (z.B. google.de) ist die Regel. Wer also als öffentliche Stelle solche Daten ins Internet einstellt, nimmt rechtlich und tatsächlich Datenübermittlungen ins Ausland vor. Diese sind nur unter den engen Voraussetzungen des § 13 Abs. 2 DSG-LSA zulässig.
Auch wenn - wie in diesem Fall - die Einsichtsmöglichkeit für jedermann in das Vereinsregister nach § 79 BGB bestand, rechtfertigt dies nicht das Einstellen der gleichen Information in das Internet (zur Einsicht in/Auskunft aus einem Register siehe auch Ziff. 26.3). Denn eine Veröffentlichung über das Internet stellt rechtlich wie tatsächlich eine andere Qualität des Informationszugangs dar.
Deshalb kommt als Rechtsgrundlage für ein weltweit einsehbares Einstellen personenbezogener Daten in der Regel nur die informierte Einwilligung der Betroffenen gemäß § 4 Abs. 2 DSG-LSA in Betracht. Deren Erklärung muss sich ausdrücklich auf das Internet beziehen.

Im vorliegenden Fall konnte der Landesbeauftragte unmittelbar nach Bekannt werden des Sachverhalts die Entfernung der Anlage aus dem Internetangebot des Landtages veranlassen.
Ob bei diesem Sachverhalt auch eine eigene Verantwortung der Landtagsverwaltung bei einer solchen Nutzung elektronischer Medien zum Tragen kommt, wird z.Zt. noch bundesweit diskutiert. Eine abschließende Meinungsbildung steht noch aus.

16. Personalwesen

Der datenschutzbewußte Umgang der öffentlichen Stellen des Landes mit Personaldaten hat im Berichtszeitraum einen überwiegend erfreulichen Eindruck hinterlassen. Zunehmend gerät das Personalwesen jedoch wieder in den Blickpunkt. Insbesondere rationalisierungsbedingte Veränderungen in der Behördenstruktur des Landes und die Umsetzung des notwendigen Personalabbaus führen zu zunehmender Fluktuation der Daten.

Die Anzahl personalwirtschaftlicher Vorgänge steigt überproportional. Damit steigen auch die Gefahren für die betroffenen Bediensteten. Der Landesbeauftragte geht daher davon aus, dass die verantwortlichen Stellen die erforderlichen Maßnahmen treffen, um den gesetzlichen Anforderungen an das Personalaktengeheimnis und den Personaldatenschutz auch bei erhöhtem Informationsbedarf entsprechend Rechnung zu tragen.

16.1 Personaldaten im Internet

Der Landesbeauftragte konnte der Adressenliste einer E-Mail einer Obersten Landesbehörde entnehmen, dass die Behörde ihren Organisationsplan mit personenbezogenen Angaben von Bediensteten über das Internet versandt hat. Dazu hatte der Landesbeauftragte bereits früher (V. Tätigkeitsbericht, Ziff. 14.4) darauf hingewiesen, dass die Übermittlung personenbezogener Daten nur zulässig ist, wenn das DSG-LSA oder eine andere Rechtsvorschrift sie erlaubt oder die Betroffenen eingewilligt haben.
Für die Personaldaten der Beamten gelten die bereichsspezifischen Übermittlungsregelungen der §§ 90 ff BG LSA. Gemäß § 28 Abs. 1 DSG-LSA gelten diese Bestimmungen auch für Beschäftigte in einem privatrechtlich ausgestalteten Beschäftigungsverhältnis. Nach § 90g Abs. 1 Satz 2 BG LSA ist die Übermittlung von Personalaktendaten nur nach Maßgabe des § 90d BG LSA zulässig. Mit § 90d Abs. 1 BG LSA hat der Gesetzgeber die Fälle, in denen eine Übermittlung ohne Einwilligung des Beschäftigten zulässig ist, abschließend bestimmt.

Auch wenn man - wie das Ministerium des Innern - Personaldaten im Rahmen von Organigrammen (nur) als **Sachakten**daten qualifiziert, gilt für ihre Verarbeitung bzw. Nutzung allgemeines Datenschutzrecht und die von der Veröffentlichung betroffenen Bediensteten sind nicht schutzlos. Der vom Verfassungsrecht vorgegebene Grundsatz der Zweckbindung der Daten und die Fürsorgepflicht des Dienstherrn erlauben keinen grenzenlosen Umgang mit den Daten. Bei der Verwendung des Internets kommt systembedingt rechtlich stets eine Übermittlung ins Ausland (§ 13 DSG-LSA) und an nicht-öffentliche Stellen in Betracht, weil der Absender den Weg der E-Mail weder kennen noch bestimmen kann.
Der Absender ist jedoch verantwortlich (§ 13 Abs. 3 DSG-LSA) und hat zudem zu gewährleisten, dass die Daten nur von Befugten zur Kenntnis genommen werden (vgl. § 6 Abs. 2 Nr. 1 DSG-LSA).
Die zustimmende Antwort der Landesregierung zur Darstellung des Landesbeauftragten im V. Tätigkeitsbericht (Ziff. 14.4) in der LT-Drs. 3/5152 ist bei einigen Landesbehörden wohl schon in Vergessenheit geraten.

Die betroffene Behörde hat nach kontroverser Diskussion mangels eines sicheren Übertragungsweges bis auf weiteres davon Abstand genommen, das Organigramm via E-Mail zu versenden.

16.2 Zeiterfassung

Kontrollen und Beratungsanfragen sind häufig Anlass, die Behandlung von sog. Gleitzeitkarten oder automatisierten Dokumentationen zur täglichen Arbeitszeit zu erörtern.

Dem Dienstvorgesetzten obliegt die Kontrolle der Einhaltung der täglichen Arbeitszeit. Grundsätzlich darf auch der jeweilige Vorgesetzte im Rahmen der Dienstaufsicht aus arbeitsorganisatorischen Gründen An- und Abwesenheitslisten über seine Mitarbeiter führen. Übersichten über An- und Abwesenheit gehören zu den Aufgaben der Personalverwaltung.

Automatisierte Zeiterfassungen sind mitbestimmungspflichtig. Dienstanweisungen oder Dienstvereinbarungen sollten detailliert Umfang, Dauer der Erhebung und Verarbeitung von Beschäftigtendaten sowie Auswertungsmöglichkeiten festlegen.
Die Zweckbindung (entsprechend der ArbeitszeitVO) ist zu beachten.

Im technisch-organisatorischen Bereich sind die notwendigen Schutzvorkehrungen zu treffen. Programmfunktionen müssen nicht vorgesehene Auswertungsmöglichkeiten technisch unterbinden. Die Zugriffsrechte sind exakt und auf das notwendige Maß (Vorgesetzte, Dienststellenleitung) beschränkt festzulegen. Aktualisierungs- bzw. Korrekturverfahren sind ebenfalls detailliert zu regeln, wie z.B. die befugte Korrekturperson, die Korrekturgrundlage (z.B. vom Vorgesetzten gezeichneter Beleg), das Passwort und die Verschlüsselung. Den Gefahren des unbefugten Zugriffs auf Stempelkarten bzw. des Kartenverlustes ist vorzubeugen.

Gleitzeitkarten bzw. monatliche Ausdrucke zur Arbeitszeit sind als zunächst nicht grundlegende Daten zum Arbeitszeitstatus als Sachakten anzusehen, so dass allgemeines Datenschutzrecht auf die Erhebung, Verarbeitung und Nutzung Anwendung findet. Danach ist die regelmäßige **Vollkontrolle** der Gleitzeitdaten **aller** Mitarbeiter durch unmittelbare Dienst- oder Fachvorgesetzte bedenklich (Bewegungs- bzw. Gewohnheitsbilder von Mitarbeitern). Datenschutzrechtlich unbedenklich sind die üblichen Stichproben und Anlasskontrollen in Einzelfällen (z.B. bei häufiger Abwesenheit oder Leistungsdefizit).

16.3 Schutz von Personaldaten bei Privatisierung der Reinigung

Eine Stadt prüfte im Interesse der Haushaltskonsolidierung die Möglichkeiten der Übertragung von Reinigungsaufgaben an private Unternehmer (Outsourcing). Fünf private Reinigungsunternehmen wurden gebeten, Angebote zu unterbreiten, auch bezüglich der Übernahme des kommunalen Reinigungspersonals. Zum Zwecke der Angebotsaufbereitung übermittelte das Personalamt den Unternehmen eine Liste, die die einzelnen Objekte

aufführte und Einzelangaben zum Reinigungspersonal enthielt, u.a. zu Alter, Familienstand, Lohnsteuerklasse und Kindern. Namen wurden nicht genannt, in einzelnen Einrichtungen waren jedoch lediglich ein oder zwei Personen als Reinigungspersonal beschäftigt.

Auch wenn eine namentliche Erwähnung der Bediensteten nicht stattfand, gilt der gesetzliche Schutz, wenn die betroffenen Personen bestimmbar sind (vgl. § 2 Abs. 1 Satz 1 DSG-LSA). Eine (ausreichende) Anonymisierung ist nach § 2 Abs. 7 DSG-LSA erst dann anzunehmen, wenn personenbezogene Daten derart verändert werden, dass Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.
Mit Hilfe der zahlreichen Einzelangaben in der Liste konnten die betroffenen Personen einfach festgestellt werden. Die Übermittlung der personenbezogenen Daten der Beschäftigten ist für diesen Fall in den Vorschriften der § 28 Abs. 1 DSG-LSA i.V.m. §§ 90g Abs. 1 Satz 2, 90d Abs. 2 BG LSA geregelt. Die dort genannten gesetzlichen Voraussetzungen waren nicht erfüllt. Die Betroffenen hatten in die Übermittlung auch nicht eingewilligt.

Damit lag eine unzulässige Übermittlung von personenbeziehbaren Daten vor, die die Betroffenen in ihrem Grundrecht auf informationelle Selbstbestimmung (Art. 6 Abs. 1 LVerf) verletzte.

Auf den Hinweis des Landesbeauftragten hat die Stadt die Fehlerhaftigkeit ihres Vorgehens eingeräumt und umgehend die übermittelten Informationen zurückgefordert. Die Stellungnahme der Stadt ließ die künftige Beachtung der datenschutzrechtlichen Anforderungen erwarten, so dass nach § 24 Abs. 3 DSG-LSA von einer Beanstandung abgesehen wurde.

16.4 Personalführungsgespräche, Zielvereinbarungen gem. § 5 GGO LSA I

Im Zusammenhang mit Personalführungsgesprächen und der Festlegungen von Zielvereinbarungen gem. § 5 GGO LSA I wurde der Landesbeauftragte auf die unterschiedliche Verfahrensweise und rechtliche Unsicherheiten bei der Durchführung in den Obersten Landesbehörden aufmerksam gemacht. Zur Optimierung des Vorgehens, unter Berücksichtigung datenschutzrechtlicher Gesichtspunkte, wies der Landesbeauftragte die Häuser auf folgendes hin:

Auf der rechtlichen Grundlage der §§ 90 ff BG LSA, die nach Maßgabe des § 28 Abs. 1 DSG-LSA auch für die nicht verbeamteten Mitarbeiter gelten, ist zu differenzieren zwischen personalaktenrelevanter Datenverarbeitung für die Personalverwaltung einerseits und der Verarbeitung von Daten zum Zweck der Personalwirtschaft andererseits. Personalwirtschaft-

liche Maßnahmen gehen über das einzelne Dienstverhältnis hinaus. Sie werden ihrer Zweckbestimmung nach im Regelfall in Sachakten beim Personalreferat geführt.
Für die Zuordnung eventueller Vorgänge kommt es maßgeblich auf den Zweck an, für den die Vorgänge vorrangig bestimmt sind. In Übereinstimmung mit dem Ministerium des Innern ist festzuhalten, dass die Personalführungsgespräche Einzelgespräche sind und im wesentlichen in den Bereichen

- Zusammenarbeit Vorgesetzter – Mitarbeiter
- Führung
- Veränderungs- und Entwicklungsperspektiven
- Arbeitsaufgaben
- Arbeitsumfeld

folgenden Zwecken dienen:

- verdeckte Probleme aufzudecken
- Missverständnisse und Vorurteile abzubauen
- das gegenseitige Verständnis zu fördern und
- das Gemeinschaftsgefühl zu stärken.

Ein Vermerk darüber wird sich im Regelfall auf die Dokumentation der Tatsache der Durchführung eines Personalführungsgespräches reduzieren. Eine Dokumentation von Inhalten sollte vom ausdrücklichen Wunsch des Betroffenen abhängen.

Auch für Personalverwaltungszwecke können personenbezogene Informationen nach den vorstehend genannten Vorschriften durch den Vorgesetzten erhoben werden.
Wenn dabei im Einzelfall die Informationen schwerpunktmäßig auf die Ausgestaltung des individuellen Beschäftigungsverhältnisses gerichtet sind, wären sie der Personalakte zuzuführen. Die Möglichkeit der Verwendung in Sachvorgängen zum Zweck der Personalplanung und des Personaleinsatzes bleibt unbenommen.

Zielvereinbarungen dienen der Arbeitsorganisation auf Referats- oder Abteilungsebene.

Soweit eine Dokumentation erfolgt, überwiegt das Interesse der Dienststelle am Einsatz optimierender Steuerungsmethoden in der Regel gegenüber dem Interesse der Beschäftigten. Solche Vorgänge liegen grundsätzlich im Verantwortungsbereich des Referats-/Abteilungsleiters, werden bei ihm geführt und in der Regel in der Gesamtheit der Organisationseinheit erörtert. Auch hierbei sind ggf. Grenzen zu beachten, wenn die personenbezogene Information das Persönlichkeitsrecht des Beschäftigten nach Abwägung mit den Interessen der Dienststelle unzumutbar beeinträchtigt.

16.5 Aufbewahrungsfristen für Dienstaufsichtsbeschwerden

Der Landesbeauftragte wurde darauf aufmerksam gemacht, dass in dem Bericht Nr. 16/1990 "Kommunale Schriftgutverwaltung" der Kommunalen Gemeinschaftsstelle für Verwaltungsvereinfachung (KGSt) empfohlen sei, Aufsichtsbeschwerden - in einer Generalakte - bis zu 15 Jahre aufzubewahren.

Das Führen von Generalakten zu Dienstaufsichtsbeschwerden ist datenschutzrechtlich bedenklich.
Nach § 90 Abs. 1 Satz 2 BG LSA gehören alle Unterlagen zur Personalakte - einschließlich ihrer Teilakten -, die mit dem Dienstverhältnis des Beamten in einem unmittelbaren inneren Zusammenhang stehen. Dazu gehören auch Unterlagen über mit dem Dienstverhältnis zusammenhängende Beschwerden, Behauptungen und Bewertungen, die nicht zu einem Disziplinarverfahren geführt haben. Dabei sind die Tilgungsregelungen des § 90e BG LSA zu beachten.

§ 28 Abs. 1 DSG-LSA sieht vor, dass für das Erheben, Verarbeiten oder Nutzen von Personaldaten über Angestellte, Arbeiter und Auszubildende, die in einem privatrechtlich ausgestalteten Ausbildungsverhältnis stehen, die §§ 90 bis 90g des BG LSA grundsätzlich entsprechend gelten.

Die KGSt hat daraufhin in ihrer Info 18/2002 (S. 149) einen entsprechenden Hinweis aufgenommen. Der Städte- und Gemeindebund Sachsen-Anhalt hat in den Kommunalnachrichten Sachsen-Anhalt Ausgabe 10, Nr. 618, den Hinweis des Landesbeauftragten abgedruckt.

17. Polizei

17.1 Novellierung des SOG LSA

17.1.1 Einführung der Videoaufzeichnung

Die mit der Novellierung des SOG LSA im Kalenderjahr 2000 eingeführte Möglichkeit, an sog. Kriminalitätsschwerpunkten (gefährlichen Orten) eine Videoüberwachung durchführen zu können, soll durch einen neuen Gesetzesvorschlag der Landesregierung dahingehend erweitert werden, dass künftig neben der Videoüberwachung auch Video**aufzeichnungen** vorgenommen werden können. Schon jetzt sind Aufzeichnungen im Einzelfall möglich, um eine Gefahrensituation zu dokumentieren und die Beweisführung für eine Straftat zu erleichtern.
Die neu vorgesehene Regelmöglichkeit zur Aufzeichnung soll erforderlich sein, um die Effektivität der Gefahrenabwehr, insbesondere der Straftatenverhütung, zu erhöhen. Dies überzeugt nicht, denn die bisherige Beobachtung stellt eine schnelle Reaktion zur Gefahrenabwehr sicher; die

Aufzeichnung hilft bestenfalls, geschehenes Unrecht strafrechtlich abzuarbeiten, wenn Stunden oder Tage später auf eine Anzeige reagiert wird.

Unklar bleibt auch, warum die bisherige offene Beobachtung künftig nicht mehr ausreichen soll, wenn doch grundsätzlich weiterhin auf den Einsatz von Aufzeichnungsgeräten hinzuweisen ist (vgl. § 16 Abs. 3 SOG LSA).

Gründe der Verwaltungsvereinfachung reichen nach der Rechtsprechung des Bundesverfassungsgerichts nicht aus, um derartig weitgehende Eingriffe in das Recht auf informationelle Selbstbestimmung zu rechtfertigen.

Mit der Schaffung der Aufzeichnungsmöglichkeit sieht der Landesbeauftragte daneben die Gefahr, dass digitale Aufzeichnungen langfristig und an den verschiedensten Stellen gespeichert werden können, ohne dass der unbeteiligte Bürger jemals davon etwas erfährt. Außerdem entsteht mit dieser neuen Regelaufzeichnung die Gefahr unkontrollierter Abgleiche von Gesichtsfelderkennungen.

17.1.2 Änderung der Vorschriften über die Rasterfahndung (§ 31 SOG LSA)

Nach dem neuen Gesetzentwurf soll die Rasterfahndung bereits zulässig sein, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass künftig Straftaten von **erheblicher Bedeutung** begangen werden und die vorbeugende Bekämpfung dieser Straftaten anders nicht möglich erscheint.
Die Abwehr einer **gegenwärtigen Gefahr** ist nicht mehr vorgesehen.

Die die Rasterfahndung rechtfertigende **Annahme** künftiger Straftaten von erheblicher Bedeutung ist sehr weitreichend.
In der Gesetzesbegründung werden aber keine Negativfeststellungen aufgeführt, die eine Veränderung der Rechtslage als notwendig erscheinen lassen.
Die Mitteilung im Gesetzesentwurf, die Rasterfahndung sei - ohne die vorgesehene Änderung - in der Regel als Maßnahme zur Terrorismusbekämpfung ungeeignet, ist angesichts der anderen Erfahrungen bei der Rasterfahndung nach dem 11. September 2001 hier im Lande kein tragfähiger Grund zur Änderung des Gesetzes. Ein forscher Beschluss der Innenministerkonferenz ersetzt nicht die Rechtsgüterabwägung durch den Gesetzgeber.

Als weitere wichtige Änderung sieht der Gesetzentwurf den **Wegfall der richterlichen Zustimmung** vor der Durchführung der Rasterfahndung vor. Die Streichung des Richtervorbehaltes und stattdessen die bloße Einführung einer polizeilichen Anordnung erscheint angesichts des Ausmaßes der möglichen Eingriffe äußerst bedenklich. Diese Streichung ist zudem nicht erforderlich, weil Eilfälle bereits nach bisherigem Recht abgesichert waren. Es mangelt auch dafür an einer eingehenden Begründung,

welche die Verschlechterung der Rechtssituation für die überwiegende Zahl der betroffenen gesetzestreuen Bürger trägt.
Die durch das bisherige richterliche Prüfverfahren gegebene Schutzfunktion ist umso wichtiger, je niedriger die Eingriffsschwelle gesetzt wird.

17.2 Mobiltelefon-Überwachung mit IMSI-Catcher

Das Gerät identifiziert betriebsbereite Mobiltelefone und erfasst nicht nur Kartendaten eines konkret gesuchten Handys, sondern auch alle aktiven Mobiltelefone in seinem räumlichen Umfeld (ca. 100 - 150 m).

Für den Einsatz dieses Gerätes bei der Strafverfolgung mangelte es der Polizei bisher an einer entsprechenden Rechtsgrundlage. Mitte 2002 hatte der Gesetzgeber mit einer neuen Vorschrift in der StPO (§ 100i) der Polizei bei Straftaten von erheblicher Bedeutung die Möglichkeit eingeräumt, Karten- und Gerätenummern von Mobiltelefonen, deren Rufnummern und deren Nutzer zu ermitteln. Außerdem wird mit dieser Vorschrift auch die Suche nach Verdächtigen mit Hilfe des IMSI-Catchers ermöglicht.
Die Gesetzesänderung sieht vor, dass für den Einsatz eine richterliche Anordnung erforderlich ist und die Daten Dritter nach dem Einsatz dieses Geräts unverzüglich zu löschen sind.
Bereits vor der Änderung der StPO erlaubte das zum 01.01.2002 in Kraft getretene Anti-Terror-Gesetz dem Verfassungsschutz und dem MAD den IMSI-Catcher zu nutzen.

Die rechtlichen Bedenken der Datenschutzbeauftragten des Bundes und der Länder bestehen darin, dass in die Überwachung mit dem IMSI-Catcher wegen der Umfelderfassung zwangsläufig eine Vielzahl unverdächtiger Personen einbezogen werden.
Weiterhin wird kritisiert, dass die Anknüpfung an den zu weiten Rechtsbegriff "Straftat von erheblicher Bedeutung" anders als bei den Katalogstraftaten des § 100a StPO ein sehr weites Einsatzfeld für die Polizei eröffnet wird. Schon ein Ladendiebstahl kann jetzt im Wiederholungsfall eine Straftat von erheblicher Bedeutung sein.
Damit dürfte ein weiterer Schritt auf dem Weg zur allumfassenden Überwachung auch rechtstreuer Bürgern getan sein.

17.3 Unzulässigkeit einer Ed-Behandlung

Anlässlich des deutsch-spanischen Gipfeltreffens im Oktober 2001 in Quedlinburg hatte sich die Polizei zum Ziel gesetzt, eventuelle Störungen schon im Ansatz zu unterbinden. Im Laufe der Veranstaltung störten Jugendliche bei Annäherung der Regierungsdelegation durch Rufe wie "Mörder" oder "Kriegstreiber". Zur Vermeidung weiterer Störungen wurde die Ingewahrsamnahme von vier Jugendlichen verfügt. Nach der Aufnahme eines Protokolls über freiheitsentziehende Maßnahmen wurden bei

den Jugendlichen anschließend erkennungsdienstliche Maßnahmen durchgeführt.

Leider war in der festgesetzten Gruppe zumindest ein unbeteiliger Jugendlicher, dessen Vater sich beim Landesbeauftragten beschwerte. Wie die datenschutzrechtliche Überprüfung ergab, war die Ed-Behandlung vom Gesetz nicht gedeckt, weil die rechtlichen Voraussetzungen des § 21 Abs. 2 Nrn. 1 und 2 SOG LSA (Behandlung zur Identitätsfeststellung oder Verdacht einer Straftat) nicht gegeben waren. Weder bestanden in diesem Fall Zweifel an der Identität des Sohnes des Petenten noch wurde er einer Straftat verdächtigt.

Die zuständige Polizeidirektion löschte die Daten des Jugendlichen und hat diesen Vorfall zum Anlass genommen, die beteiligten Polizeibeamten diesbezüglich für künftige Großveranstaltungen noch einmal zu unterweisen.

17.4 Eindeutige Empfängeranschrift bei Vorladungen zur Beschuldigtenvernehmung

Ein Bürger beschwerte sich beim Landesbeauftragten darüber, dass er im Vorladungsschreiben eines Polizeireviers zusammen mit dem Namen eines angeblichen Mitbewohners, der einer Straftat verdächtigt wurde, zur Beschuldigtenvernehmung aufgeführt war. Erst nach Öffnung des Briefes habe er aus der persönlichen Anrede in dem Vorladungsschreiben erkennen können, dass er gar nicht betroffen war.

Wie sich nach der Stellungnahme durch das Polizeirevier herausstellte, hatte dieses - wie bei Untermietern vorgeschrieben - es versäumt, hinter dem ersten Namen des Beschuldigten und vor dem Namen des Beschwerdeführers (Hauptmieter) das Wort "bei" einzufügen, so dass für den Bürger der Eindruck entstehen musste, auch er sei Empfänger des Vorladungsschreibens.

Das Ministerium des Innern hat diesen Vorgang zum Anlass genommen, auf die Beachtung der Schreib- und Gestaltungsregeln für die Textverarbeitung (DIN 5008) hinzuweisen.

17.5 Halterdaten auf der Mängelanzeige am Fahrzeug

Einem aufmerksamen Polizeibeamten war an einem Fahrzeug aufgefallen, dass Haupt- und Abgasuntersuchung überfällig waren. Also fertigte er eine Mängelanzeige an, die er hinter dem Scheibenwischer des Wagens hinterließ. So weit, so gut.

Nicht gut, und vor allem datenschutzrechtlich nicht erforderlich war jedoch, dass der Name der Halterin auch noch für jeden zufälligen Passanten sichtbar auf der Anzeige vermerkt war.

Darüber hat sich die Petentin zu Recht beim Landesbeauftragten beschwert, was auch die Dienststelle des Beamten sofort einsah.

18. Rechtspflege

18.1 "Personalaktenführung in der Justiz" oder "Jeder will alles im eigenen Hause haben"

Bei der Prüfung eines Amtsgerichts wurden auch stichprobenweise Personalvorgänge des nichtrichterlichen Personals geprüft.
Aus dem Ergebnis dieser Prüfung lassen sich nicht nur Rückschlüsse auf die drei Ebenen der ordentlichen Gerichtsbarkeit ziehen, sondern auch auf Eigenheiten bei der Personalaktenführung schließen, die nicht im Einklang mit den allgemeinen gesetzlichen Bestimmungen stehen dürften.

In einigen Personalakten fanden sich sog. personelle Sammelverfügungen oder Berichte, in denen die jeweils anderen betroffenen Bediensteten nicht geschwärzt worden waren. In der Personalakte einer Justizangestellten befand sich ein Bericht des Direktors des **Amtsgerichts** über den Präsidenten des **Landgerichts** an die Präsidentin des **Oberlandesgerichts**, in dem auch andere weibliche Bedienstete namentlich erwähnt sind, die zu ebenfalls genannten Zeitpunkten aufgrund von Schwangerschaft Mutterschutz antreten würden.
Eine Anhäufung sensibler Daten, mit der so gesetzlich nicht umgegangen werden darf. Die Auflistung von personenbezogenen Daten Dritter in Sammelverfügungen kann (z.B. bei Einsichtnahmen in die Personalakte) datenschutzrechtlich zur Übermittlung personenbezogener Informationen führen, für welche die gesetzlichen Voraussetzungen nicht vorliegen. Gründe der "Verwaltungsbequemlichkeit" reichen als Rechtfertigung für ein solches Verfahren bekanntermaßen nicht aus. Auch in der Justizverwaltung muss sich der Umgang mit Personaldaten an den §§ 90 ff BG LSA orientieren, die über § 28 Abs. 1 DSG-LSA auch für die angestellten Bediensteten gelten.

Des Weiteren stellte sich bei den Stichproben heraus, dass in der Regel an mindestens drei Stellen Akten über die Bediensteten geführt werden (Amts-, Land- und Oberlandesgericht). Angaben zu Grund-/Teil- und Nebenpersonalakten waren auf bzw. in den vorgelegten Akten nicht ersichtlich. Die Existenz weiterer Personal(Teil-)akten war aus den vorgelegten Akten allenfalls indirekt zu erschließen.
Zudem konnte auch auf Nachfrage kein Hinweis zu einer Verfügung hinsichtlich der Ausübung der personalrechtlichen Befugnisse in den Einzelfällen gegeben werden.

Diese Praxis bei der Führung der Personalakten widerspricht den in § 90 BG LSA geregelten Grundsätzen, u.a. der Einheit der Personalakte.
Der Erlass des Ministeriums der Justiz zur Ausübung der personalrechtlichen Befugnisse (vom 05.11.1997, JMBl. 1997, 375) trifft keine Regelung

zur Personalaktenführung. Er scheint jedoch - entgegen § 90 Abs. 2 Satz 2 BG LSA - so verstanden zu werden, als sei der Originalentwurf über eine personalbezogene Maßnahme bei der personalrechtlich befugten und nicht bei der für die Führung der Grundakte zuständigen Dienststelle zu den Akten zu nehmen.

Der Landesbeauftragte hat auf diese Mängel hingewiesen. Inzwischen hat das Ministerium der Justiz dazu eine Allgemeinverfügung herausgegeben, die am 01. Januar 2003 in Kraft getreten ist.

18.2 Fehlende Anonymisierung bei Beschlüssen zur DNA-Untersuchung

Die Rechtsmedizinischen Institute in Halle und Magdeburg führen u.a. im Rahmen von strafrechtlichen Ermittlungsverfahren DNA-Untersuchungen durch. Rechtliche Voraussetzung ist eine entsprechende richterliche Anordnung, welche die Staatsanwaltschaft beantragt. In der Regel werden die ergangenen Beschlüsse bei der zuständigen Geschäftsstelle des Gerichtes unmittelbar von Polizeivollzugsbeamten zur weiteren Bearbeitung abgeholt. Danach gibt die zuständige Ermittlungsbehörde die Körperzellen des Beschuldigten zur molekulargenetischen Untersuchung an den im Gerichtsbeschluss bezeichneten Sachverständigen zur Untersuchung weiter. Dies hat nach § 81f Abs. 2 Satz 3 StPO so zu geschehen, dass diesem mit dem Material weder Name und Anschrift noch Geburtstag und Geburtsmonat mitgeteilt werden.

Bei der Prüfung der Institute wurden jedoch Kopien einer Reihe von Beschlüssen verschiedener Amtsgerichte gefunden, welche den Beschuldigten bzw. andere Betroffene unter voller Nennung von Name, Vorname, Anschrift sowie Geburtsdatum bezeichneten. Dies war in einem Fall besonders prekär, da der Richter in der Beschlussbegründung sogar auf die Notwendigkeit einer Anonymisierung hingewiesen hatte.

Die Fehler bei der contra legem unterlassenen Anonymisierung lagen im Verantwortungsbereich der betroffenen Staatsanwaltschaften und der Polizeibehörden. In einem Fall lag die Falschbehandlung in der fehlerhaften Verfügungstechnik einer Richterin - dieser Fall wurde aber im Hinblick auf die richterliche Unabhängigkeit nicht näher untersucht.
Soweit die aufgefundenen Vorgänge Fälle betrafen, welche von Behörden außerhalb Sachsen-Anhalts bearbeitet wurden, wurden diese an die entsprechenden Landesbeauftragten weitergegeben.

Erwartungsgemäß haben allerdings die angeschriebenen Staatsanwaltschaften mitgeteilt, dass die Polizei die weitere Bearbeitung solcher Sachverhalte übernehme. Womit die Verantwortung der Staatsanwaltschaft aber nicht entschwunden ist.

Auffällig war auch, dass eine der Staatsanwaltschaften und zwei der betroffenen Polizeidirektionen erst nach erneuter Anfrage und längerem Suchen den Erlass des Landesbeauftragten gefunden hatten.
Die bisher vorliegenden Antworten zu dem gesetzwidrigen Verhalten weisen auf eher unspezifische Einzelfehler hin.

Seit 28.10.2002 ist das Verfahren per Erlass durch das Ministerium des Innern geregelt worden. Es bleibt abzuwarten, inwieweit die Fehlerquote damit zurückgeht.

18.3 Adresssammlungen beim Verwaltungsgericht

Im Rahmen eines Informationsbesuches bei einem Verwaltungsgericht hat der Landesbeauftragte festgestellt, dass in einem Vorzimmer auf einem Einzelplatz-PC seit Einführung einer Software namens "EUREKA" im Jahre 1996 sämtliche Namen und Adressdaten aller seit diesem Zeitpunkt an Verfahren Beteiligten, gleich ob Kläger, Beklagte, Anwälte, Sachverständige, gespeichert waren. Eine Dienstanweisung o.ä., wie mit personenbezogenen Daten umzugehen ist, insbesondere zur Sicherung, Aktualisierung und vor allem Löschung bestand nicht. § 16 Abs. 2 Satz 1 DSG-LSA war nicht im Blick.

Als wäre sie bestellt worden, erreichte den Landesbeauftragten kurze Zeit nach der Prüfung die Beschwerde einer Petentin, nennen wir sie Frau X. Frau X. erhielt von der Landeszentralkasse in Dessau, welche auch die Buchungen im Bereich der Justiz durchführt, eine Kostenrechnung, welche sie innerhalb von 14 Tagen begleichen sollte. Dieser Betrag sollte durch einen Rechtsstreit zwischen ihr und der Landeshauptstadt Magdeburg begründet sein. Da Frau X. einen solchen Rechtsstreit nicht geführt hatte, teilte sie dies dem zuständigen Verwaltungsgericht mit und legte vorsorglich Widerspruch ein. Daraufhin erhielt sie vom Verwaltungsgericht die Mitteilung, dass der Widerspruch zurückgewiesen werde, da sie wegen eines - vom Verwaltungsgericht beigefügten - Urteils zur Zahlung verpflichtet sei. Dieses Urteil lautete tatsächlich auf den Namen von Frau X. und enthielt auch ihre Adresse. Allerdings war ihr der Prozessinhalt fremd, da es um Wohngeldstreitigkeiten ging, sie aber noch nie Wohngeld beantragt hatte. Nach langem Zureden gelang es ihr doch noch, das Verwaltungsgericht davon zu überzeugen, dass das Urteil an die falsche Person zugestellt worden war.
Nach dieser beunruhigenden Erfahrung beim Umgang mit ihren persönlichen Daten wandte sich Frau X. an den Landesbeauftragten, da sie die Löschung ihrer Daten sicherstellen wollte.
Das zuständige Gericht hatte in der Zwischenzeit die Verwechslung aufklären können und sich bei der Petentin für das Versehen entschuldigt. Darüber hinaus hat der Systemadministrator des Gerichts in diesem Fall für die physikalische Löschung der Daten der Petentin Sorge getragen.

Da die Leitung des Gerichtes nach eigener Prüfung die Rechtsauffassung des Landesbeauftragten teilte, um eine angemessene Klärung der Datenhaltung besorgt war und zudem ankündigte, sich berichtsweise bezüglich der datenschutzrechtlichen Probleme an das Justizministerium wenden zu wollen, konnte von einer Beanstandung abgesehen werden.

Die Prüfungen bei anderen Gerichten wie auch die Beschwerde haben zwei Aspekte deutlich gemacht:
Zum einen werden die Gerichte verstärkt darauf achten müssen, in welchem Umfang sie Daten speichern, verändern oder nutzen. Die Grundregelung des § 10 Abs. 1 Satz 1 DSG-LSA lässt dies nur zu, soweit solches für die Erfüllung der gerichtlichen Aufgaben erforderlich ist.
Die Speicherung von Klägern und Beklagten steht nicht zur Diskussion, aber ein unbegrenztes Vorhalten der Daten von Personen, die in irgendeiner Weise in einen Prozess involviert waren, entspricht dieser Bestimmung und dem ihr zugrunde liegenden verfassungsrechtlichen Anspruch nicht.
Zudem ist jedes Gericht als öffentliche Stelle verpflichtet, in eigener Verantwortung für eine datenschutzgerechte Bearbeitung von Vorgängen Sorge zutragen. Dies heißt, dass bis zu einer Überarbeitung rechtlich bedenklicher Softwareprodukte u.U. Übergangslösungen gefunden werden müssen.

Zum anderen ist deutlich geworden, dass das zuständige Ministerium § 22 Abs. 4 Satz 2 DSG-LSA missachtet hat. Danach ist der Landesbeauftragte über Planungen des Landes zum Aufbau automatisierter Informationssysteme rechtzeitig zu unterrichten, sofern in ihnen personenbezogene Daten verarbeitet oder genutzt werden sollen. Das bei der Prüfung dem Datenschutzbeauftragten aufgefallene Softwarepaket "EUREKA" stellt ein Verfahren dar, bei welchem der Landesbeauftragte schon lange hätte beteiligt werden müssen. Dies ist bis heute nicht geschehen, obwohl weitere Module der landesweit bei unterschiedlichen Gerichten eingesetzten Software - so etwa im Bereich Vollstreckung - eingeführt werden sollen.
Der Landesbeauftragte weist nachdrücklich auf dieses Unterrichtungsgebot hin.

18.4 Auskunft aus dem bei den Amtsgerichten geführten Schuldnerverzeichnis

Ein Beschwerdeführer wandte sich an den Landesbeauftragten, da er der Auffassung war, ihm werde zu Unrecht die Einsicht in die über ihn im Schuldnerverzeichnis gespeicherten Daten verwehrt.

In der Tat war es zu einer rechtlichen Fehleinschätzung in der Verwaltungstätigkeit des Amtsgerichts gekommen.
Entgegen der Auffassung des Gerichtsdirektors ist dem Betroffenen nach § 15 Abs. 1 DSG-LSA auf Antrag Auskunft u.a. über die zu seiner Person

im Schuldnerverzeichnis gespeicherten Daten einschließlich deren Herkunft zu erteilen. Diese Bestimmung ist anwendbar, da andere bereichsspezifische Rechtsvorschriften nicht bestehen.
Insbesondere half vorliegend die in der ZPO geregelte Auskunftsnorm (siehe § 915b i.V.m. § 915 Abs. 3 ZPO) nicht weiter, da dort lediglich - zum Schutz des Betroffenen - die Auskunftserteilung über Daten des Betroffenen an Dritte geregelt ist. Gleiches gilt im konkreten Fall auch hinsichtlich § 21 EGGVG, der sich auf den hier nicht relevanten Auskunftsanspruch hinsichtlich übermittelter Daten und deren Empfänger bezieht.

Der Petent hatte sich zugleich im Wege einer Dienstaufsichtsbeschwerde an den Präsidenten des Landgerichts gewandt. Aus dessen Antwort ging hervor, dass dieser zur gleichen rechtlichen Einschätzung wie der Landesbeauftragte gelangt war.

18.5 Getrübte Freuden am Interneteinkauf - Fehler im Schuldnerverzeichnis

Kaufvorgänge, die über das Internet abgewickelt werden, stellen inzwischen eine alltägliche Situation dar. Allerdings bedeutet dies nicht, dass damit Probleme, die beim direkten Kauf auftreten können, passé wären.

Ein Petent, der sich an den Landesbeauftragten gewandt hatte, machte entsprechende besondere Erfahrungen.
Er hatte über das Internetangebot eines Modeherstellers Kleidung bestellt. Nach kurzer Zeit erhielt er von dieser Firma ein Schreiben, in welchem ihm - unter Hinweis auf eine neutrale Auskunft der Schutzgemeinschaft für allgemeine Kreditsicherung e.V. (SCHUFA) - höflich mitgeteilt wurde, dass man seine Bestellung nicht ausführen könne. Letztlich wurde er damit für kreditunwürdig erklärt.

Im Unterschied zum Kauf von Angesicht zu Angesicht, sehen viele Internethändler die Notwendigkeit, sich hinsichtlich der Erfüllung der Zahlungspflicht ihrer Kunden abzusichern. Dies geschieht z.T. dadurch, dass der Kauf über Kreditkarten abgewickelt wird. Viele Händler greifen jedoch auf die Daten der SCHUFA zurück. Bei dieser - wie auch anderen ähnlichen - Auskunfteien sind Daten gespeichert, welche nicht nur Banken, sondern auch Kaufleuten, u.a. einen Eindruck über die Zahlungsfähigkeit ihrer potentiellen Kunden vermitteln sollen. Die grundlegenden Daten erhält die SCHUFA u.a. aus dem Schuldnerverzeichnis der Amtsgerichte in einem automatisierten Verfahren.

Wie der Petent dann durch Einsichtnahme in das Schuldnerverzeichnis feststellte, war dort ein gegen ihn gerichteter Haftbefehl eingetragen. Diese Haftanordnung in einer Zwangsvollstreckungssache war aber durch das Landgericht bereits lange aufgehoben worden. Die Korrektur des Schuldnerverzeichnisses erfolgte jedoch nicht sofort nach Rechtskraft der

Entscheidung des Landgerichts, sondern erst nachdem der Petent eine Dienstaufsichtsbeschwerde eingelegt hatte - sechs Monate später. Dies hatte zur Folge, dass er - bedingt durch die automatisierte Übermittlung der fehlerhaften Daten vom Amtsgericht an die SCHUFA - in der Zwischenzeit bei der SCHUFA als finanziell "unsicherer Kandidat" geführt wurde.

Der Landesbeauftragte weist angesichts dieses Falles nachdrücklich auf die jederzeitige gesetzliche Pflicht der öffentlichen Stellen hin, die Integrität der in ihrem Zuständigkeitsbereich verarbeiteten und genutzten Daten gewährleisten zu müssen.

Nur wegen der angemessenen Reaktion des Landgerichtspräsidenten hat er auf eine förmliche Beanstandung verzichtet.

18.6 Unvermeidliche (?) Nachlässigkeit

Im Rahmen eines zivilgerichtlichen Verfahrens hatte ein Bürger, um Prozesskostenhilfe beantragen zu können, detaillierte Unterlagen über seine finanziellen Verhältnisse in Kopie dem Gericht übersandt. Das entsprechende Schreiben ist beim betreffenden Amtsgericht eingegangen. Auf dem Eingangsstempel sind im entsprechenden Feld auch etliche Anlagen zahlenmäßig vermerkt worden. Die diesem Vermerk entsprechenden Anlagen gelangten jedoch nicht zur Verfahrensakte.
Bei einer ihm gewährten Akteneinsicht bemerkte der Betroffene dies und weitere Mängel in der Aktenführung. Nachdem ein unglücklich formuliertes Schreiben des Gerichts für zusätzliche Verärgerung gesorgt hatte, wandte er sich mit der Bitte an den Landesbeauftragten, den Verbleib der Unterlagen zu klären.
Auch der Landesbeauftragte stellte Mängel in der praktischen Handhabung der Aktenführung fest, konnte aber den Verbleib der für den Petenten wichtigen Kopien auch nicht klären. Die Überprüfung von Organisation und Postlauf des Gerichts ergab keine grundsätzlichen organisatorischen Defizite. Es blieben allgemeine Fehlerquellen, die im alltäglichen Ablauf von Verwaltungsstellen, so auch bei der Geschäftsstelle eines Gerichtes, nicht immer vermeidbar sind.

Die Leitung des Amtsgerichts versicherte, dass die verhaltensbezogenen und organisatorischen Defizite aufgearbeitet wurden.
Auf eine förmliche Beanstandung konnte letztlich verzichtet werden.

18.7 Durchführungsbestimmungen zum Gesetz über die Prozesskostenhilfe (DB-PKHG)

Aus einem anderen Bundesland wurde der Landesbeauftragte darüber informiert, dass die Justizminister des Bundes und der Länder eine Neufassung der DB-PKHG beabsichtigten.

Die Prozesskostenhilfe dient dazu, Personen, welche aus wirtschaftlichen Gründen nicht in der Lage sind, ein Gerichtsverfahren vollständig oder teilweise aus eigenen Mitteln zu betreiben, unter bestimmten Voraussetzungen finanzielle Unterstützung zur Durchsetzung ihrer Interessen zu gewähren. Nach dem Gesetz über die Prozesskostenhilfe haben Personen, welche eine solche Unterstützung begehren, in umfassender Weise über ihre Einkünfte und Vermögenswerte Auskünfte zu erteilen. Durchführungsbestimmungen sollen gewährleisten, dass in den Verwaltungen der Gerichte - auch zum Schutz der Antragsteller - ein gleichmäßiges Verfahren in der Bearbeitung solcher Anträge stattfindet.

Die dem Landesbeauftragten aufgefallene Regelung in den Durchführungsbestimmungen betraf das Verfahren der Übersendung der bzw. Einsichtnahme in die Prozessakten. Da den Prozessakten das PKH-Beiheft mit den detaillierten wirtschaftlichen und sozialen Daten des PKH-Antragstellers beigeheftet ist, sehen die DB-PKHG vor, dieses Heft bei Versendung der Akte oder Vorlage zur Einsichtnahme durch die gegnerische Partei oder nicht beteiligte Behörden zu entnehmen.
Da sich aus Bestimmungen der ZPO und dem EGGVG ergibt, dass auch Aktenversendungen an bzw. Akteneinsichtnahmen durch sonstige Dritte denkbar sind, ist nach Auffassung des Landesbeauftragten eine entsprechende Ergänzung der DB-PKHG über den schon genannten Empfängerkreis hinaus vorzunehmen. Dies ist auch deshalb notwendig, weil erfahrungsgemäß Durchführungsbestimmungen in der Praxis ohne Prüfung im Einzelfall als Arbeitsgrundlage angewendet werden.

Nach einigem Hin und Her scheint sich eine entsprechende Anpassung der DB-PKHG in Richtung einer datenschutzfreundlicheren Formulierung abzuzeichnen.

18.8 Mitteilungen in Zivilsachen (MiZi)

Der Landesbeauftragte hatte schon mehrfach Anlass, zu vorgesehenen Änderungen dieser Justizverwaltungsvorschrift Stellung zu nehmen.
Nach dem JuMiG (vgl. hierzu den III. Tätigkeitsbericht, Ziff. 21.2) sind aus Verfahren der streitigen Zivilgerichtsbarkeit und der freiwilligen Gerichtsbarkeit von Amts wegen Datenübermittlungen an öffentliche Stellen vorgesehen. Die MiZi dienen dazu, die Handhabung dieser Datenübermittlungsregelungen durch die Gerichte bundesweit zu vereinheitlichen; eine eigenständige rechtliche Grundlage für Übermittlungen sind sie nicht.

Vor einiger Zeit hatte das Justizministerium eines anderen Bundeslandes auf Anregung der Bundesnotarkammer vorgeschlagen, dass den Notarkammern schon die **Erhebung** von Feststellungsklagen wegen Amtspflichtverletzungen - neben den dazu ergangenen Entscheidungen oder geschlossenen Vergleichen - mitgeteilt werden sollten. Dagegen hatte sich auch der Landesbeauftragte gewandt. Denn zum einen sind - entsprechende Straftaten vorausgesetzt - bereits Hinweise über Verfehlungen,

z.B. an Finanzbehörden oder eben die Kammern der freien Berufe (Notare, Rechtsanwälte, Steuerberater, etc.) nach der korrespondierenden Verwaltungsvorschrift der Mitteilungen in Strafsachen (hier: Nrn. 23 oder 24) möglich. Zum anderen unterliegen Feststellungsbegehren besonderen Zulässigkeitsvoraussetzungen. Es ist nicht erforderlich, einer Notarkammer bereits Vorerwägungen und Details von später ggf. als unzulässig verworfenen Feststellungsklagen gegen Notare mitzuteilen.
Letztlich wurde die Regelung zwar dem Wunsch der Bundesnotarkammer folgend in die MiZi eingefügt, jedoch mit dem Zusatz, dass Anlagen zur Klageschrift in der Regel den Kammern nicht mit übersandt werden sollten.

Der Landesbeauftragte bedauert, dass bei den letzten Änderungen keine Regelung in die MiZi aufgenommen wurde, welche die Gerichte dazu anhält, Betroffene, deren Daten aus einem gerichtlichen Verfahren übermittelt wurden und die nicht von Amts wegen zu unterrichten waren, über den **Umstand**, dass eine solche Übermittlung veranlasst wurde, zu informieren.
Eine solche Festlegung würde den verfassungsrechtlichen Anspruch umsetzen, dass jeder Betroffene die Möglichkeit haben muss zu wissen, wer was, wann und bei welcher Gelegenheit über ihn weiß. Die derzeitige Antragsregelung läuft in der Praxis leer, da Betroffene regelmäßig nicht einmal wissen, dass ihre Daten übermittelt werden dürfen. Diese Gefahr war schon im Gesetzgebungsverfahren gesehen worden (vgl. BT-Drs. 13/7513).

18.9 Forderungssicherungsgesetz

Der Bundesrat hat erneut beschlossen, den o.g. Gesetzentwurf (BR-Drs. 902/02) in den Bundestag einzubringen. Einige der darin vorgesehenen Gesetzesänderungen erscheinen aus datenschutzrechtlicher Sicht bedenklich.

a) So soll durch einen neu einzufügenden § 750a ZPO einem Gläubiger die Möglichkeit eingeräumt werden, sich polizeilicher Fahndungshilfsmittel zu bedienen.
Auch unter Berücksichtigung der im Gesetzentwurf vorgesehenen Begrenzung der möglichen Fahndungsmittel bestehen bereits grundsätzliche Bedenken, Instrumentarien der Strafverfolgung zur Durchsetzung privater Forderungen einzusetzen.
Angesichts der Schwere eines solchen Eingriffs in das Grundrecht auf informationelle Selbstbestimmung ist auch die im Entwurf vorgesehene Festlegung eines letztlich immer willkürlich gewählten Betrages einer Mindestsumme als einzige Zugangsvoraussetzung zu polizeilichen Fahndungshilfsmitteln nicht ausreichend. Die insoweit vorgesehene Gleichstellung Privater mit rechtlich wesentlich enger gebundenen öffentlichen Gläubigern ist schwerlich zu rechtfertigen.

b) Ferner sieht der Entwurf vor, durch Einfügen eines neuen Absatzes 4 in § 39 StVG (Übermittlung von Fahrzeugdaten und Halterdaten zur Verfolgung von Rechtsansprüchen) die Auskunftsmöglichkeit auf privatrechtliche Titel zu erweitern.
Der bislang herrschende Grundsatz, dass Privatpersonen nur Auskunft aus dem Fahrzeugregister erhalten, wenn sie einen möglichen Rechtsanspruch im Zusammenhang mit der Teilnahme am Straßenverkehr darlegen können, wird damit durchbrochen. Die Abkehr von diesem Prinzip ist aus datenschutzrechtlicher Sicht problematisch, weil eine bisher zu Recht als sinnvoll erachtete Begrenzung des Auskunftsrechts aufgehoben werden soll.
Vergleichbar den Beschränkungen der Datenübermittlung aus dem Verkehrszentralregister hat der Gesetzgeber die Durchbrechung des Sozialgeheimnisses bislang ausschließlich zur Durchsetzung von öffentlich-rechtlichen Ansprüchen zugelassen.

c) Eine weitere Neuregelung soll bewährte Regeln des Sozialgeheimnisses aufbrechen und die Übermittlung von Daten über die Anschrift des Betroffenen und seine Aufenthaltsorte, die bei den Sozialversicherungsträgern unter einer konkreten Zweckbindung vorhanden sind, zur Vollstreckung privatrechtlicher Titel an Private freigeben.

Diese systemwidrige Veränderung der Datenübermittlungsregelungen im Sozialrecht würden nicht nur das Vertrauen in das Sozialgeheimnis untergraben, sondern auch zu gravierenden Verhaltensänderungen der Betroffenen führen. Deren Auswirkungen auf das Bürger-/Staatsverhältnis und die sozialen Sicherungssysteme sind kaum absehbar.

Über diese Bedenken, die von Landesbeauftragten anderer Länder geteilt werden, wurde das Ministerium der Justiz unterrichtet. Der Landesbeauftragte wird die weitere Entwicklung verfolgen.

18.10 Aktenaufbewahrungsgesetz für die Justiz

Bei Gerichten und Staatsanwaltschaften werden in beachtlichem Umfang Daten verarbeitet und genutzt. Diese reichen von reinen Adressdaten bis hin zu solchen Daten, welche von besonderer Sensibilität sind. Letzteres ist z.B. auch in Verfahren zur Bewilligung von Prozesskostenhilfe der Fall, in welchen quasi ein Finanzspiegel des Antragstellers entsteht.
Die Notwendigkeit für ein Gesetz, welches insbesondere die Aufbewahrung und Löschung regelt, wird bei den Justizministern nach jahrelangem Mahnen der Datenschutzbeauftragten des Bundes und der Länder durchaus gesehen. So hatten sie auf ihrer 72. Sitzung im Juni 2001 beschlossen, eine entsprechende Arbeitsgruppe einzusetzen, um einen Entwurf für ein Aufbewahrungsgesetz zu erarbeiten. Seit diesem Beschluss ist bisher nichts zur Umsetzung geschehen.

Auch der Landesbeauftragte hat diese Thematik immer wieder aufgegriffen (zuletzt im V. Tätigkeitsbericht, Ziff. 16.6). Nur eine normative Regelung entspricht der Forderung des Bundesverfassungsgerichts, dass durch Rechtsnorm eindeutig festgelegt werden muss, für welchen Zweck und wie personenbezogene Daten durch öffentliche Stellen verarbeitet und genutzt werden dürfen. Verwaltungsvorschriften reichen hierfür nicht.

Auch wenn dem Landesbeauftragten inzwischen bekannt wurde, dass ein entsprechender Gesetzentwurf auf den Weg gebracht worden sein soll, hält er einen erneuten Hinweis auf die Forderung der Datenschutzbeauftragten des Bundes und der Länder nach einem solchen Gesetz für notwendig.

18.11 Insolvenz und Zwangsversteigerungen im Internet

Die Insolvenzordnung regelt nicht nur die Eröffnung des Insolvenzverfahrens oder die Anordnung von Verfügungsbeschränkungen. Diese für den einzelnen schon gravierenden Entscheidungen sind nach diesem Gesetz darüber hinaus **öffentlich** bekannt zu machen, um anderen Teilnehmern am Geschäftsverkehr zu ermöglichen, sich auf die Insolvenzsituation des Betroffenen einzustellen.
Zur Klarstellung: Die Regelungen können nicht nur juristische Personen betreffen, sondern in gleicher Weise - insbesondere im Rahmen eines Verbraucherinsolvenzverfahrens - jedermann.

Bisher erfolgten derartige Bekanntmachungen in Papierform, vor allem in Zeitungen. Zwecks Kostenreduktion wie auch zur erleichterten Wahrnehmbarkeit für Interessierte wurde durch eine Novellierung der Insolvenzordnung und einer auf diesem Gesetz fußenden Rechtsverordnung die Möglichkeit geschaffen, die notwendigen Bekanntmachungen auch im Internet vorzunehmen.
Ökonomische Vorteile sind aber in einem Rechtsstaat nicht die einzige Messlatte. Der Landesbeauftragte hält - wie seine Kollegen - diese Form der Veröffentlichung schon im Grundsatz für problematisch. Das Internet war und ist für solche Zwecke nicht konzipiert, insbesondere lässt sich der Informationsfluss weder geografisch noch qualitativ adäquat steuern, geschweige denn begrenzen.
Informationen, einmal im Internet, sind nicht mehr rückholbar. Die Einstellung ins Internet führt außerdem regelmäßig zu einer Übermittlung in das Ausland - insbesondere auch in solche Länder, in denen die Menschenrechte und damit auch der Schutz personenbezogener Daten eine zu vernachlässigende bzw. unbeachtete Größe sind. Daher lassen die Datenschutzgesetze des Bundes und der Länder mit Recht solche Übermittlungen insbesondere durch öffentliche Stellen nur in wenigen Fällen und unter engen Voraussetzungen zu.

Die Datenschutzbeauftragten des Bundes und der Länder haben im Rahmen einer Entschließung vom 24.04.2001 **(Anlage 2)** auf die Risiken dieser Bekanntmachungsform hingewiesen und besondere Maßnahmen zum Schutz der Betroffenen eingefordert.
Die Hinweise wurden im Gesetzgebungsverfahren berücksichtigt und haben letztlich Niederschlag in der im Februar 2002 erlassenen Bekanntmachungsverordnung gefunden.

Die grundsätzliche Problematik besteht in gleicher Weise bei Veröffentlichungen von Zwangsversteigerungen im Internet. Hier sollten zumindest ähnliche Begrenzungsregelungen im ZVG getroffen werden, wie sie in der Bekanntmachungsverordnung vorgesehen sind. So wäre es bereits unter geltendem Recht möglich, datenschutzgerecht zu verfahren, indem § 38 ZVG verfassungskonform ausgelegt und auf die Benennung des Grundstückeigentümers bei der Bekanntmachung eines Versteigerungstermins in der Regel verzichtet würde.

Der Landesbeauftragte geht davon aus, dass die Landesregierung seine Bedenken und Anregungen im Rahmen von Rechtssetzungsverfahren auch durch eigene Initiativen adäquat berücksichtigen wird.

19. Schulen

19.1 Einsichtsfähigkeit Minderjähriger

Im V. Tätigkeitsbericht (Ziff. 8.1) hat der Landesbeauftragte zur Frage der Einwilligung in die PISA-Studie der OECD darauf hingewiesen, dass Schülerinnen und Schüler mit zunehmendem Alter ein eigenständiges Zustimmungsrecht (je nach Einsichtsfähigkeit) haben.
Das Problem der Einsichtsfähigkeit minderjähriger Schüler und die Befugnis zur eigenverantwortlichen Ausübung des Rechtes auf informationelle Selbstbestimmung wird häufig erörtert. Gelegentlich wird angenommen, dass minderjährige Schüler in Anlehnung an die Religionsmündigkeit ab 14 Jahren regelmäßig über die erforderliche Einsichtsfähigkeit verfügen, selbst über die Preisgabe Ihrer personenbezogenen Daten in solch einer Studie zu entscheiden.

Hierzu ist auf folgendes hinzuweisen:
Die Rechte minderjähriger Schülerinnen und Schüler auf Auskunft, Einsicht in Unterlagen, Berichtigungen, Sperrungen oder Löschungen von Daten werden nach § 84a Abs. 4 Satz 1 Schulgesetz durch deren Erziehungsberechtigte ausgeübt. Darüber hinaus ist für die Einwilligung in die Erhebung und Verarbeitung personenbezogener Daten zu beachten, dass auch das minderjährige Kind Grundrechtsträger ist und damit Anspruch auf Achtung seiner Menschenwürde und Entfaltung seiner Persönlichkeit hat. Eine Einschränkung dieser Grundrechtsausübung durch das Eltern-

recht ist daher nur insoweit zulässig, als dies die Hilfs- und Schutzbedürftigkeit des Minderjährigen erfordert. Das Elternrecht muss seinem Wesen und Zweck nach gegenüber der Grundrechtsausübung des Minderjährigen zurücktreten, wenn der Minderjährige eine genügende Reife zur selbständigen Beurteilung der Lebensverhältnisse und zum eigenverantwortlichen Auftreten im Rechtsverkehr erlangt hat. Maßgeblich ist die individuelle Einsichtsfähigkeit. Mit der notwendigen Einzelfallabwägung lässt sich die pauschale Annahme einer **generellen** Einsichtsfähigkeit ab 14 Jahren nicht vereinbaren.
Eine Beteiligung der Eltern kommt im Hinblick auf das Elternrecht immer dann in Betracht, wenn die Einsichtsfähigkeit des Minderjährigen im konkreten Einzelfall nicht zweifelsfrei festgestellt werden kann.

19.2 Übermittlung von Lehrerdaten an die Kirchen

Zur Sicherstellung des Religionsunterrichtes wurde geprüft, ob Anschriften von Lehrern von der Schulverwaltung an eine Kirche übermittelt werden dürfen. Die Kirche wollte die Lehrer, die die staatliche und kirchliche Lehrbefähigung haben, jedoch in anderen Fächern unterrichten, motivierend ansprechen. Das Kultusministerium hatte datenschutzrechtliche Bedenken, die vom Landesbeauftragten bestätigt wurden.
Eine bereichsspezifische Rechtsgrundlage für die Übermittlung von Personaldaten von Lehrkräften war für diese Datenübermittlung nicht ersichtlich. Auch allgemeine Regelungen auf verfassungsrechtlicher Grundlage zur gemeinsamen Verantwortung für den Religionsunterricht waren als reine Aufgabenzuweisungen nicht ausreichend.
Auch eine sog. Widerspruchslösung (Mitteilung der Schulverwaltung an die Lehrkräfte, dass die Adressen an die Kirche übermittelt werden, falls nicht rechtzeitig ein Widerspruch eingeht) wurde geprüft. Ohne Rechtsgrundlage sind aber Datenübermittlungen an Dritte nach einem allgemeinen und in § 4 Abs. 1 DSG-LSA normierten Grundsatz lediglich bei Vorliegen der Einwilligung der Betroffenen zulässig. Die Widerspruchslösung wird dem Erfordernis einer ausdrücklichen, informierten Einwilligung (§ 4 Abs. 2 DSG-LSA) deshalb nicht gerecht.
In Gesprächen konnten jedoch drei Lösungsmöglichkeiten aufgezeigt werden, an denen sich Kirche und Kultusministerium orientieren können.

19.3 Offenbarung von Gesundheitsdaten in einem Elternbrief

Anlässlich einer Umgebungsuntersuchung im Rahmen von Ermittlungen nach dem Infektionsschutzgesetz wurde festgestellt, dass ein Schüler einer Grundschule an einer meldepflichtigen Krankheit litt.

Daraufhin wandte sich das Gesundheitsamt mit der Bitte um Angabe der vermutlichen Kontaktpersonen (Namen und Adressen der Schüler der entsprechenden Klasse) an die Schulleiterin. Diese Datenübermittlung, die nach den Vorschriften des Infektionsschutzgesetzes zulässig war, erfolgte

umgehend. Auch wurde auf Bitten der Schulleitung eine Informationsveranstaltung in Zusammenarbeit mit dem Gesundheitsamt in der Schule durchgeführt.
Darüber hinaus verfasste die Schulleiterin einen Brief an alle Eltern, in dem auf die besondere Situation und die erforderlichen Schutzmaßnahmen hingewiesen wurde. Im Rahmen des Elternbriefes wurde aber leider auch der Name des erkrankten Schülers und die Klasse genannt.
Der Vater, der diesen Elternbrief erhielt, war darüber nicht erbaut und wandte sich an den Landesbeauftragten mit der Bitte um Prüfung.

Die Angabe einer Erkrankung im Zusammenhang mit dem Namen des Erkrankten zählt zu den personenbezogenen Daten besonderer Art nach § 2 Abs. 1 Satz 2 DSG-LSA. Eine solche Offenlegung war deshalb nur auf gesetzlicher Grundlage zulässig (vgl. § 38 Abs. 8 InfSchG) oder mit ausdrücklicher Einwilligung des Betroffenen (hier: der Eltern als Erziehungsberechtigte). Beides lag nicht vor.
Die Schulleiterin wurde entsprechend belehrt.

19.4 Ehrenamtliche Tätigkeit im Prüfungsausschuss gem. § 37 Abs. 3 BBiG

Auf der Grundlage des § 37 Abs. 3 BBiG war ein Lehrer durch das zuständige Staatliche Schulamt gegenüber der Industrie- und Handelskammer (IHK) als Mitglied des Prüfungsausschusses vorgeschlagen worden. Als er in dem Ausbildungsberuf, für den er als Prüfer benannt worden war, nicht mehr unterrichtend tätig war, teilte das Staatliche Schulamt dies ohne sein Wissen der IHK mit und benannte ein Ersatzmitglied. Der Lehrer beklagte sich beim Landesbeauftragten über die Übermittlung der Information.

Die Beschwerde des Petenten war begründet. Das Berufsbildungsgesetz selbst enthält keine normenklare Regelung, wann und in welchem Umfang in einem solchen Fall des Unterrichtswechsels personenbezogene Daten des betroffenen Lehrers übermittelt werden dürfen. Demgemäß gelten die allgemeinen datenschutzrechtlichen Regelungen des § 11 DSG-LSA. Für die Rechtmäßigkeit der Datenübermittlung kam es daher entscheidend darauf an, ob die Mitteilung aus Sicht des Staatlichen Schulamtes für die Entscheidung der IHK erforderlich war oder nicht. Da seitens der IHK rechtlich einwandfrei entschieden wurde, dass der Lehrer nicht sofort mit dem Wechsel des Unterrichtsfaches seine Sachkunde und damit seine Befähigung zum Prüfer verliert, war die Mitteilung des Staatlichen Schulamtes - streng rechtlich gesehen - nicht erforderlich. Die Rechtsauslegung und -anwendung der IHK war jedoch dem Staatlichen Schulamt nicht bekannt. Das hatte - in Unkenntnis der Auswahlkriterien der IHK - die Erforderlichkeit der Datenübermittlung schlicht falsch bewertet.

Der Landesbeauftragte hat der IHK empfohlen, eine grundsätzliche Klärung bezüglich der Sachkunde eines Lehrers, der in Prüfungsausschüssen

der IHK mitarbeitet, in Zusammenarbeit mit den Vertretern der Schulämter vorzusehen. Dann entfallen künftig solche Mitteilungen, die einen Eingriff in das Grundrecht des Betroffenen nach Artikel 6 Abs. 1 LVerf darstellen.

19.5 Vortragsangebot an Gymnasien

Die Datenschutzbeauftragten des Bundes und der Länder haben anlässlich ihrer letzten bundesweiten Umfrage-Studie ("Der gläserne Konsument - die Zukunft von Datenschutz und Privatsphäre in einer vernetzten Welt") erfahren, dass ein besonderes Problem in der Unkenntnis vieler Bürgerinnen und Bürger über ihre Grundrechte besteht.
Dies trifft auch auf das Recht auf informationelle Selbstbestimmung zu. Nicht einmal 1/3 der Bevölkerung (28 %) gibt an, schon einmal von den Medien über ihre Rechte informiert worden zu sein. Zwei von fünf Befragten (37 %) wurden erst durch die Studie auf ihr "gesetzliches Widerspruchsrecht" (z.B. in § 4 des DSG-LSA) aufmerksam gemacht. Dies traf vor allem auf die jüngeren Bürgerinnen und Bürger zu.
Aufgrund dieses Ergebnisses hat der Landesbeauftragte sich entschlossen, bei den jüngeren Staatsbürgern anzusetzen und zunächst den Gymnasien des Landes in den Jahrgangsstufen 11 und 12 Referate im Unterricht zum Thema "Datenschutz und seine verfassungsrechtlichen Grundlagen" angeboten.

Das Echo war dürftig. Von bisher 28 angeschriebenen Schulen erhielt der Landesbeauftragte leider nur zwei Rückmeldungen. Der Landesbeauftragte hofft, dass noch mehr Schulen dieses Angebot nutzen werden.

19.6 Nutzung des Internets

In immer mehr Schulen wird das Medium Internet als Unterrichtsmittel eingesetzt, da dem Erlangen von Medienkompetenz in der heutigen Gesellschaft eine große Bedeutung zukommt. Bereits in seinen bisherigen Tätigkeitsberichten (III. Tätigkeitsbericht, Ziff. 23.2; V. Tätigkeitsbericht, Ziff. 17.1) hat der Landesbeauftragte dazu Hinweise gegeben bzw. auf die Risiken und Gefahren hingewiesen, die beim Anschluss von Schulnetzen an das Internet bestehen.
Entscheidend für die datenschutzrechtlichen Anforderungen ist auch die jeweilige **Nutzungsform**. So kann die Schule ihren Schülern neben der ausschließlichen Nutzung für schulische Zwecke auch die private Nutzung des Internets außerhalb des Unterrichts gestatten, oder sie kann sich mit einer eigenen Homepage im Internet präsentieren.

Nutzung ausschließlich für schulische Zwecke
Ist die Nutzung des Internet ausschließlich für schulische Zwecke gestattet, so ist die Schule gegenüber den Lehrern und Schülern **nicht** Anbieter im Sinne des TKG. Die Erhebung und Verarbeitung von Verbindungs- und Inhaltsdaten, d.h. von Daten, die über das Nutzungsverhalten der Lehrer

und Schüler Auskunft geben, richtet sich für Lehrer nach den einschlägigen Vorschriften des BG LSA bzw. DSG-LSA und für Schüler nach den Vorschriften des § 84a SG i.V.m. dem DSG-LSA.
Da der Schule und insbesondere dem verantwortlichen Lehrer eine Kontroll- und Aufsichtspflicht obliegt, muss durch geeignete Mittel verhindert werden, dass die Schüler im Internet z.B. Informationen mit jugendgefährdendem oder strafrechtlichem Inhalt abrufen. Diese Kontrolle sollte sich jedoch gem. § 1 Abs. 2 DSG-LSA am Grundsatz der Datenvermeidung und Datensparsamkeit orientieren: So ist beispielsweise der Einsatz von Filtersystemen zusammen mit der unmittelbaren Kontrolle durch den aufsichtsführenden Lehrer einer nachlaufenden Kontrolle durch Protokollierung aller Zugriffe vorzuziehen.

Daten, die zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert wurden, unterliegen gem. § 10 Abs. 4 DSG-LSA einer **engen** Zweckbindung, d.h. sie dürfen **nur** für diese Zwecke und nicht etwa zu einer Verhaltens- und Leistungskontrolle verwendet werden.

Grundsätzlich empfiehlt der Landesbeauftragte, in einer Nutzungsordnung festzulegen, in welchem Umfang eine Protokollierung und Auswertung erfolgt und welche Sanktionen ein Missbrauch zur Folge hat. Des Weiteren empfiehlt sich, in der Nutzungsordnung festzulegen, dass es sich bei der Benutzung von E-Mails **ausschließlich** um eine schulische Nutzung handelt und der verantwortliche Lehrer daher von deren Inhalt Kenntnis nehmen darf. Wird dies nicht festgelegt und handelt es sich im Einzelfall um eine **private** E-Mail, wird bei der Kenntnisnahme durch den Lehrer oder die Schulleitung das Fernmeldegeheimnis (§ 85 TKG) verletzt.

Private Nutzung außerhalb des Unterrichts
Bietet die Schule ihren Schülern die Möglichkeit, Internetdienste und E-Mail auch außerhalb des Unterrichts – also **privat** – zu nutzen, so muss sie **als Anbieter** im Sinne der TKG sowohl das Fernmeldegeheimnis als auch die Vorschriften der TDSV beachten. Eine Zugriffsprotokollierung im Rahmen der auch außerhalb des Unterrichts bestehenden Aufsichtspflicht wäre dann unzulässig, da die TDSV eine Speicherung dieser Verbindungsdaten nur zu Zwecken der **Abrechnung** (§ 6 Abs. 2 TDSV) oder nach **Einwilligung** des Nutzers (§ 3 Abs. 1 TDSV) vorsieht.
Da an den Schulen im Allgemeinen keine Abrechnung erfolgt, empfiehlt der Landesbeauftragte - neben der Festlegung konkreter Regelungen in einer Nutzungsordnung -, von jedem Schüler (bei Minderjährigen bis zum Erreichen der Einsichtsfähigkeit von den Erziehungsberechtigten, s. Ziff. 19.1) eine **Einwilligungserklärung** einzuholen, die die Protokollierung im erforderlichen Umfang und eine stichprobenhafte Auswertung dieser Protokolle zur Wahrnehmung von Aufsichts- und Kontrollpflichten gestattet. Aufgrund des Fernmeldegeheimnisses sollte in der Einwilligungserklärung konkret festgelegt werden, unter welchen Umständen welche

Personen vom Inhalt privater E-Mails Kenntnis nehmen dürfen. Allerdings ist auch bei der außerschulischen Nutzung der eingangs genannte Grundsatz der Datenvermeidung und -sparsamkeit zu beachten.

Kann infolge der konkreten Gestaltung die rein schulische und die private Nutzung faktisch nicht getrennt werden, unterliegt die Gesamtnutzung dem Fernmeldegeheimnis.

Veröffentlichung eines Internetangebotes (Homepage)
Mit der Veröffentlichung eines Internetangebotes unterliegt die Schule als **Tele- bzw. Mediendiensteanbieter** einer Reihe von gesetzlichen Verpflichtungen. Dabei ist die Einordnung, ob es sich bei dem jeweiligen Angebot um einen Tele- oder einen Mediendienst handelt, unerheblich, da die Regelungen des TDG bzw. TDDSG und des MDStV in den wesentlichen Punkten identisch sind.
Einige Anforderungen an Internetangebote wie die Anbieterkennzeichnung, die datenschutzrechtliche Unterrichtung der Nutzer und die Kennzeichnung externer Links sollen im Folgenden kurz erläutert werden:

1. **Anbieterkennzeichnung (Impressum)**
   Gemäß § 6 TDG bzw. § 10 Abs. 2 MDStV hat die **Schule** als Anbieter von Tele- bzw. Mediendiensten folgende Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten:
   - Name und Anschrift
   - Angaben, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation ermöglichen, einschließlich der Adresse der elektronischen Post (E-Mail).

   Schülereigene Homepages, die im Rahmen von Arbeitsgemeinschaften oder auch privat erstellt und veröffentlicht werden, stehen, ähnlich wie Schülerzeitungen gem. § 54 Abs. 3 SG, außerhalb der Verantwortung der Schule. Darauf muss dann auch im Impressum hingewiesen werden.

2. **Datenschutzrechtliche Unterrichtung (Datenschutzhinweis, Datenschutz-Policy)**
   Gemäß § 4 Abs. 1 TDDSG bzw. § 18 Abs. 1 MDStV hat die Schule als Diensteanbieter den Nutzer **zu Beginn** des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu unterrichten. Die Unterrichtung muss jederzeit abrufbar sein.

   Auch wenn ein Internetangebot keine Formulare enthält, in die ein Nutzer personenbezogene Daten eintragen könnte, so wird doch in vielen Fällen bei der Protokollierung der Zugriffe auf das Internetangebot die **IP-Adresse des Nutzers** gespeichert. Aus der IP-Adresse, die meist dynamisch vergeben wird, kann zwar nicht direkt auf den

Nutzer geschlossen werden, mit zusätzlichen Informationen ist jedoch eine Identifizierung des Nutzers möglich. Somit handelt es sich bei dessen IP-Adresse um ein **personenbezogenes** Datum, wenn diese eine **natürliche** Person bezeichnet.

Zwar darf der Diensteanbieter gem. § 6 Abs. 1 TDDSG bzw. § 19 Abs. 2 MDStV personenbezogene Daten eines Nutzers ohne dessen Einwilligung erheben, verarbeiten und nutzen, soweit dies erforderlich ist, um die Inanspruchnahme des Dienstes zu ermöglichen (Nutzungsdaten), allerdings gilt dies gem. § 6 Abs. 4 TDDSG bzw. § 19 Abs. 5 MDStV über das Ende des Nutzungsvorgangs hinaus **nur** für Zwecke der Abrechnung, d.h. bei **kostenlosen** Internetangeboten sind die Nutzungsdaten einschließlich der IP-Adresse nach Ende des Nutzungsvorgangs **zu löschen**.

Der Landesbeauftragte empfiehlt, die datenschutzrechtliche Unterrichtung des Nutzers bereits beim Aufruf des Angebotes z.B. durch einen Link „Datenschutz-Hinweis“ auf der Startseite vorzunehmen. Da es sich bei Internetangeboten von Schulen in der Regel um **kostenlose** Informationsangebote handelt, ist der Nutzer darüber zu informieren, dass nach Ende der Nutzung dieses Angebotes **keine** personenbezogenen Daten gespeichert werden.

3. Kennzeichnung externer Links

Gemäß § 4 Abs. 5 TDDSG bzw. § 18 Abs. 5 MDStV ist dem Nutzer die Weiterleitung zu einem anderen Diensteanbieter anzuzeigen. Dies kann z.B. durch die Kennzeichnung dieser fremden Links mit **[Externer Link]** erfolgen. Der Nutzer soll damit darauf hingewiesen werden, dass er nun das Angebot der jeweiligen Schule verlässt.

Werden auf der schuleigenen Homepage Links zu fremden Angeboten bereitgestellt, so sollte darauf hingewiesen werden, dass sich die Schule bei Einrichtung des Links von der Rechtmäßigkeit der Inhalte überzeugt hat, allerdings keine Haftung übernommen wird, da nicht auszuschließen ist, dass die Inhalte mittlerweile verändert wurden.

Veröffentlichung personenbezogener Daten im Internet

Die Veröffentlichung von Lehrer- oder Schülerdaten bzw. Daten ehemaliger Schülerinnen und Schüler sowie Lehrkräfte etc. im Internet kommt einer Übermittlung ins **Ausland** gleich.
Da die diesbezüglichen Voraussetzungen des § 13 Abs. 1 DSG-LSA in der Regel nicht gegeben sind, kommt eine Veröffentlichung nur infrage, wenn Betroffene ihre Einwilligung gem. § 13 Abs. 2 Satz 3 Ziff. 1 DSG-LSA zur Veröffentlichung im Internet erklärt haben.
Für eine Einwilligung sind dabei die Bestimmungen des § 4 Abs. 2 DSG-LSA, die sog. "informierte Einwilligung", bzw. bei elektronischer Einwilligung § 4 Abs. 3 DSG-LSA zu beachten. Gerade bei der Einstellung per-

sonenbezogener Daten im Internet muss ein Betroffener über die Risiken einer weltweiten Veröffentlichung informiert werden.
Vor der Einstellung von personenbezogenen Daten sollte deshalb der **Datenschutzbeauftragte der Schule** beteiligt werden, um die Einhaltung der gesetzlichen Rahmenvorgaben zu unterstützen.

Über Gefahren bei der automatisierten Datenverarbeitung, u.a. bei der Internetnutzung, dem E-Mail-Einsatz und insbesondere durch Computerviren, hat der Landesbeauftragte bereits seit seinem III. Tätigkeitsbericht, Ziff. 13, und im IV. Tätigkeitsbericht, Ziff. 13.3, informiert. In diesem Tätigkeitsbericht verweist er auf die Ziffn. 12.1 bis 12.3 und Ziff. 12.5.

20. Sozialwesen

20.1 Mitwirkungspflichten der Antragsteller

Ein Petent beklagte sich darüber, dass ein Sozialamt die Gewährung von Hilfe zum Lebensunterhalt nach dem BSHG unter Hinweis auf die Mitwirkungspflicht von der Ausfüllung eines umfänglichen Zusatzfragebogens und einer Erklärung abhängig machte. Dieser Zusatzfragebogen verlangte neben Name und Vorname u.a.: Anschrift, EG-Ausländer(in), Bürgerkriegsflüchtling, Daten zum Erwerbsstatus, zu besonderen sozialen Situationen (z.B. Scheidung, Freiheitsentzug, Suchtabhängigkeit) und umfängliche Daten zum Schul- und zum Berufsabschluss.
Die "Erklärung über die Entbindung von der Schweigepflicht sowie datenschutzrechtliche Einwilligung" sollte die Erteilung von Auskünften und die Vorlage von Unterlagen gestatten sowie als datenschutzrechtliche Einwilligung gelten.

Der Landesbeauftragte hat das Sozialamt darauf hingewiesen, dass die Bedenken des Petenten gegen die Ausfüllung der Formulare zu Recht bestanden. Zwar trifft den Antragsteller bei Sozialhilfeleistungen nach §§ 60 ff SGB I eine Mitwirkungspflicht (vgl. dazu III. Tätigkeitsbericht, Ziff. 24.6), insbesondere sind die Voraussetzungen für die Leistung von Sozialhilfe darzulegen und ggf. nachzuweisen. Die Pflicht zur Beantwortung besteht jedoch nur, soweit dies für die Bearbeitung der beantragten Leistung erforderlich ist.
Die im Zusatzfragebogen abgefragten Daten dienten der Erstellung der Sozialhilfestatistik. Insoweit besteht zwar eine Auskunftspflicht, jedoch nur bezüglicher bestehender Leistungen, nicht für beantragte, und diese richtet sich zudem nicht an den Antragsteller, sondern an den Träger der Sozialhilfe.

Auch die Zustimmung zur Erteilung von Auskünften durch Dritte fordert § 60 Abs. 1 Satz 1 Nr. 1 SGB I nur, soweit die Auskünfte erforderlich sind. Dies ist im konkreten Einzelfall für die jeweils begehrte Auskunft zu prüfen.

Eine pauschale Zustimmung mit einer noch darüber hinausgehenden, inhaltlich zudem unbestimmten Einwilligungserklärung findet im Gesetz keine Grundlage.
Der Sozialleistungsträger hat sein Vorgehen geändert.

20.2 Datenerhebung bei Dritten

Leider werden dem Landesbeauftragten immer wieder Fälle bekannt, in denen die öffentlichen Stellen unzulässigerweise personenbezogene Daten bei Dritten erheben. Dem steht der datenschutzrechtliche Grundsatz entgegen, dass personenbezogene Daten grundsätzlich beim Betroffenen zu erheben sind. Der Grundsatz ist verfassungsrechtlich vorgegeben und in vielen Fachgesetzen ausdrücklich formuliert (vgl. u.a. § 67a Abs. 2 SGB X, § 9 Abs. 2 DSG-LSA). Diese Regelungen gewährleisten, dass der Betroffene jederzeit weiß, welche öffentliche Stelle was wann über ihn weiß.

So wurde der Landesbeauftragte durch eine Eingabe darauf aufmerksam, dass ein Sozialamt zur Überprüfung der Einkommensverhältnisse des Leistungsempfängers dessen Arbeitgeber befragte. Dies führte faktisch dazu, dass die dem Sozialgeheimnis unterliegende Information, Sozialhilfeempfänger zu sein, dem Arbeitgeber unzulässig bekannt wurde. Die Datenerhebung beim betroffenen Sozialhilfeempfänger hätte hier vollkommen genügt. Der Betroffene hatte auch auf die gleichzeitig auch an ihn gerichtete Anfrage reagiert.
Auf die Hinweise des Landesbeauftragten hat das Sozialamt umgehend Maßnahmen getroffen, um die unzulässige Datenerhebung bei Dritten künftig zu unterbinden.

20.3 Hausbesuch durch das Jugendamt

Im V. Tätigkeitsbericht (Ziff. 18.1) wurde die Amtsleiterin eines Jugendamtes erwähnt, die wegen ihrer unzureichenden Rechtskenntnisse aufgefallen war. Es ist mehr als bedenklich, dass in jenem Jugendamt offenbar noch immer keine Zeit gefunden wurde, die gesetzlichen Grundlagen zur Kenntnis zu nehmen, die Art und Umfang des Tätigwerdens gegenüber dem Bürger gestatten. So ließ eine neue Beschwerde über das Amt nicht lange auf sich warten.

Mit einem DIN A 5 großen Notizzettel im Briefkasten der Beschwerdeführerin unter dem Aufdruck "Landkreis..... Der Landrat" ohne Angabe des Amtes bzw. des Aktenzeichens wurde ein Hausbesuch angekündigt. Lediglich ein Name und eine Durchwahlnummer waren angegeben. Der Mitarbeiter schrieb kurz handschriftlich, dass er sich zur Klärung eines Sachverhalts zu einem bestimmten Termin zum Hausbesuch anmelden möchte.

Erst auf wiederholte Anfrage der Betroffenen teilte der Mitarbeiter mit, dass er für das Jugendamt tätig sei und einem anonymen Hinweis nach-

gehe, wonach das Kind der Beschwerdeführerin von der betreuenden fremden Person nicht ausreichend versorgt werde.

Die Überprüfung des Falls ergab erneut erhebliche fachliche Defizite beim Vorgehen des Jugendamtes. Leitung und Mitarbeiter des Amtes konnten auch auf wiederholte und eingehende Nachfrage nicht darlegen, zur Erfüllung welcher Aufgabe auf welcher rechtlichen Grundlage welche Informationen konkret für erforderlich gehalten worden waren.

Das Jugendamt hätte insbesondere die Vorschriften des SGB VIII zur Datenerhebung, -verarbeitung und -nutzung beachten müssen. Danach ist auf die Rechtsgrundlage der Informationserhebung hinzuweisen und die konkrete Informationserhebung hätte sich am Grundsatz der Erforderlichkeit orientieren müssen. Selbstverständlich hätte sich aus der Besuchsankündigung auch das handelnde Amt ergeben müssen.

Dem Landrat wurde daher empfohlen, geeignete Maßnahmen zu ergreifen, um den Mitarbeitern endlich die gesetzlichen Grundlagen ihrer Tätigkeit näher zu bringen.

20.4 Hausbesuch durch Sozialhilfeermittler

Durch eine Eingabe wurde bemängelt, dass Mitarbeiter des Sozialamtes wiederholt und eindringlich Hausbesuche ankündigten. Anlass war der wiederholte Antrag auf finanzielle Leistungen für ein Möbelstück.

Es wurde festgestellt, dass die Maßnahmen in diesem Einzelfall jedenfalls im Ergebnis vertretbar waren. Es bestand aufgrund der vorherigen Leistung Anlass, die Bedarfssituation als Voraussetzung für eine weitere Leistungsbewilligung vor Ort zu überprüfen.

Der Landesbeauftragte hatte jedoch in diesem und anderen Fällen den Eindruck, dass die rechtlichen Grundlagen für Hausbesuche von Sozialhilfeermittlern nicht ausreichend bekannt sind. Er weist deshalb noch einmal auf deren Grundlagen hin:

Der Einsatz von Sozialhilfeermittlern ist aus datenschutzrechtlicher Sicht nur zulässig, wenn dieser besondere Weg der Datenerhebung erforderlich und verhältnismäßig ist. Die Verhältnismäßigkeit setzt voraus, dass die Erhebung der erforderlichen Informationen durch weniger eingreifende, andere Ermittlungsmethoden nicht möglich ist oder die Beratung der auf Hilfe angewiesenen Bürger im Einzelfall diese Form zwingend erfordert. Voraussetzung eines **Hausbesuches** sind konkrete Anlässe, ggf. konkrete Anhaltspunkte für die Notwendigkeit der Überprüfung von Angaben sowie ein genau definierter Auftrag. Der Besuch eines Ermittlers zur Verdachtsfindung ist - mangels Erforderlichkeit - unzulässig. Die Betroffenen sind darauf hinzuweisen, dass keine rechtliche Verpflichtung zur Gewährung des Zutritts in die Wohnung besteht.

Stets ist der Zweck des Besuches zu erläutern. Besteht nach dem Gesetz eine Auskunftspflicht, ist auf die entsprechende Rechtsvorschrift, die Voraussetzungen für die Gewährung von Rechtsvorteilen sowie die Folgen der Verweigerung von Angaben hinzuweisen. Besteht keine Auskunftspflicht, ist auf die Freiwilligkeit der Angaben hinzuweisen (§ 67a Abs. 3 Satz 3 SGB X).

20.5 Anforderung von Patientenunterlagen durch eine Betriebskrankenkasse

Bereits im V. Tätigkeitsbericht (Ziff. 18.7) hatte der Landesbeauftragte darauf hingewiesen, dass die Anforderung von Patientenunterlagen durch Krankenkassen bei den Krankenhäusern unzulässig ist. Besonders eine Betriebskrankenkasse fiel durch besondere Hartnäckigkeit in diesem Punkt auf.
Die Anforderung verstößt eindeutig gegen § 301 SGB V. Dort ist enumerativ festgelegt, welche Daten von den Krankenhäusern an Krankenkassen zu übermitteln sind.

Diesem rechtswidrigen Verfahren hat das Bundessozialgericht mit seiner Entscheidung vom 23.07.2002 - B 3 KR 64/01 R - endgültig einen Riegel vorgeschoben. In der Entscheidung wird sowohl die Anforderung von Patientenunterlagen wie auch die Zurückbehaltung des dem Krankenhaus zustehenden Entgeltes für unzulässig erklärt.

20.6 Datenerhebung durch einen Pflegedienst auf Veranlassung des MDK

Aufgrund der Beschwerde eines Pflegedienstes, dass der MDK ohne Rechtsgrundlage Listen über Pflegebedürftige abfordere und dadurch personenbezogene Daten unzulässig erhebe, wurde eine Kontrolle beim MDK durchgeführt.

Bei der Kontrolle wurde festgestellt, dass der Vorwurf berechtigt war. Der MDK forderte von den Pflegediensten nicht nur Daten von Pflegebedürftigen, für die kein Prüfauftrag der zuständigen Pflegekasse vorlag, sondern auch Einzelangaben (z.B. Familienstand), deren Abforderung gesetzlich nicht zugelassen ist. Des Weiteren wurden Daten von privat Versicherten abgefordert, für die der MDK gar nicht zuständig ist.
Grundlage war eine selbst erstellte Prüfanleitung. Den Mitarbeitern des MDK war nicht klar, dass eine solche Anleitung auch gegenüber gesetzlich versicherten Mitgliedern keine **gesetzliche** Grundlage darstellt, um personenbezogene Informationen bei Dritten abzurufen.
Warum der MDK auf die Angabe der Religion der Petenten bei einem ambulanten, nicht konfessionellen Pflegedienst Wert legte, war ebenfalls unerfindlich.

Die unzulässig erhobenen Daten wurden gelöscht und die ohne Rechtsgrundlage abgeforderte Liste der Pflegebedürftigen an den Pflegedienst zurückgegeben.

20.7 Personaldaten von Pflegefachkräften

Bei den Leistungserbringern treten in der letzten Zeit vermehrt Irritationen im Zusammenhang mit der Erhebung bzw. Übermittlung personenbezogener Daten von Mitarbeitern in Pflegeeinrichtungen auf. So wurde beispielsweise gefordert, dass bei Neueinstellungen, Entlassungen und Personenstandsänderungen (!) eine vollständig ausgefüllte Personalbestandsanzeige an die Aufsichtsbehörde zu senden sei.

Sicherlich ist aufgrund von Vorfällen in den letzten Jahren verständlich, dass die Aufsichtsbehörden ihrer Kontrolltätigkeit in Altenpflegeeinrichtungen intensiver nachkommen und damit auch im Interesse der Heimbewohner handeln. Dass aber Geburtsdatum und Privatanschrift der dort eingesetzten Pflegekräfte ohne gesetzliche Grundlage gefordert werden, erschien dem Landesbeauftragten doch bemerkenswert. Eine Einwilligungserklärung der betroffenen Mitarbeiter zur Übermittlung der personenbezogenen Daten lag der Beschäftigungsstelle nicht vor.

§ 12 Abs. 1 Ziffern 4 und 5 Heimgesetz fordern bei der Anzeige der Betriebsaufnahme die vorgesehene Anzahl der Mitarbeiterstellen, den Namen, die berufliche Ausbildung und den Werdegang der **Heimleitung** und bei Pflegeheimen auch der **Pflegedienstleitung** sowie Namen und berufliche Ausbildung der **Betreuungskräfte** anzugeben. Änderungen im Personalbestand sind ebenfalls anzugeben.
Darüber hinaus kann nach § 12 Abs. 2 Heimgesetz die zuständige Behörde weitere Angaben verlangen, soweit sie zur zweckgerichteten Aufgabenerfüllung erforderlich sind.

Dass diese nicht erforderlich waren, zeigte die - zutreffende - Reaktion auf eine Nachfrage des Landesbeauftragten bei der abfragenden Behörde. Die Leistungserbringer wurden von der Behörde schnell darauf hingewiesen, dass die zusätzlich geforderten Angaben entbehrlich seien.

20.8 Der "Datenabgleich"-Bereich des BAföG

Sein Verständnis für den Datenabgleich im Rahmen der Terrorismusbekämpfung äußerte ein Petent gegenüber dem Landesbeauftragten. Dass dieser Datenabgleich aber auch im Bereich des Bundessausbildungsförderungsgesetzes möglich sein solle, könne er nicht einsehen.
Der Landesbeauftragte konnte ihn aber darauf hinweisen, dass diese Maßnahme nicht auf den Gesetzen zur Terrorismusbekämpfung nach dem 11. September 2001 fußte.

Die Vorschrift, die den Datenabgleich im Rahmen der Gewährung von Sozialleistungen gestattet, wurde bereits durch das Gesetz vom 23.10.2000 (BGBl. I S. 1433) eingeführt und lässt den Abgleich nach § 45d EStG zwischen dem Bundesamt für Finanzen und den jeweiligen Sozialleistungsträgern - also nicht nur BAföG-Behörden - zu.

Der Sozialleistungsträger hatte zuvor vom Bundesrechnungshof deutliche Hinweise erhalten, dass bei der Berechnung der Leistungen nach dem BAföG in erheblichem Umfang Einkünfte aus Kapitalvermögen bei der Antragstellung nicht angegeben würden.
Bei dem Abgleich stellte sich heraus, dass in mehr als 20 % (!) aller Anträge solche Einkünfte nicht angegeben wurden.
Auch der Petent hatte vergessen, dem Sozialleistungsträger mitzuteilen, dass er Einkünfte aus Kapitalvermögen bezog. Insofern war er seiner Meldepflicht nach § 60 SGB I nicht nachgekommen. Der durchgeführte Datenabgleich war in diesem Fall gesetzlich vertretbar.

Der Landesbeauftragte hat aber betont, dass eine dauerhafte vollständige Abfrage beim Bundesamt für Finanzen mangels spezieller gesetzlicher Grundlage unzulässig bleibt (§ 67 Abs. 1 SGB X).

20.9 Ermäßigungs-/Erlassanträge zu Elternbeiträgen in Kindertagesstätten

Im V. Tätigkeitsbericht (Ziff. 18.1) hatte der Landesbeauftragte als Problem den Fall aufgezeigt, dass in einer Gebührensatzung "Abwaschgebühren" festgesetzt wurden, ohne die Höhe und die Fälligkeit anzugeben.
Die durch den Landesbeauftragten eingeschaltete Kommunalaufsicht hat die Gemeinde nochmals darauf hingewiesen, dass hier für die separate Erhebung einer Abwaschgebühr keine rechtliche Regelung vorgegeben ist und es somit an einer Erhebungsgrundlage fehlt. Die Gemeinde wurde angewiesen,

- von einer solchen Gebührenerhebung abzusehen und
- bisher eingenommene Gebühren an die Betroffenen zurückzuerstatten.

Im Berichtszeitraum wurde die Kontrolle der Nutzung personenbezogener Daten im Rahmen der Kindertagesstätten erneut aufgenommen. Hierbei war wiederum festzustellen, dass trotz mehrfacher Hinweise des Landesbeauftragten in seinen Tätigkeitsberichten und der Beratung der Jugendamtsleiter im Rahmen ihres Arbeitskreises die Rechtsgrundlagen der Datenerhebung falsch interpretiert wurden.
Lediglich ein Landkreis hatte die Erhebungsbögen entsprechend überarbeitet.

Der Landesbeauftragte weist nochmals darauf hin, dass die Antragsformulare nach Form und Inhalt benutzerfreundlich sein müssen. Unklare und unverständliche Formulare gehen zu Lasten der Behörde (BVerwGE 10, 12, 15). Die Behörde hat die Pflicht in einem Antragsformular Stellen für alle rechtlich relevanten Eintragungen vorzusehen. Fehlt eine notwendige Stelle und unterbleibt deshalb eine relevante Mitteilung, muss sich die Behörde so behandeln lassen, als hätte sie rechtzeitig Kenntnis erlangt.

Der Landesbeauftragte wird daher die Kontrollen der Fragebögen weiterhin durchführen.

20.10 Ausweis zur Gebührenermäßigung

Eine Stadt führte als freiwillige Leistung einen Ausweis zur Gebührenermäßigung im kulturellen, sportlichen und Freizeitbereich ein, der einem bestimmten Personenkreis die Teilnahme finanziell ermöglichen sollte. Nur Personen, die ihren Hauptwohnsitz in der Stadt gemeldet hatten und deren gem. § 76 BSHG bereinigtes Einkommen den hundertzehnprozentigen Sozialhilfebedarf nicht überstieg, sollte diese Vergünstigung zugute kommen.

Der Umfang der zur Antragstellung erforderlichen Unterlagen wurden vom Landesbeauftragten datenschutzrechtlich überprüft. Das Ergebnis der Überprüfung ergab, dass weder das "Merkblatt" noch der "Antrag auf Ausstellung" den gesetzlichen Vorgaben entsprachen. In mehreren Beratungsgesprächen wurden die Antragsunterlagen besprochen und anschließend entsprechend den gesetzlichen Vorgaben überarbeitet. Pikant war, dass der Ausweis lediglich eine Laufzeit von 6 Monaten hatte und bei Antragstellung Nachweise abgefordert wurden, die den Zeitraum "3 Monate vor Antragstellung" glaubhaft machen sollten. Hierbei wurde nicht einmal berücksichtigt, ob es sich um einen Erst- oder Folgeantrag handelte.

Der Landesbeauftragte konnte erreichen, dass künftig den Antragstellern ein Hinweisblatt ausgehändigt wird, auf dem die Behörde ankreuzt, welche Unterlagen zur Antragstellung erforderlich sind (Datensparsamkeit). Durch dieses Verfahren wird die bisher praktizierte, aber unzulässige Doppelerhebung ausgeschlossen.

20.11 Kfz-Halter-Daten für das Sozialamt

§ 117 Abs. 3 Satz 4 f BSHG ermächtigt die Träger der Sozialhilfe, zur Vermeidung rechtswidriger Inanspruchnahme von Sozialhilfe, Daten u.a. zur "Eigenschaft als Kraftfahrzeughalter" zu erheben. Das Grundrecht auf informationelle Selbstbestimmung erfordert dabei im Zweifel eine **enge** Auslegung dieser **Erhebungs**befugnis. Das heißt, ohne nähere Anhaltspunkte oder Gründe im Einzelfall gibt es keine Grundlage **generell** für Abfragen.
Problematisch war außerdem, auf welcher Grundlage die Straßenverkehrsbehörden Antworten übermitteln durften.
Seit dem 01.01.2003 findet sich die normenklare Rechtsgrundlage für solche Übermittlungen nunmehr in § 35 Abs. 5 Nr. 6 StVG i.V.m. § 9a Fahrzeugregisterverordnung (vgl. Ziff. 26.2).

20.12 Taschengeld für die Dauer der U-Haft

Ein Petent hatte bei der für ihn zuständigen Sozialbehörde einer Stadt für die Dauer der U-Haft Taschengeld beantragt. Ein Schreiben des Sozialamtes der Stadt mit ausführlichen Berechnungen zum Taschengeld war

dem Petenten dann in der Justizvollzugsanstalt offen ausgehändigt worden. Dies lag daran, dass sich das Schreiben zwar an den Petenten richtete, im Adressfeld jedoch die Justizvollzugsanstalt mit Postfach und Postleitzahl angegeben war.
Da das Taschengeld auf der Grundlage des BSHG gewährt wird, handelte es sich um besonders geschützte Sozialdaten, die auf diese Weise einer Vielzahl von Mitarbeitern in der Justizvollzugsanstalt bekannt gegeben wurden.

Auf den Hinweis des Landesbeauftragten hat die Stadt die Fehler eingeräumt und die erforderlichen Maßnahmen getroffen, um entsprechende Fehler bei der Adressierung künftig zu vermeiden.

20.13 Kinderförderungsgesetz (KiFöG)

Mit dem Inkrafttreten des neuen KiFöG am 08.03.2003 haben die Träger der Einrichtungen die geänderten Kinderbetreuungsansprüche zu beachten.

Bereits im Vorfeld der neuen Bestimmungen zeichnete sich bei den Trägern der Einrichtungen eine hohe Verunsicherung über die neuen Betreuungskriterien ab. Rundschreiben und neue Anmeldevordrucke mit teilweise abenteuerlichen Datenerhebungen wurden erarbeitet und verteilt.
Eine Stadt verteilte in ihren Kindertagesstätten ein Rundschreiben mit folgendem Hinweis: Zur Begründung des Anspruchs auf einen Ganztagsplatz sind folgende Nachweise entsprechend der jeweiligen Tätigkeit erforderlich:

- nicht selbständige Tätigkeit: aktuelle Meldung zur Sozialversicherung von Krankenkasse oder letzte Lohn-/Gehaltsbescheinigung mit Arbeitsstundenangaben vom Arbeitgeber
- selbständige Tätigkeit: aktueller Nachweis über Einkommensteuerveranlagung vom Finanzamt oder Steuerberater, Gewerbeanmeldung vom Gewerbeamt, Anmeldung zur berufsständischen Kammer von Berufskammer
- Aus-, Fort- oder Weiterbildung: Bescheid über Bildungsmaßnahme vom Bildungsträger oder Arbeitsamt
- bei Alleinerziehenden zusätzlich: Vaterschaftsanerkennung und Einwohnermeldeamtsbescheinigung.

Im Einzelfall sollten noch weitere Unterlagen auf Verlangen vorgelegt werden.

Der Landesbeauftragte hat die Stadt darauf hingewiesen, dass sich die Erhebung von Sozialdaten in der Kinder- und Jugendhilfe am "Erforderlichkeitsgrundsatz" des § 62 Abs. 1 SGB VIII auszurichten hat. So kann z.B. der Bedarf für einen ganztägigen Platz in einer Einrichtung durch Auszüge aus Arbeitsverträgen nachgewiesen werden. Dabei dürfen nicht

erforderliche Angaben vorher geschwärzt werden. Kann kein Arbeitsvertrag vorgelegt werden, wäre u.a. auch eine Bescheinigung des Arbeitgebers ausreichend. Für Selbständige ist eine Bestätigung des Finanzamtes oder des Steuerberaters möglich.
Es sollten allerdings keine eigenen Vordrucke der öffentlichen Stellen zur Ausfüllung durch Dritte verwendet werden (unzulässige Datenübermittlung gem. § 64 Abs. 2 SGB VIII i.V.m. § 69 SGB X), da Arbeitgeber durch ein solches Formular die Tatsache des Kontakts zu einem Sozialleistungsträger erfahren können.

Die Stadt wurde aufgefordert, das Verfahren auf eine erforderliche Datenerhebung zur Bedarfsüberprüfung zu beschränken und bereits erhobene Unterlagen, die gesetzlich nicht vorgesehen sind, entweder zu vernichten oder umgehend zurückzugeben. Andernfalls würde eine unzulässige Erhebung und Speicherung von Sozialdaten (§ 63 SGB VIII) vorliegen.

21. Statistik

Geplante Einführung einer bundeseinheitlichen Wirtschaftsnummer

Das Bundesministerium für Wirtschaft und Technologie bereitet bereits seit Ende des Jahres 2000 gemeinsam mit den Wirtschaftsressorts der Länder die Einführung einer bundeseinheitlichen Wirtschaftsnummer vor. Diese Nummer, so heißt es im Gesetzentwurf vom 11.02.2002 (BT-Drs. 14/8211), soll im Verkehr mit Behörden, der amtlichen Statistik und anderen öffentlichen Stellen zur Bezeichnung und Identifizierung des wirtschaftlich Tätigen verwendet werden und die bestehende Nummernvielfalt ersetzen. Der Vorteil für die Unternehmen sei, dass sie in großem Umfang von Meldungen und damit von bürokratischen Hemmnissen entlastet würden.

Der zunächst entstehende durchaus vorteilhafte Eindruck wird jedoch durch die Betrachtung des gesamten Ansinnens aus datenschutzrechtlichem Blickwinkel erheblich beeinträchtigt.
Unternehmen in diesem Zusammenhang nämlich würden nicht nur Großbetriebe sein, sondern **jeder** gewerblich Tätige, also jeder selbständige Malermeister, jeder selbständige Taxifahrer. Aber damit nicht genug: Jeder, der in seiner Wohnung eine Haushaltshilfe beschäftigt, würde eine solche Wirtschaftsnummer erhalten.
Die Nummern sollen voraussichtlich in der Zentralen Datensammel- und Abgleichstelle der Bundesanstalt für Arbeit vergeben und gespeichert werden, die auch den hinter jeder Nummer stehenden elfteiligen Stammdatensatz, u.a. aus Name, Vornamen, Anschrift und Handels-, Partnerschafts-, Genossenschaft- oder Vereinsregistereintrag, verwalten soll. Die Bundesanstalt für Arbeit würde den Stammdatensatz bzw. ihr bekannt gewordene Änderungen einer Vielzahl verschiedener Stellen, z.B. den Finanzämtern und den für die Entgegennahme von Gewerbeanzeigen zuständigen Behörden, mitteilen.

Datenschutzrechtlich bedeutsam erscheint dem Landesbeauftragten u.a., dass damit das **übergreifende Personenkennzeichen** - und als solches muss die Betriebsnummer wegen ihres bundeseinheitlichen Charakters und bundesweiten Verwendungszwecks bei natürlichen Personen wohl angesehen werden -, durch die Hintertür wieder eingeführt wird. Dies ist u.a. wegen der Gefahr der Erstellung von Persönlichkeitsprofilen abzulehnen. Bereits 1976 erklärte dazu der Rechtsausschuss des Deutschen Bundestages, dass "die einheitliche Nummerierung der Bevölkerung" durch ein "Personenkennzeichen als unzulässig" angesehen wird. Diese damalige Einschätzung wurde mit dem sog. Volkszählungsurteil des Bundesverfassungsgerichts vom 15.12.1983 bestätigt.

Die Implementierung der Wirtschaftsnummer wird bei den beteiligten Stellen erheblichen Aufwand verursachen. Aus diesem Grunde hat sich der Bundesgesetzgeber entschlossen, die Verwendung dieser Nummer in Regensburg und dem Landkreis Neumarkt (beide Bayern) bis zum 31. Oktober 2003 erproben zu lassen.

Die Datenschutzbeauftragten des Bundes und der Länder werden die Erprobung der Wirtschaftsnummer und den Prozess ihrer tatsächlichen bundesweiten Einführung kritisch begleiten und darauf achten, dass sich die in der Erprobungsphase gewonnenen Erkenntnisse im Sinne des Datenschutzrechts in einem Wirtschaftsnummer-Einführungsgesetz widerspiegeln.

22. Strafvollzug

22.1 Gefangene erhalten Behördenpost offen

Im Berichtszeitraum mehrten sich die Beschwerden Gefangener, dass sie Behördenpost offen (ohne Umschlag) ausgehändigt bekämen.
Die Stellungnahmen der betroffenen Justizvollzugsanstalten ähnelten sich wie ein Ei dem anderen: Es sei Praxis, dass Behörden (insbesondere Gerichte und Staatsanwaltschaften) ihre Schreiben an Gefangene per Sammelpost (ohne eigenen Umschlag) der Justizvollzugsanstalt zustellen würden (vgl. Ziff. 20.12).

Mit diesem Sachverhalt hatte der Landesbeauftragte das Ministerium der Justiz schon einmal konfrontiert. Daraufhin sollen die Behörden im Geschäftsbereich des Ministeriums auf diese Problematik hingewiesen worden sein. Genützt hat es leider bisher nicht viel.

22.2 Einsichtnahme des Gefangenen in seine Personalakte

Ein anderer Gefangener beschwerte sich beim Landesbeauftragten, weil ihm ohne Begründung die Einsicht in seine Personalakte verwehrt worden sei.

Wie sich herausstellte, entsprach diese Behauptung nicht den Tatsachen. Tatsächlich hatte der Gefangene seinen Wunsch nach Einsichtnahme nicht begründet.
Nach der geltenden Rechtslage erhält ein Gefangener grundsätzlich lediglich **Auskunft** aus seiner Personalakte. Nur soweit eine Auskunft für die Wahrnehmung seiner rechtlichen Interessen nicht ausreicht und er hierfür auf die Einsichtnahme angewiesen ist, ist ihm Akteneinsicht zu gestatten.

Weil der Gefangene seinen Antrag auf Akteneinsicht nicht begründet hatte, blieb der Justizvollzuganstalt nichts anderes übrig, als den Antrag abzulehnen. Das war auch aus Sicht des Landesbeauftragten datenschutzrechtlich vertretbar. Er hat jedoch angeregt, im Rahmen einer verfassungskonformen Auslegung des Auskunftsanspruches in Zukunft ggf. auch einzelne Ablichtungen aus der Gefangenenpersonalakte auszuhändigen.

23. Telekommunikations- und Medienrecht

23.1 Informationsangebote öffentlicher Stellen im Internet

Immer mehr öffentliche Stellen nutzen das Internet nicht nur zur schnellen Informationsbeschaffung und Kommunikation, sondern sie präsentieren sich auch mit einer eigenen Homepage. Unabhängig davon, ob diese Angebote als Medien- oder Teledienste einzuordnen sind, unterliegen Tele- bzw. Mediendiensteanbieter einer Reihe von gesetzlichen Pflichten, auf die der Landesbeauftragte, auch im Hinblick auf den Start des neuen Portals der Landesregierung im Januar 2003, hinweisen möchte.

Anbieterkennzeichnung (Impressum)
Gemäß § 6 Teledienstegesetz (TDG) bzw. § 10 Abs. 2 Mediendienste-Staatsvertrag (MDStV) haben Anbieter von Tele- bzw. Mediendiensten folgende Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten:
- Name und Anschrift
- Angaben, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation ermöglichen, einschließlich der Adresse der elektronischen Post (E-Mail).

Datenschutzrechtliche Unterrichtung
Gemäß § 4 Abs. 1 Teledienstedatenschutzgesetz (TDDSG) bzw. § 18 Abs. 1 MDStV haben Diensteanbieter den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu unterrichten. Die Unterrichtung muss jederzeit abrufbar sein.
Auch wenn ein Internetangebot keine Formulare enthält, in die ein Nutzer personenbezogene Daten eintragen könnte, so wird doch in vielen Fällen

bei der Protokollierung der Zugriffe auf das Internetangebot die IP-Adresse des Nutzers gespeichert. Aus der IP-Adresse, die meist dynamisch vergeben wird, kann zwar nicht direkt auf den Nutzer geschlossen werden, mit zusätzlichen Informationen ist jedoch eine Identifizierung des Nutzers möglich. Somit handelt es sich bei der IP-Adresse natürlicher Personen um ein personenbezogenes Datum.
Zwar darf der Diensteanbieter gem. § 6 Abs. 1 TDDSG bzw. § 19 Abs. 2 MDStV personenbezogene Daten eines Nutzers ohne dessen Einwilligung erheben, verarbeiten und nutzen, soweit dies erforderlich ist, um die Inanspruchnahme des Dienstes zu ermöglichen (Nutzungsdaten), allerdings gilt dies gem. § 6 Abs. 4 TDDSG bzw. § 19 Abs. 5 MDStV über das Ende des Nutzungsvorgangs hinaus nur für Zwecke der Abrechnung, d. h. bei kostenlosen Internetangeboten sind die Nutzungsdaten einschließlich der IP-Adresse nach Ende des Nutzungsvorgangs zu löschen.

Verstöße gegen die Verpflichtung zur Anbieterkennzeichnung und zur datenschutzrechtlichen Unterrichtung sowie die unzulässige Speicherung personenbezogener Daten können als Ordnungswidrigkeiten mit einer Geldbuße bis zu 50.000,- € geahndet werden.

Der Landesbeauftragte fordert deshalb alle öffentlichen Stellen des Landes, die über eine eigene Internetpräsenz (Homepage) verfügen, auf, diese gesetzlichen Verpflichtungen ordnungsgemäß umzusetzen. Öffentliche Stellen sollten in diesem Zusammenhang immer **ihren** Beauftragten für den Datenschutz beteiligen und zu Rate ziehen, denn dies gehört mit zu den Aufgaben eines behördlichen Datenschutzbeauftragten gem. § 14a Abs. 4 DSG-LSA (vgl. Ziff. 12.1).

23.2 Internet und E-Mail am Arbeitsplatz

Immer mehr öffentliche Stellen ermöglichen ihren Beschäftigten die Nutzung des Internets zur schnellen Informationsbeschaffung und zum Informationsaustausch per E-Mail. Dabei sind jedoch bestimmte datenschutzrechtliche Anforderungen zu beachten, die davon abhängen, ob den Beschäftigten neben der **dienstlichen** auch die **private** Nutzung von Internetdiensten und E-Mail gestattet wird.

Die grundsätzlichen Anforderungen an eine datenschutzgerechte Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz hat die 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 07./ 08.03.2002 in einer Entschließung beschrieben **(Anlage 14)**.
Der Arbeitskreis Medien der Konferenz hat bezüglich der Problematik der dienstlichen und privaten Nutzung eine Orientierungshilfe veröffentlicht, deren wesentliche Aussagen im folgenden Beitrag zusammengefasst werden. Die gesamte Orientierungshilfe steht auf der Homepage des Landesbeauftragten zum Herunterladen zur Verfügung.

Dienstliche Nutzung
Gestattet der öffentliche Arbeitgeber die Nutzung von Internetdiensten und E-Mail **ausschließlich** zu dienstlichen Zwecken, ist er **nicht** Anbieter im Sinne des Telekommunikationsgesetzes (TKG), da im Dienstverhältnis die Mitarbeiter gegenüber ihrem öffentlichen Arbeitgeber **nicht** Dritte sind (§ 3 Ziff. 5 TKG).
Die Erhebung und Verarbeitung von Verbindungs- und Inhaltsdaten, d.h. von Daten, die über das Nutzungsverhalten der Beschäftigten Auskunft geben, richtet sich für Beamte nach den einschlägigen Vorschriften des BG LSA bzw. für Tarifbedienstete des Landes nach den Vorschriften des DSG-LSA.

Der öffentliche Arbeitgeber ist hierbei grundsätzlich berechtigt, die dienstliche Nutzung von Internetdiensten und E-Mail stichprobenartig zu kontrollieren. Dabei ist jedoch der Grundsatz der **Datenvermeidung** bzw. der **Datensparsamkeit** zu beachten (§ 1 Abs. 2 DSG-LSA). Das bedeutet z.B., dass bei einer Protokollierung zunächst von der Möglichkeit einer anonymen Aufzeichnung Gebrauch gemacht werden sollte.

Weitergehende Kontrollen bis hin zu einer automatisierten Vollkontrolle von Beschäftigten ist nur bei einem konkreten Missbrauchsverdacht unter strikter Beachtung des Verhältnismäßigkeitsgrundsatzes zulässig. Es empfiehlt sich, in Zusammenarbeit mit dem Personalrat eine Dienstvereinbarung zu erstellen, in der der Umfang der Protokollierung, die Auswertung und mögliche Sanktionen bei Missachtung des Verbots der privaten Nutzung geregelt werden.

Erfolgt eine Protokollierung der Nutzung von Internetdiensten und E-Mail zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage, unterliegen diese Daten der engen Zweckbindung des § 10 Abs. 4 DSG-LSA, d.h. sie dürfen nur für diese Zwecke verwendet werden. Die Nutzung dieser Daten für eine Verhaltens- und Leistungskontrolle der Beschäftigten ist gem. § 28 Abs. 4 DSG-LSA unzulässig.

Ein- und ausgehende **dienstliche** E-Mails seiner Beschäftigten darf der öffentliche Arbeitgeber in demselben Maße zur Kenntnis nehmen wie dienstlichen Schriftverkehr. Demzufolge könnte der Vorgesetzte - ähnlich wie bei einer zentralen Poststelle - verfügen, dass ihm alle ein- und ausgehenden E-Mails zur Kenntnis gegeben werden.

Private Nutzung
Die Gestattung der - wenn auch nur gelegentlichen - privaten Nutzung von Internet und E-Mail ist mit erheblichen datenschutzrechtlichen Problemen verbunden, da der öffentliche Arbeitgeber dann gegenüber seinen Beschäftigten zum Telekommunikationsdiensteanbieter wird und damit gem. § 85 Abs. 2 TKG zur Einhaltung des Fernmeldegeheimnisses (§ 85 Abs. 1 TKG) verpflichtet ist.

Zum Schutz der personenbezogenen Daten der an der Telekommunikation Beteiligten wurden auf der Grundlage der Verordnungsermächtigung aus § 89 Abs. 1 Satz 1 TKG mit der Telekommunikations-Datenschutzverordnung (TDSV) die entsprechenden Regelungen erlassen.

Das hat zur Folge, dass eine Protokollierung der privaten Nutzung von Internetdiensten und E-Mail nur zu Abrechnungszwecken erlaubt ist. Da in der Praxis bei den öffentlichen Stellen im Allgemeinen keine Abrechnung erfolgt und insbesondere beim Surfen im Internet eine Unterscheidung zwischen dienstlicher und privater Nutzung nicht ohne größeren technischen Aufwand möglich ist, ist eine Protokollierung problematisch.

Eine Möglichkeit, dieses Problem zu lösen, bietet die individuelle Einwilligungserklärung. Dabei muss dem öffentlichen Arbeitgeber gestattet werden, die private Nutzung von Internetdiensten und E-Mail wie die dienstliche zu behandeln, d.h. die Nutzung im erforderlichen Umfang zu protokollieren und stichprobenartig auszuwerten. In dieser Einwilligungserklärung muss detailliert beschrieben werden, welche Daten für welche Zwecke protokolliert und wie lange sie gespeichert werden. Weiterhin muss festgelegt werden, unter welchen Umständen welche Personen vom Inhalt privater E-Mails Kenntnis nehmen dürfen (z.B. Vertretungsregelung; Systemverwalter bei Virenalarm u.ä.).
Beschäftigten, die eine solche Einwilligungserklärung nicht unterzeichnen möchten, dürfen daraus keine Nachteile entstehen, allerdings ist für sie die private Nutzung verboten.

Der Landesbeauftragte weist darauf hin, dass eine allgemeine Dienstvereinbarung auch mit Beteiligung des Personalrates die individuelle Einwilligungserklärung durch den einzelnen Beschäftigten nicht ersetzen kann, da es sich hier um einen Eingriff in das Persönlichkeitsrecht handelt. Dienstvereinbarungen basieren auf dem Personalvertretungsrecht, das vornehmlich der Vertretung kollektiver Interessen dient. § 70 PersVG LSA sieht zudem lediglich vor, dass über die in § 65 Abs. 1 Satz 1 Nrn. 1 bis 7 PersVG LSA genannten Fragen (Bereiche der Mitbestimmung in sozialen Angelegenheiten) Dienstvereinbarungen abgeschlossen werden können. Als Rechtsvorschriften, die Eingriffe in das Persönlichkeitsrecht über das gesetzlich zugelassene Maß hinaus gestatten, kommen sie in der Regel nicht in Betracht.

Öffentliche Stellen, die die private Nutzung von Internetdiensten und E-Mail nicht ausdrücklich in einer Dienstanweisung verboten und diesbezüglich keine individuelle Einwilligung ihrer Beschäftigten eingeholt haben, verstoßen im Falle einer Protokollierung des Nutzungsverhaltens gegen das Fernmeldegeheimnis (§ 85 TKG) sowie gegen die Bestimmungen der TDSV.

Fazit
Nicht nur vor dem Hintergrund der genannten Problematik bei der - wenn auch nur gelegentlichen - privaten Nutzung von Internetdiensten und E-Mail am Arbeitsplatz weist der Landesbeauftragte darauf hin, dass aus Gründen der Datensicherheit im Einzelfall abgewogen werden muss, ob tatsächlich jeder Beschäftigte einer Behörde Internetdienste und E-Mail für die Erfüllung seiner dienstlichen Aufgaben benötigt.

Insbesondere durch die Möglichkeit des Herunterladens von Dateien aus dem Internet und durch die Verbreitung von Computerviren u.a. per E-Mail kann es zu einer Gefährdung der Sicherheit und Verfügbarkeit des Behördennetzes und damit u.U. auch zu einer Gefährdung bei der Verarbeitung personenbezogener Daten kommen (vgl. Ziff. 12.3).

Die Staatssekretärskonferenz stimmte am 29.01.2001 der privaten Nutzung von Internetdiensten und E-Mail im Ausnahmefall unter einschränkenden Bedingungen zu. Das Ministerium des Innern legte dazu eine ressortübergreifende Musterdienstanweisung vor, gegen die der Landesbeauftragte für eine Übergangszeit keine datenschutzrechtlichen Bedenken erhoben hat.

Das Ministerium des Innern hat in seinen organisatorischen Regelungen zum Einsatz der Informationstechnik diese Musterdienstanweisung in vorbildlicher Weise berücksichtigt.

Der Landesbeauftragte geht davon aus, dass auch andere Ressorts die Musterdienstanweisung in ähnlicher Weise umgesetzt haben.

24. Umwelt und Natur

Standortverzeichnisse von Mobilfunkanlagen

Bei der Regulierungsbehörde für Telekommunikation und Post wird ein Standortverzeichnis der Mobilfunkanlagen geführt. Städte und Gemeinden können dort in ihrem Bereich liegende Standorte abfragen und sind in einigen anderen Bundesländern mittlerweile zum Teil dazu übergegangen, diese zu veröffentlichen.
Auch dies ist ein Thema für den Datenschutz, weil zusammen mit den Standorten auch die personenbezogenen Daten der Grundstückseigentümer und Antennenbetreiber gespeichert werden.

Der Landesbeauftragte hat die Kommunen des Landes deshalb darauf hingewiesen, dass die Speicherung personenbezogener Daten in eigenen Verzeichnissen (Kataster) mangels einer Rechtsgrundlage datenschutzrechtlich unzulässig ist, soweit die Grundstückseigentümer und Antennenbetreiber nicht ausdrücklich eingewilligt haben. Demzufolge dürfen diese

Daten (mit Personenbezug) auch grundsätzlich nicht übermittelt oder veröffentlicht werden. Dieses betrifft sowohl die Einstellung der Daten in das Internet als auch die Zusammenfassung auf Karten und anschließende Veröffentlichung (z.B. durch Aushängen in der Gemeinde).
Nur für einzelne Bürger des Landes, die wissen wollen, ob in ihrer Nähe Mobilfunkanlagen betrieben werden, kann sich aus den Vorschriften des Umweltinformationsgesetzes etwas anderes ergeben, was jeweils von der betreffenden Gemeinde im Einzelfall geprüft werden muss.

Genauso haben sich der Landesbeauftragte und seine Kollegen aus Bund und den Ländern in einer Entschließung **(Anlage 18)** geäußert.

25. Verfassungsschutz

Zweckbindung und Kennzeichnungspflicht

Der Landesbeauftragte erfragte bei der Verfassungsschutzabteilung des Ministeriums des Innern die dortige Rechtsauffassung zur Kennzeichnung von Daten, welche unter besonderen Bedingungen heimlich erhoben werden.

Anlass war zum einen die z.Zt. in Fachkreisen geführte Diskussion zur generellen Kennzeichnungspflicht von Daten zur Sicherung der Zweckbindung bei deren weiterer Nutzung. Zum anderen sollte in Erfahrung gebracht werden, inwieweit aus einem Urteil des Bundesverfassungsgerichtes zur Fernmeldeüberwachung (durch den BND) bereits praktische Konsequenzen gezogen worden sind.

Das Gericht hat in seiner Entscheidung festgestellt, dass Daten, welche aus solchen besonderen Erhebungen stammen, zu kennzeichnen sind. Im Einzelnen hatte es ausgeführt, dass sich "die Zweckbindung nur gewährleisten lässt, wenn auch nach der Erfassung erkennbar bleibt, dass es sich um Daten handelt, die aus Eingriffen in das Fernmeldegeheimnis stammen. Eine entsprechende Kennzeichnung ist daher von Verfassungs wegen geboten" (NJW 2000, 55 ff., 57 und 60).
Bei der noch gravierenderen Wirkung eines Eingriffs in den Schutzbereich der Unverletzlichkeit der Wohnung (Art. 13 GG) durch einen sog. Lauschangriff ist folglich ebenfalls eine entsprechende Kennzeichnung zu übermittelnder Daten vorzunehmen, um die Zweckbindung gewährleisten zu können.

Das Ministerium des Innern teilt diese Rechtsauffassung und zeigte in seiner Antwort mögliche Verfahrensweisen auf, wie in der praktischen Anwendung die Kennzeichnung so gewonnener Daten gewährleistet werden könnte.

Der Landesbeauftragte hat dies mit Interesse zur Kenntnis genommen. Er regt darüber hinaus eine Prüfung über gesetzgeberische Maßnahmen zur Kennzeichnungspflicht von personenbezogenen Daten bei deren Erhebung an, um - entsprechend der Rechtsprechung des BVerfG - die Zweckbindung der betreffenden Daten während ihrer gesamten Nutzungsdauer zu sichern.

26. Verkehr

26.1 Parkerleichterung für Schwerbehinderte

In seinem V. Tätigkeitsbericht (Ziff. 22.3) hatte der Landesbeauftragte auf die Probleme eines Landkreises bei der Umsetzung eines Gemeinsamen Runderlasses des Ministeriums für Wohnungswesen, Städtebau und Verkehr - jetzt Ministerium für Bau und Verkehr - und des Ministeriums für Gesundheit und Soziales vom 24.02.1998 zur Erteilung von Ausnahmegenehmigungen nach § 46 StVO zur Parkerleichterung für Schwerbehinderte hingewiesen. Im Gegensatz zur etwas anders gestalteten Bundesregelung sollten die Begünstigten hier im Lande nach dem Erlass statt eines Ausweisblatts ohne Personenbezug, den gesamten Bescheid in ihrem Fahrzeug sichtbar auslegen.

Der Landesbeauftragte hatte daraufhin gebeten zu prüfen, ob auch für die Landesregelung die datenschutzgerechte Verfahrensweise der Bundesregelung übertragen werden könnte.
Bereits ein Vierteljahr später informierte das damalige Ministerium für Wohnungswesen, Städtebau und Verkehr den Landesbeauftragten darüber, dass es mit einem Änderungserlass den datenschutzrechtlichen Bedenken Rechnung getragen hätte.

Von der Einführung eines separaten Ausweises im Land wurde zwar weiterhin aus Kostengründen sowie wegen einer Verwechslungsgefahr mit dem noch geltenden bundeseinheitlichen und dem schon geltenden europäischen Ausweis abgesehen. Jedoch wird nicht mehr der Name des Schwerbehinderten, sondern lediglich die ausstellende Behörde und eine Ausnahmegenehmigungsnummer aus der Ausnahmegenehmigung zu ersehen sein.
Auch das Ministerium des Innern hält diese Angaben für Kontrollzwecke im Ruhenden Verkehr für ausreichend.

Die zügige Umsetzung der Hinweise des Landesbeauftragten trägt Vorbildcharakter für andere Ressorts.

26.2 Datenübermittlung der Kfz-Zulassungsbehörde an das Sozialamt

Der Landesbeauftragte weist auch in diesem Abschnitt seines Tätigkeitsberichtes noch einmal auf den unter Ziff. 20.11 behandelten Fall hin. Seit

dem 01. Januar 2003 muss jeder Antragsteller von Sozialhilfeleistungen nach dem BSHG mit einer Nachfrage des Sozialamtes bei der Kfz-Zulassungsbehörde rechnen, ob er Halter eines oder mehrerer Kraftfahrzeuge ist. Er tut gut daran, auf entsprechende Fragen wahrheitsgemäß zu antworten.

26.3 Fahrzeug- und Halterdaten **nicht** "offenkundig"

Die Entscheidungen des Hanseatischen Oberlandesgericht Hamburg (Beschluss vom 22.01.1998) und des Bayerischen Obersten Landesgerichts (Beschluss vom 18.01.1999) zu Fragen der Strafbarkeit des unbefugten Abrufs aus dem Zentralen Verkehrsinformationssystems (ZEVIS) bzw. dem INPOL-Systems und der Weitergabe (Übermittlung) dieser in § 39 Abs. 1 StVG aufgeführten und nach § 33 Abs. 1 StVG gespeicherten Fahrzeug- und Halterdaten an Dritte durch Polizeibeamte waren in den Kreisen der Datenschutzbeauftragten des Bundes und der Länder auf Unverständnis gestoßen.
Im Tenor beider OLG-Entscheidungen wurden diese Fahrzeug- und Halterdaten als "offenkundig" eingestuft, die deswegen weder dem Schutzzweck des § 203 StPO noch dem des § 43 BDSG unterfallen sollten.

Diese umstrittene Auslegung hat nunmehr der Bundesgerichtshof (BHG) in seinem Urteil vom 08.10.2002 (1 StR 150/02) als unzutreffend zurückgewiesen und klargestellt, dass Fahrzeug- und Halterdaten, die im Rahmen einer einfachen Registerauskunft nach § 39 Abs. 1 StVG übermittelt werden, nicht offenkundig sind und somit unter den Schutz des § 203 Abs. 2 Satz 2 StGB fallen.

Der Landesbeauftragte regt an, dass sich sowohl die Polizeibehörden als auch die Kfz-Zulassungsbehörden der Landkreise und kreisfreien Städte mit diesem Grundsatzurteil des BGH intensiv befassen, es auswerten und in ihrer Verwaltungspraxis beachten.

Anlage 1

Organisationsplan

Landesbeauftragter für den Datenschutz Sachsen-Anhalt
Herr Kalk

Referat 1	Referat 2	Referat 3
Geschäftsstellenleitung, Landtag, Rechtspflege, Justizverwaltung, Justizvollzug, Rechtshilfe, Verfassungsschutz, Nachrichtendienste	Grundsatzfragen des Datenschutzes, Allgemeines Ordnungswidrigkeitenrecht, Öffentlicher Dienst, Rundfunk- und Presserecht, Hochschulen	Grundsatzfragen der Technik und Organisation des Datenschutzes und der Informationstechnik, Wirtschaft, Verkehr, Raumordnung und Landesplanung
Polizei, Finanzen, Kommunalrecht	Sozialwesen, Gesundheitswesen	Betriebs- und Datenbanksysteme, Statistik, Handwerk und Gewerbe, Wohnungswesen
Gefahrenabwehrrecht, Bau- und Bodenangelegenheiten, Natur- und Umweltschutz, Landwirtschaft und Forsten, Ausländer, Aussiedler, Staatsangehörigkeit, Europol und Schengen, Internationaler Datenschutz	Personenstandswesen, Kindertageseinrichtungen, Kultur, Denkmalschutz, Archivwesen, Wissenschaft und Forschung, Schulen Jugendhilfe	Telekommunikation, Netze, Neue Medien, Vermessungs- und Katasterwesen --- Gleichstellungsfragen
Verwaltungsangelegenheiten der Geschäftsstelle	Ausweis-, Meldewesen, Feuerwehr, Katastrophenschutz, Personalaktenrecht, Personalvertretung, Wahlen	
Registratur		
Bücherei		

Dienstgebäude: Berliner Chaussee 9
39114 Magdeburg

Postanschrift: Postfach 19 47
39009 Magdeburg

Telefon: (0391) 8 18 03 - 0
Telefax: (0391) 8 18 03 - 33

Internet: http://www.datenschutz.sachsen-anhalt.de

Stand: 31.03.2003

Anlage 2

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. April 2001:

Veröffentlichung von Insolvenzinformationen im Internet

Dem Bundestag liegt ein Gesetzentwurf der Bundesregierung zur Änderung der Insolvenzordnung (BT-Drs. 14/5680) vor. Danach sollen gerichtliche Entscheidungen – vor allem in Verbraucherinsolvenzverfahren – künftig auch über das Internet veröffentlicht werden können, um Kosten für Bekanntmachungen in Printmedien zu sparen.
Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass Informationen aus Insolvenzverfahren, die in das Internet eingestellt sind, durch die Justiz nicht räumlich begrenzt werden können. Darüber hinaus ist deren Speicherung zeitlich nicht beherrschbar, und die Daten können vielfältig ausgewertet werden. Dies kann dazu führen, dass Dritte, etwa Auskunfteien oder Wirtschaftsinformationsdienste, die Daten auch nach Abschluss eines Insolvenzverfahrens speichern und diese über längere Zeit im Internet verfügbar sind. Die mit der Insolvenzordnung bezweckte Chance der Schuldner auf einen wirtschaftlichen Neubeginn würde letztlich auf Dauer beeinträchtigt, wenn sie zeitlebens weltweit abrufbar am Schulden-Pranger stehen.
Der Gesetzgeber muss das Risiko für die betroffenen Verbraucherinnen und Verbraucher, aufgrund einer möglichen Auswertung justizieller Veröffentlichungen im Internet dauerhaft Einbußen bei der Teilnahme am Wirtschaftsverkehr zu erleiden, sorgfältig mit dem Interesse an der beabsichtigten Senkung von Bekanntmachungskosten abwägen. Hierbei ist auch die gesetzgeberische Wertung zu berücksichtigen, dass Personen, für die ein Insolvenzverfahren eröffnet wurde, gerade nicht in das Schuldnerverzeichnis beim Amtsgericht aufgenommen werden. Das Internet bietet im Gegensatz zu einem gerichtlichen Verzeichnis letztlich keine Gewähr, die ordnungsgemäße Pflege und die Löschung personenbezogener Daten sicherzustellen, die für die Betroffenen von entscheidender wirtschaftlicher Bedeutung sein können.

Die Datenschutzbeauftragten appellieren daher an den Gesetzgeber und an die Justizverwaltungen der Länder, die aufgezeigten Risiken insbesondere für Verbraucherinsolvenzen neu zu bewerten. Die vorgenannten Überlegungen sind im Gesetzgebungsverfahren bisher nicht in ausreichendem Maße berücksichtigt worden. Dabei sollten die Erwägungen des Bundesverfassungsgerichts im Beschluss vom 09.03.1988 - 1 BvL 49/86 - zu einem vergleichbaren Sachverhalt einbezogen werden.

Es erscheint zu einfach, die Informationen im Internet in gleicher Weise abzubilden wie in der Zeitung. Gerade das Internet bietet neue Chancen und Möglichkeiten, Informationen gezielt nur denen zugänglich zu machen, die es angeht. Gerade hier sind neue Wege möglich, die mit herkömmlichen Medien nicht erreicht werden konnten. Es gilt deshalb, insbesondere zu untersuchen, ob dem Prinzip der Publizität bei

Veröffentlichungen im Internet nicht ein anderer Stellenwert zukommt und wie gravierende Nachteile für die Betroffenen vermieden werden können.
Bevor die geplante Änderung des § 9 InsO verabschiedet wird, ist daher vorrangig zu klären, wie das Recht auf informationelle Selbstbestimmung der Betroffenen besser geschützt werden kann.
Auch in anderen Bereichen wird das Internet bereits genutzt, erprobt oder die Nutzung erwogen, um justizielle Informationen bereitzustellen, z.B. die Handels-, Vereins-, Genossenschafts- und Partnerschaftsregister oder in Zwangsvollstreckungsverfahren. Inwieweit das Internet als Medium der im Ergebnis unbegrenzbaren Informationsverarbeitung datenschutzrechtlich angemessen ist und welches Datenprofil ins Internet eingestellt werden darf, muss differenziert in Übereinstimmung mit dem gesetzlich bezweckten Grad der Publizität der jeweiligen Daten entschieden werden. Jede gesetzgeberische Entscheidung für eine Veröffentlichung über das Internet sollte aber im Hinblick auf deren besondere Risiken regeln, dass Veröffentlichungen befristet sind und dass spezielle Vorkehrungen getroffen werden, um die Identität und die Authentizität zu sichern sowie eine automatische Übernahme der Daten zu verhindern (Kopierschutz).

Sollte sich der Gesetzgeber nach sorgfältiger Abwägung für eine Veröffentlichung über das Internet entscheiden, so muss er die Auswirkungen der Regelung auf Grund aussagefähiger Berichte der Landesjustizverwaltungen überprüfen. Gegenstand dieser Überprüfung muss auch sein, ob die eingetretene Kostensenkung tatsächlich, wie von der Bundesregierung erwartet, einer größeren Anzahl von Schuldnerinnen und Schuldnern den Weg zur Restschuldbefreiung eröffnet hat.

Anlage 3

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 01. Oktober 2001:

Terrorismusbekämpfung

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen mit Nachdruck den Kampf des demokratischen Rechtsstaats gegen Terrorismus und organisierte Kriminalität. Sie sind heute zu einem Sondertreffen in Bonn zusammengekommen, um die aktuelle Situation nach den Terroranschlägen zu erörtern. Im politischen Raum werden zahlreiche Forderungen und Vorschläge zur Verbesserung der inneren Sicherheit diskutiert, die auch Auswirkungen auf den Datenschutz haben.
Die Datenschutzbeauftragten weisen darauf hin, dass die Sicherheits- und Strafverfolgungsbehörden zur Terrorismusbekämpfung bereits über weitreichende Befugnisse zur Datenverarbeitung verfügen. So ist z.B. die Rasterfahndung zu Strafverfolgungszwecken generell möglich, in den meisten Ländern auch zur Gefahrenabwehr durch die Polizei. Das Bundesamt für die Anerkennung ausländischer Flüchtlinge kann bereits heute Erkenntnisse über terroristische Aktivitäten an den Verfassungsschutz und die Polizei übermitteln. Auch ist eine effektive Zusammenarbeit zwischen Polizei und Verfassungsschutz durch die geltende Rechtslage gewährleistet; Vollzugsdefizite sind kein Datenschutzproblem. Zu pauschalen Forderungen nach Einschränkung des Bürgerrechts auf Datenschutz besteht deshalb kein Anlass. Die Datenschutzbeauftragten betonen, dass Datenschutz nie Täterschutz war und auch in Zukunft nicht sein wird.
Die Datenschutzbeauftragten sind zu einem offenen und konstruktiven Dialog über etwa notwendige Anpassungen an die neue Bedrohungslage bereit. Sie erwarten, dass sie rechtzeitig beteiligt werden. Die Datenschutzbeauftragten warnen vor übereilten Maßnahmen, die keinen wirksamen Beitrag zur Terrorismusbekämpfung leisten, aber die Freiheitsrechte der Bürgerinnen und Bürger einschränken. Sie sprechen sich dafür aus, alle neu beschlossenen Eingriffsbefugnisse zu befristen und tiefgreifende Eingriffsbefugnisse, damit auch die laufende Rasterfahndung, einer ergebnisoffenen Erfolgskontrolle zu unterziehen.

Bei der künftigen Gesetzgebung sind die grundlegenden Rechtsstaatsprinzipien, das Grundrecht der freien Entfaltung der Persönlichkeit, das Verhältnismäßigkeitsprinzip, die Unschuldsvermutung und das Gebot besonderer gesetzlicher Verwendungsregelungen für sensible Daten selbstverständlich zu beachten. Diese verfassungsrechtlichen Garantien prägen den Rechtsstaat, den wir gemeinsam zu verteidigen haben.

Anlage 4

Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. - 26. Oktober 2001:

EUROJUST – Vorläufer einer künftigen europäischen Staatsanwaltschaft?

Der Europäische Rat hat im Herbst 1999 in Tampere die Einrichtung einer gemeinsamen Stelle EUROJUST zur justiziellen Zusammenarbeit beschlossen. EUROJUST soll zur Bekämpfung der schweren organisierten Kriminalität eine sachgerechte Koordinierung der nationalen Staatsanwaltschaften erleichtern und die strafrechtlichen Ermittlungen unterstützen sowie die Erledigung von Rechtshilfeersuchen vereinfachen. Zusätzlich beschloss der Rat im Dezember 2000 die Einrichtung einer vorläufigen Stelle zur justiziellen Zusammenarbeit, PRO-EUROJUST genannt, die am 1. März 2001 ihre Arbeit aufgenommen hat. Diese Stelle soll bis zur Einrichtung von EUROJUST die Zusammenarbeit der Ermittlungsbehörden auf dem Gebiet der Bekämpfung der schweren grenzüberschreitenden Kriminalität verbessern und die Koordinierung von Ermittlungen anregen und verstärken. Ein Beschluss des Rates über die Einrichtung von EUROJUST soll bis Ende des Jahres 2001 verabschiedet werden.

Die Aufgabenstellung von EUROJUST führt möglicherweise dazu, dass eine europäische Großbehörde heranwächst, die Daten nicht nur über verdächtige Personen, sondern auch über Opfer und Zeugen sammeln soll, und damit zwangsläufig tiefgreifende Eingriffe in Bürgerrechte vornehmen würde. In diesem Falle käme als Grundlage für EUROJUST nur eine Konvention in Betracht, da für künftige Grundrechtseingriffe durch EUROJUST eine demokratische Legitimation notwendig wäre.

Mit Blick auf die sensiblen personenbezogenen Daten, die von EUROJUST erhoben, verarbeitet und genutzt werden sollen, und unter Berücksichtigung der eigenen Rechtspersönlichkeit von EUROJUST sind umfassende Datenschutzvorschriften erforderlich. Diese müssen sowohl Regelungen zur Verarbeitung, Speicherung, Nutzung, Berichtigung, Löschung als auch zum Auskunftsanspruch des Betroffenen sowie zu einer Kontrollinstanz von EUROJUST enthalten.
Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder sind folgende datenschutzrechtliche Anforderungen an EUROJUST zu stellen:

- Informationsaustausch mit Partnern
  Der Informationsaustausch mit Partnern sollte EUROJUST dann erlaubt sein, wenn er zur Erfüllung seiner Aufgaben erforderlich ist. Bei Weiterleitung dieser Daten an Drittstaaten und –stellen ist die Zustimmung des Mitgliedstaates einzuholen, von dem diese Daten geliefert wurden. Sind personenbezogene Daten betroffen, so muss grundsätzlich eine Übereinkunft zwischen EUROJUST und der Partnerstelle über den Datenschutzstandard getroffen werden. Nur in absoluten Ausnahmefällen, die einer restriktiven Regelung bedürfen, sollte eine Datenübermittlung auch bei Fehlen einer solchen Vereinbarung zulässig sein.

- Verarbeitung personenbezogener Daten
  Der Katalog der personenbezogenen Daten, die automatisiert verarbeitet werden dürfen, ist streng am Maßstab der Erforderlichkeit und an den Aufgaben von EUROJUST zu orientieren. Eine zusätzliche Öffnungsklausel, die letztlich die Speicherung aller Daten zulassen würde, ist abzulehnen. Eine Verarbeitung der Daten von Opfern und Zeugen darf, wenn überhaupt erforderlich, nur unter einschränkenden Bedingungen vorgenommen werden.

- Ermittlungsindex und Dateien
  Der Ermittlungsindex sollte so ausgestaltet sein, dass es sich um eine reine Vorgangsverwaltung handelt. Sofern zusätzlich Arbeitsdateien geführt werden, sind sie genau zu bezeichnen.

- Auskunftsrecht
  Wenn EUROJUST Daten verarbeitet, die ursprünglich von einem Mitgliedstaat geliefert wurden, handelt es sich im Ergebnis um Daten von EUROJUST. Insofern ist ein eigener Auskunftsanspruch von Betroffenen gegenüber EUROJUST unverzichtbar. Für den Fall, dass im Strafverfolgungsinteresse oder aus sonstigen Gründen des Gemeinwohls von einer Auskunft an den Betroffenen abgesehen werden soll, muss eine Abwägung mit den Interessen des Betroffenen an einer Auskunftserteilung vorangegangen sein.

- Änderung, Berichtigung und Löschung
  Es sollte auch eine Regelung zur Sperrung von Daten ausgenommen werden, die dazu führt, dass Daten unter bestimmten Voraussetzungen nicht gelöscht, sondern lediglich gesperrt werden.

- Speicherungsfristen
  Sofern Daten nach Ablauf bestimmter sonstiger Fristen zu löschen sind, z.B. nach Ablauf der Verjährungsfrist einzelner Mitgliedstaaten, sollte sich die Speicherungsfrist bei EUROJUST nach der Frist des Mitgliedstaates richten, in dem sie am kürzesten ist, um eine mögliche Umgehung nationaler Löschungsfristen zu vermeiden. Die Prüffristen sollten zwei Jahre betragen und auch für Folgeprüfungen nicht länger sein.

- Datensicherheit
  Erforderlich sind konkrete Vorschriften zur Datensicherheit. Um den Text des Beschlusses nicht zu überfrachten, könnte eine Regelung entsprechend Art. 22 der Verordnung EG 45/2001 oder § 9 BDSG vorgesehen werden.

- Gemeinsame Kontrollinstanz
  Die Erforderlichkeit einer gemeinsamen Kontrollinstanz für EUROJUST muss außer Frage stehen. Die Unabhängigkeit dieser gemeinsamen Kontrollinstanz ist bereits durch die personelle Zusammensetzung zu gewährleisten. Sowohl für die EUROJUST-Mitglieder als auch das Kollegium müssen die Entscheidungen der gemeinsamen Kontrollinstanz bindender Charakter haben.

- Rechtsschutz
  Dem Betroffenen ist ein angemessener Rechtsschutz gegenüber EUROJUST zu gewähren. Es sollte festgelegt werden, welche nationale oder supranationale Gerichtsbarkeit für Klagen auf Auskunft, Löschung, Berichtigung und Schadensersatz zuständig ist.

- Rechtsetzungsbedarf
  Zur Erfüllung seiner Aufgaben muss EUROJUST Auskünfte über strafrechtliche Ermittlungsverfahren einholen. Nach geltendem Recht (§ 474 StPO) können die Ermittlungsbehörden der Bundesrepublik Deutschland derartigen Ersuchen nicht stattgeben.
  Darüber hinaus bedarf der Zugriff des deutschen EUROJUST-Mitglieds auf das Bundeszentralregister und auf das Zentrale Staatsanwaltschaftliche Verfahrensregister einer eindeutigen gesetzlichen Grundlage.

Anlage 5

Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. - 26. Oktober 2001:

Entschließung zur gesetzlichen Regelung von genetischen Untersuchungen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder konkretisiert ihre Forderungen an Bundestag und Bundesrat, genetische Untersuchungen am Menschen gesetzlich zu regeln. Geboten sind besondere Regelungen für genetische Untersuchungen zu medizinischen Zwecken, zur Klärung von Identität und Abstammung, im Zusammenhang mit Arbeits- und Versicherungsverhältnissen sowie zu Forschungszwecken. Außer dem „genetischen Fingerabdruck“ für Zwecke der Strafverfolgung – in der Strafprozessordnung bereits normiert – sind typische Anwendungsfelder für genetische Untersuchungen zu regeln. Von besonderer Bedeutung sind das Informations- und Entscheidungsrecht der betroffenen Personen. Die Kernanliegen der Datenschutzbeauftragten sind:

- Stärkung des Selbstbestimmungsrechts durch einen grundsätzlichen Einwilligungsvorbehalt für die Durchführung genetischer Untersuchungen;
- Information und Transparenz für die betroffene Person durch Umschreibung des notwendigen Aufklärungsumfangs;
- Qualität und Sicherheit genetischer Tests durch Arzt- und Zulassungsvorbehalte;
- Schutz von Ungeborenen, Minderjährigen und nicht einsichtsfähigen Personen durch abgestufte Beschränkung zugelassener Untersuchungsziele;
- Gewährleistung des Rechts auf Nichtwissen durch differenzierte Entscheidungs- und Offenbarungsoptionen;
- Verhinderung heimlicher Gentests durch das Gebot der Probennahme direkt in ärztlicher Praxis oder Labor;
- Verhinderung von missbräuchlicher Nutzung genetischer Erkenntnisse im Arbeitsleben und im Versicherungsverhältnis durch ein grundsätzliches Verbot, Gentests oder Testergebnisse zu fordern oder entgegen zu nehmen;
- Selbstbestimmung der Betroffenen auch im Forschungsbereich durch einen grundsätzlichen Einwilligungsvorbehalt bei einzelnen Forschungsprojekten und Proben- und Gendatenbanken;
- Sicherung zuverlässiger Pseudonymisierungsverfahren bei Proben- und Gendatenbanken durch externe Datentreuhänderschaft;
- Hilfe für die Betroffenen durch die Pflicht, im Rahmen der Forschung, individuell bedeutsame Untersuchungsergebnisse mitzuteilen;
- Absicherung der Regelungen durch die Einführung von Straftatbeständen.

Neben diesen bereichsspezifischen Bestimmungen zu den verschiedenen Zwecken genetischer Untersuchungen fordert die Konferenz der Datenschutzbeauftragten eine grundlegende Strafnorm im Strafgesetzbuch, um Gentests ohne gesetzliche Ermächtigung oder ohne die grundsätzlich nur für Zwecke der medizinischen Behandlung oder Forschung wirksame Einwilligung der betroffenen Person zu unterbinden.

Die Datenschutzbeauftragten des Bundes und der Länder verstehen ihre Vorschläge als Anregungen zu anstehenden Gesetzesinitiativen und zur gesellschaftspolitischen Diskussion.

Anlage 6

Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. - 26. Oktober 2001:

"Neue Medienordnung"

Bund und Länder beraten gegenwärtig über die Grundzüge einer neuen Medienordnung. Zu den dabei zu beachtenden verfassungsrechtlichen Rahmenbedingungen gehören neben den Gesetzgebungskompetenzen von Bund und Ländern auch die Grundrechte auf Schutz der Privatsphäre und der personenbezogenen Daten, Meinungsfreiheit und Vertraulichkeit der Kommunikation. Diese Rechte müssen in einer neuen Medienordnung durchgängig gewährleistet bleiben.

Angesichts der technischen Entwicklung und der Konvergenz der Medien darf der Grad der Vertraulichkeit nicht mehr allein davon abhängig sein, ob ein Kommunikationsvorgang der Telekommunikation, den Tele- oder den Mediendiensten zugeordnet wird. Vielmehr muss für alle Formen der Kommunikation und der Mediennutzung ein angemessen hoher Schutz gewährleistet werden.

Aus diesem Grund fordert die Konferenz, das Fernmeldegeheimnis nach Art. 10 GG zu einem allgemeinen Kommunikations- und Mediennutzungsgeheimnis weiter zu entwickeln und einfachgesetzlich abzusichern.

Die Konferenz tritt in diesem Zusammenhang dafür ein, die einschlägigen Rechtsvorschriften inhaltlich stärker einander anzugleichen, klarer zu strukturieren und für Nutzende und Anbietende verständlicher zu gestalten.

Anlage 7

Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. - 26. Oktober 2001:

Datenschutzrechtliche Anforderungen an den "Arzneimittelpass" (Medikamentenchipkarte)

Vor dem Hintergrund der Lipobay-Diskussion hat das Bundesministerium für Gesundheit die Einführung eines "Arzneimittelpasses" in Form einer (elektronisch nutzbaren) Medikamentenchipkarte befürwortet; auf der Karte sollen alle ärztlichen Verordnungen verzeichnet werden. Damit soll eine größere Transparenz der Arzneimittelverordnungen erreicht werden. Bisher ist nicht ansatzweise belegt, dass die bekannt gewordenen Gefahren für die Patientinnen und Patienten dadurch entstanden sind, dass verschiedene Ärztinnen und Ärzte ohne Kenntnis voneinander unverträgliche Medikamente verordnet hätten. Deswegen ist auch nicht ersichtlich, dass die aufgetretenen Probleme mit einem Arzneimittelpass hätten verhindert werden können.

Aus datenschutzrechtlicher Sicht bestehen erhebliche Bedenken gegen eine Medikamentenchipkarte als **Pflichtkarte**. Die Datenschutzbeauftragten begrüßen es daher ausdrücklich, dass der Gedanke einer Pflichtkarte fallen gelassen wurde. Die Patientinnen und Patienten würden sonst rechtlich oder faktisch gezwungen, die ihnen verordneten Medikamente und damit zumeist auch ihre Erkrankung bei jedem Arzt- und/oder Apothekenbesuch ohne ihren Willen zu offenbaren. Dies würde eine wesentliche Einschränkung des Arztgeheimnisses bewirken, das auch gegenüber anderen Ärztinnen und Ärzten gilt. Zudem würde sich dadurch das Vertrauensverhältnis, das für die Behandlung und für eine funktionierende Gesundheitsfürsorge insgesamt unabdingbar ist, grundlegend verändern. Darüber hinaus wäre das Einholen einer unbeeinflussten Zweitmeinung nahezu ausgeschlossen.

Die freie und unbeeinflusste Entscheidung der Patientinnen und Patienten über Einsatz und Verwendung der Karte muss gewährleistet werden (**Grundsatz der Freiwilligkeit**).

Die Datenschutzbeauftragten des Bundes und der Länder haben bereits auf ihrer 47. Konferenz im März 1994 und auf ihrer 50. Konferenz im November 1995 zum freiwilligen Einsatz von Chipkarten im Gesundheitswesen Stellung genommen; deren Zulässigkeit wird dort von verschiedenen Bedingungen zur Sicherung des Persönlichkeitsrechts der Patientinnen und Patienten abhängig gemacht. Grundlegende Voraussetzung ist vor allem die freie Entscheidung der Betroffenen (auch als Versicherte). Sie müssen entscheiden können,

- ob ihre Daten auf einer Chipkarte gespeichert werden,
- welche ihrer Gesundheitsdaten auf die Karte aufgenommen werden,
- welche ihrer Daten auf der Karte wieder gelöscht werden,
- ob sie die Karte bei einem Arzt- oder Apothekenbesuch vorlegen und
- welche ihrer Daten sie im Einzelfall zugänglich machen (die Technik muss eine partielle Freigabe ermöglichen).

Die Verantwortung für die Wahrung der Arzneimittelsicherheit tragen grundsätzlich die Ärztinnen und Ärzte sowie die Apothekerinnen und Apotheker. Sie darf nicht auf die Betroffenen abgewälzt werden. Dies gilt auch, wenn sie von dem "Arzneimittelpass" keinen Gebrauch machen.

Der Chipkarteneinsatz darf nicht zur Entstehung neuer zentraler Datensammlungen über Patientinnen und Patienten führen.

Datenschutzrechtlich problematisch wäre es, den "Arzneimittelpass" auf der **Krankenversichertenkarte** gemäß § 291 SGB V zu implementieren. Eine solche Erweiterung wäre allenfalls vertretbar, wenn die "Funktion Krankenversichertenkarte" von der "Funktion Arzneimittelpass" informationstechnisch getrennt würde, so dass die Patientinnen oder Patienten bei einem Arzt- oder Apothekenbesuch nicht gezwungen werden, ihre gesamten Gesundheitsdaten ungewollt zu offenbaren. Ihre Entscheidungsfreiheit, wem gegenüber sie welche Gesundheitsdaten offen legen, müsste also durch die technische Ausgestaltung der Karte gewährleistet sein.

Die Betroffenen müssen ferner das Recht und die Möglichkeit haben, ihre auf der Chipkarte gespeicherten Daten vollständig zu lesen.

Die Verwendung der Karte außerhalb des medizinischen Bereichs, z.B. durch Arbeitgeberinnen und Arbeitgeber oder Versicherungen, muss gesetzlich verboten und sanktioniert werden.

Anlage 8

Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. - 26. Oktober 2001:

Lkw-Maut auf Autobahnen und zur allgemeinen Maut auf privat errichteten Bundesfernstraßen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, bei der technischen Realisierung und bei der anstehenden internationalen Normierung elektronischer Mautsysteme datenschutzrechtliche Anforderungen durchzusetzen.

Das Bundeskabinett hat am 15. August 2001 den Gesetzentwurf für die Einführung eines solchen Mautsystems beschlossen. Ab 2003 ist neben der manuellen Erfassung der Gebühren ein automatisches System geplant, mit dem eine streckenbezogene Autobahnbenutzungsgebühr (Maut) für Lastkraftwagen erhoben werden soll. Das Bundesministerium für Verkehr, Bau- und Wohnungswesen prüft zurzeit Angebote, die im Ergebnis einer europaweiten Ausschreibung eingegangen sind.

Für das automatische System sollen das Satellitennavigationssystem GPS und die Mobilfunktechnologie genutzt werden. Dadurch werden stationäre Erfassungseinrichtungen entbehrlich. Relativ einfach könnte so das mautpflichtige Straßennetz beispielsweise auf den Bereich der Bundesstraßen ausgedehnt werden. Selbst ein grenzüberschreitender Einsatz derartiger Systeme wäre aus technischer Sicht leicht zu realisieren. Entsprechendes Interesse aus dem benachbarten Ausland ist bereits bekundet worden.

Die verfügbare, im Gesetzentwurf nicht festgeschriebene Technik ermöglicht es prinzipiell, den Fahrweg der Mautpflichtigen detailliert zu dokumentieren und zu archivieren und auf diese Weise exakte Bewegungsprofile zu erstellen. Damit würden die Voraussetzungen geschaffen, dass Systembetreiber und andere nachvollziehen können, wer wann wohin gefahren ist. Die Datenschutzbeauftragten des Bundes und der Länder halten es deshalb für unverzichtbar, elektronische Mautsysteme datenschutzgerecht auszugestalten.
Insbesondere ist dafür Sorge zu tragen, dass die Erhebung und Speicherung ausschließlich für Abrechungszwecke verwendet werden.

Weiterhin ist bei Gestaltung und beim Betrieb der erforderlichen Erfassungs- und Kontrollsysteme das im Bundesdatenschutzgesetz normierte Prinzip der Datensparsamkeit sicherzustellen. Das erfordert den Einsatz von Verfahren, bei denen Mautgebühren vorab entrichtet werden können, ohne dass dafür die Erhebung und Speicherung personenbeziehbarer Daten erforderlich ist.

Insbesondere ist sicherzustellen, dass damit keine oder so wenig personenbezogene Daten wie möglich erhoben, verarbeitet oder genutzt werden. Soweit personenbezogene Daten beispielsweise für Abrechnungs- oder Kontrollzwecke gespeichert werden, sind sie zum frühestmöglichen Zeitpunkt, spätestens jedoch nach Entrichtung

der Straßenbenutzungsgebühr beziehungsweise nach Abschluss eines Mauterstattungsverfahrens zu löschen, wenn sie nicht mehr für die Abwicklung des Mautverfahrens oder für erforderliche Kontroll- oder Prüfverfahren benötigt werden.

Bereits 1995 haben die Datenschutzbeauftragten des Bundes und der Länder Anforderungen an Systeme zur automatischen Erhebung von Straßennutzungsgebühren formuliert. Insbesondere die folgenden Aspekte sind nach wie vor aktuell:

- Die Überwachung der Gebührenzahlung darf nur stichprobenweise erfolgen. Die Identität der Mautpflichtigen darf nur dann aufgedeckt werden, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Gebühren nicht entrichtet worden sind.
- Die Verfahren der Gebührenerhebung und -kontrolle müssen für die Mautpflichtigen durchschaubar sein. Sie müssen sich jederzeit über den Abrechnungsvorgang informieren sowie den eventuellen Kontrollvorgang erkennen können.
- Alle datenschutzrelevanten Systemkomponenten sind so auszugestalten, dass sie weder vom Betreiber noch von anderer Seite beeinträchtigt oder zurückgenommen werden können.
- Es ist sicherzustellen, dass anfallende personenbezogenen Daten von allen beteiligten Stellen vertraulich behandelt werden und einer strikten Zweckbindung unterliegen.

Außerdem liegt ein Gesetzentwurf vor, der zur Erhebung von Mautgebühren an Brücken, Tunneln und Gebirgspässen im Zuge von Bundesautobahnen und Bundesstraßen sowie an mehrspurigen Bundesstraßen mit getrennten Fahrbahnen berechtigt, soweit sie von Privaten errichtet sind. Die Mautpflicht gilt für alle Kraftfahrzeuge. Deshalb muss an der im Entwurf vorgesehenen Barzahlungsmöglichkeit ohne Verarbeitung personenbezogener Daten unbedingt festgehalten werden. Ihre Ausgestaltung sollte kundenfreundlich erfolgen. Diese Zahlungsweise vermeidet die weitergehende Datenerfassung für alle Mautpflichtigen (Kennzeichen und Bilder der Fahrzeuge). In der zu erlassenden Rechtsverordnung muss deshalb insbesondere sichergestellt werden, dass keine Datenerfassung bei Personen erfolgt, die die Gebühr unmittelbar entrichten.

Anlage 9

Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. - 26. Oktober 2001:

Biometrische Merkmale in Personalausweisen und Pässen

Im Entwurf eines Terrorismusbekämpfungsgesetzes ist vorgesehen, die Möglichkeit zu eröffnen, in deutschen Personalausweisen und Pässen neben dem Lichtbild und der Unterschrift weitere biometrische Informationen wie zum Beispiel Fingerabdrücke, Handgeometrie, Gesichtsgeometrie u.a. aufzunehmen. Auch die Verwendung genetischer Daten wird nicht ausgeschlossen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass diese Maßnahme schon allein wegen des technischen und zeitlichen Aufwandes, der mit der Einführung derartiger Dokumente verbunden wäre, keinen kurzfristigen Beitrag zur Lösung der mit dem internationalen Terrorismus derzeit verbundenen Probleme leisten kann, zumal Ausländerinnen und Ausländer, die sich in Deutschland aufhalten, nicht erfasst werden.

Die Nutzung biometrischer Merkmale in Personalausweisen und Pässen sowie die damit verbundenen Folgeprobleme (zum Beispiel Art und Ort der Speicherung von Referenzdaten; Vermeidung von Überschussinformationen) werfen eine Vielzahl schwieriger Fragen auf, die einer ausführlichen Diskussion bedürfen. Die zuständigen Stellen werden hierzu aufgefordert, die Notwendigkeit und die rechtlichen und technischen Einzelheiten einer Realisierung dieser Maßnahmen darzulegen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist bereit, sich unter diesen Voraussetzungen mit der Frage zu befassen, ob und wie es möglich ist, mit Hilfe geeigneter zusätzlicher Merkmale in Identifikationspapieren deren Missbrauch zu verhindern, ohne dabei die Grundsätze des Datenschutzes zu verletzen.

Anlage 10

Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. - 26. Oktober 2001:

Grundsätze zur Übermittlung von Telekommunikationsverbindungsdaten

Die Bundesregierung hat den Gesetzentwurf für eine Nachfolgeregelung zu § 12 FAG vorgelegt, der eine Reihe datenschutzrechtlich positiver Ansätze enthält. Der Bundesrat hat sich demgegenüber in seiner Stellungnahme für eine Regelung ausgesprochen, die wesentlichen datenschutzrechtlichen Anforderungen nicht gerecht wird. Die Datenschutzbeauftragten des Bundes und der Länder lehnen den Vorschlag des Bundesrates entschieden ab.

Sie halten es für nicht vertretbar, Auskünfte über zurückliegende Aktivmeldungen von Mobiltelefonen auch bei reinem Stand-by-Betrieb zu erteilen und Diensteanbieter zur Aufzeichnung von Telekommunikationsverbindungsdaten eigens für Zwecke der Strafverfolgung zu verpflichten.

Auch die vom Bundesrat vorgeschlagene Regelung des § 18a BVerfSchG zur Übermittlung von Telekommunikationsverbindungsdaten an die Verfassungsschutzbehörden halten die Datenschutzbeauftragten des Bundes und der Länder für nicht akzeptabel. Sie fordern eine deutliche Klarstellung im Wortlaut des Gesetzes, dass Verbindungsdaten an den Verfassungsschutz nur dann übermittelt werden dürfen, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand eine in § 3 Abs. 1 G 10 genannte Straftat plant, begeht oder begangen hat oder sonst an gewalttätigen Bestrebungen oder sicherheitsgefährdenden Tätigkeiten teilnimmt. Eine Übermittlung der Verbindungsdaten für den gesamten Aufgabenbereich des Verfassungsschutzes ginge dagegen erheblich zu weit.

Ferner halten es die Datenschutzbeauftragten für geboten, hinsichtlich der Kennzeichnung und Zweckbindung der Daten, der Mitteilungen an Betroffene und der parlamentarischen Kontrolle einen dem G 10 möglichst gleichwertigen Standard zu gewährleisten.

Die Bundesregierung und der Deutsche Bundestag werden gebeten, diese datenschutzrechtlichen Mindestanforderungen im weiteren Gesetzgebungsverfahren zu berücksichtigen.

Anlage 11

Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. - 26. Oktober 2001:

Freiheits- und Persönlichkeitsrechte dürfen bei der Terrorismusbekämpfung nicht verloren gehen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass zahlreiche Vorschläge in der gegenwärtigen Debatte um notwendige Konsequenzen aus den Terroranschlägen vom 11. September 2001 die erforderliche sachliche und verantwortungsbewusste Abwägung mit den grundgesetzlich geschützten Freiheits- und Persönlichkeitsrechten der Einzelnen vermissen lassen.
Der Entwurf eines Terrorismusbekämpfungsgesetzes und der Antrag der Länder Baden-Württemberg, Bayern und Hessen im Bundesrat zur wirksamen Bekämpfung des internationalen Terrorismus und Extremismus (BR-Drs. 807/01) übertreffen die in der Entschließung der Konferenz vom 1. Oktober 2001 geäußerte Befürchtung, dass übereilt Maßnahmen ergriffen werden sollen, die keinen wirksamen Beitrag zur Terrorismusbekämpfung leisten, aber die Freiheitsrechte der Bürgerinnen und Bürger unangemessen einschränken.
Gegenwärtig wird ohne Rücksicht auf das grundrechtliche Übermaßverbot vorgeschlagen, was technisch möglich erscheint, anstatt zu prüfen, was wirklich geeignet und erforderlich ist. Außerdem müsste der Frage nachgegangen werden, ob es nicht in den Geheimdiensten und in der Strafverfolgung Vollzugsdefizite gibt. Dabei müsste auch untersucht werden, welche Resultate die vielen Gesetzesverschärfungen der letzten Jahre gebracht haben.
Persönlichkeitsrechte haben über ihre grundrechtssichernde Wirkung hinaus – mit den Worten des Bundesverfassungsgerichts – auch Bedeutung als „elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich demokratischen Gemeinwesens".

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert daher sehr eindringlich an alle Beteiligten, nicht Persönlichkeitsrechte

vorschnell und ohne die gebotene sorgsam abwägende Prüfung über die bereits bestehenden Eingriffsmöglichkeiten hinaus dauerhaft einzuschränken und so den Ausnahmezustand zur Norm zu erheben.
Alle neu erwogenen Maßnahmen müssen sich daran messen lassen, ob sie für eine wirkungsvolle Bekämpfung des Terrorismus wirklich zielführend und erforderlich sind und ob sie den Verfassungsgrundsatz der Verhältnismäßigkeit einhalten. Einseitiges Streben nach einer umfassenden Sicherheit darf nicht den bisherigen gesellschaftlichen Konsens über die wertsetzende Bedeutung bürgerlicher Freiheits- und Persönlichkeitsrechte so überlagern, dass es in unserem Land zu einer langwirkenden Verschiebung zugunsten staatlicher Überwachung und zu Lasten freier und unbeobachteter Aktion, Bewegung und Kommunikation der Bürgerinnen und Bürger kommt.
Wesentliche im BMI-Entwurf eines Terrorismusbekämpfungsgesetzes enthaltene Eingriffsmöglichkeiten führen zwangsläufig dazu, dass eine Vielzahl völlig unbescholtener Einzelpersonen zentral erfasst oder verdeckt in Datenerhebungen einbezogen

werden, ohne dass eine konkrete Verdachts- oder Gefahrenlage verlangt wird. Zugleich werden Auskunftspflichten und Ermittlungskompetenzen in einer Weise ausgedehnt, dass Eingrenzungen verloren gehen, die aus rechtsstaatlichen Gründen unverzichtbar sind.
Der Verfassungsschutz soll künftig zur Erfüllung aller seiner Aufgaben von den Banken die Kontenbewegungen, von den Luftverkehrsunternehmen alle Reisedaten und von den Post – und Telekommunikationsunternehmen alle Informationen darüber erhalten können, wer von wem Post erhalten und wann mit wem telefoniert hat. All dies soll ohne Wissen der Betroffenen erfolgen und bis zu 15 Jahren gespeichert werden.
Die geplante Befugnis des BKA, Vorermittlungen ohne Anfangsverdacht im Sinne der StPO zu ergreifen, führt zu Eingriffen in das Persönlichkeitsrecht, die weit über das verfassungsrechtlich Zulässige hinausreichen und das tradierte System der Strafverfolgung sprengen. Dies verschiebt die bisher klaren Grenzen zwischen BKA und Verfassungsschutz sowie zwischen Gefahrenabwehr und Strafverfolgung. Ohne jeden Anfangsverdacht soll das BKA künftig Daten über nicht näher eingegrenzte Personenkreise erheben dürfen.

Dies kann im Prinzip jede Bürgerin und jeden Bürger betreffen, ohne dass sie sich auf die Schutzmechanismen der Strafprozessordnung verlassen können.
Auch die Vorschläge der Länder enthalten unvertretbare Einschränkungen von grundgesetzlich geschützten Rechtspositionen. So soll die Gefahrenschwelle für den verdeckten Einsatz technischer Mittel in Wohnungen übermäßig abgesenkt werden. Telekommunikationsunternehmen und Internetprovider sollen gesetzlich verpflichtet werden, Verbindungsdaten (zum Beispiel über den Besuch einer Website oder einer Newsgroup) länger zu speichern, als diese zu Abrechnungszwecken benötigt werden, um sie Sicherheitsbehörden zur Verfügung zu stellen.
Die Datenschutzbeauftragten des Bundes und der Länder fordern, dass neue Eingriffsbefugnisse nicht pauschal ausgerichtet, sondern zielgenau auf konkrete Gefährdungssituationen im terroristischen Bereich zugeschnitten und von vornherein befristet werden. Eine unabhängige Evaluierung nach festgelegten Fristen ist unerlässlich, um Geeignetheit und Erforderlichkeit für die Zukunft sachgerecht beurteilen zu können.

Anlage 12

Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 07./08. März 2002:

Biometrische Merkmale in Personalausweisen und Pässen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eingehend über Geeignetheit, Erforderlichkeit und Angemessenheit der beabsichtigten Einführung biometrischer Merkmale in Ausweisen und Pässen diskutiert. Sie hat ein Positionspapier des Arbeitskreises Technik, das detaillierte Prüfpunkte für die Erprobungsphase einer solcher Maßnahme nennt, zustimmend zur Kenntnis genommen. Für den Fall, dass das Vorhaben trotz noch bestehender Bedenken realisiert werden sollte, hat sie übereinstimmend folgende Anforderungen formuliert:

1. Fälschliche Zurückweisungen berechtigter Personen durch automatisierte Personenerkennungssysteme sind auch bei ständiger Verbesserung der Technik prinzipiell nicht zu vermeiden. Es dürfen deshalb nur Verfahren in Betracht gezogen werden, bei denen die Fehlerquote zumutbar gering ist. In Fehlerfällen muss dafür Sorge getragen werden, dass eine die Betroffenen nicht diskriminierende rasche Aufklärung erfolgt.
2. Zu berücksichtigen ist, dass bei der Anwendung biometrischer Verfahren Zusatzinformationen anfallen können (z.B. Krankheits-, Unfall-, Beschäftigungsindikatoren). Es muss sichergestellt werden, dass die gespeicherten und verarbeiteten Daten keine Rückschlüsse auf zusätzliche personenbezogene Merkmale erlauben.
3. Systeme, die biometrische Daten aus Ausweisen ohne Kenntnis der Betroffenen verarbeiten (sog. passive Systeme), sind abzulehnen.
4. Der Gesetzgeber hat die Verwendung biometrischer Daten in Ausweisen und Pässen grundsätzlich auf die Feststellung beschränkt, dass die dort gespeicherten Daten mit den Merkmalen der jeweiligen Ausweisinhaber und -inhaberinnen übereinstimmen; dies muss erhalten bleiben. Die Verwendung der biometrischen Merkmale für andere öffentliche Zwecke (außer der gesetzlich zugelassenen Verwendung aus dem Fahndungsbestand) wie auch für privatrechtliche Zwecke (Versicherung, Gesundheitssystem) ist auszuschließen. Deshalb hat der Gesetzgeber zu Recht die Einrichtung zentraler Dateien ausgeschlossen. Diese gesetzgeberische Entscheidung darf nicht durch den Aufbau dezentraler Dateien umgangen werden.
5. Die Entscheidung über das auszuwählende biometrische Erkennungssystem verlangt ein abgestimmtes europäisches Vorgehen.

Anlage 13

Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 07./08. März 2002:

Neues Abrufverfahren bei den Kreditinstituten

Nach der Novelle des Gesetzes über das Kreditwesen soll die zuständige Bundesanstalt die von den Kreditinstituten vorzuhaltenden Daten, wer welche Konten und Depots hat, ohne Kenntnis der Kundinnen und Kunden zur eigenen Aufgabenerfüllung oder zu Gunsten anderer öffentlicher Stellen abrufen können. Dies ist ein neuer Eingriff in die Vertraulichkeit der Bankbeziehungen.

Dieser Eingriff in die Vertraulichkeit der Bankbeziehungen muss gegenüber den Kundinnen und Kunden zumindest durch eine aussagekräftige Information transparent gemacht werden. Die Konferenz fordert daher, dass zugleich mit der Einführung dieses Abrufverfahrens eine Verpflichtung der Kreditinstitute zur generellen Information der Kundinnen und Kunden vorgesehen wird und diese die Kenntnisnahme schriftlich bestätigen. Dadurch soll zugleich eine effektive Wahrnehmung des Auskunftsrechts der Kundinnen und Kunden gewährleistet werden.

Die Erweiterung der Pflichten der Kreditinstitute, Kontenbewegungen auf die Einhaltung gesetzlicher Bestimmungen mit Hilfe von EDV-Programmen zu überprüfen, verpflichtet die Kreditinstitute außerdem zu einer entsprechend intensiven Kontenüberwachung (sog. "know your customer principle"). Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass die Überprüfung in einer Weise stattfindet, die ein datenschutzkonformes Vorgehen sicherstellt.

Anlage 14

Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 07./08. März 2002:

Zur datenschutzgerechten Nutzung von E-Mail und anderen Internet-Diensten am Arbeitsplatz

1. Die Arbeitsplätze mit Internet-Zugang sind so zu gestalten, dass keine oder möglichst wenige personenbezogene Daten erhoben werden. Die Nutzung des Internet am Arbeitsplatz darf nicht zu einer vollständigen Kontrolle der Bediensteten führen. Präventive Maßnahmen gegen eine unbefugte Nutzung sind nachträglichen Kontrollen vorzuziehen.
2. Die Beschäftigten sind umfassend darüber zu informieren, für welche Zwecke sie einen Internet-Zugang am Arbeitsplatz nutzen dürfen und auf welche Weise der Arbeitgeber die Einhaltung der Nutzungsbedingungen kontrolliert.
3. Fragen der Protokollierung und einzelfallbezogenen Überprüfung bei Missbrauchsverdacht sind durch Dienstvereinbarungen zu regeln. Die Kommunikation von schweigepflichtigen Personen und Personalvertretungen muss vor einer Überwachung grundsätzlich geschützt bleiben.
4. Soweit die Protokollierung der Internet-Nutzung aus Gründen des Datenschutzes, der Datensicherheit oder des ordnungsgemäßen Betriebs der Verfahren notwendig ist, dürfen die dabei anfallenden Daten nicht zur Leistungs- und Verhaltenskontrolle verwendet werden.
5. Wird den Beschäftigten die private E-Mail-Nutzung gestattet, so ist diese elektronische Post vom Telekommunikationsgeheimnis geschützt. Der Arbeitgeber darf ihren Inhalt grundsätzlich nicht zur Kenntnis nehmen, und hat dazu die erforderlichen technischen und organisatorischen Vorkehrungen zu treffen.
6. Der Arbeitgeber ist nicht verpflichtet, die private Nutzung des Internet am Arbeitsplatz zu gestatten. Wenn er dies gleichwohl tut, kann er die Gestattung unter Beachtung der hier genannten Grundsätze davon abhängig machen, dass die Beschäftigten einer Protokollierung zur Durchführung einer angemessenen Kontrolle der Netzaktivitäten zustimmen.
7. Die gleichen Bedingungen wie bei der Nutzung des Internet müssen prinzipiell bei der Nutzung von Intranets gelten.

Die Datenschutzbeauftragten fordern den Bundesgesetzgeber auf, auch wegen des Überwachungspotentials moderner Informations- und Kommunikationstechnik am Arbeitsplatz die Verabschiedung eines umfassenden Arbeitnehmerdatenschutzgesetzes nicht länger aufzuschieben.

Anlage 15

Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 07./08. März 2002:

Umgang mit personenbezogenen Daten bei Anbietern von Tele-, Medien- und Telekommunikationsdiensten

Mit der rasch wachsenden Nutzung des Internet kommt dem datenschutzgerechten Umgang mit den dabei anfallenden Daten der Nutzerinnen und Nutzer immer größere Bedeutung zu. Die Datenschutzbeauftragten haben bereits in der Vergangenheit (Entschließung der 59. Konferenz "Für eine freie Telekommunikation in einer freien Gesellschaft") darauf hingewiesen, dass das Telekommunikationsgeheimnis eine unabdingbare Voraussetzung für eine freiheitliche demokratische Kommunikationsgesellschaft ist. Seine Geltung erstreckt sich auch auf Multimedia- und E-Mail-Dienste.
Die Datenschutzbeauftragten betonen, dass das von ihnen geforderte in sich schlüssige System von Regelungen staatlicher Eingriffe in das Kommunikationsverhalten, das dem besonderen Gewicht des Grundrechts auf unbeobachtete Telekommunikation unter Beachtung der legitimen staatlichen Sicherheitsinteressen Rechnung trägt, nach wie vor fehlt. Die Strafprozessordnung (und seit dem 1.1.2002 das Recht der Nachrichtendienste) enthält ausreichende Befugnisse, um den Strafverfolgungsbehörden (und den Nachrichtendiensten) im Einzelfall den Zugriff auf bei den Anbietern vorhandene personenbezogene Daten zu ermöglichen. Für eine zusätzliche Erweiterung dieser Regelungen z.B. hin zu einer Pflicht zur Vorratsdatenspeicherung besteht nicht nur kein Bedarf, sondern eine solche Pflicht würde dem Grundrecht auf unbeobachtete Kommunikation nicht gerecht, weil damit jede Handlung (jeder Mausklick) im Netz staatlicher Beobachtung unterworfen würde.
In keinem Fall sind Anbieter von Tele-, Medien- und Telekommunikationsdiensten berechtigt oder verpflichtet, generell Daten über ihre Nutzerinnen und Nutzer auf Vorrat zu erheben, zu speichern oder herauszugeben, die sie zu keinem Zeitpunkt für eigene Zwecke (Herstellung der Verbindung, Abrechnung) benötigen. Sie können nur im Einzelfall berechtigt sein oder verpflichtet werden, bei Vorliegen ausdrücklicher gesetzlicher Voraussetzungen Nachrichteninhalte, Verbindungsdaten und bestimmte Daten (Nutzungsdaten), die sie ursprünglich für eigene Zwecke benötigt haben und nach den Bestimmungen des Multimedia-Datenschutzrechts löschen müssten, den Strafverfolgungsbehörden (oder Nachrichtendiensten) zu übermitteln.

Anlage 16

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. Mai 2002:

Geplanter Identifikationszwang in der Telekommunikation

Das Bundesministerium für Wirtschaft und Technologie hat einen Entwurf zur Änderung des Telekommunikationsgesetzes veröffentlicht. Der Entwurf hat das Ziel, jeden Anbieter, der geschäftsmäßig Telekommunikationsdienste erbringt, dazu zu verpflichten, Namen, Anschriften, Geburtsdaten und Rufnummern seiner Kundinnen und Kunden zu erheben. Die Kundinnen und Kunden werden verpflichtet, dafür ihren Personalausweis vorzulegen, dessen Nummer ebenfalls gespeichert werden soll. Die beabsichtigten Änderungen sollen in erster Linie dazu führen, auch Nutzerinnen und Nutzer von Prepaid-Karten (also die Erwerberinnen und Erwerber von SIM-Karten ohne Vertrag) im Mobilfunk erfassen zu können. Die erhobenen Daten sollen allein dem Zweck dienen, den Sicherheitsbehörden zum jederzeitigen Online-Abruf über die Regulierungsbehörde für Telekommunikation und Post bereitzustehen. Im gleichen Zuge sollen die Zugriffsmöglichkeiten der Sicherheitsbehörden auf diese Daten dadurch erheblich erweitert werden, indem auf die Kundendateien nach abstrakten Merkmalen zugegriffen werden kann.
Die Datenschutzbeauftragten des Bundes und der Länder lehnen dieses Vorhaben ab. Unter der unscheinbaren Überschrift "Schließen von Regelungslücken" stehen grundlegende Prinzipien des Datenschutzes zur Disposition. Kritikwürdig an dem geplanten Gesetz sind insbesondere die folgenden Punkte:

- Der geplante Grundrechtseingriff ist nicht erforderlich, um die Ermittlungstätigkeit der Sicherheitsbehörden zu erleichtern. Seine Eignung ist zweifelhaft: Auch die Gesetzesänderung wird nicht verhindern, dass Straftäterinnen und Straftäter bewusst und gezielt in kurzen Zeitabständen neue Prepaid-Karten erwerben, Strohleute zum Erwerb einsetzen, die Karten häufig - teilweise nach jedem Telefonat - wechseln oder die Karten untereinander tauschen. In der Begründung wird nicht plausibel dargelegt, dass mit dem geltenden Recht die Ermittlungstätigkeit tatsächlich behindert und durch die geplante Änderung erleichtert wird. Derzeit laufende Forschungsvorhaben beziehen diese Frage nicht mit ein.

- Der Entwurf widerspricht auch dem in den Datenschutzrichtlinien der Europäischen Union verankerten Grundsatz, dass Unternehmen nur solche personenbezogenen Daten verarbeiten dürfen, die sie selbst zur Erbringung einer bestimmten Dienstleistung benötigen.

- Die Anbieter würden eine Reihe von Daten auf Vorrat speichern müssen, die sie selbst für den Vertrag mit ihren Kunden nicht benötigen. Die ganz überwiegende Zahl der Nutzerinnen und Nutzer von Prepaid-Karten, darunter eine große Zahl Minderjähriger, würde registriert, obwohl sie sich völlig rechtmäßig verhalten und ihre Daten demzufolge für die Ermittlungstätigkeit der Strafverfolgungsbehörden nicht benötigt werden. Das Anhäufen von sinn- und nutzlosen Datenhalden wäre die Folge.

- Die gesetzliche Verpflichtung, sich an dem Ziel von Datenvermeidung und Datensparsamkeit auszurichten, würde konterkariert. Gerade die Prepaid-Karten sind ein gutes praktisches Beispiel für den Einsatz datenschutzfreundlicher Technologien, da sie anonymes Kommunizieren auf unkomplizierte Weise ermöglichen. Die Nutzung dieser Angebote darf deshalb nicht von der Speicherung von Bestandsdaten abhängig gemacht werden.

- Mit der Verpflichtung, den Personalausweis vorzulegen, würden die Anbieter zusätzliche Informationen über die Nutzerinnen und Nutzer erhalten, die sie nicht benötigen, z. B. die Nationalität, Größe oder Augenfarbe. Die vorgesehene Pflicht, auch die Personalausweisnummern zu registrieren, darf auch künftig keinesfalls dazu führen, dass die Ausweisnummern den Sicherheitsbehörden direkt zum Abruf bereit gestellt werden und sie damit diese Daten auch für die Verknüpfung mit anderen Datenbeständen verwenden können.

- Auch Krankenhäuser, Hotels, Schulen und Hochschulen sowie Unternehmen und Behörden, die ihren Mitarbeiterinnen und Mitarbeitern das private Telefonieren gestatten, sollen verpflichtet werden, die Personalausweisnummern der Nutzerinnen und Nutzer zu registrieren.

- Die Befugnis, Kundendateien mit unvollständigen oder ähnlichen Suchbegriffen abzufragen, würde den Sicherheitsbehörden eine Vielzahl personenbezogener Daten unbeteiligter Dritter zugänglich machen, ohne dass diese Daten für ihre Aufgaben erforderlich sind. Die notwendige strikte Beschränkung dieser weitreichenden Abfragebefugnis durch Rechtsverordnung setzt voraus, dass ein entsprechender Verordnungsentwurf bei der Beratung des Gesetzes vorliegt.

Der Formulierungsvorschlag des Bundeswirtschaftsministeriums lässt eine Auseinandersetzung mit dem Recht auf informationelle Selbstbestimmung der Kundinnen und Kunden der Telekommunikationsunternehmen weitgehend vermissen.
Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung und den Gesetzgeber auf, auf die geplante Änderung des Telekommunikationsgesetzes zu verzichten und vor weiteren Änderungen die bestehenden Befugnisse der Sicherheitsbehörden durch unabhängige Stellen evaluieren zu lassen.

Anlage 17

Entschließung der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24./25. Oktober 2002:

Datenschutzgerechte Vergütung für digitale Privatkopien im neuen Urheberrecht

Zur Umsetzung der EU-Urheberrechtsrichtlinie wird gegenwärtig über den Entwurf der Bundesregierung für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft beraten. Hierzu hat der Bundesrat die Forderung erhoben, das bisherige System der Pauschalabgaben auf Geräte und Kopiermedien, die von den Verwertungsgesellschaften auf die Urheberinnen und Urheber zur Abgeltung ihrer Vergütungsansprüche verteilt werden, durch eine vorrangige individuelle Lizenzierung zu ersetzen. Zugleich hat der Bundesrat die Gewährleistung eines ausreichenden Schutzes der Nutzerinnen und Nutzer vor Ausspähung personenbezogener Daten über die individuelle Nutzung von Werken und die Erstellung von Nutzungsprofilen gefordert.

Die Datenschutzbeauftragten des Bundes und der Länder weisen in diesem Zusammenhang auf Folgendes hin: Das gegenwärtig praktizierte Verfahren der Pauschalvergütung beruht darauf, dass der Bundesgerichtshof eine individuelle Überprüfung des Einsatzes von analogen Kopiertechniken durch Privatpersonen zur Durchsetzung von urheberrechtlichen Vergütungsansprüchen als unvereinbar mit dem verfassungsrechtlichen Schutz der persönlichen Freiheitsrechte der Nutzerinnen und Nutzer bezeichnet hat. Diese Feststellung behält auch unter den Bedingungen der Digitaltechnik und des Internets ihre Berechtigung. Die Datenschutzkonferenz bestärkt den Gesetzgeber, an diesem bewährten, datenschutzfreundlichen Verfahren festzuhalten. Sollte der Gesetzgeber – wie es der Bundesrat fordert – jetzt für digitale Privatkopien vom Grundsatz der Pauschalvergütung (Geräteabgabe) tatsächlich abgehen wollen, so kann er den verfassungsrechtlichen Vorgaben nur entsprechen, wenn er sicherstellt, dass die urheberrechtliche Vergütung aufgrund von statistischen oder anonymisierten Angaben über die Nutzung einzelner Werke erhoben wird. Auch technische Systeme zur digitalen Verwaltung digitaler Rechte (Digital Rights Management) müssen datenschutzfreundlich gestaltet werden.

Anlage 18

Entschließung der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24./25. Oktober 2002:

Speicherung und Veröffentlichung der Standortverzeichnisse von Mobilfunkantennen

Die Speicherung und die Veröffentlichung der Standortdaten von Mobilfunkantennen durch die Kommunen oder andere öffentliche Stellen stehen zur Zeit in verstärktem Maße in der öffentlichen Diskussion. Mehrere kommunale Spitzenverbände haben sich diesbezüglich bereits an die jeweiligen Landesdatenschutzbeauftragten gewandt. Unbeschadet bereits bestehender Landesregelungen und der Möglichkeit, Daten ohne Grundstücksbezug zu veröffentlichen, fordert die 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder aufgrund der bundesweiten Bedeutung der Frage den Bundesgesetzgeber auf, im Rahmen einer immissionsschutzrechtlichen Regelung über die Erstellung von Mobilfunkkatastern zu entscheiden.

Dabei ist zu bestimmen, wie derartige Kataster erstellt werden sollen. Die gegenwärtige Regelung des Bundesimmissionsschutzgesetzes sieht keine ausdrückliche Ermächtigung zur Schaffung von Mobilfunkkatastern vor, so dass deren Erstellung und Veröffentlichung ohne Einwilligung der Grundstückseigentümer und -eigentümerinnen und der Antennenbetreiber keine ausdrückliche gesetzliche Grundlage hat. Bei der Novellierung ist insbesondere zu regeln, ob und unter welchen Bedingungen eine Veröffentlichung derartiger Kataster im Internet oder in vergleichbaren Medien zulässig ist. Individuelle Auskunftsansprüche nach dem Umweltinformationsgesetz oder den Informationsfreiheitsgesetzen bleiben davon unberührt.

Anlage 19

Entschließung der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24./25. Oktober 2002:

Systematische verdachtslose Datenspeicherung in der Telekommunikation und im Internet

Gegenwärtig werden sowohl auf nationaler als auch auf europäischer Ebene Vorschläge erörtert, die den Datenschutz im Bereich der Telekommunikation und der Internetnutzung und insbesondere den Schutz des Telekommunikationsgeheimnisses grundlegend in Frage stellen.

Geplant ist, alle Anbieter von Telekommunikations- und Multimediadiensten zur verdachtslosen Speicherung sämtlicher Bestands-, Verbindungs-, Nutzungs- und Abrechnungsdaten auf Vorrat für Mindestfristen von einem Jahr und mehr zu verpflichten, auch wenn sie für die Geschäftszwecke der Anbieter nicht (mehr) notwendig sind. Das so entstehende umfassende Datenreservoir soll dem Zugriff der Strafverfolgungsbehörden, der Polizei und des Verfassungsschutzes bei möglichen Anlässen in der Zukunft unterliegen. Auch auf europäischer Ebene werden im Rahmen der Zusammenarbeit der Mitgliedsstaaten in den Bereichen “Justiz und Inneres” entsprechende Maßnahmen – allerdings unter weitgehendem Ausschluss der Öffentlichkeit - diskutiert.

Die Datenschutzbeauftragten des Bundes und der Länder treten diesen Überlegungen mit Entschiedenheit entgegen. Sie haben schon mehrfach die Bedeutung des Telekommunikationsgeheimnisses als unabdingbare Voraussetzung für eine freiheitliche demokratische Kommunikationsgesellschaft hervorgehoben. Immer mehr menschliche Lebensäußerungen finden heute in elektronischen Netzen statt. Sie würden bei einer Verwirklichung der genannten Pläne einem ungleich höheren Überwachungsdruck ausgesetzt als vergleichbare Lebensäußerungen in der realen Welt. Bisher muss niemand bei der Aufgabe eines einfachen Briefes im Postamt seinen Personalausweis vorlegen oder in einer öffentlichen Bibliothek registrieren lassen, welche Seite er in welchem Buch aufschlägt. Eine vergleichbar umfassende Kontrolle entsprechender Online-Aktivitäten (E-Mail-Versand, Nutzung des WorldWideWeb), wie sie jetzt erwogen wird, ist ebenso wenig hinnehmbar.

Zudem hat der Gesetzgeber erst vor kurzem die Befugnisse der Strafverfolgungsbehörden erneut deutlich erweitert. Die praktischen Erfahrungen mit diesen Regelungen sind von unabhängiger Seite zu evaluieren, bevor weitergehende Befugnisse diskutiert werden.

Die Konferenz der europäischen Datenschutzbeauftragten hat in ihrer Erklärung vom 11. September 2002 betont, dass eine flächendeckende anlassunabhängige Speicherung sämtlicher Daten, die bei der zunehmenden Nutzung von öffentlichen Kommunikationsnetzen entstehen, unverhältnismäßig und mit dem Menschenrecht auf Achtung des Privatlebens unvereinbar wäre. Auch in den Vereinigten Staaten sind vergleichbare Maßnahmen nicht vorgesehen.

Mit dem deutschen Verfassungsrecht ist eine verdachtslose routinemäßige Speicherung sämtlicher bei der Nutzung von Kommunikationsnetzen anfallender Daten auf Vorrat nicht zu vereinbaren. Auch die Rechtsprechung des Europäischen Gerichtshofs lässt eine solche Vorratsspeicherung aus Gründen bloßer Nützlichkeit nicht zu.

Die Konferenz fordert die Bundesregierung deshalb auf, für mehr Transparenz der Beratungen auf europäischer Regierungsebene einzutreten und insbesondere einer Regelung zur flächendeckenden Vorratsdatenspeicherung nicht zuzustimmen.

Anlage 20

Empfehlungen und Hinweise zu Aufgaben, Befugnisse und Zuständigkeiten des Beauftragten für den Datenschutz (BfdD) bei öffentlichen Stellen des Landes Sachsen-Anhalt

Gliederungsübersicht

1. Einsetzung des BfdD
2. Stellung und Befugnisse
3. Aufgaben des BfdD in der öffentlichen Stelle

- Beratung der Leitung der öffentlichen Stelle, der Mitarbeiter und des Personalrates
- Kontrollen der Datenverarbeitungsprozesse
- Datenschutzrechtliche Vorabkontrolle und Freigabe
- Führung des Verfahrensverzeichnisses
- Unterrichtung des Landesbeauftragten für den Datenschutz Sachsen-Anhalt (LfD LSA) über die Einrichtung automatisierter Abrufverfahren
- Unterrichtung des LfD LSA bei der Auftragsdatenverarbeitung durch nicht-öffentliche Stellen
- Kontrolle der Einhaltung des Datenschutzes bei der Verarbeitung oder Nutzung personenbezogener Daten bei Auftragnehmern
- Rechtzeitige Unterrichtung des LfD LSA über Planungen des Landes zum Aufbau automatisierter Informationssysteme nach § 22 Abs. 4 Satz 2 DSG-LSA
- Mitwirkung am Erlass von Richtlinien und anderen verwaltungsinternen Regelungen
- Mitwirkung bei der Erstellung datenschutzgerechter Verwaltungsunterlagen (Vordrucke und Merkblätter)
- Mitarbeit bei der Gewährleistung der Rechte Betroffener, Mitbearbeitung von Bürgereingaben
- Beteiligung bei der Konzeption und Auswertung von Protokolldateien
- Schulung der Mitarbeiter
- Zusammenarbeit mit dem IT-Sicherheitsbeauftragten
- Verbindung zum LfD LSA und zu Datenschutzbeauftragten anderer Stellen

1. Einsetzung des BfdD gem. § 14a Abs. 1 DSG-LSA

In Deutschland ist das Wirken behördlicher und betrieblicher Datenschutzbeauftragter ein wichtiger Garant für de Gewährleistung des Datenschutzes. Die Selbstkontrolle geht der Fremdkontrolle durch den LfD LSA und die Aufsichtsbehörden vor.
Aus diesem Grunde hat auch der Landesgesetzgeber bei der Novellierung des Gesetzes zum Schutz personenbezogener Daten der Bürger (DSG-LSA) im Jahre 2001 den **öffentlichen** Stellen die Pflicht zur Einsetzung eines BfdD auferlegt.

In welchen öffentlichen Stellen sind BfdD einzusetzen?

Die Verpflichtung zur Einsetzung eines BfdD gilt gem. § 14a Abs. 1 DSG-LSA für jede öffentliche Stelle im Sinne des § 3 Abs. 1 DSG-LSA, wenn diese zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten automatisierte (d.h. programmgesteuerte) Verfahren einsetzt. § 14a Abs. 1 Satz 3 DSG-LSA sieht aber Einschränkungen und Ausnahmen für Notare und die in § 3 Abs. 1 Satz 2 DSG-LSA genannten Stellen (u.a. Beliehene) vor. Ein BfdD muss auch dann nicht eingesetzt werden, wenn ausschließlich Verfahren, die der Unterstützung der allgemeinen Bürotätigkeit (§ 14 Abs. 4 Nr. 2 DSG-LSA) dienen, zum Einsatz kommen.
Durch die Einsetzung eines BfdD wird die Verantwortung der öffentlichen Stelle, insbesondere die deren Leitung, für die Sicherstellung des Datenschutzes in ihrem Verantwortungsbereich nach § 14 Abs. 1 DSG-LSA nicht ersetzt.

Welche Kriterien sind bei der Auswahl des BfdD zu beachten (§ 14a Abs. 2 DSG-LSA)?

Als BfdD darf nur eingesetzt werden, wer über die erforderliche Fachkunde in Fragen des Datenschutzes und der Datensicherheit und die erforderliche Zuverlässigkeit verfügt.
Bei fehlender fachlicher Qualifikation in Teilbereichen sollte ihm Gelegenheit gegeben werden, sich diese durch entsprechende Schulungsmaßnahmen anzueignen.
Um eine effektive Arbeit leisten zu können, sollte der BfdD eine Vertrauensperson sein, die mit den Aufgaben und der Arbeitsweise der öffentlichen Stelle möglichst aus eigener Erfahrung vertraut ist. Soll ein externer BfdD eingesetzt werden, ist die effektive Aufgabenerfüllung durch geeignete interne Ansprechpartner zu gewährleisten.

Darf der BfdD noch andere Aufgaben erfüllen?

Gem. § 14a Abs. 2 Satz 4 DSG-LSA ist der BfdD im erforderlichen Umfang von anderen Aufgaben freizustellen. Er muss jedoch nicht ausschließlich mit Aufgaben des Datenschutzes betraut sein. Je nach Größe der öffentlichen Stelle, Art und Umfang der Verarbeitung personenbezogener Daten und der damit möglicherweise verbundenen Datenschutzprobleme können ihm weitere Aufgaben übertragen werden. Dabei sind jedoch Interessenkonflikte oder Abhängigkeiten möglichst auszuschließen, die eine Aufgabenerfüllung gefährden würden.

Interessenkonflikte können insbesondere auftreten, wenn der BfdD gleichzeitig Aufgaben in Organisationseinheiten mit einer sehr umfangreichen oder sensiblen

Verarbeitung personenbezogener Daten wahrnimmt oder z.B. Leiter des IT-Bereiches ist.
Geeignet sein können Mitarbeiter aus den Bereichen Justitiariat / Recht, Organisation, Rechnungsprüfung oder auch der IT-Sicherheitsbeauftragte, falls dieser nicht organisatorisch unmittelbar dem IT-Bereich zugeordnet ist.

Über welche Kenntnisse sollte der BfdD verfügen?
Er sollte die einschlägigen Rechtsvorschriften kennen und sicher anwenden können. Dazu gehören insbesondere

- die Grundrechte mit einem Bezug zum Datenschutz (vorrangig Art. 1 Abs. 1 und Art. 2 Abs. 1 GG sowie Art. 6 Abs. 1 LVerf),
- das Gesetz zum Schutz personenbezogener Daten der Bürger (DSG-LSA),
- die zur Anwendung gelangenden spezialgesetzlichen Datenschutzbestimmungen,
- in bestimmten Fällen das BDSG.

Daneben sollte er

- über organisatorische Kenntnisse und Fähigkeiten,
- Verwaltungserfahrung sowie
- über ausreichende Kenntnisse auf dem Gebiet der Informations- und Kommunikationstechnik (IuK) verfügen.

Da der BfdD die Mitarbeiter der öffentlichen Stelle in allen Fragen des Datenschutzes beraten und unterstützen soll, würde eine einseitige Orientierung des BfdD auf Kenntnisse der IuK den gestellten Anforderungen ebenso wenig gerecht werden wie eine einseitige Orientierung auf Rechtskenntnisse.

Wie erfolgt die Einsetzung des BfdD?
Im Allgemeinen wird der BfdD durch die Leitung der öffentlichen Stelle eingesetzt. Unterliegt die öffentliche Stelle einer Dienstaufsicht, kann gem. § 14a Abs. 1 Satz 2 DSG-LSA die Einsetzung auch durch die Dienstaufsichtsbehörde erfolgen. Die Einsetzung des BfdD hat schriftlich zu erfolgen und sollte im Wege einer Organisationsverfügung bzw. durch die Darstellung im Geschäftsverteilungsplan allen Mitarbeitern bekannt gemacht werden.

2. Stellung
Die gesetzlich garantierte Unabhängigkeit und organisatorisch herausgehobene Stellung ist für eine wirkungsvolle Tätigkeit des BfdD von ausschlaggebender Bedeutung. Er darf bei der Wahrnehmung seiner Aufgaben nicht den Weisungen der Organisationseinheiten unterliegen, die er zu kontrollieren hat (§ 14a Abs. 2 Satz 1 DSG-LSA). In seiner Funktion als BfdD sollte er im Sinne einer Stabsfunktion dem Leiter der öffentlichen Stelle zugeordnet sein. Der BfdD hat das direkte Vortragsrecht beim Leiter der öffentlichen Stelle (§ 14a Abs. 2 Satz 2 DSG-LSA). Soweit ein Bezug zu seiner Tätigkeit besteht, ist er umfassend und frühzeitig zu unterrichten. Dies kann geschehen durch:

- Beteiligung an Leitungsbesprechungen,
- Bekanntgabe von Planungen, die den Umgang mit personenbezogenen Daten betreffen,
- Verpflichtung aller Organisationseinheiten, den BfdD an datenschutzrelevanten Vorgängen zu beteiligen.

Wichtig ist auch, dass der BfdD von der Leitung der öffentlichen Stelle und von allen Mitarbeitern unterstützt wird. Soweit erforderlich, sind ihm Hilfspersonal sowie Einrichtungen, Geräte und Mittel zur Verfügung zu stellen. Für den Fall, dass er vertiefte rechtliche oder technische Beratung benötigt, sollten ihm geeignete Ansprechpartner zur Verfügung stehen, auf die er bei Bedarf zurückgreifen kann.
Werden nach Auffassung des BfdD bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten die Bestimmungen des DSG-LSA oder anderer Vorschriften zum Datenschutz verletzt, hat er die Verantwortlichen oder die Leitung der öffentlichen Stelle darauf hinzuweisen. Ein Weisungsrecht gegenüber den datenverarbeitenden Organisationseinheiten steht ihm nicht zu.

3. Aufgaben des BfdD in der öffentlichen Stelle (§ 14a Abs. 4 DSG-LSA)
Der BfdD soll dazu beitragen, dass die ihn einsetzende öffentliche Stelle den Erfordernissen des Datenschutzes umfassend Rechnung trägt. Er hat die Einhaltung der Vorschriften des Datenschutzes in allen Bereichen zu überwachen. Er nimmt seine Aufgaben vorrangig durch Beratung, aber auch durch Kontrollen wahr.
Für die Mitarbeiter der öffentlichen Stelle sollte der BfdD Ansprechpartner in allen Fragen des Datenschutzes sein, an den sie sich jederzeit vertrauensvoll wenden können. Bei erkannten Schwachstellen und Versäumnissen sollte er zunächst gemeinsam mit den Beteiligten nach konstruktiven Lösungen suchen.
Wichtig ist, den Mitarbeitern bewusst zu machen, dass Datenschutz positiv und nützlich ist und im Hintergrund stets der Betroffene mit seinen gesetzlich und verfassungsrechtlich verbrieften Rechten steht. Bei angemessener Verwirklichung wird der Datenschutz Arbeitsabläufe im Ergebnis eher fördern als erschweren.

Wenn eine öffentliche Stelle zu viele personenbezogene Daten sammelt, personenbezogene Daten zu schnell oder zu spät löscht oder personenbezogene Daten unberechtigt übermittelt, verstößt sie nicht nur gegen Datenschutzrecht, sondern verursacht auch unnütze Bürokratie und Mehrkosten. Datenschutz ist Element einer bürgerfreundlichen Verwaltung und trägt damit zum Gesamterfolg öffentlichen Handelns bei.
Der BfdD hilft der Leitung der öffentliche Stelle, ihre Verantwortung für die Wahrung des Persönlichkeitsschutzes wahrzunehmen und Zwischenfälle zu vermeiden, die dem Ansehen der öffentliche Stelle abträglich wären.
Zur sachgemäßen Durchführung seiner Aufgaben ist eine regelmäßige Weiterbildung des BfdD notwendig. Dazu können

- Fortbildungsseminare zum Datenschutz, die von den verschiedensten Stellen angeboten werden,
- Fachliteratur zum Datenschutz sowie

- Möglichkeiten des Erfahrungsaustausches mit anderen BfdD des gleichen Geschäftsbereiches oder aus öffentlichen Stellen mit verwandten Aufgaben

genutzt werden.
Der spezielle Zuschnitt der Aufgaben des BfdD richtet sich im Einzelfall nach den Aufgaben, der Größe, dem Aufbau und der Gliederung der jeweiligen öffentlichen Stelle. Der folgende Katalog gibt einen Überblick über die Aufgaben, die dem BfdD in jeder öffentlichen Stelle gesetzlich obliegen oder zusätzlich übertragen werden können:

Grundlegende Aufgaben

- Beratung der Leitung der öffentliche Stelle, des Personalrats und der Mitarbeiter in datenschutzrelevanten Fragen.
- Durchführung von Kontrollen.

Zu diesem Zweck hat er Zutritt zu allen Diensträumen und kann alle dienstlichen Unterlagen einsehen, die personenbezogene Daten enthalten oder den Umgang mit diesen betreffen, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist (§ 14a Abs. 3 Satz 1 und 3 DSG-LSA). Gem. § 14a Abs. 3 Satz 2 DSG-LSA gilt dies nicht, wenn Berufs- oder besondere Amtsgeheimnisse (z.B. das Arzt- oder Steuergeheimnis) entgegenstehen.

Übersichten und Register

- Führung des Verfahrensverzeichnisses gem. § 14a Abs. 4 Satz 1 DSG-LSA.
- Sammlung der Nachweise zur datenschutzrechtlichen Vorabkontrolle (§ 14a Abs. 4 Satz 2 Ziffer 2 DSG-LSA) von automatisierten Verfahren.

Automatisierte Abrufverfahren und Auftragsdatenverarbeitung

- Unterrichtung des LfD LSA über die Einrichtung automatisierter Abrufverfahren (§ 7 Abs. 3 DSG-LSA).
- Unterrichtung des LfD LSA über die Auftragsdatenverarbeitung nicht-öffentlicher Stellen (§ 8 Abs. 6 DSG-LSA).
- Kontrolle der Einhaltung des Datenschutzes bei Auftragnehmern bei der Verarbeitung oder Nutzung personenbezogener Daten im Auftrag (§ 8 DSG-LSA)

Mitwirkung

- Erarbeitung oder Mitwirkung bei der Erstellung von Richtlinien, Rundschreiben, Dienstvereinbarungen und weiteren allgemeinen Verlautbarungen, die den Umgang mit personenbezogenen Daten betreffen.
- Mitwirkung bei der Erarbeitung und Anwendung datenschutzgerechter Verwaltungsunterlagen (Vordrucke und Merkblätter).
- Mitwirkung bei Auskunfts-, Berichtigungs-, Löschungs- und Sperrungsverlangen nach §§ 15 und 16 DSG-LSA, bei der Erstellung von Bürgerinformationen sowie bei allgemeinen Bürgereingaben und Anfragen zum Datenschutz.

- Beteiligung bei der Konzeption und Auswertung von Protokolldateien mit Personenbezug.

Schulung und Zusammenarbeit

- Schulung der Mitarbeiter zu Fragen des Datenschutzes und der Datensicherheit.
- Regelmäßige oder gelegentliche Berichte an die Leitung der öffentlichen Stelle über den Stand der Sicherstellung des Datenschutzes und der Datensicherheit innerhalb der öffentlichen Stelle.
- Zusammenarbeit mit dem IT-Sicherheitsbeauftragten.
- ggf. Zusammenarbeit mit den Datenschutzbeauftragten der Aufsichtsbehörde, anderer öffentlichen Stellen des Geschäftsbereichs und öffentlicher Stellen mit verwandten Aufgaben.
- Zusammenarbeit mit dem Personalrat

Besondere gesetzliche Regelungen zum Verhältnis zwischen Personalvertretung und BfdD bestehen nicht. Es ist aber vom Gebot der Zusammenarbeit auszugehen, denn der BfdD ist Teil der Dienststelle, und es gibt bei beiden gleichgerichtete Interessen. Deshalb unterstützt der BfdD die Personalvertretung. Er hat seinerseits die Unabhängigkeit der Personalvertretung zu beachten. Insoweit besteht kein Kontrollrecht des BfdD.

Erläuterungen zu den Einzelaufgaben:

- **Beratung der Leitung der öffentlichen Stelle, der Mitarbeiter und des Personalrates**

Der BfdD berät die Leitung der öffentlichen Stelle, die Organisationseinheiten, die personenbezogene Daten verarbeiten, und den Personalrat in allen Fragen des Datenschutzes sowie der datenschutzgerechten Organisation.
Dabei ist zu berücksichtigen, dass der Datenschutz sehr weit reicht und maßgeblich auch die innere Organisation der öffentlichen Stelle beeinflussen kann.
Dies betrifft auch Fragen der Zutrittsberechtigung (z.B. bei der Organisation von Reinigungs- oder Reparaturarbeiten), der Postbearbeitung oder Archivierung bis hin zur Gestaltung und Ausstattung von Diensträumen (u.a. hinsichtlich der Verschlusssicherheit von Räumen und Mobiliar und zur Gewährleistung der Vertraulichkeit bei Bürgergesprächen).
Der BfdD sollte bei Bedarf rechtzeitig über die Planung und Beschaffung von Hard- und Software, mit der personenbezogene Daten verarbeitet werden soll, sowie über die Einführung oder Änderung von IT-Verfahren informiert werden, um eventuelle datenschutzrechtliche Probleme vorab klären zu können.
Gleichzeitig sollte der BfdD darauf hinwirken, dass bei der Einführung oder Änderung von IT-Vorhaben ein spezifisches Sicherheitskonzept erarbeitet wird und die jeweils festgelegten Sicherheitsmaßnahmen auch umgesetzt werden. Maßstab für die Sicherheitsmaßnahmen bei der automatisierten Verarbeitung personenbezogener Daten bilden die Sicherheitsziele in § 6 Abs. 2 DSG-LSA.

- **Kontrolle der Datenverarbeitungsprozesse**

Kontrolle ist darauf gerichtet, Mängel zu erkennen und abzustellen. In der Regel ist es deshalb sinnvoll, schon während der Kontrolle mit den Beteiligten über mögliche Abhilfen zu sprechen. Beim Erarbeiten von Lösungen ist zu beachten, dass es nicht in erster Linie darauf ankommt, die vorgefundenen Symptome zu beseitigen. Es müssen vielmehr die Ursachen für Mängel festgestellt und über technische und organisatorische Maßnahmen hinaus ggf. auch die Organisationsstrukturen verändert werden. Hierbei kommt es darauf an, die Sensibilität und die Motivation der Verantwortlichen so zu fördern, dass der Datenschutz besser gewährleistet wird.

Werden erkannte Mängel von den verantwortlichen Organisationseinheiten auch nach Anmahnung nicht abgestellt, wird der BfdD die Leitung der öffentlichen Stelle spätestens dann unterrichten und deren Entscheidung herbeiführen müssen.

- **Datenschutzrechtliche Vorabkontrolle und Freigabe**

Gemäß § 14 Abs. 2 DSG-LSA ist vor dem erstmaligen Einsatz der dort genannten automatisierten Verfahren zu überprüfen, ob sie datenschutzrechtlich zulässig und die gem. § 6 Abs. 2 DSG-LSA zu treffenden technischen und organisatorischen Maßnahmen ausreichend sind. Diese Prüfung ist so rechtzeitig durchzuführen, dass erforderliche Änderungen ohne Schwierigkeiten vor Einführung oder besser bereits bei der Programmierung bzw. vor Erwerb des Verfahrens realisiert werden können. Die Unterlagen zur Vorabkontrolle sollten vorzugsweise beim BfdD gesammelt werden.

- **Führung des Verfahrensverzeichnisses gem. § 14a Abs. 4 DSG-LSA**

Der BfdD führt das Verfahrensverzeichnis i.S. des § 14 Abs. 3 DSG-LSA.
Für dieses Verzeichnis besteht eine interne Meldepflicht für die die Verfahren betreibenden Organisationseinheiten innerhalb der öffentlichen Stelle. Für die schriftlichen Festlegungen gem. § 14 Abs.3 Nrn. 1 bis 9 DSG-LSA sind die Nutzer der Verfahren (Fachbereiche) verantwortlich, die den Nachweis der Erforderlichkeit und Zulässigkeit der im Verfahren verarbeiteten personenbezogenen Daten führen müssen.
Bei den Festlegungen über die genutzten Verfahren sollte der BfdD darauf achten, dass die Zwecke hinreichend präzisiert sind und jede Zweckänderung nur im Rahmen der Anforderungen des § 10 Abs. 2 DSG-LSA oder spezialgesetzlicher Regelungen erfolgt.

- **Unterrichtung des LfD LSA über die Einrichtung automatisierter Abrufverfahren**

Gem. § 7 Abs. 3 DSG-LSA ist der LfD LSA **vor** der Einrichtung eines automatisierten Abrufverfahrens zu unterrichten. Diese Unterrichtung unter Mitteilung der Festlegungen nach § 7 Abs. 2 DSG-LSA sollte durch den BfdD oder im Benehmen mit ihm erfolgen.

- **Unterrichtung des LfD LSA bei der Auftragsdatenverarbeitung durch nicht-öffentliche Stellen**

Ein Auftrag zur Verarbeitung oder Nutzung personenbezogener Daten durch andere Stellen ist nach § 8 Abs. 2 DSG-LSA schriftlich zu erteilen. Der BfdD sollte beim Erteilen derartiger Aufträge stets beteiligt werden. Dabei sollte er in den Fällen des § 8 Abs. 6 DSG-LSA darauf achten, dass vertraglich sichergestellt wird, dass der private Auftragnehmer die Bestimmungen des DSG-LSA befolgt und sich der Kontrolle durch den LfD LSA unterwirft.

Die Auftragsdatenverarbeitung durch nicht-öffentliche Stellen ist bei öffentlichen Aufgaben besonders sensibel. Deshalb hat der Gesetzgeber in § 8 Abs. 6 DSG-LSA zusätzliche Sicherheitsregeln vorgesehen. Die bei der Beauftragung nicht-öffentlicher Stellen geforderte Unterrichtung des LfD LSA (§ 8 Abs. 6 Satz 2 DSG-LSA) sollte durch den BfdD oder im Benehmen mit ihm vorgenommen werden.

- **Kontrolle der Einhaltung des Datenschutzes bei Auftragnehmern bei der Verarbeitung oder Nutzung personenbezogener Daten im Auftrag**

Gemäß § 8 Abs. 3 DSG-LSA darf der Auftragnehmer die Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten oder nutzen. Der BfdD sollte in geeigneter Weise kontrollieren, ob die Weisungen des Auftraggebers im jeweiligen Einzelfall eingehalten werden. Außerdem hat er sich gem. § 8 Abs. 2 DSG-LSA von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.

- **Rechtzeitige Unterrichtung des LfD LSA über Planungen des Landes zum Aufbau automatisierter Informationssysteme nach § 22 Abs. 4 Satz 2 DSG-LSA**

Soweit die öffentliche Stelle dafür zuständig ist, hat sie nach § 22 Abs. 4 DSG-LSA die Verpflichtung, den LfD LSA rechtzeitig über Planungen des Landes zum Aufbau automatisierter Informationssysteme zu unterrichten, sofern in ihnen personenbezogene Daten verarbeitet oder genutzt werden sollen. Hierbei kann und muss der BfdD eine umfassende und zeitgerechte Vorarbeit leisten.

- **Mitwirkung am Erlass von Richtlinien und anderen verwaltungsinternen Regelungen**

Richtlinien, Rundschreiben o.ä., die die Leitung der öffentlichen Stelle als Querschnittsregelungen zum Umgang mit personenbezogenen Daten erlässt, sollten unter Beteiligung des BfdD erarbeitet werden.
Für Regelungen im IT-Bereich können die in den Tätigkeitsberichten des LfD LSA gegebenen Empfehlungen Anhaltspunkte geben.
Bei der Erarbeitung von Dienstvereinbarungen zwischen der Dienststelle und dem Personalrat über den Umgang mit personenbezogenen Daten sollte der BfdD hinzugezogen werden.

- **Mitwirkung bei der Erstellung datenschutzgerechter Verwaltungsunterlagen (Vordrucke und Merkblätter)**

In der Verwaltung werden zur Rationalisierung der Verwaltungsabläufe Vordrucke eingesetzt. Dabei zeigt sich immer wieder, dass vielfach Daten über das erforderliche Maß hinaus erhoben werden. Ursache kann sein, dass nach Änderung von Rechtsvorschriften keine Anpassung der Vordrucke an die geänderte Rechtslage erfolgt ist, gemeinsame Vordrucke für verschiedene Verwaltungsaufgaben verwendet werden oder Vordrucke anderer Bundesländer übernommen werden, ohne vorher geprüft zu haben, ob in Sachsen-Anhalt die gleichen rechtlichen Voraussetzungen zum Umgang mit personenbezogenen Daten vorliegen.
Zur Gewährleistung des Datenschutzes sollte deshalb der BfdD die von der öffentlichen Stelle genutzten Vordrucke in seine Prüfung permanent einbeziehen und zumindest bei Eigenentwicklungen in die Prüfung der Zulässigkeit der Datenerhebung einbezogen werden.

- **Mitarbeit bei der Gewährleistung der Rechte der Betroffenen, Mitbearbeitung von Bürgereingaben**

Die Arbeitsteilung zwischen dem BfdD und den zuständigen Fachabteilungen hängt wesentlich vom speziellen Aufgabenbereich und von der Größe der öffentlichen Stelle ab. Bei der Beantwortung allgemeiner Bürgereingaben und -anfragen zum Datenschutz sollte der BfdD grundsätzlich hinzugezogen werden. Ansonsten wird besonders bei aus datenschutzrechtlicher Sicht problematischen oder bedeutsamen Angelegenheiten eine Einbindung des BfdD erforderlich sein. Dementsprechend sollte er auch bei der Einführung neuer Auskunftsverfahren, bei der Erstellung von Merkblättern für Bürger und bei der datenschutzgerechten Gestaltung von Formularen gehört werden (s.o.).

- **Beteiligung bei der Konzeption und Auswertung von Protokolldateien**

Bei der Einführung automatisierter Verfahren sollte grundsätzlich die Erforderlichkeit und der Umfang zur Führung von Protokolldateien geprüft und festgelegt werden. Auch eine Protokolldatei kann datenschutzrechtliche Risiken in sich bergen.
Auch die Auswertung personenbezogener Protokolldaten (i.d.R. nur in Form von Stichproben) sollte unter Beteiligung des BfdD erfolgen (vgl. z.B. § 28 Abs. 4 DSG-LSA).

- **Schulung der Mitarbeiter**

Für die Schulung und sonstige Unterrichtung der Mitarbeiter, die personenbezogene Daten erheben, verarbeiten oder nutzen, bieten sich an:

  - Einweisung neuer Mitarbeiter, Hinweis auf das Datengeheimnis (§ 5 DSG-LSA)
  - Schulung im Rahmen der allgemeinen Aus- und Fortbildung der Bediensteten
  - Vorträge oder Referate für einzelne Abteilungen oder Mitarbeitergruppen
  - Ausgabe von Merkblättern, die nach Bedarf aktualisiert werden

- Mitteilungen am Schwarzen Brett
- Mitteilungen in Dienstbesprechungen
- Berichte bei Personalversammlungen
- Beiträge zu Hauszeitschriften und sonstigen internen Mitteilungsblättern
- Verteilung geeigneter Literatur (z.B. Informationsmaterial des LfD LSA)
- Hinweise auf das Informationsangebot des LfD LSA oder anderer Einrichtungen im Intranet bzw. Internet

- **Zusammenarbeit mit dem IT-Sicherheitsbeauftragten**

Sofern die öffentliche Stelle einen IT-Sicherheitsbeauftragten bestellt hat und keine Personalunion mit dem BfdD besteht, empfiehlt sich naturgemäß eine enge Zusammenarbeit. Der BfdD sollte vor allem bei der Erstellung eines IT-Sicherheitskonzeptes hinzugezogen werden, damit auch aus datenschutzrechtlicher Sicht die Belange der Datensicherheit (§ 6 Abs. 2 DSG-LSA) im erforderlichen Maß berücksichtigt werden.
Auch bei der Überprüfung, ob die im IT-Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen in der Praxis umgesetzt werden, ist ein gemeinsames koordiniertes Vorgehen wünschenswert.

- **Verbindung zum LfD LSA und zu Datenschutzbeauftragten anderer Stellen**

Für auch durch Beratung mit der zuständigen Fachaufsichtsbehörde nicht lösbare Probleme auf den Gebieten Datenschutz und Datensicherheit und bei der Erledigung seiner Aufgaben nach § 14a Abs. 4 Satz 2 Nr. 2 DSG-LSA in Zweifelsfällen findet der BfdD Ansprechpartner beim LfD LSA. Bei der letztgenannten Aufgabe muss der Dienstweg nicht einzuhalten werden.
Gleichartige datenschutzrechtliche Fragestellungen treten häufig in mehreren öffentlichen Stellen parallel auf. Deshalb sollte dem Erfahrungsaustausch große Beachtung geschenkt werden. Dazu sollte der BfdD den Informationsaustausch zum BfdD seiner Fachaufsichtsbehörde und insbesondere zu den BfdD von öffentlichen Stellen mit verwandten Aufgaben suchen.
Auch sollten die im Abstand von 2 Jahren erscheinenden Tätigkeitsberichte des LfD LSA (§ 22 Abs. 4a DSG-LSA) sowie dessen Homepage (www.datenschutz.sachsen-anhalt.de) als wichtige Informationsquellen genutzt werden.

Abkürzungsverzeichnis

A

AAÜG	Anspruchs-Anwartschafts-Überleitungs-Gesetz
ADV	Automatisierte Datenverarbeitung
AFIS	Automatisiertes Fingerabdruckidentifizierungssystem
AG	Aktiengesellschaft
AGE	Automatische Gebührenerhebung
AGIHKG	Gesetz über die Industrie- und Handelskammern in Sachsen-Anhalt
AKB e.V.	Arbeitsgemeinschaft Kammerleitstelle für Bemessungsgrundlagen e.V.
AKG GmbH	Arbeitsgemeinschaft Kammerleitstelle für Bemessungsgrundlagen GmbH
AktO-oG	Aktenordnung für die Gerichte der ordentlichen Gerichtsbarkeit und die Staatsanwaltschaften des Landes Sachsen-Anhalt
ALB	Verfahren Automatisiert geführtes Liegenschaftsbuch
AO	Abgabenordnung
APIS	Arbeitsdatei PIOS - Innere Sicherheit
ArchG-LSA	Landesarchivgesetz
AuslG	Ausländergesetz
a.F.	alte Fassung

B

BAföG	Bundesausbildungsförderungsgesetz
BAG	Bundesarbeitsgericht
BArchG	Bundesarchivgesetz
BAT	Bundesangestelltentarifvertrag
BAT-O	Bundesangestelltentarifvertrag-Ost
BauGB	Baugesetzbuch
BauO LSA	Bauordnung des Landes Sachsen-Anhalt
BBiG	Berufsbildungsgesetz
BDSG	Bundesdatenschutzgesetz (neue Fassung)
BDSG 77	Bundesdatenschutzgesetz (alte Fassung)
BevStatG	Bevölkerungsstatistikgesetz
BfV	Bundesamt für Verfassungsschutz
BGB	Bürgerliches Gesetzbuch
BGBl. I	Bundesgesetzblatt, Teil I
BGH	Bundesgerichtshof
BG LSA	Beamtengesetz Sachsen-Anhalt
Bit	Binary Digit (binäres Zeichen - kleinste Informationseinheit in der Datenverarbeitung)
BKA	Bundeskriminalamt
BKAG	Gesetz über die Einrichtung eines Bundeskriminalpolizeiamtes (Bundeskriminalamt)
BKK	Betriebskrankenkasse

BND	Bundesnachrichtendienst
BNotO	Bundesnotarordnung
BRRG	Beamtenrechtsrahmengesetz
BSHG	Bundessozialhilfegesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BStatG	Bundesstatistikgesetz
BT-Drs.	Bundestagsdrucksache
Btx	Bildschirmtext
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungssammlung des Bundesverfassungsgerichts
BVerfSchG	Bundesverfassungsschutzgesetz
BVerwG	Bundesverwaltungsgericht
BZR	Bundeszentralregister
BZRG	Bundeszentralregistergesetz

C

CC	Common Criteria for Information Technology Security Evaluation/CC 2.1 (Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik; angepasst 1999 an den internationalen Standard ISO/IEC 15408)
CCITT	Comité Consultatif International Télégraphique et Téléphonique, Internationaler Normungsausschuss für Telekommunikation
CD-ROM	Compact-Disk-Read-Only-Memory (im Pressverfahren erstellter bzw. einmal beschreibbarer und mehrfach lesbarer, optischer Datenträger im CD-Format)
CGI	Common Gateway Interface; CGI-Skripte dienen dem Anlegen interaktiver WWW-Seiten
CNPV LSA	Corporate Network der Polizei und der Verwaltung des Landes Sachsen-Anhalt

D

DB-PKHG	Durchführungsbestimmungen zum Gesetz über die Prozesskostenhilfe
DENIC	DENIC Domain Verwaltungs- und Betriebsgesellschaft eG, Frankfurt am Main
DEVO	Datenerfassungsverordnung
DIHT	Deutscher Industrie- und Handelstag e.V.
DNA	Deoxyribonucleic acid (Desoxyribonukleinsäure)
DNS	Domain Name Service
DONot	Dienstordnung für Notare
DORA	Dialogorientiertes Recherche- und Informationssystem
DÖV	Die öffentliche Verwaltung
Drs.	Drucksache
DSG-LSA	Datenschutzgesetz des Landes Sachsen-Anhalt
DV	Datenverarbeitung

E

ED	Erkennungsdienst
Ed-Behandlung	Erkennungsdienstliche Behandlung
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
EGGVG	Einführungsgesetz zum Gerichtsverfassungsgesetz
E-Mail	Electronic-Mail
ESP	Encapsulation Security Payload
EStG	Einkommenssteuergesetz
EU	Europäische Union
EUROCAT	Europäisches Register über große Fehlbildungen
Europol	Europäisches Polizeiamt

F

FA	Finanzamt
FeV	Fahrerlaubnis-Verordnung
FGG	Gesetz über die Angelegenheiten der freiwilligen Gerichtsbarkeit
FISCUS	Föderales integriertes standardisiertes computergestütztes Steuersystem
FRV	Fahrzeugregisterverordnung
FRZ	Finanzrechenzentrum
FTP	File Transfer Protocol
FVG	Finanzverwaltungsgesetz
FZR	Fahrzeugzentralregister

G

GBl.	Gesetzblatt der DDR
GBO	Grundbuchordnung
GDG-LSA	Gesundheitsdienstgesetz Sachsen-Anhalt
GemHVO	Gemeindehaushaltsverordnung
GewO	Gewerbeordnung
GEZ	Gebühreneinzugszentrale
GG	Grundgesetz für die Bundesrepublik Deutschland
GGO LSA I	Beschluss der Landesregierung über die Gemeinsame Geschäftsordnung der Ministerien - Allgemeiner Teil -
GLKA	Gemeinsames Landeskriminalamt
GO LSA	Gemeindeordnung des Landes Sachsen-Anhalt
GVBl. LSA	Gesetz- und Verordnungsblatt des Landes Sachsen-Anhalt
GVG	Gerichtsverfassungsgesetz
GwG	Geldwäschegesetz
GWZ	Gebäude- und Wohnungszählung

H

HAMISSA	Haushalts-Aufstellung, -Management- und Informations-System Sachsen-Anhalt
HandwO	Gesetz zur Ordnung des Handwerks (Handwerksordnung)
HBauStatG	Hochbaustatistikgesetz
HGB	Handelsgesetzbuch

HK	Handwerkskammer
HTML	HyperText Markup Language; Definitionssprache für WWW-Dokumente
HTTP	HyperText Transport Protocol; Protokoll zur Kommunikation zwischen WWW-Client und WWW-Server

I

IABV	Integriertes Automatisiertes Besteuerungsverfahren
IHK	Industrie- und Handelskammer
IHK-G	Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern
IHK-GfI	IHK Gesellschaft für Informationsverarbeitung mbH Dortmund
IMA-IT	Interministerieller Arbeitskreis Informationstechnik
IMSI	International Mobile Subscriber Identity - netzinterne Teilnehmerkennung
INPOL	Informationssystem der Polizei auf Bundesebene
IPSec	IPSecurity, Protokoll mit Sicherheitsfunktionen wie Verschlüsselung, Aktualisierung als IP-Protokoll (Version 4) verfügbar
IRG	Gesetz über die internationale Rechtshilfe in Strafsachen
IT	Informationstechnik
IT-KA	Koordinierungsausschuss Informationstechnik
ITN-LSA	Informationstechnisches Netz Sachsen-Anhalt
IuK	Informations- und Kommunikationstechnik
IVBB	Informationsverbund Bonn-Berlin (Intranet der Bundesverwaltung)

J

JAPrO	Ausbildungs- und Prüfungsordnung für Juristen
JBeitrO	Justizbeitreibungsordnung
JGG	Jugendgerichtsgesetz
JuMiG	Justizmitteilungsgesetz

K

KAG-LSA	Kommunalabgabengesetz des Landes Sachsen-Anhalt
KAI	Kriminalaktenindex
KAN	Kriminalaktennachweis
KBA	Kraftfahrt-Bundesamt
Kfz	Kraftfahrzeug
KGHB-LSA	Gesetz über die Kammern für Heilberufe Sachsen-Anhalt
KGSt	Kommunale Gemeinschaftsstelle für Verwaltungsvereinfachung
KiBeG	Gesetz zur Förderung und Betreuung von Kindern
KiFöG	Kinderförderungsgesetz
KNSA	Kommunalnachrichten Sachsen-Anhalt
komsaNet	Kommunales Sachsen-Anhalt Netz
KpS	Kriminalpolizeiliche personenbezogene Sammlungen
KunstUrhG	Kunsturheberrechtsgesetz

L

LAN	Lokal Area Network
LBA	Luftfahrt-Bundesamt

LDAP	Lightweight Directory Access Protocol
LFI	Landesförderinstitut
LIT	Landesleitstelle Informationstechnik
LIZ	Landesinformationszentrum Sachsen-Anhalt
LKA	Landeskriminalamt
LKO LSA	Landkreisordnung des Landes Sachsen-Anhalt
LRZ	Landesrechenzentrum (in Halle)
LSA	Land Sachsen-Anhalt
LSA-NET	Bezeichnung für das interne Landesverwaltungsnetz (Intranet) bzw. für die Domain des Landes „lsa-net“ Land Sachsen-Anhalt-Netz
LuftVG	Luftverkehrsgesetz
LuftVZO	Luftverkehrs-Zulassungs-Ordnung
LVerf	Verfassung des Landes Sachsen-Anhalt
LWG	Landeswahlgesetz

M

MAD	Militärischer Abschirmdienst
MAN	Metropolitan Area Network
MBl. LSA	Ministerialblatt des Landes Sachsen-Anhalt
MdE	Minderung der Erwerbsfähigkeit
MDK	Medizinischer Dienst der gesetzlichen Krankenversicherung
MDR	Mitteldeutscher Rundfunk
MDStV	Mediendienste-Staatsvertrag
MeldDÜVO LSA	Meldedatenübermittlungsverordnung des Landes Sachsen-Anhalt
MfS	Ministerium für Staatssicherheit
MG LSA	Meldegesetz des Landes Sachsen-Anhalt
MHS	Message Handling System
MiStra	Anordnung über die Mitteilungen in Strafsachen
MiZi	Anordnung über die Mitteilungen in Zivilsachen
MO	Magnetic-Optical (optischer Datenträger auf der Basis magnetischer Beschichtung), als - WORM-MO (nur einmal beschreibbar, mehrfach lesbar) und als - ROD-MO (Rewritable Optical Disc, mehrfach wiederbeschreib- und lesbar)
MRRG	Melderechtsrahmengesetz
MTA	Message Transfer Agent

N

NADIS	Nachrichtendienstliches Informationssystem
NJW	Neue Juristische Wochenschrift
NNTP	Network News Transfer Protocol; Protokoll zum Austausch von Nachrichten in sog. Newsgroups - öffentlichen, thematisch gegliederten Diskussionsforen
NotVO	Verordnung über die Tätigkeit von Notaren in eigener Praxis
NVwZ	Neue Zeitschrift für Verwaltungsrecht
n.F.	neue Fassung

O

ÖbVermIng	Öffentlich bestellter Vermessungsingenieur
OECD	Internationale Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OFD	Oberfinanzdirektion
OLG	Oberlandesgericht
OrgKG	Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität
OSPF	Open Shortest Path First - "kürzester Weg zuerst"
OVG	Oberverwaltungsgericht
OWiG	Ordnungswidrigkeitengesetz

P

PBefG	Personenbeförderungsgesetz
PC	Personal Computer
PersVG LSA	Landespersonalvertretungsgesetz Sachsen-Anhalt
PET	Privacy enhancing technology
PISA	Programme for International Student Assessment
PKH	Prozesskostenhilfe
PKI	Public Key Infrastructure
PKZ	Personenkennziffer
POLAS	Polizeiliche Auskunftssysteme
POLIS	Polizeiliches Informationssystem Sachsen-Anhalt
ProdGewStatG	Gesetz über die Statistik im Produzierenden Gewerbe
PVS	Personalverwaltungssystem

R

RettDG-LSA	Rettungsdienstgesetz des Landes Sachsen-Anhalt
RiStBV	Richtlinien für das Straf- und Bußgeldverfahren
RiVASt	Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten
RuStAG	Reichs- und Staatsangehörigkeitsgesetz

S

Schufa	Schutzgemeinschaft für allgemeine Kreditsicherung
SchuVVO	Verordnung über das Schuldnerverzeichnis
SchwbG	Schwerbehindertengesetz
SG	Schulgesetz des Landes Sachsen-Anhalt
SGB	Sozialgesetzbuch
SGB VIII	Sozialgesetzbuch - Kinder- und Jugendhilfe (8. Buch)
SGB X	Sozialgesetzbuch - Verwaltungsverfahren (10. Buch)
SGSA	Städte- und Gemeindebund Sachsen-Anhalt
SigG	Signaturgesetz
SigV	Signaturverordnung
SLA	Statistisches Landesamt
SOG LSA	Gesetz über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt

SPUDOK	Spurendokumentation
SSL	Secure Socket Layer
StARegG	Gesetz zur Regelung von Fragen der Staatsangehörigkeit
StatG-LSA	Landesstatistikgesetz Sachsen-Anhalt
StBerG	
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StUG	Stasi-Unterlagen-Gesetz
StVÄG	Strafverfahrensänderungsgesetz
StVG	Straßenverkehrsgesetz
StVO	Straßenverkehrsordnung
StVollzG	Strafvollzugsgesetz
StVZO	Straßenverkehrszulassungsordnung

T

TCP/IP	Transmission Control Protocol/Internet Protocol
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TDSV	Telekommunikations-Datenschutzverordnung
TESTA	Trans-European Services für Telematics between Administrations
TKG	Telekommunikationsgesetz
TPA	Technisches Polizeiamt
TÜV	Technischer Überwachungs-Verein

U

UIG	Umweltinformationsgesetz
UNIFA	Unix im Finanzamt
UVollzG	Gesetz über den Vollzug der Untersuchungshaft

V

VerfSchG-LSA	Gesetz über den Verfassungsschutz im Land Sachsen-Anhalt
VermG	Vermögensgesetz
VermKatG	Vermessungs- und Katastergesetz des Landes Sachsen-Anhalt
VO	Verordnung
VONot	Verordnung über die Tätigkeit von Notaren in eigener Praxis
VPN	Virtual Private Network - "virtuelles privates Netz"
VRZ	Verbindungsstelle zum Finanzrechenzentrum
VV	Verwaltungsvorschrift
VwGO	Verwaltungsgerichtsordnung
VwKostG LSA	Verwaltungskostengesetz des Landes Sachsen-Anhalt
VwVfG	Verwaltungsverfahrensgesetz
VZR	Verkehrszentralregister

W

WAN	Wide Area Network
WoGG	Wohngeldgesetz
WoStatG	Wohnungsstatistikgesetz

WORM	Write Once Read Many (einmal beschreibbarer und mehrfach lesbarer, optischer Datenträger)
WWW	World Wide Web

X

X.25	Protokoll für Datenpaketvermittlung
X.400	Empfehlungen der Serie X.400 des CCITT (1984) für ein MHS

Z

ZER	Zentrales Einwohnermelderegister (DDR)
ZEVIS	Zentrales Verkehrsinformationssystem
ZFER	Zentrales Fahrerlaubnisregister
ZFR	Zentrales Fahrzeugregister
ZPO	Zivilprozessordnung
ZStV	Zentrales Staatsanwaltschaftliches Verfahrensregister
ZVG	Gesetz über die Zwangsversteigerung und die Zwangsverwaltung

Stichwortverzeichnis *

A

* Fundstelle zitiert nach Tätigkeitsbericht und Seite, ab VI. Tätigkeitsbericht nach Tätigkeitsbericht und Ziffer

* Fundstelle zitiert nach Tätigkeitsbericht und Seite, ab VI. Tätigkeitsbericht nach Tätigkeitsbericht und Ziffer

B

* Fundstelle zitiert nach Tätigkeitsbericht und Seite, ab VI. Tätigkeitsbericht nach Tätigkeitsbericht und Ziffer

* Fundstelle zitiert nach Tätigkeitsbericht und Seite, ab VI. Tätigkeitsbericht nach Tätigkeitsbericht und Ziffer

* Fundstelle zitiert nach Tätigkeitsbericht und Seite, ab VI. Tätigkeitsbericht nach Tätigkeitsbericht und Ziffer

* Fundstelle zitiert nach Tätigkeitsbericht und Seite, ab VI. Tätigkeitsbericht nach Tätigkeitsbericht und Ziffer

G

* Fundstelle zitiert nach Tätigkeitsbericht und Seite, ab VI. Tätigkeitsbericht nach Tätigkeitsbericht und Ziffer

* Fundstelle zitiert nach Tätigkeitsbericht und Seite, ab VI. Tätigkeitsbericht nach Tätigkeitsbericht und Ziffer

* Fundstelle zitiert nach Tätigkeitsbericht und Seite, ab VI. Tätigkeitsbericht nach Tätigkeitsbericht und Ziffer

* Fundstelle zitiert nach Tätigkeitsbericht und Seite, ab VI. Tätigkeitsbericht nach Tätigkeitsbericht und Ziffer

L

* Fundstelle zitiert nach Tätigkeitsbericht und Seite, ab VI. Tätigkeitsbericht nach Tätigkeitsbericht und Ziffer

* Fundstelle zitiert nach Tätigkeitsbericht und Seite, ab VI. Tätigkeitsbericht nach Tätigkeitsbericht und Ziffer

* Fundstelle zitiert nach Tätigkeitsbericht und Seite, ab VI. Tätigkeitsbericht nach Tätigkeitsbericht und Ziffer

* Fundstelle zitiert nach Tätigkeitsbericht und Seite, ab VI. Tätigkeitsbericht nach Tätigkeitsbericht und Ziffer

* Fundstelle zitiert nach Tätigkeitsbericht und Seite, ab VI. Tätigkeitsbericht nach Tätigkeitsbericht und Ziffer

S

* Fundstelle zitiert nach Tätigkeitsbericht und Seite, ab VI. Tätigkeitsbericht nach Tätigkeitsbericht und Ziffer

* Fundstelle zitiert nach Tätigkeitsbericht und Seite, ab VI. Tätigkeitsbericht nach Tätigkeitsbericht und Ziffer

T

U

* Fundstelle zitiert nach Tätigkeitsbericht und Seite, ab VI. Tätigkeitsbericht nach Tätigkeitsbericht und Ziffer

* Fundstelle zitiert nach Tätigkeitsbericht und Seite, ab VI. Tätigkeitsbericht nach Tätigkeitsbericht und Ziffer

* Fundstelle zitiert nach Tätigkeitsbericht und Seite, ab VI. Tätigkeitsbericht nach Tätigkeitsbericht und Ziffer