Landtag von Sachsen-Anhalt **Drucksache 4/2189**
Vierte Wahlperiode **25.05.2005**

Unterrichtung

Datenschutzbeauftragter des Landes Sachsen-Anhalt

Magdeburg, 18. Mai 2005

Siebenter Tätigkeitsbericht des Landesbeauftragten für den Datenschutz für die Zeit vom 1. April 2003 bis 31. März 2005

Sehr geehrter Herr Präsident,

gemäß § 22 Abs. 4a Satz 1 Datenschutzgesetz Sachsen-Anhalt (DSG-LSA) erstatte ich meinen Siebenten Tätigkeitsbericht für den Zeitraum vom 1. April 2003 bis 31. März 2005. Er schließt an den sechsten Tätigkeitsbericht an, der als Drucksache 4/839 vorliegt und in den Ausschüssen für Inneres und für Recht und Verfassung beraten wurde.

Mit freundlichen Grüßen

Dr. Harald von Bose

Verfügung des Präsidenten des Landtages von Sachsen-Anhalt:

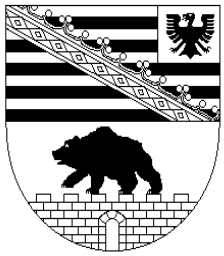
Die Unterrichtung des Landtages erfolgt gemäß § 54 Abs. 1 Satz 2 der Geschäftsordnung des Landtages (GO.LT).

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.

Hinweis: *Die Drucksache steht vollständig digital im Internet/Intranet zur Verfügung.*
Die Anlage wird aufgrund des Umfangs zur Einsichtnahme in der Bibliothek des Landtages von Sachsen-Anhalt bereitgestellt und kann in gedruckter Form abgefordert werden.

(Ausgegeben am 25.05.2005)

Landesbeauftragter
für den Datenschutz
Sachsen-Anhalt



VII. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

**für die Zeit
vom
1. April 2003 bis 31. März 2005**

VII. 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

Vorwort

Dieser Tätigkeitsbericht umfasst den Zeitraum vom 1. April 2003 bis zum 31. März 2005.

Nach der Wahl durch den Landtag von Sachsen-Anhalt am 3. März und mit der Amtsübergabe am 16. März 2005 habe ich die Nachfolge von Klaus-Rainer Kalk als Landesbeauftragter für den Datenschutz angetreten. Der nach seinem Ausscheiden erstellte Bericht ist insofern maßgeblich sein Bericht. Ein besonderer Dank gilt den Mitarbeiterinnen und Mitarbeitern der Geschäftsstelle.

An mehreren Textpassagen des Berichts habe ich noch systematische und inhaltliche Akzentuierungen vorgenommen, zumal im Hinblick auf Themen, die sich auch im folgenden Berichtszeitraum stellen werden. Unter Ziffer 1. habe ich Entwicklungslinien der Datenschutzpolitik und des Datenschutzrechts und aktuelle und zukünftige Schwerpunkte beschrieben. Das Urteil des Bundesverfassungsgerichts vom 12. April 2005 (Az. 2 BvR 581/01 - NJW 2005, 1338) zur satellitengestützten polizeilichen Überwachung mittels des Ortungssystems GPS (Global Positioning System) macht exemplarisch deutlich, dass im informationstechnischen Wandel Technikrisiken stecken, die der Gesetzgeber ebenso beobachten und ggf. minimieren muss wie die verfahrensrechtlichen Sicherungen gegen eine Rundumüberwachung stärken.

Der Bericht dient der Berichterstattung gegenüber dem Landtag, zusammen mit der Stellungnahme der Landesregierung wird der Bericht Gegenstand der parlamentarischen Beratungen sein. Der Bericht ist zudem als Darstellung zur Situation des Datenschutzes Mittel der Öffentlichkeitsarbeit und Handreichung für Behörden, behördliche Datenschutzbeauftragte und interessierte Bürgerinnen und Bürger. Für Zuspruch, auch Kritik, für Reaktionen und Diskussionen über die Themen des Datenschutzes in Sachsen-Anhalt und darüber hinaus als Teil eines Diskurses über das Verständnis von Rechtsstaat und Gesellschaft wäre ich dankbar.

Magdeburg, den 18. Mai 2005

Dr. Harald von Bose
Landesbeauftragter für den Datenschutz Sachsen-Anhalt

Inhaltsverzeichnis

Anlagenverzeichnis

1. Entwicklung und Situation des Datenschutzes - Grundsätzliche Anmerkungen und Ausblick

Die Menschenwürde und die Freiheit des allgemeinen Persönlichkeitsrechts in ihrer besonderen Ausprägung des Grundrechts der informationellen Selbstbestimmung und damit ein wesentliches Stück des rechtsstaatlichen Fundaments des Gemeinwesens sind weiter in Gefahr geraten.
Im Berichtszeitraum war es zwanzig Jahre her, dass das Bundesverfassungsgericht im Urteil zum Volkszählungsgesetz Leit- und Grundsätze für die Erhebung, Verarbeitung und Auswertung personenbezogener Daten aufgestellt hat (Urteil vom 15. Dezember 1983, BVerfGE 65, 1). An diese vom Gericht später fortentwickelten Maßstäbe des Grundrechts auf informationelle Selbstbestimmung, das in Artikel 6 Abs. 1 der Landesverfassung ausdrücklich festgeschrieben ist, muss nachdrücklich erinnert werden: Die Datenerhebung und Datenverarbeitung ist grundsätzlich an die Einwilligung des Betroffenen gebunden, was eine transparente Aufklärung über Inhalte, Zweck und Umfang der Datenerhebung voraussetzt. Im Übrigen einschränkende Regelungen haben durch normenklare Gesetze zu erfolgen, die dem Gebot der Verhältnismäßigkeit entsprechen. Vor der Erhebung steht die Frage nach der Notwendigkeit der Erhebung im Sinne von Datenvermeidung und Datensparsamkeit. Der Grundsatz der Zweckbindung und das Verbot der Vorratsdatenspeicherung gehören zu den Kernprinzipien des Grundrechts. Technische und organisatorische Vorkehrungen begleiten die gesetzlichen Regelungen. Institutionalisierte Datenschutzkontrollen unterstützen den Grundrechtsschutz. Angesichts der Weiterentwicklung der modernen Datenverarbeitung und ihrer Komplexität und Mobilität kommt dem Datenschutz durch Technik stetig zunehmende Bedeutung zu. Die Gefahren für den Grundrechtsschutz sind im Falle automatisierter Datenverarbeitung ungleich größer als bei nichtautomatisierter Verarbeitung. Konsequent ist insofern die Aussage, dass es kein belangloses personenbezogenes Datum gibt. Das Grundrecht gilt aber gleichermaßen unabhängig von der Art der Erhebung und Verarbeitung oder Nutzung.

Diese Maßstäbe wurden im Zuge der Terrorismusbekämpfung seit 2001, die mehr und mehr als allgemeingültige Rechtfertigung für zahlreiche Maßnahmen benutzt wird, und auch im Übrigen infolge der Faszination der Technik, wirtschaftlicher Erwägungen und von Effektivitätsgesichtspunkten in vielen Bereichen vernachlässigt, ja missachtet. Zum Ende des Berichtszeitraums im März 2005 wiesen mehrere große Tages- und Wochenzeitungen auf Entwicklungen zur Schaffung des „gläsernen Bürgers“ und die damit verbundenen Gefährdungen hin. Der Datenschutz war öffentliches Thema - allerdings sahen alle Kommentatoren den Datenschutz in der Defensive, fast auf verlorenem Posten, angesichts eines Staates in der Entwicklung zum „Big Brother“ im Sinne des Orwellschen Vorbilds. Dass die Würde des Menschen antastbar geworden ist, belegen aktuelle Beispiele und Vorhaben. So geht es um den

- gläsernen Bankkunden (Kontenkontrolle) - siehe Ziff. 8.1.2 und **Anlage 25**
- gläsernen Arbeitnehmer (Jobkarte)
- gläsernen Patienten (Gesundheitskarte) - siehe Ziff. 10.2 und **Anlage 27**
- gläsernen Touristen (biometrische Ausweise) - siehe VI. Tätigkeitsbericht, Ziff. 5.1
- gläsernen Telekommunikationsteilnehmer (Telefon-, SMS-, E-Mail-Daten) - siehe Ziff. 23.2
- gläsernen Beschuldigten und Nichtbeschuldigten (DNA-Analyse) - siehe Ziff. 18.3 und **Anlage 26**

Besondere Brisanz entsteht dann, wenn es zu Verknüpfungen einzelner Datenbereiche und Datenverbünden kommt, wie etwa im Falle der geplanten Chip-Karten oder einer erwogenen Wiedereinführung einer einheitlichen Personenkennziffer **(**vgl. **Anlage 15).**

Der Landesbeauftragte betrachtet solche Entwicklungen vor dem Hintergrund des grundrechtlichen Schutzes mit großer Sorge (vgl. auch die zusammenfassende Kritik der Konferenz der Datenschutzbeauftragten von Bund und Ländern vom März 2003 in **Anlage 1**). Ob tatsächlich die Schwelle zum „Big Brother“ schon überschritten ist, mag zwar angesichts des Funktionierens rechtsstaatlicher Gegenmechanismen fraglich sein, und ob in allen genannten Fällen eine vollständige Erfassung des Bürgers mittels umfassender Erhebung seiner Daten erfolgt, kann dahinstehen. Die Häufung und Intensität der Vorhaben sind aber auffällig und alarmierend und geben Anlass zu besonderer Warnung. Geradezu unglaublich wäre die angedachte Nutzung der Gesundheitskarte für die Terrorabwehr. Offenbar gibt es kaum noch Tabus.

Der **Kernbereich privater Lebensgestaltung** freier Menschen muss aber der Einwirkung jeglicher staatlichen Gewalt entzogen bleiben.

Bei der Diskussion über diese Themen ist immer wieder einer Reihe von Irrtümern entgegenzutreten:
So ist insbesondere dem vermeintlichen Argument zu widersprechen, der rechtstreue Bürger lasse sich nichts zuschulden kommen und sei daher offen gegenüber jeglicher Sammelwut des Staates. Wenn er über den Umfang der Sammelflut und die Konsequenzen aufgeklärt wird, sieht er die Sache schnell sehr viel sensibler. Dann fordert er doch seine informationelle Selbstbestimmung ein, zumal als Beteiligter etwa im Falle der Kontodatenabfrage, aber auch als Unbeteiligter, und will - wie es das Bundesverfassungsgericht für den Bereich des Schutzes der Wohnung formuliert hat - in Ruhe gelassen werden. Aus dem Datenschutzbewusstsein erwächst die Inanspruchnahme seines Grundrechts.
Dabei ist zu bedenken, dass der höchstpersönliche Schutz privater Kommunikation auch in Form eines Schutzes digitaler Kommunikation kaum geringer ausfallen darf als der räumliche Schutz für vertrauliche Kommunikation gegenüber staatlicher Wohnraumüberwachung; insofern sind staatliche Zielsetzungen wie etwa die Effektivität staatlicher Strafrechts-

pflege selbst in Zeiten terroristischer Bedrohung auch gegenüber der Würde des Menschen und seinem Datenschutzgrundrecht generell nicht vorrangig, gerade bei Nichtbeschuldigten.

Auch ist es eine - zumal oft sehr pauschale - unzutreffende Behauptung, dass der Datenschutz die Verbrechens-, insbesondere die Terrorismusbekämpfung behindere. Der Landesbeauftragte verfolgt diese Diskussion gelassen. Der Schutz von Sicherheit und Freiheit der Bürgerinnen und Bürger ist gemeinsam Teil der rechtsstaatlichen Ordnung. Das zweifellos vorhandene Spannungsverhältnis beider Rechte bestätigt dies nur zu sehr. Eine Kritik am Datenschutz im Sinne von „Täterschutz“ würde auch eine Schelte an Medien, an der Wissenschaft, hier und da auch am Gesetzgeber, jedenfalls oftmals an der Judikative bedeuten. Eine allmächtige Terrorismusbekämpfung würde gleich auch andere Rechte miterdrücken. Immer ist zu beachten, dass die allermeisten Bürger unbeteiligt und unbescholten sind und insofern nicht im Sinne eines Generalverdachts in Terrorismusbekämpfungsmaßnahmen einbezogen werden dürfen; in diesem Zusammenhang kann auch auf Entschließungen der Konferenz der Datenschutzbeauftragten von Bund und Ländern vom Oktober 2001 verwiesen werden (VI. Tätigkeitsbericht, Anlagen 3 und 11). Vor allem ist einer der Kerngrundsätze des Datenschutzrechts gemäß der unnachgiebigen Rechtsprechung des Bundesverfassungsgerichts hervorzuheben: **Nicht jeder Zweck ist rechtlich zulässig, ein zulässiger Zweck heiligt nicht jedes Mittel. Der Überwachungsstaat wäre nicht mehr Rechtsstaat.** Die Grundrechte besitzen zwar einen abwehrenden Charakter gegen den Staat, beinhalten zugleich aber auch einen Schutzauftrag. Dies gilt für jedes Freiheitsrecht, dabei geht es um Sicherheit vor Angriffen Privater. Dies gilt auch für die informationelle Selbstbestimmung, beim Schutzcharakter dieses Grundrechts geht es ebenfalls um den Schutz vor Eingriffen durch andere Grundrechtssubjekte. Eines der Probleme besteht dabei darin, dass der Staat einerseits bei den von ihm selbst vorgenommenen Einschränkungen den Kernbereich dieses Grundrechts zu wahren, andererseits selbst die Aufgabe des Schutzes wahrzunehmen hat.

In diesem Zusammenhang betrachtet der Landesbeauftragte auch die Aussage der Landesregierung - wie auch Überlegungen auf Bundesebene - in deren Stellungnahme zum VI. Tätigkeitsbericht (LT-Drs. 4/1257 - zu Ziff. 1 (S. 5)) skeptisch, im Rahmen einer Vereinfachung des Datenschutzrechts bedürfe es eines radikalen Abbaus bereichsspezifischen Datenschutzrechts, ohne hierbei den Datenschutz substantiell abzusenken. Der Landesbeauftragte zieht eine substantielle Anhebung des Datenschutzes vor und sieht stets Bedarf für strenge bereichsspezifische **Zweckbindungsregelungen**. Der Landesbeauftragte wird darauf achten, dass bei Änderungsgesetzen auch erneut der datenschutzrechtliche Regelungsbedarf im Stammgesetz in den Blick genommen wird. Auch sollten Gesetze generell stärker einer Evaluation unterworfen werden. Transparenz und Verständlichkeit der Regelungen, für die auch der Grundsatz der Datensparsamkeit als Teil der Rechtsvereinfachung gelten muss, bleiben natürlich ein wichtiger Maßstab. Nur mit Generalklauseln kommt man aber nicht aus.

Die Aufgabenwahrnehmung der Datenschutzbeauftragten hat bei alledem trotzdem mit der notwendigen Sachlichkeit zu erfolgen. Der Beratung im Vorfeld der Formulierung von Regelungswerken und der Einführung von neuen technischen Verfahren kommt vorrangige Bedeutung zu. Die Kontrollen bleiben aber wichtige Möglichkeiten des Anstoßes. Der Landesbeauftragte sieht sich in der Verantwortung, jeweils kritisch, mahnend und warnend dem Datenschutz zum Erfolg zu verhelfen. Aus seiner unabhängigen Position und seinem Datenschutzgewissen heraus wird der Landesbeauftragte die Dinge weiterhin beharrlich beim Namen nennen - und zugleich Veränderungs- und Verbesserungsvorschläge machen. In diesem Bericht sind, verbunden mit Erläuterungen zur Rechtslage, zahlreiche Beispiele dargestellt, wo dies gelungen ist. Auch das gehört zur Zustandsbeschreibung des Datenschutzes dazu. Dabei ist auch die konstruktive Zusammenarbeit mit dem Innenministerium hervorzuheben.

Die Konferenz der Datenschutzbeauftragten von Bund und Ländern hat im Übrigen im Tätigkeitszeitraum eine Reihe von wichtigen Entschließungen zu aktuellen Problemfeldern einschließlich der oben aufgeführten Themen gefasst, die bei den einzelnen Beiträgen und als Anlagen zu diesem Bericht aufgeführt sind. Diese Zusammenarbeit ist für die Durchsetzung datenschutzrechtlicher Forderungen ein überaus gewichtiger und immer wieder auch wirkungsvoller Faktor.
Im Jahr 2006 wird Sachsen-Anhalt erstmals den Vorsitz dieser Konferenz übernehmen.

Zu zukünftigen Fragestellungen wird die Diskussion über die Zusammenarbeit öffentlicher Stellen für die staatliche Sicherheitsvorsorge im Sinne eines erweiterten Sicherheitsbegriffs gehören. Der weitgreifende Ansatz der Innenministerkonferenz für eine neue Strategie zum Schutz der Bevölkerung (vor terroristischen Gefährdungen und Naturkatastrophen) hat bereits zu mehr Kooperationen und Kommunikationen geführt. Dies gilt auch im Hinblick auf Überlegungen des Bundesinnenministers und innerhalb der Föderalismuskommission für eine neue Sicherheitsarchitektur. Dass dabei auch personenbezogene Daten berührt sein können, liegt gerade beim Bereich der Aufgaben von Polizei und Verfassungsschutz auf der Hand. Die neuen Kooperationsformen dürfen nicht zu einer Aufweichung des Trennungsgebotes sowie der Datenübermittlungsgrundsätze führen.
Weitere Begehrlichkeiten für Datenzugriffe im Rahmen angedachter Verschärfungen der Anti-Terror-Gesetze sind erkennbar geworden, es wäre aber verfassungswidrig, grundrechtswidrig und maßlos, die gesamte Gesellschaft etwa in ihrem Freizeitverhalten in den Dienst der Terrorismusgefahrenabwehr einzubeziehen. Das Gemeinwesen benötigt ein Vertrauensfundament, das nicht allein auf den Schutz der Bürger und deren Sicherheit abhebt.

Zum Ausblick gehört auch die Frage nach einem **Informationsfreiheitsgesetz** des Landes. Ein in der vierten Legislaturperiode von einem Teil der Opposition erneut vorgelegter Gesetzentwurf schien bei der Landesregierung und den Koalitionsfraktionen nicht auf große Zustimmung zu stoßen. Auch der auf Bundesebene diskutierte Entwurf hat viel Wider-

spruch erfahren. Der Landesbeauftragte hat im Rahmen einer Anhörung im Ausschuss für Recht und Verfassung im Landtag keine gravierenden Bedenken erhoben und empfiehlt hier nach wie vor mehr Gelassenheit und den Blick über die Landesgrenzen, nach Berlin, Brandenburg, Nordrhein-Westfalen und Schleswig-Holstein, und auch insbesondere ins europäische Ausland. Der deutsche Staat, der sich vor gravierenden Eingriffen in das Grundrecht auf informationelle Selbstbestimmung nicht scheut, ist bei der Frage nach seinem eigenen Demokratieverständnis und einem entsprechenden transparenten Verwaltungshandeln insgesamt doch noch sehr zögerlich.

Schließlich noch ein nachdenklicher, weiter reichender Blick in die Zukunft: Im nicht-öffentlichen Bereich ist die **technische Entwicklung** noch rasanter als im Bereich des Staates. Die Erfahrung zeigt, dass Ergebnisse dieser technischen Entwicklung, wenn auch mit entsprechender Verzögerung, sich auch im öffentlichen Bereich durchsetzen bzw. von Landes- und Kommunalbehörden intensiv genutzt werden. Erinnert sei hier z.B. an die Vernetzung der Landesverwaltung und Bundesverwaltung (ITN-LSA, TESTA-Deutschland) sowie die Nutzung des Internets und der Internettechnologien (eGovernment, Landesportal Sachsen-Anhalt, www.sachsen-anhalt.de).
Seit Jahren sind dabei in der Entwicklung der Informations- und Kommunikationstechnik (IuK) bestimmende Tendenzen zu beobachten. Dazu gehören:

- die günstige Verfügbarkeit von PC-Technik für Staat, Wirtschaft und Privathaushalte infolge Preisverfall bei Prozessoren und Speichermedien

- die weitere **rapide Miniaturisierung** von informationstechnischen Komponenten (z.B. bei der Chipherstellung oder den Speichermedien). Die Umsetzung der Forschungsergebnisse aus einer der Zukunftstechnologien, der Nanotechnologie, wird hier die weitere Entwicklung in den nächsten Jahren bestimmen. Die Nanotechnologie befasst sich ganz allgemein mit der Herstellung, Untersuchung und Anwendung von Strukturen und molekularen Materialien in einer Dimension bzw. mit Fertigungstoleranzen unterhalb 100 Nanometer.
  Hieraus ergeben sich neue Funktionalitäten und Eigenschaften zur Verbesserung bestehender oder Entwicklung neuer Produkte und Anwendungen. Ein Nanometer (nm) bezeichnet den millionstel Teil eines Millimeters (zum Vergleich: der Querschnitt eines menschlichen Haars ist 50.000 mal größer).

- die stetig **zunehmende und umfassende Vernetzung** von IuK-Systemen. Das Internet ist in der sogenannten Informationsgesellschaft zwar bereits Alltag. Aber auch zukünftig werden auf diese Informationsgesellschaft neue und unter Datenschutzaspekten völlig neue Herausforderungen zukommen.

Bereits jetzt bilden die sich ausbreitenden drahtlosen Kommunikationstechniken (Wireless LAN) die Grundlage für eine nächste Basistechnologie, die kurz mit dem Begriff **RFID** (Radio Frequency Identification) umschrieben wird.
Mit RFID wird die Technologie bezeichnet, bei der durch Funkwellen eine kontaktlose automatische Identifikation von Gegenständen ermöglicht wird, die mit einem sogenannten RFID-tag (RFID-Etikett) versehen sind. Diese RFID-tags, die nach dem Prinzip des Transponders (Transmitter und Responder) arbeiten, bestehen aus einem Chip, je nach Bauart ein Speicher- oder ein Prozessorchip, und einer Antenne. Grundsätzlich werden diese RFID-tags noch in passive und aktive (mit eigener Energiequelle) Bauelemente unterteilt.
Zurzeit sind Hauptanwendungsgebiete in den Bereichen Industrieautomation, Zutrittssysteme, Warenmanagement und Logistik sowie Diebstahlsicherung (z.B. an Kleidungsstücken) zu finden. Das Spektrum der Anwendungen wird sich aber schnell erweitern, etwa auf Ausweisdokumente und Chipkarten, z.B. im öffentlichen Personennahverkehr. RFID-tags können der Identifizierung von Waren, Objekten, aber auch von Personen dienen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat erste Datenschutzhinweise gegeben **(Anlage 19).**

- die Identifizierung ist aber längst nicht alles, was miniaturisierte IuK-Technik zu leisten im Stande ist. Viele Forschungsvorhaben, die sich mit allgegenwärtiger (ubiquitous) oder um sich greifender (pervasive) Informationstechnologie teils visionär, aber auch schon in konkreten Pilotprojekten befassen, beziehen auch die Gewinnung von Informationen und Messwerten aus der Alltagswelt mit ein. Möglich wird dies durch die bereits angesprochene rapide Miniaturisierung auch im Bereich der Sensortechnik, die mittlerweile auf Streichholzkopfgröße geschrumpft ist.
  Diese **Informatisierung des Alltags**, d.h. die absehbare Durchdringung unserer Welt mit Informationstechnik - **Ubiquitous Computing** -, die Gegenwart von „smarten“, weil intelligenten Gegenständen des Alltags, die miteinander drahtlos kommunizieren und mittels Sensortechnik auch in der Lage sind, Informationen aus ihrer Umgebung aufzunehmen und durch Vernetzung (sog. Sensornetze) weiterzugeben, wird zur grundsätzlichen Auseinandersetzung mit diesem Thema in Politik und Gesellschaft und nicht zuletzt natürlich in der Gesetzgebung und insofern auch im Datenschutz führen müssen, um das informationelle Selbstbestimmungsrecht auch unter zukünftigen technischen Entwicklungen in der Informationsgesellschaft sicherzustellen.

2. Der Landesbeauftragte

2.1 Tätigkeit im Berichtszeitraum

Schwerpunkt der Tätigkeiten des Landesbeauftragten und seiner Mitarbeiter war auch in diesem Zeitraum die Bearbeitung der schriftlichen Ge-

schäftseingänge, der überwiegend telefonisch vorgetragenen Anliegen und Eingaben der Bürgerinnen und Bürger und der Beratungs- und Informationsanfragen durch die öffentlichen Stellen des Landes.
2003 gab es 3.296 registrierte schriftliche Eingänge, im Jahre 2004 waren es 3.233. 2003 sind dazu 790 und 2004 805 schriftliche Stellungnahmen erarbeitet worden. Im Regelfall nicht besonders registriert, aber datenschutzrechtlich ausgewertet und ggf. in die Bearbeitung einbezogen, wurden alle Landtagsdrucksachen. Die Zahl der telefonischen Anfragen hat sich, wie in den Vorjahren auch, zwischen 900 und 1.000 pro Jahr eingependelt. Zugenommen hat das Geschäftsaufkommen durch die moderne Kommunikation per E-Mail.
Der Wunsch zu persönlichen Anfragen und Vorsprachen der Bürger in der Behörde ist aufs Jahr gesehen weiterhin gering. Gleich geblieben ist wie in den Berichtsjahren zuvor in etwa die Zahl der Bürgereingaben (ca. 150 bis 160 pro Jahr).

Im Berichtszeitraum gab es **drei formelle Beanstandungen** nach § 24 DSG-LSA. Die Fälle sind in den entsprechenden Sachabschnitten des Berichtes aufgeführt (Ziff. 12.5, 16.5, 20.18). Darüber hinaus gab es in den beiden Berichtsjahren mehrere Fälle mit erheblichen Rechtsverstößen. Der bereits im letzten Tätigkeitsbericht festgestellte rückläufige Trend bei Fehlern und Mängeln im Umgang mit personenbezogenen Daten hat sich aber fortgesetzt.
Dies resultiert aus der verbesserten Aus- und Fortbildung der Bediensteten in den öffentlichen Stellen, zunehmend aber auch aus dem verbesserten Beratungsangebot in den öffentlichen Stellen vor Ort durch die dort mit der letzten Gesetzesnovellierung im August 2001 eingeführten Beauftragten für den Datenschutz (§ 14a DSG-LSA). Den neu eingesetzten Personen kann man im Großen und Ganzen viel Sensibilität und Rechtsgefühl bestätigen. Wenn Fehler auftreten, liegt es häufiger daran, dass die Behördenleitung die eigenen Datenschutzbeauftragten nicht rechtzeitig eingebunden oder deren Rat nicht befolgt hat. Die Aufgaben, Befugnisse und Zuständigkeiten dieser behördlichen Beauftragten sind in Anlage 20 des VI. Tätigkeitsberichts näher beschrieben und auch im Informationsangebot der Homepage des Landesbeauftragten enthalten.

Ein unveränderter Schwerpunkt liegt bei der automatisierten Datenverarbeitung und den damit verbundenen besonderen Problemen der Datensicherheit; Einzelheiten dazu sind unter den Ziffern 7 und 12 dargestellt. Die vom Landesbeauftragten anlassunabhängig festgesetzten Querschnittskontrollen wurden bei den Ausländer- und einer Meldebehörde fortgesetzt; darüber hinaus gab es bei den Ausländerbehörden eine größere Zahl gezielter Einzelfallkontrollen in vom Bundesbeauftragten für den Datenschutz übermittelten Fällen nach dem Schengener Durchführungsübereinkommen (siehe Ziff. 4).

Fortgesetzt wurden auch die Kontrollen bei einem Finanzamt, zwei Polizeibehörden und zwei Staatsanwaltschaften. Erstmals wurden zwei Waffenbehörden des Landes kontrolliert. Landesweit mussten bei den Kommunen erneut erhebliche Probleme beim Umgang mit personenbezoge-

nen Daten in den Kindertagesstätten festgestellt werden (siehe Ziff. 20.17 ff.).
Wieder aufgegriffen wurde in drei Fällen die Prüfung der Erhebung, Verarbeitung und Nutzung von Personaldaten bei verschiedenen Fachbehörden.

Die Mitarbeiterinnen und Mitarbeiter haben zusammen mit dem Landesbeauftragten wieder als Dozenten oder Vortragende beim Fortbildungsprogramm für die Allgemeine Verwaltung, im Bereich der Aus- und Fortbildung der Polizei und bei mehreren Einzelveranstaltungen mit anderen öffentlichen Stellen mitgewirkt und sich selbst fortgebildet.

Auch in diesem Berichtszeitraum gab es in der Geschäftsstelle des Landesbeauftragten einen Personalwechsel auf zwei Mitarbeiterstellen als Folge altersbedingten Ausscheidens. Einen Wechsel von Gesetzes wegen gab es auch im Amt des Landesbeauftragten für den Datenschutz am 16. März 2005 (siehe Vorwort).
Im Zuge der Neubesetzungen ist die Aufgabenzuweisung in den Referaten der Geschäftsstelle geändert worden. Die aktuelle Aufgabenzuweisung kann dem anliegenden Organigramm **(Anlage 29)** entnommen werden.

Im Berichtszeitraum hat sich die Internet-Homepage des Landesbeauftragten **(www.datenschutz.sachsen-anhalt.de)** zu einem wesentlichen Bestandteil seiner Öffentlichkeitsarbeit entwickelt. In den letzten 12 Monaten des Berichtszeitraumes ist das Angebot von über 61.000 Besuchern in Anspruch genommen worden, die sich fast 200.000 Seiten anzeigen ließen, z.B. eine Fülle von Informationsmaterialien. Die hohen Zugriffszahlen sind nicht zuletzt auch eine Bestätigung für den Landesbeauftragten, dass der bereits im Jahre 2000 eingeschlagene Weg, die interessierte Öffentlichkeit ebenso wie die Behörden und Ämter des Landes auch über das Internet aktuell zu unterrichten, richtig war. Über den Inhalt des Internet-Angebotes, das ständig erweitert und aktualisiert wird, hatte der Landesbeauftragte in seinem VI. Tätigkeitsbericht unter Ziff. 2.3 umfassend informiert.
In diesem Zusammenhang bedankt sich der Landesbeauftragte beim Landesinformationszentrum, das zuverlässig und kompetent das Hosting seines Internetangebotes leistet.

2.2 Zusammenarbeit mit anderen Institutionen

Komplikationslos und geprägt von Sachlichkeit und gegenseitigem Vertrauen hat sich auch im Berichtszeitraum die Zusammenarbeit mit dem **Landtag** im parlamentarischen Bereich bewährt. Kommt es zu datenschutzrechtlichen Fragen oder Problemen, so werden diese durch Stellungnahmen während der Ausschussberatungen oder über Schriftsätze geklärt. Das verfassungsrechtlich verankerte Recht des Landesbeauftragten, sich jederzeit an den Landtag wenden zu können, unterstreicht und unterstützt seine Unabhängigkeit.

Unverändert offen und vertrauensvoll ist auch die Zusammenarbeit mit dem Landtagspräsidenten Prof. Dr. Spotka und der von ihm geführten Landtagsverwaltung. Eine Mitarbeiterin aus der Geschäftsstelle des Landesbeauftragten fungiert zugleich als behördliche Datenschutzbeauftragte für die Landtagsverwaltung.

Zwei grundlegende Aufgaben des Landesbeauftragten sind die Beratung und die Kontrolle der **Exekutive**. Dabei reicht das Spektrum vom einfachen Verwaltungshandeln bis zur Gesetzesausarbeitung. Die für den Datenschutz wichtige Schlüsselfunktion hat dort das Ministerium des Innern, insbesondere das Referat 41. Es soll erneut betont werden, dass der dort erforderliche Spagat zwischen den Anforderungen der Politik und der Bewahrung der Freiheits- und Persönlichkeitsrechte der Bürgerinnen und Bürger bei der Gestaltung der Rechtsvorschriften und -umsetzung von diesem Referat in jahrelanger Kontinuität, mit einem hohen Sachverstand und in einem fairen Austausch mit dem Landesbeauftragten für den Datenschutz geleistet wird. Eine gute und sachorientierte Zusammenarbeit gibt es, unbeschadet sachlicher Meinungsunterschiede, auch mit den übrigen Obersten Landesbehörden.

Eine tragende Säule der Zusammenarbeit im nationalen Bereich ist und bleibt die **Konferenz der Datenschutzbeauftragten des Bundes und der Länder** und die von ihr eingerichteten Arbeitskreise. Angesichts der Vielfalt der in den einzelnen Lebensbereichen auftretenden datenschutzrechtlichen Probleme ermöglicht die gegenseitige Zusammenarbeit auch die Konzentration auf und die nötige Arbeitskraft für spezielle Diskussionen und sachorientierte Lösungen in der bundesweiten täglichen Arbeit.

Die bereits in den letzten Tätigkeitsberichten angesprochenen neuen Formen der Zusammenarbeit mit den in Europa und international eingesetzten unabhängigen Kolleginnen und Kollegen haben sich insbesondere in Europa positiv verfestigt. Vor allem in Europa beobachtet man im Verlauf der letzten fünf Jahre starke Verschiebungen in der Verantwortung von den einzelnen Mitgliedsländern hin zur Europäischen Rechtsebene (vgl. Ziff. 6.).
Zum 31. Dezember 2004 wurde im Hinblick auf den Wechsel im Amt des Landesbeauftragten die an die Person geknüpfte Nebentätigkeit für den Bundesrat als zweiter unabhängiger deutscher Vertreter in der Gemeinsamen Kontrollinstanz für Europol beendet.

Im internationalen Bereich bleiben die USA mit ihrer weltweit dominierenden Stellung auch im Datenschutz eine schwierige Größe. Immerhin sind zwischenzeitlich in den USA auch auf der Bundesebene erste unabhängige Datenschutzbehörden eingerichtet worden. Deren Mitarbeiter bemühen sich, im Schulterschluss mit ihren europäischen, auch deutschen Kollegen, Anschluss an die im „alten Europa“ entwickelten Datenschutzstandards zu finden. Dies gelingt zunehmend, ohne dass die für das US-amerikanische Selbstverständnis erforderlichen individuellen Ausprägungen zu deutlich hervortreten. Der Landesbeauftragte hat über seine Arbeit der Gemeinsamen Kontrollinstanz für Europol interessante Einblicke auf

der Ebene des US-amerikanischen Justizministeriums und insbesondere in den Arbeitsbereich des neu gegründeten US-Heimatschutzministeriums erhalten.

Darüber hinaus hat der Landesbeauftragte im Berichtszeitraum an einer europäischen und zwei internationalen Datenschutzkonferenzen teilgenommen und dabei auch kollegiale Kontakte geknüpft, die die Lösung global auftretender neuer Rechtsfragen erleichtern.

3. Archivwesen

Akteneinsicht beim Jugendamt

Eine Petentin hatte bei dem für ihren Sohn zuständigen Jugendamt einer Stadt Akteneinsicht in einen Vorgang beantragt, der mehr als 20 Jahre zurück lag. Da dieser Antrag unter zum Teil widersprüchlichen Angaben sowohl vom Jugendamt als auch vom Stadtarchiv abgelehnt wurde, wandte sich die Betroffene an den Landesbeauftragten.
Nachdem schriftliche Aufklärungsversuche keinen Erfolg hatten, wurde eine Kontrolle vor Ort erforderlich, die in beiden Arbeitsbereichen rechtlich bedenkliche Verfahrensweisen und Unsicherheiten in der Rechtsanwendung aufgedeckt hat. Im Einzelnen hat der Landesbeauftragte folgende Mängel festgestellt:

- Das Jugendamt hat den Antrag auf Akteneinsicht mit widersprüchlichen Begründungen abgelehnt; einmal gab es keine Unterlagen oder ein andermal sollen die Kriterien für die Akteneinsicht nicht vorgelegen haben. Außerdem wurde mit § 25 SGB X eine falsche Rechtsgrundlage herangezogen. Da das Verfahren aber vor Jahren abgeschlossen wurde und die Petentin den datenschutzrechtlichen Auskunftsanspruch geltend machte, hätte eine Auskunft nach § 83 SGB X bzw. ein Archivierungshinweis erteilt werden müssen.

- Auf Empfehlung des Landesbeauftragten wandte sich die Petentin zusätzlich an das Stadtarchiv. Das Archiv bestätigte zwar das Vorhandensein von Unterlagen, es sei aber ohne Zustimmung des Jugendamtes nicht berechtigt, Informationen herauszugeben. Die Erörterung ergab, dass die Unterlagen des Jugendamtes richtigerweise als Archivgut an das Stadtarchiv abgegeben und dort übernommen wurden. Daher wäre eine Auskunft gem. § 6 ArchG-LSA in Verantwortung des Archivs möglich gewesen.
  Dies schließt nicht aus, dass sich das Archiv dazu ohne Personenbezug mit dem Fachamt über spezialgesetzliche Anforderungen vorher berät. Die Archivmitarbeiter waren sich dieser Verantwortung zunächst jedoch nicht bewusst.

Nach dieser Kontrolle wurden die entsprechenden Unterlagen durch das Stadtarchiv an die Petentin übersandt.

4. Ausländerangelegenheiten

Ausschreibungen zur Festnahme nach dem Schengener Durchführungsübereinkommen

Ausländer aus einem Staat, der nicht der EU angehört und die ausgewiesen oder abgeschoben worden sind, werden nach dem Schengener Durchführungsübereinkommen im Schengener Informationssystem zur Festnahme ausgeschrieben. Dabei ist es bundesweit bei den Ausländerbehörden in der Vergangenheit immer wieder zu falschen Ausschreibungen gekommen. Von diesem Problem sind wohl auch die anderen EU-Länder betroffen. Deshalb hat die Gemeinsame Kontrollinstanz für das Schengener Durchführungsübereinkommen eine koordinierte Kontrolle des Ausschreibungsverfahrens beschlossen. In Ausführung dieses Beschlusses hat der Bundesbeauftragte für den Datenschutz eine Liste von Prüffällen nach einem Zufallsgenerator erstellen lassen und an die Länder übermittelt. In Sachsen-Anhalt hat sich der Landesbeauftragte von den zuständigen Ausländerbehörden die Akten der betreffenden Ausländer übersenden lassen. Dabei hat er gravierende Mängel festgestellt:

In mehreren Fällen war kein Ausschreibungsgrund erkennbar, d.h., der Ausländer war weder tatsächlich ausgewiesen noch abgeschoben worden. In einem Fall war eine Ausschreibung erfolgt, obwohl aus der Akte hervorging, dass der Ausländer im Inland verstorben war.

Nach dem Durchführungsübereinkommen haben die Ausländerbehörden die Erforderlichkeit der weiteren Speicherung spätestens drei Jahre nach der Einspeicherung zu überprüfen. Aus keiner der geprüften Ausländerakten ging hervor, dass diese Überprüfung stattgefunden hatte, obwohl die Mehrzahl der betreffenden Ausländer bereits mehr als sechs Jahre eingespeichert war.

Der Landesbeauftragte erwartet, dass das Ministerium des Innern des Landes zur Sicherung des Verfahrens auf die Ausländerbehörden einwirkt. Selbst hat er sich vorgenommen, bei seinen regelmäßigen Prüfungen der Ausländerbehörden jetzt auch die Ausschreibungspraxis mit zu untersuchen.

5. Baurecht

Übermittlung der persönlichen Daten Verfahrensbeteiligter an ein privates Bauplanungsbüro

Schon in den vergangenen Jahren hat der Landesbeauftragte mitunter über datenschutzrechtliche Probleme im (Bau-)Planungsrecht berichtet. Im Berichtszeitraum wandte sich ein Bürger an ihn, der sich durch Anregungen und Bedenken an einem Bebauungsplan beteiligt hatte und nun empört darüber war, dass seine Angaben von der Stadtverwaltung an ein privates Planungsbüro übermittelt und als Drucksache ins Internet gestellt worden waren.

Wie sich herausstellte, hatte die am Verfahren beteiligte Grundstücks-GmbH ohne Wissen der Stadtverwaltung die personenbezogenen Daten des Petenten mit seinen Anregungen und Bedenken tatsächlich an ein privates Planungsbüro weitergeleitet. Die Stadtverwaltung hat dies als datenschutzrechtliches Fehlverhalten erkannt und - um Wiederholungen in der Zukunft auszuschließen - in ihren Vertragsformularen mit Erschließungsträgern einen Passus zum Datenschutz aufgenommen. Später ist diese Maßnahme sogar in den Anti-Korruptionsplan der Stadt mit eingeflossen.
Bezüglich der Veröffentlichung der (verkürzten) personenbezogenen Anregungen und Bedenken in einer Drucksache zum Bebauungsplan zeigte sich die Stadt nicht ganz so einsichtig. Doch konnte der Landesbeauftragte die Verwaltung unter Hinweis auf einen Beschluss des Bundesverfassungsgerichts vom 24. Juli 1990 (NVwZ 1990, S. 1162) davon überzeugen, dass es keine Notwendigkeit gibt, Anregungen und Bedenken zusammen mit den personenbezogenen Daten des Einwenders zu veröffentlichen. Diese können nämlich genauso gut pseudonymisiert werden, ohne dass die Öffentlichkeit des Bauleitverfahrens darunter leidet.

6. Europäischer Datenschutz

Auf der europäischen Rechtsebene ist wieder Bewegung beim Thema Datenschutz zu beobachten. Der Schutz personenbezogener Daten hat als Grundrecht Eingang in die Europäische Verfassung gefunden. Im Februar 2004 hat der neue **Datenschutzbeauftragte der EU** Peter Hustinx sein Amt übernommen, der zwischenzeitlich ein gefragter Gesprächspartner gleichermaßen beim Europäischen Parlament und bei der Europäischen Kommission geworden ist. Als Spätfolge bei der Bekämpfung des internationalen Terrorismus hat der Europäische Rat für die Ermittlungsbehörde Eurojust und die Europäische Polizeibehörde Europol neue Aufgaben und eine Konzentration der Abwehr durch ergänzende Rechtsakte vorgesehen.
Dazu gehört auch eine Überarbeitung des Schengener Durchführungsübereinkommens, mit dessen Hilfe u.a. das Aufenthaltsrecht von Bürgern aus Drittstaaten und die Abwehr und Fahndung von bzw. nach Straftätern in den Schengenstaaten geregelt werden (vgl. oben Ziff. 4). Bekanntlich sind bis heute nicht alle Mitgliedsstaaten der Europäischen Union auch dem Schengener Abkommen beigetreten.

Hinzuweisen ist ferner auf die Bemühungen der Datenschutzbeauftragten der EU-Mitgliedsländer (jetzt 25), beim Europäischen Rat mit Hilfe der Europäischen Kommission und des Europäischen Parlaments darauf zu dringen, dass die bisher in der sog. Dritten Säule (Justiz und Polizei) nebeneinander existierenden datenschutzrechtlichen Kontrollinstanzen zusammengelegt und auf einheitliche datenschutzrechtliche Bestimmungen gestellt werden. Zur Zeit gibt es vier Kontrollinstanzen - schon mit einem gemeinsamen Sekretariat - in der Dritten Säule und - wie bereits vorstehend ausgeführt - in der Ersten Säule, den neuen Datenschutzbeauftragten der Europäischen Union. Die entstehende Europäische Verfassung sieht diese Möglichkeit auf der Grundlage eines europäischen Gesetzes

vor. Ein erster Anstoß zur Änderung erfolgte auf der Konferenz der Datenschutzbeauftragten aus Europa im April 2004 in Rotterdam, und deren nächste Konferenz im April 2005 in Krakau wird diesem Thema einen Schwerpunkt widmen.

6.1 Eurojust

Wie bereits im letzten Tätigkeitsbericht dargestellt, hat der Rat der Europäischen Union mit Blick auf die Verstärkung des Kampfes gegen schwere Kriminalität die Gründung von Eurojust beschlossen. Die Datenschutzbeauftragten des Bundes und der Länder hatten in einer Entschließung im Oktober 2001 bereits Anforderungen an den Umgang mit personenbezogenen Daten bei Eurojust definiert.

Nachdem die Bundesregierung den Entwurf eines Eurojust-Gesetzes im August 2003 auf den Weg brachte, trat dieses am 18. Mai 2004 in Kraft.
Die im Errichtungsbeschluss des Rates der EU bestehenden Unklarheiten durch die mangelnde Bestimmtheit von Aufgaben- und Befugnisregelungen konnten zwar im Laufe des Gesetzgebungsverfahren nur im Rahmen des Vorgegebenen präzisiert werden. Die von den Datenschutzbeauftragten vorgeschlagenen Klarstellungen fanden jedoch weitgehend Berücksichtigung.
Da nur die Ergebnisse der Arbeit der strafermittelnden Behörden (in Deutschland vor allem Staatsanwaltschaft, Polizei und Finanzverwaltung), auch soweit sie die Mitwirkung von Eurojust genutzt haben, einer gerichtlichen Kontrolle unterliegen, nicht dagegen jedoch die Arbeit von Eurojust selbst, sind die im Eurojust-Beschluss festgeschriebenen Schutzregelungen beim Umgang mit personenbezogenen Daten von besonderem Belang.
Eurojust führt neben einem zentralen Ermittlungsindex auch temporäre Arbeitsdateien. Auf diese Datenbestände haben nur nationale Mitglieder und hierzu befugte Mitarbeiter von Eurojust unmittelbaren Zugriff. Die zu beachtende strenge Zweckbindung bei der Verarbeitung von personenbezogenen Daten, auf welche von deutschen Stellen bei deren Übermittlung gesondert hinzuweisen ist, wird durch einen internen Datenschutzbeauftragten sowie eine Gemeinsame Kontrollinstanz überwacht. Eine gewisse Begrenzung erfährt die Datennutzung bei Eurojust durch eine als abschließend gedachte Auflistung von Datenkategorien.

Jede Person kann Auskunftsansprüche gegenüber Eurojust geltend machen. Daneben dürfte, soweit die Weitergabe von personenbezogenen Daten an Eurojust problematisch ist, gegenüber deutschen Stellen eine Klage bezüglich der Einhaltung des Eurojust-Gesetzes und damit u.U. subsidiär auch des Bundesdatenschutzgesetzes möglich sein.
Auch wenn eine rechtswidrige Datenverarbeitung eine Schadenersatzpflicht von Eurojust auslösen kann, ist - gerade auch in diesem Zusammenhang - als Manko festzuhalten, dass eine dem deutschen Strafverfahrensrecht vergleichbare Pflicht, Betroffene nach Abschluss der Ermittlungen durch die ermittelnden Behörden über die Erhebung, Verarbeitung und Weitergabe ihrer Daten zu informieren, für Eurojust nicht festge-

schrieben wurde. Auch wenn man in Rechnung stellt, dass sich Eurojust nicht mit „kleinen Fischen“ befasst, gilt in gleicher Weise der Erfahrungssatz, dass unter den datenschutzrechtlich Betroffenen etliche brave Einwohnerinnen und Einwohner Europas erfasst sein dürften. Diese können sich gegen einen Datenmissbrauch jedoch nur wehren, wenn sie von den Umständen der Nutzung ihrer Daten Kenntnis erlangen.

6.2 Europol

Europol hat sich im Berichtszeitraum in Den Haag nicht nur bei der Zahl der Mitarbeiter weiter vergrößert, sondern zeigt zunehmend Erfolge bei der Abstimmung und Koordinierung von Einsätzen von Polizeikräften aus den Mitgliedsstaaten der Union. Schwerpunkte waren der weitere Ausbau der Analysedateien, die Integration der 10 neuen Mitgliedsländer und der weitere Abschluss von Abkommen mit Drittstaaten. Verbesserungsbedürftig ist die Zusammenarbeit auf dem Gebiet der Terrorismusbekämpfung.

Gesetzlicher Änderungsbedarf zeigt sich bei den Regelungen über die Unterstützung und Zusammenarbeit mit Drittländern (z.B. der Drogenbekämpfung in Südamerika und Vorderasien). Auch die Speicherdauer der Daten in den Analysedateien soll von bisher 3 auf 5 oder 10 Jahre verlängert werden.
Rechtliche Änderungen sind aber bei der Europolkonvention angesichts der Anzahl zu beteiligender Mitgliedsländern nicht einfach.

Die Gemeinsame Kontrollinstanz (GKI) hat auch in den Jahren 2003 und 2004 wieder jeweils eine Kontrolle durchgeführt, die Schwachstellen bei der technischen Absicherung, aber auch Mängel bei den aus den Mitgliedsländern angelieferten Unterlagen und deren Verarbeitung bei Europol ergeben haben.
Einzelheiten können dem zweiten Tätigkeitsbericht der GKI für die Zeit von 2002 bis 2004 entnommen werden. Die Sprachfassungen sind im Februar 2005 fertiggestellt worden.

In den letzten Tätigkeitsberichten ist darüber berichtet worden, dass der Landesbeauftragte in Person seit 1998 zweites deutsches Mitglied in der GKI für Europol war und dieses Gremium zuletzt von Oktober 2002 bis 2004 als Präsident geleitet hat. In dieser Zeit ist eine Zusammenarbeit mit der neuen (ersten) US-amerikanischen Datenschutzbehörde bei dem neu errichteten US-Heimatschutzministerium begründet worden.
Obwohl der Bundesrat den Landesbeauftragten im Oktober 2003 noch einmal für fünf Jahre als Kontrollmitglied gewählt hatte, ist diese Aufgabe im Hinblick auf den inzwischen vollzogenen Amtswechsel in Sachsen-Anhalt zum 31. Dezember 2004 niedergelegt worden. Der Bundesrat hat als Nachfolger für die Bundesländer auf Vorschlag der Konferenz der Datenschutzbeauftragten des Bundes und der Länder den Hessischen Datenschutzbeauftragten Prof. Ronellenfitsch gewählt.

7. Entwicklung der automatisierten Datenverarbeitung

7.1 eGovernment-Konzept in Sachsen-Anhalt

Bereits in seinem V. Tätigkeitsbericht (Ziff. 6.1) und zuletzt im VI. Tätigkeitsbericht (Ziff. 7.1) hat der Landesbeauftragte über das Thema eGovernment informiert und die Beachtung datenschutzrechtlicher Belange eingefordert.
In ihrer Stellungnahme zum VI. Tätigkeitsbericht des Landesbeauftragten hat sich die Landesregierung zur Beachtung sowohl der Anforderungen des Telekommunikations-, Tele- und Medienrechts als auch der Verbesserung der Sicherheitsbedingungen für das eGovernment, insbesondere zur Umsetzung der Datensicherheit, gemäß den Schutzzielen des § 6 DSG-LSA zur Wahrung der Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz, bekannt. Mit dem vorliegenden eGovernment-Konzept hat sich die Landesregierung sehr ehrgeizige Ziele gesetzt.

Am 29. April 2003 wurde durch die Landesregierung das „Grundkonzept eGovernment in Sachsen-Anhalt“ (Fassung vom 5. Februar 2003) beschlossen und das Ministerium des Innern mit der Erstellung eines Aktionsplanes beauftragt.
Im Grundkonzept ist die eGovernment-Strategie des Landes Sachsen-Anhalt festgeschrieben. Das eGovernment-Konzept des Landes besteht damit aus dem **Grundkonzept**, dem Aktionsplan für die Jahre 2004 bis 2010 und den daraus abgeleiteten Anwendungen, die sich im **Maßnahmenplan** 2005/2006 wiederfinden. Die so fixierten Projekte und Vorhaben werden von den Ressorts in Abstimmung mit der eGovernment-Koordinierungsstelle, die im Juli 2004 wieder in die Landesleitstelle IT (LIT) des Ministeriums des Innern integriert wurde, ausgestaltet und umgesetzt.
Mit dem von der Landesregierung am 17. August 2004 verabschiedeten eGovernment-Aktionsplan (Version 2.0 vom 3. Juni 2004), der im Zeitraum Januar bis Mai 2004 mit externer Unterstützung einer Beratungsfirma durch das Ministerium des Innern und in enger Zusammenarbeit mit den Ressorts erarbeitet wurde, konnten über 200 ressortübergreifende und ressortinterne Vorhaben im Rahmen einer Bestandsaufnahme ermittelt werden. Diese wurden dann unter Beachtung ihres Nutzens und der entstehenden Kosten einer Bewertung und anschließenden Priorisierung unterzogen. Im Ergebnis dieser Untersuchung und Bewertung erfolgte die Festlegung von 16 Leitprojekten. Neben diesen Leitprojekten sind bis 2010 weitere 97 sog. priorisierte Vorhaben zur stufenweisen Umsetzung geplant.

Ein weiteres Ziel des Aktionsplanes besteht in der möglichst schnellen Bereitstellung von sog. **Basiskomponenten**. Hierzu zählen:

- Dienstleistungsportal (Landesportal) und Content Management System
- Formularserver
- Zahlungsverkehrsplattform
- Digitale Signatur/Virtuelle Poststelle

- Geodaten- und Metadatenserver
- Vorgangsbearbeitung und Dokumentenmanagementsystem.

Diese Basiskomponenten bilden die Grundlage für die Umsetzung der Leitprojekte. Dabei sind oft mehrere Basiskomponenten für ein Leitprojekt notwendig, was zu einer engen Verbindung zwischen Basiskomponenten und Leitprojekten führt.
Zu den 16 **Leitprojekten** gehören:

- Nr.1 Fördermittelmanagement - System "efREporter" - Modul Vorgangsbearbeitungskern
- Nr. 2 IBA STADT MONITOR (Dokumentation/Visualisierung von Projekten des Stadtumbaus)
- Nr. 3 Elektronische Vergabe und Beschaffung
- Nr. 4 Zentrale Stellenbörse
- Nr. 5 KIS - Kabinettsinformationssystem
- Nr. 6 Internetportal (Landesportal www.sachsen-anhalt.de)
- Nr. 7. Fortbildungsangebote LSA (Portal zur Aus- und Fortbildung für alle Ressorts)
- Nr. 8 Datenaustausch Grundbuch - Liegenschaftskataster
- Nr. 9 Geoinformationsdienste (Geobasisinformationen und Bodenkaufpreisinformationen)
- Nr. 10 OPREG/DAP (Systemverbund für eine strategischen Regierungsplanung)
- Nr. 11 Aufsichtsmaßnahmen Bildung MLU
- Nr. 12 Bürgerinformationssystem der Landesverwaltung (Call-Center)
- Nr. 13 Elektronische Einsicht in das maschinell geführte Register (MJ)
- Nr. 14 Automatisiertes gerichtliches Mahnverfahren
- Nr. 15 Elektronischer Rechtsverkehr in Grundbuchsachen
- Nr. 16 Elektronische Steuererklärung.

Bereits die Aufzählung der Projektvorhaben lässt erkennen, dass bei der überwiegenden Mehrheit auch die Belange des Datenschutzes und der Datensicherheit eine wesentliche Rolle spielen.

Allerdings ist der Landesbeauftragte bisher **nur** im **Leitprojekt Nr. 1** Fördermittelmanagement - System "efREporter" direkt beteiligt worden. Im Rahmen dieses Projektes ist die Einführung einer elektronischen Signatur als Pilotverfahren für das Zuwendungsverfahren Fördermittel für die EU-Strukturfonds vorgesehen. Bei erfolgreicher Umsetzung bildet es zugleich den Ausgangspunkt zur landesweiten Einführung der elektronischen Signatur mit gleichzeitigem Aufbau der dazu notwendigen Public Key Infrastructure (PKI) für Sachsen-Anhalt.

Der Landesbeauftragte geht davon aus, dass er bei den übrigen eGovernment-Vorhaben (Basiskomponenten und Leitprojekte) gem. § 22 Abs. 4 Satz 2 DSG-LSA **rechtzeitig** von den Ressorts unterrichtet bzw. dies für die bereits begonnenen Projekte nachgeholt wird. Zur Zeit liegt ihm nur das Feinkonzept des Leitprojektes Nr. 1 vor. Er geht weiterhin davon aus, dass sich die behördlichen Datenschutzbeauftragten der Res-

sorts intensiv mit der Problematik eines datenschutzkonformen eGovernment befassen werden.
Nicht zuletzt lässt auch die Landesregierung, zumindest in den Leitlinien (Thesen) ihres „Grundkonzeptes eGovernment in Sachsen-Anhalt“, erkennen, dass bei grundlegenden Diensten zur umfassenden Information, Kommunikation, Transaktion und Kooperation die Verfügbarkeit, Vertraulichkeit und Integrität der (sicherlich auch) personenbezogenen Informationen gewährleistet werden muss.
Denn bei der Umsetzung von eGovernment sind die Sicherheitsbedürfnisse aller Partner, dazu zählen insbesondere die Bürgerinnen und Bürger des Landes, zu beachten. Nur ein datenschutzkonformes eGovernment wird zur Akzeptanz und zur Nutzung der angebotenen Dienste durch die Bevölkerung führen, denn letztendlich ist eGovernment kein Selbstzweck für die Landesverwaltung.
Vor dem Hintergrund der rasanten technischen Entwicklungen in der Informations- und Kommunikationstechnik und insbesondere aus Gründen des Datenschutzes und der Datensicherheit hält der Landesbeauftragte einen kontinuierlichen Ausbau der grundlegenden Sicherheitsmechanismen für eGovernment und deren ständige Anpassung an den Stand der Technik gem. § 6 Abs. 1 Satz 3 DSG-LSA für erforderlich.

7.2 Die Virtuelle Poststelle

Rechtsgrundlagen für elektronisches Verwaltungshandeln werden zunehmend gelegt. Die technische Ausstattung der privaten Haushalte nimmt ebenso zu wie der Wunsch, elektronisch mit der Verwaltung kommunizieren zu können. Doch nur eine sichere und vertrauliche Kommunikation und ein ausreichender Schutz der personenbezogenen Daten lässt die Bürgerinnen und Bürger die eGovernment-Anwendungen akzeptieren.

Die entstehenden Kommunikations- und Interaktionsprozesse bedürfen einer sicheren technischen Basis. Vielfältige technische Funktionen sind zu gewährleisten, wie beispielsweise die Authentifizierung, die Signaturprüfung und -erstellung, das Ver- und Entschlüsseln eingehender und ausgehender Informationen, die Überprüfung von Nachrichten auf schädliche Inhalte oder richtige Adressierungen. Ein Lösungsweg hierfür ist die so genannte Virtuelle Poststelle. Sie stellt die Schnittstellen für gesicherte Kommunikation zur Verfügung und fungiert als zentrales Security-Gateway.

Die Datenschutzbeauftragten des Bundes und der Länder wollten die Entwicklung unterstützen und begleiten. Eine Arbeitsgruppe unter Leitung des niedersächsischen Datenschutzbeauftragten hatte daher entsprechende Empfehlungen formuliert und als Handreichung „Die Virtuelle Poststelle im datenschutzgerechten Einsatz“ veröffentlicht. In enger Kooperation insbesondere mit den kommunalen Spitzenverbänden in Niedersachsen und dem Bundesamt für Sicherheit in der Informationstechnik beschreibt die Handreichung die datenschutzrechtlichen und technischen sowie organisatorischen Anforderungen, die zu beachtenden Sicherheitsaspekte und die Architektur der Virtuellen Poststelle. Der Landesbeauftragte hat die Handreichung auf seiner Homepage eingestellt.

8. Finanzwesen

8.1 Neuheiten in der Abgabenordnung

Im Berichtszeitraum wurde die AO (Abgabenordnung) vielfach geändert. Nicht allen Änderungen kam unter dem Gesichtspunkt des Schutzes der personenbezogenen Daten der Bürgerinnen und Bürger Bedeutung zu. Allerdings haben die datenschutzrechtlich relevanten Änderungen erhebliche Auswirkungen auf die Rechte der Bürgerinnen und Bürger.

8.1.1 Nummerierung

Durch das Zweite Gesetz zur Änderung steuerlicher Vorschriften (Steueränderungsgesetz 2003) vom 15. Dezember 2003 (BGBl. I, S. 2645) wurde in die AO das sogenannte Identifikationsmerkmal in den §§ 139a ff eingeführt. Dahinter verbirgt sich für natürliche Personen eine **Identifikationsnummer**, die der eindeutigen Identifizierung in Besteuerungsverfahren durch ein einheitliches und dauerhaftes Merkmal dient.

Neben den Finanzbehörden dürfen auch andere öffentliche und nichtöffentliche Stellen diese Identifikationsnummer erheben und verwenden, soweit dies für Datenübermittlungen zwischen ihnen und den Finanzbehörden erforderlich ist. In der Konsequenz bedeutet dies für den Bürger, dass z.B. auch der Arbeitgeber diese Nummer erheben und verwenden darf, wenn er die Angaben zu den Einkommen seiner Beschäftigten an die Finanzbehörden übermittelt.
Um eine eindeutige Zuordnung von Steuerpflichtigen zu Identifikationsnummern oder Finanzämtern zu ermöglichen, speichert das Bundesamt für Finanzen folgende Daten zu natürlichen Personen:

Identifikationsnummer,	Ordensnamen/Künstlernamen,
Wirtschafts-Identifikationsnummer,	Tag und Ort der Geburt,
Familienname,	Geschlecht,
frühere Namen,	gegenwärtige oder letzte bekannte Anschrift,
Vornamen,	zuständige Finanzämter,
Doktorgrad,	Sterbetag.

Die erforderlichen Angaben für die erstmalige Zuteilung einer Identifikationsnummer stellen - soweit als möglich - die Meldebehörden zur Verfügung. Sie übermitteln auch jede ihnen bekannt werdende Änderung.

8.1.2 Kontodatenabruf

Eine weitere einschneidende Änderung in der AO erfolgte durch das Gesetz zur Förderung der Steuerehrlichkeit vom 23. Dezember 2003 (BGBl. I, S. 2928). Die Änderung ermächtigt die Finanzbehörden ab 1. April 2005 über das Bundesamt für Finanzen zum **Abruf einzelner Kontodaten bei den Kreditinstituten.** Konkret ist der Abruf nach § 93 Abs. 7 AO durch die Finanzbehörden - in Sachsen-Anhalt die Finanzäm-

ter, die Oberfinanzdirektion und das Ministerium der Finanzen - bei den Kreditinstituten über das Bundesamt für Finanzen zulässig, wenn er zur Festsetzung oder Erhebung von Steuern erforderlich ist und ein Auskunftsersuchen an den Steuerpflichtigen nicht zum Ziele geführt hat oder keinen Erfolg verspricht. Neben den Finanzbehörden sind über den § 93 Abs. 8 AO jedoch noch eine Vielzahl anderer Behörden und Gerichte zum Einholen von Kontoinformationen berechtigt. Nach dieser Vorschrift sollen die Finanzbehörden auf Ersuchen von Behörden und Gerichten, die für die Anwendung von Gesetzen zuständig sind, in denen an Begriffe des Einkommensteuergesetzes angeknüpft wird, über das Bundesamt für Finanzen einzelne Daten abrufen und der ersuchenden Behörde bzw. dem ersuchenden Gericht mitteilen. In dem Ersuchen ist zu versichern, dass eigene Ermittlungen nicht zum Ziele geführt haben oder keinen Erfolg versprechen.

Nach § 93b Abs. 1 AO haben die Kreditinstitute die nach § 24c Abs. 1 des Kreditwesengesetzes zu führende Datei auch für die Abrufe nach § 93 Abs. 7 und 8 AO vorzuhalten. In dieser Datei, die an sich zunächst nur der Bekämpfung der Geldwäsche im Rahmen der Terrorismusabwehr diente, werden die sogenannten Kontostammdaten der Bankkunden und sonstigen Verfügungsberechtigten, wie z.B. Name, Geburtsdatum, Kontonummern und Depots, vorgehalten. Kontenstände und -bewegungen werden in dieser Datei nicht gespeichert und können demnach auf diese Weise durch die Finanzbehörden nicht abgerufen werden. Wenn also ein Finanzamt eine Abfrage zu einem Bürger veranlasst hat, wird es danach wissen, wie viele Konten und Depots der Betroffene hat, unter welchen Kontonummern und seit wann diese geführt werden. Mit diesen Informationen wird das Finanzamt dann an die Bürgerin oder den Bürger herantreten, die/der von der heimlichen Abfrage bislang nichts weiß.

Praktisch sind Abrufe von Kontoinformationen bei den Kreditinstituten nur durch das Bundesamt für Finanzen vorzunehmen. Das Bundesamt wird wiederum nur auf Anforderung durch die Finanzbehörden tätig. Die Finanzbehörden können Abrufe zu eigenen Zwecken - Steuerfestsetzung - und auf Ersuchen anderer Behörden und Gerichte vornehmen lassen. Das Finanzamt kann sich z.B. im Rahmen der Festsetzung der Einkommensteuer eines Bürgers an das Bundesamt für Finanzen wenden und alle Kontostammdaten zu diesem Bürger erfragen. Das Sozialamt oder auch ein Sozialgericht kann sich zur Feststellung von Kontoinformationen nicht direkt an das Bundesamt für Finanzen wenden. Diese Behörden bzw. Gerichte wenden sich an die Finanzbehörden. Die Abfrage beim Bundesamt für Finanzen erfolgt dann durch die Finanzbehörden. Die so abgerufenen Kontoinformationen werden den Behörden und Gerichten über die Finanzbehörden mitgeteilt. Die Finanzbehörden erlangen somit auch Kenntnis von Kontoinformationen von Bürgerinnen und Bürgern, zu denen sie selbst keine Abfragen veranlasst haben.

Wegen der Regelungen zum Kontodatenabruf als Teil der „Förderung der Steuerehrlichkeit“ hatten ein Kreditinstitut und drei Einzelpersonen beim Bundesverfassungsgericht Verfassungsbeschwerde erhoben und den Er-

lass einer einstweiligen Anordnung gegen das Inkrafttreten des Gesetzes beantragt. Am 22. März 2005 hat das Bundesverfassungsgericht den Erlass einer einstweiligen Anordnung abgelehnt (Az. 1 BvR 2357/04, 1 BvQ 2/05; NJW 2005, 1179). Damit können die Regelungen der AO ab dem 1. April 2005 zunächst umgesetzt werden. Zunächst deshalb, weil eine abschließende Entscheidung über die offene Verfassungsbeschwerde noch aussteht. Das Gericht hat eine Abwägung zwischen dem Interesse an der Gleichmäßigkeit der Erhebung von Steuern und Sozialversicherungsbeiträgen sowie der Verhinderung des unberechtigten Bezugs von Sozialleistungen und dem Interesse der Betroffenen, die Gewinnung von personenbezogenen Informationen ohne eigene Mitwirkung zu vermeiden, vorgenommen. Der Nachteil für den Betroffenen aus dem Abrufverfahren bestehe nicht darin, dass den Finanzbehörden auf diese Weise einzelne der für die Besteuerung maßgebenden tatsächlichen Umstände bekannt werden könnten und die Steuer dementsprechend nach den gesetzlichen Vorgaben festgesetzt werden könne. Der Nachteil liege in der Kenntnis personenbezogener Daten über das Bestehen von Konten und Depots, die zur weiteren Ermittlung von steuererheblichen Tatsachen genutzt werden können. Der Steuerpflichtige sei zwar ohnehin zur Offenlegung der steuererheblichen Tatsachen verpflichtet, grundsätzlich aber nicht zur Angabe von Konten. Daran ändere die Neuregelung nichts, erlaube aber die Erkenntniserlangung ohne Mitwirkung des Steuerpflichtigen, was sein Recht auf informationelle Selbstbestimmung berühre. Bei der Abwägung hat das Gericht maßgeblich berücksichtigt, dass durch einen Anwendungserlass des Bundesministeriums der Finanzen vom 10. März 2005 Schutzvorkehrungen konkretisiert und damit die möglichen Belastungen der Betroffenen durch die neuen Ermittlungsbefugnisse abgeschwächt wurden. Nur dadurch war die Praxis des Kontodatenabrufs einstweilen „gerettet“.

8.1.3 Ausblick

Beide Änderungen der AO führen zu einer weitgehenden Einschränkung des Grundrechtsschutzes in Steuerfragen. Der viel verwendete Begriff des „gläsernen Bankkunden“ trifft die Stellung der Bürgerinnen und Bürger nach derzeitiger Rechtslage nicht wirklich im Kern. Allerdings ist es unverkennbar, dass die Entwicklung in der Gesetzgebung dahin geht, die Bürgerinnen und Bürger für den Staat immer „durchsichtiger“ werden zu lassen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich mit einer Entschließung **(Anlage 25)** gegen die Änderungen der AO zum Kontodatenabruf gewandt. Es scheint jedoch, dass die Interessen des Staates an einer möglichst unkomplizierten und effektiven Steuererhebung immer öfter das Grundrecht der Bürger auf informationelle Selbstbestimmung verdrängen. Verwaltungsökonomische Aspekte tragen aber eine Grundrechtseinschränkung nicht. Der Landesbeauftragte erwartet, dass sich auch die Landesregierung im Rahmen ihrer Möglichkeiten dafür einsetzt, dass die Rechte der Bürgerinnen und Bürger bei der Steuergesetzgebung nicht immer weiter eingeschränkt werden.

Der Bundesbeauftragte für den Datenschutz, der in Fragen der Bundesgesetzgebung zuständig ist, hat seine Bedenken gegen die Änderungen vorgebracht und wird dabei von den Landesbeauftragten unterstützt. Nicht zuletzt durch die Interventionen des Bundesbeauftragten und der Landesbeauftragten konnten - zunächst durch einen Anwendungserlass - die Folgen der Neuregelungen zum Kontodatenabruf abgeschwächt werden. Der Kontodatenabruf und auch dessen Verfahrensabläufe, einschließlich der Unterrichtung des Kontoinhabers, bedürfen aber einer präzisen gesetzlichen Regelung. Allerdings bleibt der Umstand unverändert, dass das Kontenüberwachungssystem nur auf inländische Konten zugreift; nicht angemeldete Erträge liegen aber vermutlich weiter eher auf Auslandskonten.

8.2 Die elektronische Signatur in der Finanzverwaltung - ELSTER sollte den Durchbruch bringen

Bereits im Frühjahr 2003 haben sich die Datenschutzbeauftragten des Bundes und der Länder auf ihrer 65. Konferenz mit der Frage der elektronischen Signatur im Finanzbereich auseinandergesetzt und begrüßt, dass mit dem Signaturgesetz und der Anpassung von mehr als 3.000 Rechtsvorschriften in Deutschland die rechtlichen Voraussetzungen geschaffen wurden, um die „**qualifizierte elektronische Signatur**“ der eigenhändigen Unterschrift gleichzustellen. Die administrativen und technischen Voraussetzungen sind inzwischen weitgehend vorhanden. Mehr als zwanzig freiwillig akkreditierte Zertifizierungsdienstanbieter nach dem Signaturgesetz sind von der Regulierungsbehörde für Telekommunikation und Post (RegTP) zugelassen. Sowohl Chipkarten, die für die qualifizierte elektronische Signatur zugelassen sind, als auch die dafür erforderlichen Lesegeräte sind verfügbar.

Für die elektronische Kommunikation zwischen der Finanzverwaltung und den Bürgerinnen und Bürgern ist die „qualifizierte elektronische Signatur“ gesetzlich generell vorgeschrieben. Die Nutzung einer fortgeschrittenen, der sogenannten „qualifizierten elektronischen Signatur mit Einschränkungen“ lehnten die Datenschutzbeauftragten bereits damals ab. Die „qualifizierte elektronische Signatur mit Einschränkungen“ bietet im Gegensatz zur „qualifizierten elektronischen Signatur“ und der „qualifizierten elektronischen Signatur mit Anbieterakkreditierung“ keine umfassend nachgewiesene Sicherheit, vor allem aber keine langfristige Überprüfbarkeit. Die mit ihr unterzeichneten elektronischen Dokumente sind unerkannt manipulierbar. Die „qualifizierte elektronische Signatur mit Einschränkungen“ hat geringeren Beweiswert als die eigenhändige Unterschrift.

Ein breites Anwendungsgebiet für die elektronische Signatur im Finanzbereich bietet die **elektronische Steuererklärung - ELSTER**. Seit dem 1. Januar 2005 dürfen die Steueranmeldungen der Arbeitgeber nach dem Einkommensteuergesetz und der Unternehmen nach dem Umsatzsteuergesetz nach einem amtlich vorgeschriebenen Vordruck nur noch auf elektronischem Wege an das Finanzamt übermittelt werden. Dazu wurde seitens der Finanzverwaltung die kostenlose Software „Elektronische Steuererklärung - ELSTER“ zur Verfügung gestellt. Im Falle der Abgabe einer

Steuererklärung auf elektronischem Wege muss natürlich sichergestellt werden, dass der Absender als eine bestimmte zur Abgabe berechtigte Person identifiziert werden kann. Zu dieser sogenannten Authentifizierung des Steuerbürgers ist nach der AO der Einsatz einer qualifizierten elektronischen Signatur vorgesehen. Eine qualifizierte elektronische Signatur ist jedoch technisch gesehen nicht der einzige Weg zu einer Authentifizierung des Steuerbürgers.

Die Finanzverwaltung hat sich nun - auch entgegen den Empfehlungen der Datenschützer - entschlossen, innerhalb von ELSTER ein eigenes Authentifizierungsverfahren zur Verfügung zu stellen, welches auf eine qualifizierte elektronische Signatur verzichtet. Dieses Authentifizierungsverfahren soll im ersten Quartal 2005 im Rahmen eines Pilotversuches in mehreren Bundesländern eingesetzt werden. Eine bundesweite Nutzung ist ab dem Jahr 2006 vorgesehen.

Diese Entscheidung der Finanzverwaltung wirft verschiedene Fragen auf. Zu aller erst stellt sich die Frage nach der rechtlichen Zulässigkeit dieser Abweichung von der AO. Hierzu ist festzustellen, dass nach der Steuerdatenübermittlungsverordnung für die Finanzverwaltung die Möglichkeit besteht, unter definierten Voraussetzungen auf eine qualifizierte elektronische Signatur zu verzichten.

Neben diesen grundsätzlichen Erwägungen stellt sich die Frage, welche Sicherheit der Steuerbürger vor Manipulationen in der Übergangszeit bis zur bundesweiten Einführung des Authentifizierungsverfahrens zum 1. Januar 2006 hat. Auf eine Anfrage des Bundesbeauftragten für den Datenschutz teilte das Bundesministerium der Finanzen mit, dass zur Vermeidung unberechtigter Erstattungen Sicherheitsmaßnahmen getroffen wurden. So würden Plausibilitätskontrollen vorgenommen und ein Risiko-Management eingeführt. Wie diese Sicherheitsmaßnahme im Einzelnen ausgestaltet sind, wurde nicht deutlich.

Die Datenschutzbeauftragten halten auch vor diesem Hintergrund an ihren Empfehlungen an die Bundesregierung anlässlich ihrer 65. Konferenz **(Anlage 6)** fest,

- dass die Finanzbehörden Steuerbescheide und sonstige Dokumente ausschließlich qualifiziert signiert versenden,
- den Bürgerinnen und Bürgern eine sichere, zuverlässige, leicht einsetzbare und transparente Technologie zur Verfügung zu stellen,
- unterschiedliche Ausstattungen für abgestufte Qualitäten und Anwendungsverfahren zu vermeiden,
- die Anschaffung von Signaturerstellungseinheiten mit zugehörigen Zertifikaten und ggf. Signaturanwendungskomponenten für „qualifizierte elektronische Signaturen mit Anbieterakkreditierung“ staatlich zu fördern,
- die vorhandenen Angebote der deutschen und sonstigen europäischen Anbieter vornehmlich heranzuziehen, um die qualifizierte elektronische Signatur und den Einsatz entsprechender Produkte zu fördern,

- e-Government- und e-Commerce-Projekte zu fördern, die qualifizierte elektronische Signaturen unterhalb der Wurzelzertifizierungsinstanz der RegTP einsetzen und somit Multifunktionalität und Interoperabilität gewährleisten,
- die Entwicklung von technischen Standards für die umfassende Einbindung der qualifizierten elektronischen Signatur zu fördern,
- die Weiterentwicklung der entsprechenden Chipkartentechnik voranzutreiben.

8.3 Auskunftsersuchen der Finanzämter - „Wie hoch ist Ihre Rente?“

Durch die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen erhielt der Landesbeauftragte den Hinweis, dass eine dortige Finanzbehörde einen Contergan-Geschädigten aufgefordert hatte, die Höhe der Rentenleistungen aufgrund seiner Conterganschädigung mitzuteilen.

Diese Mitteilung nahm der Landesbeauftragte zum Anlass, um beim Ministerium der Finanzen anzufragen, ob derartige Fälle in Sachsen-Anhalt bereits aufgetreten sind. Das Ministerium teilte daraufhin mit, dass es in Sachsen-Anhalt bisher keine entsprechenden Fälle gegeben habe. Jedoch habe man keinerlei rechtliche Bedenken gegen das Vorgehen der nordrhein-westfälischen Finanzbehörde.

Der Landesbeauftragte teilt die Auffassung des Ministerium der Finanzen nicht. Hintergrund der Bedenken des Landesbeauftragten ist der Umstand, dass die Finanzbehörden aus dem Betrag der Rentenleistung Rückschlüsse auf den Grad der Beeinträchtigung ziehen könnten. Der Grad der Beeinträchtigung ist jedoch eine sensible, besonders geschützte personenbezogene Angabe, deren Preisgabe hier nicht notwendig ist.

Das den Finanzbehörden nach § 88 AO eingeräumte Ermessen hinsichtlich der Art und des Umfangs der Ermittlungen wird durch gesetzliche Schranken, insbesondere die Verfassungsgrundsätze und auch die allgemeinen datenschutzrechtlichen Bestimmungen begrenzt. Zu den Verfassungsgrundsätzen gehört der Grundsatz der Verhältnismäßigkeit und, konkretisiert in den allgemeinen datenschutzrechtlichen Bestimmungen, der Grundsatz der Datensparsamkeit nach § 1 Abs. 2 DSG-LSA.

Nach dem Grundsatz der Verhältnismäßigkeit müssen Maßnahmen von Behörden u.a. erforderlich sein. Diese Erforderlichkeit wäre jedenfalls bei einer Anfrage an alle Rentenempfänger nicht gegeben. Es ist hier nach den jeweiligen Umständen des Einzelfalls zu differenzieren. Aus Sicht des Landesbeauftragten kann durch ein abgestuftes System - ausgerichtet an der Unerlässlichkeit der Angaben - die Anzahl der Anfragen an die Betroffenen auf das unbedingt notwendige Maß reduziert werden.

Der Grundsatz der Datensparsamkeit verpflichtet öffentliche Stellen dazu, die Erhebung, Verarbeitung und Nutzung personenbezogener Daten an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu

erheben, zu verarbeiten und zu nutzen. Auch im Hinblick darauf haben Finanzbehörden den Umfang der durch sie erhobenen personenbezogenen Daten auf das zwingend notwendige Maß zu begrenzen.

8.4 Prüfung der Finanzämter - Keine Vorratshaltung in den Akten!

Im Rahmen der Prüfung eines Finanzamtes wurde festgestellt, dass Belege, die die Steuerpflichtigen vorgelegt hatten, nicht an diese zurückgesandt worden waren. In den geprüften Akten fanden sich diverse Originalbelege.

Das **Zurückbehalten von Belegen** kann jedoch einen Verstoß gegen das verfassungsrechtlich begründete Verbot der Vorratsdatenhaltung darstellen, soweit die Notwendigkeit des weiteren Verbleibs der Unterlagen beim Finanzamt nicht bestand. Zurückbehaltene Belege sind als sogenannte Dauerbelege zu kennzeichnen.

Schlüssige Begründungen für ein Zurückbehalten von z.B. Belegen über Kapitalerträge sind in der Regel nicht gegeben, da diese nur für ein Kalenderjahr von Bedeutung sind. Für derartige Belege ist es ausreichend, wenn das Finanzamt in der Steuererklärung den Hinweis „Beleg hat vorgelegen“ anbringt und die eingereichten Bescheinigungen dem Steuerpflichtigen rückübersendet.

Eine entsprechende Empfehlung wurde dem betreffenden Finanzamt gegenüber ausgesprochen.

8.5 Verwechslung bei der Kontopfändung

Aufgrund von Presseberichten erfuhr der Landesbeauftragte, dass einem Bürger auf Veranlassung einer staatlichen Kasse das Konto gepfändet wurde, obwohl der Kontoinhaber nicht säumig war.

Nach dem zugrunde liegenden Sachverhalt war die Vollstreckung einer offenen Forderung gegen einen Schuldner fruchtlos verlaufen. Daraufhin ermittelte die Kasse in ihrer Datenbank eine Person mit dem Vor- und Zunamen des Schuldners und veranlasste eine Pfändung des Kontos. Dazu übersandte die Kasse die erforderlichen Unterlagen unter Angabe des Wohnortes an die für den Wohnort des Schuldners zuständige Sparkasse.

Bei dieser Sparkasse unterhielt der Betroffene aber kein Konto. Diesen Umstand meldete die Sparkasse nicht an die staatliche Kasse. Die Sparkasse suchte nun ihrerseits in ihrer Datenbank einen Kontoinhaber gleichen Namens und fand tatsächlich einen solchen. Ohne dass die Sparkasse die mitgemeldete Postanschrift abglich, führte sie die Pfändung des Kontos durch. Erst nachdem sich der Betroffene meldete, fiel der Sparkasse auf, dass es sich bei dem Inhaber des gepfändeten Kontos nicht um die richtige Person handelte. Die Namen stimmten zwar überein, für die Anschriften traf dies allerdings nicht zu. Nach Aufklärung des Sachverhal-

tes überwies die staatliche Kasse dem Betroffenen das gepfändete Geld umgehend zurück.
Verstöße gegen datenschutzrechtliche Grundsätze und Bestimmungen haben vorliegend beide Einrichtungen begangen. Die betroffene Sparkasse unterfällt jedoch nicht der Kontrolle durch den Landesbeauftragten. Die staatliche Kasse wurde vom Landesbeauftragten jedoch darauf hingewiesen, dass personenbezogene Daten an Dritte - wie hier ein öffentlich-rechtliches Kreditinstitut - nur übermittelt werden dürfen, wenn die Zulässigkeit der Übermittlung ausreichend geprüft wurde. Eine Übermittlung ist nur zulässig, wenn die personenbezogenen Daten zur Aufgabenerfüllung erforderlich sind. Eine Erforderlichkeit besteht aber nur dann, wenn sichergestellt ist, dass der Betroffene einer Maßnahme zumindest als Person eindeutig identifiziert ist und die Maßnahme nicht ins Leere geht.

Insbesondere bei Pfändungen ist auf die Verlässlichkeit der Informationen zu den angegebenen personenbezogenen Daten besonders zu achten. Es reicht nicht aus, eine Namensgleichheit im Kassenprogramm festzustellen und dann, ohne einen Abgleich - zumindest der Anschriften - vorzunehmen, eine Pfändungs- und Überweisungsverfügung an das vermeintlich zuständige Kreditinstitut zu senden. In Zeiten von Online-Banking und automatisiertem Bankverkehr ist der Rückschluss aus dem Wohnort des Betroffenen auf das kontoführende Institut nicht mehr zu rechtfertigen.

8.6 Hundebestandsaufnahme „Ein Hund oder kein Hund?“

Aufgrund der Eingabe eines Betroffenen erhielt der Landesbeauftragte davon Kenntnis, dass in einer Gemeinde eine Hundebestandsaufnahme durchgeführt wurde. Zur Erfassung aller Hunde auf dem Gebiet der Gemeinde wurden die Grundstückseigentümer schriftlich aufgefordert, einen sogenannten Aufnahmebogen auszufüllen und zurückzusenden. Für den Fall der Verweigerung wurde bereits im Anschreiben darauf hingewiesen, dass dies eine Ordnungswidrigkeit darstelle und die Einleitung eines Ordnungswidrigkeitenverfahrens in Aussicht gestellt. Auf dem Aufnahmebogen sollten Angaben zu Namen, Vornamen und Wohnungsnummer des Hundehalters sowie Rasse, Geschlecht, Alter und Steuernummer des Hundes gemacht werden. Die Erhebung stützte die Gemeinde auf ihre Hundesteuersatzung.

Die Rechtslage in Sachsen-Anhalt stellt sich nach wie vor so dar, dass eine Hundebestandsaufnahme unter Verpflichtung aller Grundstückseigentümer zur Auskunftserteilung einer rechtlichen Grundlage entbehrt. Auf diese Rechtslage hat der Landesbeauftragte bereits in seinem IV. Tätigkeitsbericht (Ziff. 9.2) hingewiesen und 1998 eine entsprechende Stellungnahme in den KNSA-Nachrichten des Städte- und Gemeindebundes veröffentlichen lassen.

Zur Klarstellung soll auf die bestehende Rechtslage an dieser Stelle noch einmal hingewiesen werden. Nach § 4 Abs. 1 DSG-LSA sind die Erhebung und Verarbeitung personenbezogener Daten sowie deren Nutzung nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt

oder anordnet oder soweit der Betroffene eingewilligt hat. Rechtsvorschrift im Sinne dieser Regelung sind materielle Rechtsnormen im weitesten Sinn, allerdings keine Verwaltungsvorschriften. Rechtsnormen sind auch kommunale Satzungen. Kommunale Satzungen bedürfen allerdings einer ausdrücklichen gesetzlichen Ermächtigung.

Der Landesgesetzgeber hat aber bisher keine entsprechende gesetzliche Regelung getroffen. Keine Landesvorschrift berechtigt Kommunen, mit Hundesteuersatzungen in die Grundrechte der Bürger einzugreifen. Eine nur allgemeine Regelung, nach der Kommunen Satzungen überhaupt erlassen dürfen, findet sich in § 6 GO LSA. Diese Regelung kann wegen ihres allgemeinen Charakters keine wirksame Einschränkung des verfassungsrechtlich gesicherten Rechts auf den Schutz personenbezogener Daten bewirken. Eine Hundesteuersatzung also, die sich allein auf § 6 GO LSA stützt, kann nicht wirksam in die grundrechtlich geschützte Freiheitssphäre des Bürgers eingreifen. Die Erhebung in der Gemeinde war unzulässig. Die Gemeinde wurde vom Landesbeauftragten auf die Rechtslage hingewiesen.

Der Vollständigkeit halber sei noch darauf hingewiesen, dass auch die Regelungen des § 93 der AO i.V.m. § 13 KAG-LSA keine entsprechende Grundlage bilden. Hierzu sei auf die Ausführungen unter Ziff. 9.2 des IV. Tätigkeitsberichtes verwiesen.

9. Forschung

9.1 Allgemeines

Die im VI. Tätigkeitsbericht (Ziff. 9) dargestellte gute Zusammenarbeit mit Forschungseinrichtungen wurde auch in diesem Berichtszeitraum fortgesetzt.
Im Berichtszeitraum wurde der Landesbeauftragte bei 19 neuen Forschungsprojekten datenschutzrechtlich beteiligt. Es kam wiederum nur zu wenigen datenschutzrechtlichen Hinweisen, die in den Konzepten ihre Berücksichtigung fanden.
Des Weiteren hat der Landesbeauftragte auch bereits laufende Forschungsvorhaben datenschutzrechtlich begleitet (z.B. bei der Überarbeitung und Aktualisierung von Datenerfassungsbögen).
Ein sich im Einzelnen als problematisch darstellendes Projekt ist unter Ziff. 13 näher beschrieben.

9.2 Forschungsgeheimnis für medizinische Daten

In vielen Bereichen der wissenschaftlichen Forschung werden sensible medizinische Daten verarbeitet, häufig auch mit Personenbezug. Um die entsprechenden Daten zu erlangen, bedürfen die Forscher in der Regel der Einwilligung der Betroffenen in die Übermittlung durch ihren Arzt. Ausnahmsweise greifen spezielle Regelungen (wie § 27 DSG-LSA) für personenbezogene Daten ein, die bereits für Zwecke der wissenschaftlichen Forschung erhoben worden sind. Mit der Übermittlung der Daten vom Arzt

an den Forscher verlieren die Daten aber regelmäßig den strafrechtlichen Schutz vor Offenbarung und den Beschlagnahmeschutz im Strafverfahren. Auch haben die Forscher bezüglich der Daten kein Zeugnisverweigerungsrecht. Im Interesse der Forschung, insbesondere aber zum Schutz der durch die Datenübermittlung und -verarbeitung Betroffenen, haben sich die Datenschutzbeauftragten des Bundes und der Länder dafür ausgesprochen, dass die bei den übermittelnden Stellen geschützten personenbezogenen medizinischen Daten auch nach ihrer Übermittlung zu Forschungszwecken den gleichen Schutz genießen sollten. Die diesbezügliche Entschließung der Datenschutzbeauftragten des Bundes und der Länder zur Einführung eines Forschungsgeheimnisses für medizinische Daten **(Anlage 16)** wurde der Bundesministerin der Justiz durch den Bundesbeauftragten für den Datenschutz zugeleitet. Im Bundesministerium wird der Handlungsbedarf geprüft.

10. Gesundheitswesen

10.1 Gesundheitsmodernisierungsgesetz

Die gesetzliche Krankenversicherung soll eine umfassende medizinische Versorgung gewährleisten. Mit dem Ziel, dies auch in Zukunft sicherzustellen, wurde das Gesundheitsmodernisierungsgesetz geschaffen, das am 1. Januar 2004 in Kraft trat (BGBl. I 2003, 2190). Neben der Neuordnung der Finanzierung wurde vor allem eine strukturelle Reform der gesetzlichen Krankenversicherung durchgeführt. Von besonderer Bedeutung für die Daten der Versicherten war unter anderem eine Änderung des Vergütungssystems. Dies wurde unter anderem als Begründung dafür herangezogen, auch das Verfahren der Abrechnungsprüfung zu ändern. Nunmehr erhalten die Krankenkassen im Rahmen der Abrechnung ärztlicher Leistungen Daten nicht mehr nur fallbezogen, sondern versichertenbezogen (§ 295 Abs. 2 SGB V). Die Abrechnungsprüfung durch die Krankenkassen erfolgt nach § 106a Abs. 3 SGB V.

Durch diese Neuregelungen können die Krankenkassen umfassende und intime Kenntnisse über ihre Versicherten erhalten. Die Gefahr gläserner Patientinnen und Patienten rückt damit näher. Demgemäß ist eine strenge Zweckbindung dieser Daten erforderlich. Den Krankenkassen soll es versagt bleiben, die erlangten medizinischen Daten über die gebotenen Prüfungen hinaus unter verschiedensten Gesichtspunkten auszuwerten (z.B. mit data-warehouse-Systemen). Hierzu haben die Datenschutzbeauftragten des Bundes und der Länder im September 2003 eine Entschließung zum Gesundheitsmodernisierungsgesetz gefasst **(Anlage 12).** Bereits im März 2003 hatten die Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung zu datenschutzrechtlichen Rahmenbedingungen zur Modernisierung des Systems der gesetzlichen Krankenversicherung **(Anlage 3)** nachdrücklich die Wahrung der Selbstbestimmungsrechte der Versicherten eingefordert.

10.2 Elektronische Gesundheitskarte

Die **elektronische Gesundheitskarte** soll zum 1. Januar 2006 die bisherige Krankenversichertenkarte ablösen.
In einem verpflichtenden administrativen Teil mit Lichtbild und Angaben zum Zuzahlungsstatus werden auch dieselben Informationen der bisherigen Krankenversichertenkarte enthalten sein. Darüber hinaus soll dieser Teil der Gesundheitskarte die Grundlagen für das elektronische Rezept einschließen.

Außerdem wird den Patienten in einem medizinischen Teil der Gesundheitskarte die Möglichkeit angeboten, medizinische Notfallversorgungsdaten, elektronische Arztbriefe, Arzneimitteldokumentationen, die elektronische Patientenakte und weitere Daten des Versicherten zu speichern.
Dies bedeutet, dass zwar alle Versicherten eine Gesundheitskarte erhalten, mit der administrative Funktionen, wie die Abwicklung des elektronischen Rezeptes, erledigt werden, darüber hinaus ist es ihnen allerdings freigestellt, die zusätzlichen Funktionen zu nutzen. Der Versicherte soll somit eigenständig festlegen, welche Anwendungen wie zugelassen werden und welche Daten über die Karte gespeichert werden. Außerdem soll der Versicherte bei der tatsächlichen Nutzung der Karte entscheiden, welche Daten konkret erfasst und ob und wem gegenüber gespeicherte Daten zur Einsicht freigegeben werden sollen.
Da sehr sensible Gesundheitsdaten betroffen und das Patientengeheimnis und die Verfügungsbefugnis des Versicherten zu wahren sind, begleiten auch die Datenschutzbeauftragten des Bundes und der Länder intensiv die Einführung der Gesundheitskarte. Sie haben eine entsprechende Entschließung gefasst **(Anlage 27).**

10.3 Datenübermittlung bei amtsärztlichen Untersuchungen

Ein Amtsarzt wandte sich mit Fragen zu amtsärztlichen Gutachten an den Landesbeauftragten. In diesem Fall wurde der Amtsarzt vom zukünftigen Dienstherrn einer Person beauftragt, diese amtsärztlich zu untersuchen und eine entsprechende Stellungnahme abzugeben. Der Untersuchte war mit dem Inhalt dieser Stellungnahme einverstanden und unterschrieb eine diesbezügliche Schweigepflichtbefreiung. Eine darüber hinaus gehende Übermittlung von Angaben an den Dienstherrn lehnte der Untersuchte ab.

Obwohl bereits vor Vorliegen des amtsärztlichen Gesundheitszeugnisses eine Berufung in das Beamtenverhältnis auf Widerruf erfolgte, verlangte der Dienstherr nunmehr vom Amtsarzt die Übermittlung der Anamnese und weiterer einzelner Untersuchungsergebnisse, da § 24 Abs. 2 Satz 2 Gesundheitsdienstgesetz des Landes Sachsen-Anhalt dies auch ohne Schweigepflichtentbindung erlauben würde.
Der Landesbeauftragte hat darauf hingewiesen, dass im Regelfall nur das Ergebnis der Untersuchung an den Dienstherrn zu übermitteln ist. Die vom Dienstherrn angeführte Rechtsgrundlage erlaubt zwar tatsächlich auch eine davon abweichende Übermittlung der Anamnese und einzelner Unter-

suchungsergebnisse, diese ist allerdings nur dann zulässig, wenn deren Kenntnis zur Entscheidung über die konkrete Maßnahme, zu deren Zweck die Untersuchung durchgeführt wurde, erforderlich ist. Widerspricht der Untersuchte ausdrücklich der Übermittlung bestimmter Angaben aus der Untersuchung, kann dies nicht zwangsweise gegen ihn durchgesetzt werden. Bei Weigerung muss der Untersuchte dann allerdings die eventuellen Konsequenzen, wie Nichteinstellung und Unterstellung der Dienstunfähigkeit, tragen. Darüber hinaus war auch festzustellen, dass im geschilderten Fall die Kenntnis weiterer Informationen rechtlich nicht mehr erforderlich war, da die Verbeamtung bereits erfolgt war.

10.4 Aufbewahrung von Patientenunterlagen nach Praxisaufgabe

Grundsätzlich sind ärztliche Aufzeichnungen unter standesrechtlichen Gesichtspunkten zehn Jahre aufzubewahren, soweit nicht nach anderen gesetzlichen Vorschriften eine längere Aufbewahrungspflicht besteht. Nach Ablauf der Fristen müssen die Unterlagen ordnungsgemäß vernichtet werden. Dem Arzt obliegt die Pflicht nach Aufgabe der Praxis, seine ärztlichen Aufzeichnungen und Untersuchungsbefunde entsprechend den Aufbewahrungsfristen aufzubewahren oder dafür Sorge zu tragen, dass sie in gehörige Obhut gegeben werden. Im Rahmen der Obhutspflicht müssen die Aufzeichnungen und Untersuchungsbefunde unter Verschluss gehalten werden und dürfen nur mit Einwilligung des Patienten eingesehen oder weitergegeben werden.

Die Ärztekammer Sachsen-Anhalt vertritt die Auffassung, dass für Patientenunterlagen, die aus faktischen Gründen herrenlos sind, ein öffentliches Interesse an einer sicheren Aufbewahrung besteht. Der Landesbeauftragte begrüßt, dass die Ärztekammer auch aus datenschutzrechtlichen Gründen in ihrer berufsständischen Verantwortung für eine ordnungsgemäße Aufbewahrung der Patientenunterlagen eintritt. Dies kann jedoch nur dann zutreffen, soweit der primär Aufbewahrungspflichtige oder seine Erben selbst nicht in der Lage sind, für eine solche Aufbewahrung zu sorgen.

Die Ärztekammer Sachsen-Anhalt hat unter Berücksichtigung der datenschutzrechtlichen Hinweise des Landesbeauftragten die Rahmenbedingungen geschaffen, die ggf. die Aufbewahrung von Patientenunterlagen durch eine Privatfirma datenschutzkonform gestatten.

10.5 Laborleistungen bei arbeitsmedizinischen Gutachten

Eine Universitätsklinik war mit einem arbeitsmedizinischen Gutachten nach § 200 Abs. 2 SGB VII durch eine Berufsgenossenschaft beauftragt worden. Im danach folgenden Gerichtsverfahren gegen die Berufsgenossenschaft legte der Betroffene ein Gutachten mit Laborwerten vor, die von den Ergebnissen der Begutachtung durch die Universitätsklinik abwichen. Daraufhin wurde die Universitätsklinik erneut um eine Aktenbegutachtung, insbesondere zu den neuen Laborwerten, gebeten. Der Betroffene beklagte sich über den Umgang mit den ihn betreffenden Unterlagen in der Uni-

versitätsklinik. Insbesondere seien an dem Verfahren fachübergreifend Ärzte beteiligt worden, die er niemals gesehen habe.

Die Bedenken des Betroffenen basierten auf einer grundsätzlich richtigen Annahme. Nach der beruflichen Schweigepflicht des ärztlichen Standesrechts, die auch strafrechtlich bewehrt ist, ist der Arzt verpflichtet, über die ihm in dieser Eigenschaft anvertrauten oder bekannt gewordenen Informationen Verschwiegenheit zu bewahren (Patientengeheimnis). Dies gilt auch für die kollegiale Zusammenarbeit unter Ärzten. Nach § 9 Abs. 4 der Berufsordnung der Ärztekammer Sachsen-Anhalt sind Ärzte, die gleichzeitig oder nacheinander denselben Patienten untersuchen oder behandeln, lediglich insoweit von der Schweigepflicht befreit, als das Einverständnis des Patienten vorliegt oder anzunehmen ist. Die Annahme eines solchen Einverständnisses wäre beispielsweise berechtigt, wenn der Patient dies durch eigene schlüssige Handlungen zum Ausdruck bringt (Besuch beim Facharzt) oder entsprechend ausführlich und konkret informiert wird und dem Vorhaben nicht widerspricht. Bei der Übermittlung von Patienteninformationen an Laborärzte, die der Patient nicht kennt, kann dies nicht ohne weiteres angenommen werden. Zudem fehlt oft der Raum für eine mutmaßliche Einwilligung, weil der Patient hätte gefragt werden können.

Im vorliegenden Fall war das Vorgehen der Universitätsklinik jedoch vertretbar. Inhalt und Umfang des Begutachtungsauftrages durch die Berufsgenossenschaft machten von vorn herein deutlich, dass die Einbeziehung von Ärzten unterschiedlicher Fachgebiete erforderlich sein würde. Der Betroffene selbst hatte auch die Notwendigkeit insoweit mitbegründet, als er von Spezialisten zu bewertende Labordaten in das Verfahren einführte. Damit war es dem Betroffenen verwehrt, sich nachträglich darauf zu berufen, er sei mit der Einbeziehung von Laborärzten nicht einverstanden gewesen.

Dennoch hat der Landesbeauftragte gegenüber der Universitätsklinik angeregt, künftig auch bei krankenhausinternen Beteiligungen aus anderen Fachgebieten, soweit es sich nicht um mit- oder nachbehandelnde Ärzte handelt, Laborüberweisungen nur mit Hilfe von Nummerncodes vorzunehmen. Soweit Proben vom behandelnden Arzt zu Laboruntersuchungen übermittelt werden und die Laborwerte zurückgehen, erscheint die Identifikation des betroffenen Patienten nicht erforderlich. Dabei ist selbstverständlich nicht ausgeschlossen, die aus medizinischen Gründen notwendigen Informationen, beispielsweise über das Geschlecht, das Alter oder Körpermaße sowie Vorerkrankungen, mitzuteilen.

10.6 Mammographie-Screening

Die Richtlinien des Bundesausschusses der Ärzte und Krankenkassen über die Früherkennung von Krebserkrankungen vom 15. Dezember 2003 sehen die Einführung eines Mammographie-Screenings vor. Ziel ist die Senkung der Brustkrebssterblichkeit in der anspruchsberechtigten Bevölkerungsgruppe.

Die Umsetzung wird zur Zeit durch das zuständige Ministerium und die Beteiligten in der vertragsärztlichen Versorgung geprüft. Hierzu hat der Landesbeauftragte auf einige Punkte hingewiesen, die aus datenschutzrechtlicher Sicht noch einer Klärung bedürfen.

Ein Schwerpunkt der Betrachtung ist das Einladungswesen. Probleme ergeben sich dabei aus der Tatsache, dass das Screening letztlich wohl beabsichtigt, alle Frauen einer bestimmten Altersgruppe zur Untersuchung einzuladen, also ein bevölkerungsbezogenes Screening durchzuführen. Betroffen sind daher also auch Frauen, die nicht Mitglieder der gesetzlichen Krankenversicherung sind (Privatversicherte, Krankenhilfe).

Durchgeführt werden soll die Einladung durch eine zentrale Stelle als öffentliche Stelle im Sinne des § 18 Abs. 4 Melderechtsrahmengesetz (MRRG). Die Früherkennungs-Richtlinie sieht für das Einladungswesen eine regelmäßige Übermittlung von Meldedaten vor. § 18 MRRG gestattet regelmäßige Datenübermittlungen an öffentliche Stellen, soweit dies durch Bundes- oder Landesrecht unter besonderen Festlegungen bestimmt ist. Die Richtlinien gehen danach davon aus, dass die Schaffung auf der Grundlage landesrechtlicher Bestimmungen zu erfolgen hat.
Würde eine entsprechende öffentliche Stelle geschaffen, wäre weiterhin zu prüfen, ob die Datenübermittlung zu allen Frauen der genannten Altersgruppe zur Erfüllung der in der Zuständigkeit dieser zentralen Stelle liegenden Aufgaben erforderlich ist. Eine verbindliche Aufgabenzuweisung an die zentrale Stelle für nicht von der gesetzlichen Krankenversicherung erfasste Personen erscheint zur Zeit offen.

Zur Evaluation ist nach der Richtlinie die Bildung von individuellen Kontrollnummern durch die zentrale Stelle vorgesehen, die zu Abgleichzwecken an das Krebsregister übermittelt werden. Hierbei ist aber die Identifizierung der betroffenen Person insbesondere im Hinblick auf § 8 Abs. 1 Krebsregistergesetz zu vermeiden.

Zudem hat der Landesbeauftragte dem Ministerium Hinweise zur sogenannten informierten Einwilligung als Rechtsgrundlage für die Datenerhebung von den Teilnehmerinnen gegeben, insbesondere zur erforderlichen umfänglichen Aufklärung über das Projekt und die Datenflüsse.

11. Gewerbe und Wirtschaft, Land- und Forstwirtschaft

11.1 Abfallentsorgung bei Gewerbetreibenden

In der Abfallentsorgungssatzung eines Landkreises war für Gewerbetreibende ein Anschluss- und Benutzungszwang festgelegt worden. Dessen ungeachtet verabsäumte, so berichtete der Landkreis dem Landesbeauftragten, eine Vielzahl von Gewerbetreibenden aus den unterschiedlichsten Gründen, auch den für Abfallgebühren zuständigen Bereich Gebühreneinzug beim Landkreis von der Gewerbean- oder -abmeldung zu unterrichten. So komme es immer wieder vor, dass der Landkreis die in der Abfallgebührensatzung festgelegten Gebühren aus Unwissenheit nicht erhebe

oder beim Versuch der Vollstreckung festgestellt werden müsse, dass das Gewerbe bereits wieder abgemeldet worden sei.
Der Landkreis suchte nun nach einer Möglichkeit, regelmäßig von den Gewerbeämtern der Gemeinden oder von einer der in § 14 Abs. 5 GewO genannten Stellen außer den in § 14 Abs. 6 GewO genannten Daten Name, betriebliche Anschrift und angezeigtes Gewerbe auch das Datum der Anmeldung bzw. Abmeldung des Gewerbes zu erhalten. Hierfür einen Lösungsvorschlag zu unterbreiten, bat der Landkreis den Landesbeauftragten.

Dieser allerdings hatte zunächst zu konstatieren, dass die vom Gesetzgeber in § 14 Abs. 5 GewO genannte Aufzählung der öffentlichen Stellen, die regelmäßig von den für die Entgegennahme der Gewerbeanzeigen zuständigen Behörden Daten aus den Gewerbeanzeigen erhalten dürfen, abschließend ist. Die Abfallämter bzw. die für den Gebühreneinzug zuständigen Stellen der Landkreise zählen nicht zum Kreis der genannten Behörden.
Auch die Anwendung des § 14 Abs. 6 GewO wäre nicht zielführend. Zwar können danach öffentlichen Stellen Name, betriebliche Anschrift und angezeigte Tätigkeit des Gewerbetreibenden übermittelt werden. Dies gilt jedoch nur fallweise und keinesfalls regelmäßig; und es gilt nur dann, wenn die Daten zur Erfüllung der in der Zuständigkeit des Datenempfängers liegenden Aufgaben erforderlich sind.

Dabei darf der Begriff „erforderlich“ nicht gleichgesetzt werden mit „nützlich zur Aufgabenerfüllung“. Im Übrigen hat der Gesetzgeber die Übermittlung weiterer für die Aufgabenerfüllung erforderlicher Daten auf diesem Wege, nämlich Datum von Beginn bzw. Ende der Gewerbeausübung, in § 14 Abs. 6 Satz 2 GewO an das Vorliegen äußerst enger Voraussetzungen geknüpft, z.B., wenn die Daten zur Abwehr erheblicher Nachteile für das Gemeinwohl erforderlich sind. Dies dürfte im vorliegenden Fall wohl nicht zutreffen.

Der Landesbeauftragte konnte dem Landkreis allerdings anders helfen. Der Landkreis hat nämlich die Möglichkeit, seine Abfallgebührensatzung in seinem Sinne zu ändern. Er kann, so wie § 6 Abs. 1 des Abfallgesetzes des Landes Sachsen-Anhalt (AbfG LSA) es vorsieht, zu Gebührenschuldnern statt der Gewerbetreibenden die Eigentümer oder sonst dinglich Nutzungsberechtigten derjenigen Grundstücke bestimmen, die dem vom öffentlich-rechtlichen Entsorgungsträger angeordneten Anschluss- und Benutzungszwang unterliegen. Ob und wie die Grundstückseigentümer die Abfallgebühren auf ihre Mieter oder Pächter umlegen, wäre sekundär und für den Landkreis nicht von Belang.

11.2 Pilzsammler unter Videoüberwachung

Durch Pressemitteilungen und eine Kleine Anfrage eines Mitglieds des Landtages an die Landesregierung bzw. deren Beantwortung war der Landesbeauftragte auf ein "Modellprojekt Videoüberwachung von Wäldern

in Sachsen-Anhalt" aufmerksam geworden. Ziel des Projekts war das frühzeitige Erkennen von Bränden.
Da der Landesbeauftragte nicht ausschließen konnte, dass das System außer zur Feststellung von Bränden auch zur Beobachtung von Pilzsammlern, Spaziergängern oder gar die Einsamkeit suchenden Pärchen missbraucht werden könnte, kontrollierte er das zuständige Forstamt.
Schnell stellte sich heraus, dass das ganze Verfahren zur Waldbrandfrüherkennung durchaus datenschutzgerecht war.
Mit dem Ziel, zukünftig niemandem mehr die katastrophalen Arbeitsbedingungen auf den Feuerwachtürmen zuzumuten, war zunächst in einem Pilotversuch auf einem hohen Turm, also mindestens in Baumwipfelhöhe, in einem waldreichen und stark waldbrandgefährdeten Landkreis eine Kamera montiert worden. Die Bilder dieser Kamera werden per ISDN zu einem Forstamt übertragen. Dabei handelt es sich nicht um einen Videodatenstrom, sondern um Schwarz-Weiß-Fotografien. Die Kamera schwenkt automatisch, und zwar, vom im Forstamt Beschäftigten nicht beeinflussbar, innerhalb von ca. acht Minuten um einmal 360° horiz ontal im Kreis. Von jedem Sektor werden kurz hintereinander drei Fotos gemacht. Das erste Bild jeder Serie wird vom Kamerarechner zu einem Panoramabild montiert und zum Leitstand im Forstamt gesendet. Außerdem vergleicht der Kamerarechner die drei Folgebilder auf Veränderungen, z.B. eine sich bewegende Rauchwolke eines möglichen Brandherdes. Ein solcher Bereich wird automatisch farblich markiert. Der Beschäftigte im Forstamt kann den detektierten Bereich stark vergrößern und entscheiden, ob Alarm ausgelöst wird. Die Möglichkeit, die Kamera in einem solchen Fall anzuhalten oder gar vertikal zu schwenken, hat er nicht, damit würde außerdem die fein justierte Entfernungsmessung gestört werden.

Aufgrund des Umstandes, dass die Kamera Bilder mindestens aus Baumwipfelhöhe liefert, auf denen im oberen Drittel der Horizont abgebildet wird, könnten u.U. zwar Menschen oder Fahrzeuge auf freien Flächen gesehen, keinesfalls aber erkannt werden. Damit liegt keine Erhebung personenbezogener Daten vor. Dem weiteren Ausbau durch Aufstellen weiterer Kameras steht aus Sicht des Landesbeauftragten nichts entgegen, wenn die genannten Rahmenbedingungen eingehalten werden.

12. Hinweise zum technischen und organisatorischen Datenschutz

12.1 Defizite beim automatisierten Abrufverfahren

Im Zusammenhang mit der anlassbezogenen Kontrolle wegen eines unzulässigen Datenabrufs in einem Polizeirevier, welches über ein automatisiertes Abrufverfahren Zugriff auf das Melderegister einer Stadt hatte (vgl. Ziff. 17.4), waren bei der Stadt weitere Defizite bei der Umsetzung und Anwendung datenschutzrechtlicher Normen zu verzeichnen.
Diese Defizite bestanden bereits nach alter Rechtslage, denn gem. § 7 Abs. 4 DSG-LSA a.F. hätte die Stadt ihrer Unterrichtungspflicht über die Einführung eines automatisierten Abrufverfahrens nachkommen müssen. Dies war jedoch nicht der Fall. Die damalige Meldung zum Dateienregister

(§ 25 DSG-LSA a.F.) enthielt keine Information über die Einrichtung eines automatisierten Abrufverfahrens.
Eine Kontrolle der Protokollierung der Abrufe ergab, dass keine Differenzierung möglich war, um festzustellen, wer seitens der Polizei wann welche Abrufe getätigt hatte. Alle Mitarbeiter nutzten beim Abruf von Meldedaten den gleichen Benutzernamen und das gleiche Passwort. Damit lag auch ein schwerwiegender Verstoß gegen die Protokollierungspflicht vor.
Mit der Novellierung des DSG-LSA vom 21. August 2001 wurde unter Beachtung der Entwicklung in der Informationstechnik, insbesondere dem Ausbau lokaler Netze bei den Behörden sowie des Landesnetzes, der bisherige Gesetzesvorbehalt für die Einrichtung automatisierter Abrufverfahren in § 7 Abs. 1 DSG-LSA a.F. durch einen zweistufigen Kontrollmechanismus ersetzt.
Hierzu gehört als erste Stufe die **Vorabkontrolle** gem. § 14 Abs. 2 Nr. 1 DSG-LSA, bei der die datenschutzrechtliche Zulässigkeit des Verfahrens sowie die ausreichende Umsetzung der technischen und organisatorischen Maßnahmen durch die verantwortliche Stelle zu überprüfen sind. Diese Vorabkontrolle hat vor der Freigabe oder bei einer wesentlichen Änderung des Verfahrens zu erfolgen. Die beteiligten Stellen haben darüber hinaus zu gewährleisten, dass die Zulässigkeit des Abrufverfahrens kontrolliert werden kann. Dazu sind schriftliche Festlegungen gem. § 7 Abs. 2 Satz 2 DSG-LSA zu treffen.
Als zweite Stufe der Kontrolle ist die **Unterrichtung** des Landesbeauftragten **vor** der Einrichtung des Abrufverfahrens gem. § 7 Abs. 3 DSG-LSA unter Mitteilung der genannten Festlegungen durch die verantwortliche Stelle vorgesehen. Beides, sowohl die Vorabkontrolle als auch die vorherige Unterrichtung des Landesbeauftragten, hatte die Stadt als die verantwortliche Stelle versäumt, obwohl durch den Einsatz einer neuen Software im Meldeamt eine wesentliche Änderung des Verfahrens gegeben war.

Nach der Intervention durch den Landesbeauftragten wurden durch die Stadt umgehend die aufgezeigten datenschutzrechtlichen Mängel beseitigt und die erforderlichen Maßnahmen zur Vorabkontrolle und die Unterrichtung des Landesbeauftragten nachgeholt.
In Abstimmung mit dem beteiligten Polizeirevier, welches ebenfalls intern organisatorische Maßnahmen zur Verbesserung des Datenschutzes getroffen hatte, wurden die Zugriffsrechte überarbeitet und dafür Sorge getragen, dass nunmehr durch die Vergabe mehrerer Benutzernamen und Passwörter die **Revisionsfähigkeit** gem. § 6 Abs. 2 Nr. 5 DSG-LSA bei Datenabrufen durch die Polizei sichergestellt ist.
Der Empfehlung des Landesbeauftragten, als Benutzernamen Pseudonyme zu vergeben und im Polizeirevier eine Liste (für Kontrollzwecke) zu führen, aus der die Verbindung vom Benutzernamen zum jeweiligen Polizeibeamten hervorgeht, wurde gefolgt.
Für eine Festlegung und Überprüfung der Übermittlung personenbezogener Daten gem. § 7 Abs. 4 Satz 3 DSG-LSA durch das Meldeamt als übermittelnde Stelle ist nur das Pseudonym erforderlich, denn auch Protokolldateien selbst stellen Sammlungen personenbezogener Daten dar und sollten nur die unbedingt erforderlichen Daten für eine Protokollierung enthalten.

Der Landesbeauftragte empfiehlt deshalb den Beauftragten für den Datenschutz in den öffentlichen Stellen des Landes, bei der zukünftigen Einrichtung von automatisierten Abrufverfahren ihr Augenmerk auf die ordnungsgemäße Durchführung der Vorabkontrolle, die rechtzeitige Unterrichtung des Landesbeauftragten sowie die Sicherstellung der Revisionsfähigkeit durch Implementierung einer Protokollierung im erforderlichen Umfang zu richten. Aber auch die bereits eingeführten automatisierten Abrufverfahren sollten durch die jeweils verantwortlichen Stellen hinsichtlich der Revisionsfähigkeit von Datenabrufen kritisch überprüft werden.
Zu beachten ist weiterhin, dass für die Einrichtung automatisierter Abrufverfahren **innerhalb** einer öffentlichen Stelle, mit Ausnahme der Vorabkontrolle, die Regelungen des § 7 Abs. 1 und Abs. 4 DSG-LSA zu beachten sind.
Gemäß § 14a Abs. 2 Satz 2 DSG-LSA kann sich der Beauftragte für den Datenschutz bei der Vorabkontrolle in Zweifelsfällen direkt an den Landesbeauftragten wenden.

Abschließend sei noch darauf hingewiesen, dass die in § 32 Abs. 3 DSG-LSA vorgesehene Übergangsfrist von drei Jahren zur Anpassung an die neue Gesetzeslage bereits mit dem 28. Juni 2004 abgelaufen ist.

12.2 Datensicherheit bei USB-Geräten

Öffentliche Stellen haben ihre Verarbeitung personenbezogener Daten nach § 6 Abs. 2 DSG-LSA so zu gestalten, dass Vertraulichkeit und Transparenz jederzeit gewährleistet sind.
Der Landesbeauftragte hat jedoch in letzter Zeit einen Trend in der Technikentwicklung beobachtet, der dies zumindest problematisch werden lässt. Während es bisher genügte, dem unautorisierten Nutzer den Zugriff auf optische und Diskettenlaufwerke aller Art zu verwehren, um zu verhindern, dass unkontrolliert personenbezogene Daten die dienstliche Umgebung verlassen oder unerwünschte Software aufgespielt wird, so ist das heute längst nicht mehr ausreichend. Vermehrt findet man Computer ohne serielle, parallele und PS/2-Anschlüsse. Für Tastatur, Zeigegerät und Drucker werden Universal Serial Bus-Anschlüsse (USB-Anschlüsse) verwendet. Wie der Namensbestandteil "universal" sagt, können an diese Anschlüsse die unterschiedlichsten Hardwarekomponenten angeschlossen werden, z.B. auch Speichergeräte, sog. Memorysticks. Das sind handliche Geräte mit einer Kapazität von bis zu mehreren Gigabyte. Moderne Betriebssysteme erkennen angeschlossene USB-Geräte automatisch, installieren in der Regel die erforderliche Treibersoftware selbständig und machen sie sofort nutzbar. Auch ist ein Booten des PC mittels dieser Memorysticks möglich, wodurch Sicherheitseinstellungen umgangen werden können und damit unbefugte Zugriffe auf den PC möglich sind, falls im BIOS nicht entsprechende Boot-Optionen deaktiviert werden. Da viele Computer USB-Anschlüsse auch auf der Gerätevorderseite besitzen, mag die Hemmschwelle sinken, den USB-Speicher, für weit unter 100 € beim Lebensmitteldiscounter aus dem Non-Food-Bereich mitgenommen, als Datentransportmittel zwischen dem heimischen und dem dienstlichen

Computer zu verwenden. Damit drohen erhebliche Gefahren für die Datensicherheit und den Datenschutz.

Da das Problem in allen Bundesländern zu beobachten war und seine Lösung mit technischen Mitteln erheblichen Aufwand verursacht, hat der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Berichtszeitraum eine Orientierungshilfe „Datensicherheit bei USB-Geräten“ erstellt, die auch über die Homepage des Landesbeauftragten heruntergeladen werden kann.
Den betroffenen Stellen empfiehlt der Landesbeauftragte, auf jeden Fall auch zu einer organisatorischen Lösung in Form von Hausverfügungen oder Organisationsanweisungen zu greifen. Umfassende Aufklärung der Belegschaft über Verbot und Risiken des unautorisierten Verwendens von USB-Geräten, verbunden mit der Ankündigung arbeitsrechtlicher bzw. disziplinarischer Sanktionen bei Verstößen, bei entsprechender Sensibilität der in den dienstlichen Systemen gespeicherten personenbezogenen Daten ergänzt durch technische Maßnahmen aus der o.g. Orientierungshilfe, sind bei der aktuellen Bedrohungslage die Mittel der Wahl.
Der Landesbeauftragte wird bei Kontrollen auch darauf achten, ob Datensicherheit und Datenschutz noch gewährleistet sind, wenn Anschlussmöglichkeiten für USB-Geräte an den dienstlichen Computern vorhanden sind.

12.3 Verarbeitung personenbezogener Daten im Auftrag

Dem Landesbeauftragten war von einer öffentlichen Stelle anlässlich einer Kontrolle der Rahmenvertrag eines Ministeriums mit einer nicht-öffentlichen Stelle, einer GmbH, vorgelegt worden, in dem es um die Sammlung, die Vernichtung und das Recycling von Informationsträgern durch die GmbH ging. Die kontrollierte öffentliche Stelle beabsichtigte, auf Basis dieses Rahmenvertrages eigene Vertragsbeziehungen mit der GmbH einzugehen und dabei, wirtschaftlich durchaus sinnvoll, die im Rahmenvertrag abgeschlossenen Konditionen für sich zu nutzen. Allerdings hatte die öffentliche Stelle bemerkt, dass es sich bei der beabsichtigten Vernichtung von Unterlagen mit personenbezogenen Daten um eine Datenverarbeitung im Auftrag im Sinne von § 8 DSG-LSA handelt und sodann Zweifel gehegt, dass der Rahmenvertrag dieser Tatsache ausreichend Rechnung trägt.
Der Landesbeauftragte teilte diese Zweifel bereits nach einer ersten stichprobenhaften Prüfung des vorgelegten Rahmenvertrages. Das verantwortliche Ministerium hatte keinen der Hinweise des Landesbeauftragten zur Datenverarbeitung im Auftrag und zur Aktenvernichtung beachtet, die regelmäßig bei Fortbildungsveranstaltungen, Beratungen und auch in Ziff. 13.4.1 und 13.4.2 des IV. Tätigkeitsberichts gegeben wurden. Rahmenverträge, wie der vorgelegte, wären zur Begründung von Vertragsverhältnissen öffentlicher Stellen mit der GmbH jedenfalls dann völlig untauglich, wenn diese Verträge die Vernichtung von Unterlagen mit personenbezogenen Daten im Sinne des DSG-LSA zum Inhalt hätten.

Beispielsweise

- war eine unzutreffende Rechtsgrundlage angegeben (BDSG statt DSG-LSA)
- hätte der Auftragnehmer (die GmbH) sich nach dem längst nicht mehr existierenden § 32 BDSG bei der zuständigen Aufsichtsbehörde zu melden,
- war eine außerordentliche Kündigungsmöglichkeit des Auftraggebers bei Vertragsverletzungen des Auftragnehmers nicht enthalten,
- war keine Sicherheitsstufe nach DIN 32757 für die Aktenvernichtung vereinbart worden,
- hätte weder der Auftraggeber noch der Landesbeauftragte die Möglichkeit gehabt, die ordnungsgemäße Vertragsdurchführung zu überprüfen.

Das Ministerium, vom Landesbeauftragten auf diese Tatsachen angesprochen, hob kurzerhand den Vertrag auf.

Das Ministerium des Innern hatte sich im Berichtszeitraum ebenfalls intensiv mit Fragen des Outsourcing und der Abgrenzung von Datenverarbeitung im Auftrag und Funktionsübertragung beschäftigt. Ergebnis der Arbeit, bei der zeitweise auch der Landesbeauftragte mitwirkte und dabei seine Erfahrungen aus vielen Kontrollen und Beratungen einbringen konnte, waren

- ein Mustervertrag über die Vernichtung von Datenträgern,
- ein Mustervertrag zur Verarbeitung personenbezogener Daten im Auftrag in den Ausprägungen für
  - öffentliche Stellen (nach § 8 DSG-LSA) und
  - nicht-öffentliche Stellen (nach § 11 BDSG) und
- eine Handreichung zur Auslagerung von Aufgaben (Outsourcing).

Der Landesbeauftragte empfiehlt bei der Vernichtung personenbezogener Daten in Akten mindestens die Sicherheitsstufe 3 der DIN 32757. Bei dieser Sicherheitsstufe 3 ist die Streifenbreite und -länge sowie die Partikelfläche ausreichend gering, sodass eine Reproduktion von Daten nur unter erheblichem Aufwand möglich wäre. Für die Vernichtung sensibler personenbezogener Daten können entsprechend höhere Sicherheitsstufen vertraglich vereinbart werden.
Abschließend weist der Landesbeauftragte auf die Unterrichtungspflicht der öffentlichen Stellen gem. § 8 Abs. 6 DSG-LSA hin, falls auf Auftragnehmer die Bestimmungen des DSG-LSA keine Anwendung finden.

Die meisten der genannten Dokumente hält der Landesbeauftragte auch in seinem Internetangebot im Servicebereich zum Download bereit.

12.4 Fehlende Zugangskontrolle

Im Zuge der anlassunabhängigen Kontrollen von Ausländerbehörden fand der Landesbeauftragte in einer Kreisverwaltung ein altbekanntes Problem vor. Gelegentlich führt ein gewerbliches Gebäudereinigungsunternehmen

in den Diensträumen der Ausländerbehörde eine Grundreinigung durch. Diese aufwendigen Tätigkeiten werden regelmäßig außerhalb der gewöhnlichen Büroarbeitszeit durchgeführt, um den Dienstbetrieb in der Ausländerbehörde nicht zu beeinflussen. Die Arbeiten werden durch Mitarbeiter der Ausländerbehörde deshalb auch nicht überwacht, das Reinigungspersonal erhält zu diesem Zweck die Büroschlüssel.

Das wäre unter den Voraussetzungen, dass die Aktenschränke in der Ausländerbehörde zum Dienstschluss verschlossen werden und auch der sonstige Zugriff Unbefugter auf in den Akten gespeicherte personenbezogene Daten ausgeschlossen ist, akzeptabel, wie dies § 6 Abs. 3 DSG-LSA verlangt.
Allerdings hatte die Ausländerbehörde genau an dieser Stelle ein Problem. Sie teilte dem Landesbeauftragten in ihrer Stellungnahme zu seinem Prüfbericht mit, dass die Aktenschränke, obgleich abschließbar, ständig geöffnet bleiben müssten, um dem wechselnden Bereitschaftsdienst außerhalb der Dienstzeit den Zugriff auf die Akten zu ermöglichen, wenn dazu Bedarf bestünde.
Im übrigen wäre der Schutz der in den Akten gespeicherten personenbezogenen Daten vor dem Zugriff Unbefugter (§ 6 Abs. 3 DSG-LSA), z.B. der nach Büroschluss tätigen Reinigungsdienstmitarbeiter, nach Ansicht des Landkreises dadurch gewährleistet, dass nachträglich festgestellt werden könne, wer im Missbrauchsfall Zugang und damit Zugriff auf die Aktenbestände gehabt haben könne.

Natürlich teilte der Landesbeauftragte dem Landkreis unverzüglich mit, dass dieses Verfahren nicht im Sinne des Gesetzes sei und überhaupt nicht ausreiche. Er unterbreitete sodann die Vorschläge, die Reinigungsarbeiten so zu koordinieren, dass eine Kontrolle durch einen Beschäftigten der Ausländerbehörde möglich und gewährleistet sei oder aber, dass die Aktenschränke zum Dienstschluss stets verschlossen werden und die Schlüssel in einem Schlüsselverwahrgelass, z.B. mit einem Zahlenschloss, direkt in der Behörde hinterlegt werden, wo sie der Bereitschaftsdienst entnehmen könne.

Der Landkreis konnte sich, allerdings erst nach einer erneuten Erinnerung durch den Landesbeauftragten und direkter Einschaltung des Landrates, zu einer datenschutzgerechten Lösung entschließen.

12.5 Fehlende Bestellung eines Beauftragten für den Datenschutz nach § 14a DSG-LSA

Durch eine Eingabe wurde der Landesbeauftragte für den Datenschutz darauf aufmerksam, dass eine kreisangehörige Stadt noch im Juli 2004 keinen behördlichen Datenschutzbeauftragten bestellt hatte. Es werde vielmehr zunächst lediglich ein Anforderungsprofil erstellt, um die geeignete Person finden zu können. Daraufhin hat der Landesbeauftragte die Stadt unter Hinweis auf die einschlägigen Vorschriften um Stellungnahme gebeten. Nach § 14a DSG-LSA haben öffentliche Stellen einen behördlichen Datenschutzbeauftragten bzw. eine behördliche Datenschutzbeauf-

tragte schriftlich einzusetzen, wenn sie zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten automatisierte Verfahren einsetzen, die nicht lediglich Verfahren im Sinne des § 14 Abs. 4 Nr. 2 DSG-LSA (Unterstützung der Bürotätigkeit) sind. Diese Regelung wurde durch das Gesetz zur Änderung datenschutzrechtlicher Vorschriften vom 21. August 2001 in das DSG-LSA eingeführt. In § 32 Abs. 2 wurde für die Einsetzung eines behördlichen Datenschutzbeauftragten eine Frist bis zum 31. Januar 2002 eingeräumt.

Als die Antwort des Oberbürgermeisters im August 2004 einging, war die Frist bereits über 2 1/2 Jahre verstrichen. Personelle und organisatorische Schwierigkeiten sowie der Wunsch nach Erstellung eines Anforderungsprofils zur Unterstützung der Personalauswahl vermochten diese drastische Fristversäumnis nicht zu entschuldigen.
Sowohl im § 14a DSG-LSA selbst als auch in der Literatur finden sich Hinweise zu den Anforderungen an behördliche Datenschutzbeauftragte. Auch die Verwaltungsvorschriften zum Gesetz zum Schutz personenbezogener Daten der Bürger vom 31. August 2002 (MBl. LSA S. 1091) widmen sich dem Thema.

Zudem konnte der Landesbeauftragte für den Datenschutz auf die Veröffentlichung von „Empfehlungen und Hinweisen zu Aufgaben, Befugnissen und Zuständigkeiten des Beauftragten für den Datenschutz bei öffentlichen Stellen“ auf seiner Homepage unter „Service, sonstige Infos“ sowie auf seinen VI. Tätigkeitsbericht, Ziff. 12.1, hinweisen.

Da der Oberbürgermeister trotz der erheblichen Verfristung und der Hinweise auf die einschlägigen Vorschriften durch den Landesbeauftragten mitteilte, dass sich der Prozess der Organisation des Datenschutzes noch weitere 3 Monate hinziehen würde, war in diesem Fall eine formelle Beanstandung nicht zu vermeiden.

12.6 Einsichtsbefugnisse behördlicher Datenschutzbeauftragter in Personalakten

Einzelne Anfragen befassten sich mit den Befugnissen behördlicher Datenschutzbeauftragter. Insbesondere wurde die Frage formuliert, ob die behördlichen Datenschutzbeauftragten aufgrund ihrer Position die Befugnis hätten, in Personalakten ihrer Dienststelle Einsicht zu nehmen. Hierzu ist auf Folgendes hinzuweisen:

§ 14a Abs. 3 Satz 1 DSG-LSA gestattet dem Beauftragten für den Datenschutz grundsätzlich, zur Aufgabenerfüllung Einsicht in personenbezogene Datenverarbeitungsvorgänge zu nehmen. Nach Satz 2 gilt dies jedoch nicht, soweit Berufs- oder besondere Amtsgeheimnisse entgegenstehen. Als besonderes Berufsgeheimnis wäre hier beispielsweise die Schweigepflicht des Arztes zu benennen. Als besonderes Amtsgeheimnis wäre beispielhaft das Personalaktengeheimnis zu nennen, das der Gesetzgeber in § 90 Abs. 1 Satz 1, Satz 3 und Abs. 3 BG LSA formuliert hat. Auch wenn damit der Schutz der Personaldaten Vorrang hat, bleibt die Aufgabenerfül-

lung des behördlichen Datenschutzbeauftragten gesichert. Er kann jederzeit die Einwilligung des Betroffenen einholen, falls die Einsicht in eine konkrete Personalakte erforderlich sein sollte.

12.7 Datensparsamkeit bei der Verwaltungsmodernisierung

„Land will Dschungel an Vorschriften lichten“ ließ sich im Berichtszeitraum der Presse entnehmen. Zur Kosteneinsparung, zur Effizienzsteigerung und zur Erhöhung der Bürgerfreundlichkeit werden im Bund und in den Ländern regelmäßig Maßnahmen ergriffen. Es werden Vorschläge zur Entbürokratisierung erarbeitet, Verwaltungsreformen und Verwaltungsvereinfachungen geplant und durchgeführt, teilweise werden komplexe Modelle entwickelt, um die effizientere Wahrnehmung öffentlicher Aufgaben zu gewährleisten. Diese Bemühungen sind zu begrüßen. Sie bieten gleichzeitig die Möglichkeit, das vorhandene Datenschutzniveau zu verbessern. Verwaltungsvereinfachungen können und sollten damit einhergehen, weniger personenbezogene Daten zu verarbeiten. Neustrukturierungen und neue Regelungen bieten eine sehr gute Möglichkeit, dem grundrechtlichen Anspruch auf informationelle Selbstbestimmung, den Geboten der Datensparsamkeit und Datenvermeidung sowie der Transparenz Rechnung zu tragen. Demgemäß haben die Datenschutzbeauftragten des Bundes und der Länder die in **Anlage 24** aufgeführte Entschließung zur Datensparsamkeit bei der Verwaltungsmodernisierung gefasst.

13. Hochschulen

Projekt „Gesunder Campus“

Der Landesbeauftragte wurde darauf aufmerksam gemacht, dass an einer Hochschule Befragungen von Studierenden und Bediensteten mittels Fragebogen zum Gesundheitszustand, zu gesundheitserheblichen Verhaltensweisen, zu Arbeitsbedingungen und Motivation durchgeführt wurden. Die Hochschule teilte auf Anfrage mit, dass das Projekt "Gesunder Campus" auf der Grundlage einer Dienstvereinbarung zwischen der Hochschulleitung und dem Personalrat durchgeführt werde. Hauptziel sei es, die Hochschule zu einem Zentrum wissenschaftlichen, sozialen, gesundheitsfördernden, ökologischen und kulturellen Lebens zu entwickeln. Auf Basis von empirischen Befunden sollten u.a. betriebliche Verhältnisse gesundheitsfördernd gestaltet werden. Als ausdrückliche Orientierungspunkte wurden u.a. die Senkung des Krankenstandes, die Verbesserung der Arbeitsbedingungen und des Arbeitsklimas, die Steigerung der Arbeits- und Studienzufriedenheit, die Verbesserung des Sozialimages der Hochschuleinrichtung und die Verbesserung der innerbetrieblichen Kooperation genannt. Die Teilnahme sei freiwillig.

Das Begleitschreiben zum Fragebogen ließ keine Zweifel, dass es sich um eine Maßnahme der Hochschule handelte (Firmierung unter dem Logo der Hochschule; Unterzeichnung des Aufrufs zur Teilnahme durch Kanzler, Rektor, Personalrat und Projektteam). Ein Hinweis auf die Freiwilligkeit der Teilnahme und der Angaben war in dieser Bitte zur Mitarbeit nicht enthal-

ten. Lediglich auf dem Fragebogen selbst befand sich unter der Ziffer 1 („persönliche Daten“; fettgedruckt) der in Klammern gesetzte, nicht fettgedruckte Hinweis „Freiwillige Angabe“.

Der Landesbeauftragte hat auf die datenschutzrechtlichen Rahmenbedingungen solcher Maßnahmen hingewiesen. Unter anderem war infolge der feinen Rasterung der Fragen zu persönlichen Daten eine Bestimmbarkeit natürlicher Personen im Einzelfall gegeben. Die für die Erhebung und Verarbeitung personenbezogener Daten geltenden Regeln des DSG-LSA waren daher einzuhalten. Zu einzelnen Punkten erschien die Erforderlichkeit fraglich.

Unter Bezugnahme auf die Stellungnahme eines Professors (Projektleiter) teilte die Hochschule dann mit, dass es sich lediglich um ein "normales Lehrforschungsprojekt" handele. Diese Darstellung stand im gewissen Widerspruch zu der Konzeption des Projektes, die in vorhergehenden Schreiben der Hochschule beschrieben wurde.

Dennoch hat der Landesbeauftragte auch im Hinblick auf die Ausgestaltung als Lehrforschungsprojekt datenschutzrechtliche Hinweise gegeben. Dem Hinweis auf die eventuell gegebene Verpflichtung zur Löschung personenbeziehbarer Daten ist die Hochschule mit der vollständigen Vernichtung der Fragebögen nachgekommen. Diese Maßnahme wirkte jedoch nur für die Zukunft und war nach der Projektbeschreibung ohnehin beabsichtigt. Eine mögliche Verletzung verfassungsrechtlich geschützter Persönlichkeitsrechte durch die Erhebung und Speicherung personenbeziehbarer Daten in der Umsetzung des Projekts während eines Zeitraums von vier Monaten konnte durch die Löschung jedoch nicht rückwirkend geheilt werden.

Der Landesbeauftragte regte an, bei künftigen Projekten im Interesse der Transparenz der Datenverarbeitung hinsichtlich Trägerschaft und Verantwortlichkeit hinreichend zu differenzieren. Die Nutzung der Amtsautorität der Hochschule zu dienstlichen Zwecken ist von der Durchführung von freiwilligen Forschungsvorhaben deutlich und für den Betroffenen nachvollziehbar zu unterscheiden.

14. Kommunalverwaltung

14.1 Ratsinformationssysteme - Welche Informationen sind für wen?

Im Rahmen seiner Prüftätigkeit hat der Landesbeauftragte festgestellt, dass viele Kommunen auch sogenannte **Ratsinformationssysteme** im Internet bereitstellen. Damit können sich interessierte Nutzer z.B. über die Tagesordnung und die Protokolle von Sitzungen des Kreistages bzw. Stadtrates informieren. Der nicht-öffentliche Teil dieser Sitzungen ist mittels Namen und Passwort geschützt und kann nur von autorisierten Nutzern - den Ratsmitgliedern - eingesehen werden. Datenschutzrechtlich problematisch erscheint die Ausgestaltung solcher Informationssysteme sowohl aus rechtlicher als auch technisch-organisatorischer Sicht.

14.1.1 Gemeinderäte und Ausschüsse, Gemeinderatsmitglieder und Einwohner

Nach der GO LSA wählt jede Gemeinde einen Gemeinderat. In Städten wird dieser als Stadtrat bezeichnet. Zur Vereinfachung soll nachstehend nur von Gemeinderäten gesprochen werden. Der Gemeinderat ist im Rahmen der Gesetze für alle Angelegenheiten der Gemeinde zuständig, soweit nicht der Bürgermeister kraft Gesetzes zuständig ist. Von seinen Aufgaben kann der Gemeinderat bestimmte Angelegenheiten auf beschließende bzw. beratende Ausschüsse übertragen. Beschließende Ausschüsse entscheiden abschließend über die übertragenen Angelegenheiten, beratende Ausschüsse bereiten im Gemeinderat zu treffende Entscheidungen vor und geben dem Gemeinderat gegenüber eine Beschlussempfehlung ab. Die Ausschüsse werden mit Mitgliedern des Gemeinderates im Verhältnis der Mitgliederzahl der einzelnen Fraktionen des Gemeinderates besetzt. Sie sind sozusagen eine verkleinerte Form des Gemeinderates. Bei beratenden Ausschüssen kommt noch die Besonderheit hinzu, dass zu den Ratsmitgliedern auch sachkundige Einwohner als Ausschussmitglieder berufen werden können.

Der Gemeinderat besteht aus den gewählten ehrenamtlichen Mitgliedern (Mandatsträgern) und dem Bürgermeister. Eine jeweils durch den Gemeinderat festzulegende Anzahl dieser ehrenamtlichen Mitglieder bilden die beschließenden bzw. beratenden Ausschüsse. Da demnach nicht jedes Gemeinderatsmitglied auch Mitglied in jedem Ausschuss ist, erhält es auch nicht alle Informationen aus allen Ausschüssen.

An einem Beispiel lässt sich der von Gesetzes wegen unterschiedliche Informationsstand von Gemeinderatsmitgliedern deutlich machen.

> *In einer Gemeinde sind A und B Mitglieder des Gemeinderates. Der Gemeinderat hat einen Hauptausschuss als beschließenden Ausschuss gebildet, der u.a. über die Einstellung von Schreibkräften abschließend entscheidet. A ist Mitglied des Hauptausschusses; B nicht.*
>
> *Die Gemeinde will nun eine neue Schreibkraft einstellen und hat nach erfolgter Ausschreibung eine Vorauswahl unter den Bewerbern getroffen. Nunmehr soll der Hauptausschuss über die Einstellung entscheiden. Die Gemeinde legt dem Hauptausschuss die Bewerbungsunterlagen der drei geeignetsten Personen vor.*
>
> *Weil A Mitglied des Hauptausschusses ist, werden ihm die Bewerbungsunterlagen (Lebenslauf, Bild, Zeugnisse, ...) zur Vorbereitung der Sitzung zugesandt.*

Unabhängig davon, ob ein Mitglied des Gemeinderates auch Mitglied eines Ausschusses ist, darf nach der GO LSA jedes Gemeinderatsmitglied an den Sitzungen der Ausschüsse als Zuhörer teilnehmen.

B war als Zuhörer bei der Hauptausschusssitzung. Als Zuhörer hat er jedoch nur die Diskussion und die Abstimmung zur Kenntnis nehmen können. Die Bewerbungsunterlagen hat er nicht zur Kenntnis bekommen. In den Ausschusssitzungen werden nur die erforderlichen Aspekte angesprochen, welche dann Eingang in das Protokoll der Sitzung finden.

Diese unterschiedlichen Informationsstände der Gemeinderatsmitglieder müssen sich auch in einem Ratsinformationssystem widerspiegeln.

Diese Differenzierung im Informationszugang folgt aus der Entscheidung des jeweiligen Gemeinderats, Teile seiner Befugnisse auf einen beschließenden Ausschuss zu übertragen. Solange er diese nicht zurückholt, wird die interne Kontrolle der Entscheidungen des Ausschusses in gleicher Weise - wie im Gemeinderat selbst - durch die sich im Ausschuss widerspiegelnden Fraktionen gewährleistet.

Neben den Gemeinderatsmitgliedern haben auch die Einwohner der Gemeinde verschiedene Informationsrechte aus der GO LSA. Zunächst sind Zeit, Ort und Tagesordnung der Sitzungen des Gemeinderates und der Ausschüsse rechtzeitig ortsüblich bekannt zu geben. Zudem ist den Einwohnern Einsichtnahme in die Niederschriften über die öffentlichen Sitzungen des Gemeinderates und der Ausschüsse zu gewähren. Die Einsichtnahme ist nur in die Niederschriften der öffentlichen Sitzungen zu gewähren, weil den Einwohnern bereits die Teilnahme an nicht-öffentlichen Sitzungen verwehrt ist. Ein Ausschluss der Öffentlichkeit - und damit der Einwohner - ist immer dann vorzunehmen, wenn das öffentliche Wohl oder berechtigte Interessen Einzelner, insbesondere bei Personalangelegenheiten, Grundstücksangelegenheiten u.s.w. dies erfordern.

Die Einwohner durften an der Sitzung des Hauptausschusses nicht teilnehmen, weil die Öffentlichkeit wegen der Beratung einer Personalangelegenheit auszuschließen war.

Es bleibt festzustellen, dass beim Umfang mit Informationen, die der jeweilige Nutzer aus einem Ratsinformationssystem ziehen darf, nach Einwohnern und Gemeinderatsmitgliedern zu unterscheiden ist. Aber auch bei den Gemeinderatsmitgliedern ist nach ihren jeweiligen Aufgaben zu differenzieren, welche Informationen ihnen zugänglich gemacht werden dürfen.

Der gesetzlich garantierte Informationsumfang der einzelnen Personen lässt sich anhand der nachfolgenden Übersicht nachvollziehen.

	Zeit, Ort und Tagesordnung		Niederschrift				Tagungs-unterlagen	
			öffentlicher Teil		nicht-öffentl. Teil			
	Rat	Auss.	Rat	Auss.	Rat	Auss.	Rat	Auss.
Einwohner	**X**	**X**	**X**	**X**	**--**	**--**	**--**	**--**
Mandatsträger im Rat	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**--**
Mandatsträger als Mitglied in einem Ausschuss	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
sachkundiger Einwohner*		**X**	**X**	**X**	**--**	**X**	**--**	**X**

*(nur in beratenden Ausschüssen)

Wenn sich eine Gemeinde entschließt, ein Ratsinformationssystem zur Verfügung zu stellen, muss sie auch absichern, dass jeder Nutzer entsprechend seiner Rolle als Einwohner, Gemeinderatsmitglied oder Ausschussmitglied Zugang nur zu den ihm nach der GO LSA zustehenden Informationen erlangen kann. Die vorstehenden Ausführungen gelten auf Ebene der Landkreise für die Kreistagsmitglieder und die Einwohner des Landkreises entsprechend.

Seine Auffassung zum Zugang der verschiedenen Personen zu Informationen aus Ratsinformationssystemen hat der Landesbeauftragte dem Ministerium des Innern als oberster Kommunalaufsichtsbehörde schriftlich mitgeteilt. Das Ministerium teilt die Auffassung des Landesbeauftragten und beabsichtigt, den Gemeinden des Landes Hinweise zur datenschutzgerechten Gestaltung von Ratsinformationssystemen zu geben.

14.1.2 Technisch-organisatorische Betrachtung

14.1.2.1 Veröffentlichung im Internet

Bei der Veröffentlichung im Internet handelt es sich - wenn personenbezogene Daten enthalten sind - um eine Datenübermittlung an nicht-öffentliche Stellen gem. § 12 DSG-LSA und eine Datenübermittlung ins Ausland gem. § 13 DSG-LSA, da auf den öffentlichen Teil des Ratsinformationssystems weltweit von einem unbestimmten Personenkreis zugegriffen werden kann. Die Vorraussetzungen der §§ 12 und 13 DSG-LSA liegen jedoch in der Regel nicht vor, weil die Aufgabenerfüllung der Kommune eine beliebige Datenweitergabe nicht erfordert. Deshalb ist eine Veröffentlichung personenbezogener Daten im Internet nur zulässig, wenn der Betroffene eingewilligt hat (§ 4 DSG-LSA). Aufgrund der Tatsache, dass in der Praxis nicht in allen Fällen eine Einwilligung eingeholt werden kann, sind vor der Veröffentlichung im Internet ggf. die personenbezogenen Daten aus den Niederschriften zu entfernen bzw. die Angaben zu anonymisieren. Der Landesbeauftragte weist nachdrücklich darauf hin, dass die

Öffentlichkeitsarbeit öffentlicher Stellen nicht mit amtlichen Bekanntmachungen gleichgesetzt werden kann.

Hinsichtlich der besonderen Sensibilität von Bewerberunterlagen hält es der Landesbeauftragte für sinnvoll und möglich, diese Unterlagen den Entscheidungsträgern auch weiterhin in Papierform - bevorzugt im Wege der Einsichtnahme in der Verwaltung - zugänglich zu machen. Angesichts der Personalsituation in der öffentlichen Verwaltung in Sachsen-Anhalt geht der Landesbeauftragte davon aus, dass die Anzahl der Bewerberfälle begrenzt ist und durch dieses Verfahren kein unverhältnismäßiger Aufwand verursacht wird.

14.1.2.2 Übertragung im Internet

Datenschutzrechtlich problematisch ist die Tatsache, dass in den meisten Fällen die durch Passwort geschützten Inhalte des nicht-öffentlichen Teils völlig unverschlüsselt im Internet übertragen werden, obwohl insbesondere in den Protokollen auch personenbezogene Daten - z.B. bei Bewerbungsverfahren - enthalten sein können. Um zu verhindern, dass Unbefugte Kenntnis von sensiblen personenbezogenen Daten erhalten und somit die Vertraulichkeit gem. § 6 Abs. 2 Nr. 1 DSG-LSA gefährdet wird, sollten die Seiten des nicht-öffentlichen Teils SSL-verschlüsselt übertragen werden. Dabei empfiehlt der Landesbeauftragte, ein SSL-Zertifikat von einer bei der RegTP akkreditierten Zertifizierungsstelle zu erwerben.

14.1.2.3 Auftragsdatenverarbeitung

Bedient sich die öffentliche Stelle bei der Bereitstellung des Ratsinformationssystems einer privaten Firma und werden bei diesem Web-Hosting auch personenbezogene Daten verarbeitet, so handelt es sich hierbei um Auftragsdatenverarbeitung i. S. d. § 8 DSG-LSA. Da auf einen privaten Auftragnehmer die Vorschriften des DSG-LSA nicht anwendbar sind, ist gem. § 8 Abs. 6 DSG-LSA vertraglich sicherzustellen, dass der Auftragnehmer die Bestimmungen des DSG-LSA befolgt und sich der Kontrolle durch den Landesbeauftragten unterwirft. Der Landesbeauftragte ist über die Beauftragungen zu unterrichten (§ 8 Abs. 6 Satz 2 DSG-LSA).

14.2 Videos von öffentlichen Flächen - Im Park überwacht

Aufgrund von Presseberichten erlangte der Landesbeauftragte Kenntnis davon, dass in einer kreisfreien Stadt die **Videoüberwachung** für eine öffentliche Fläche - den Stadtpark - wieder eingeführt worden war.

Im Rahmen eines Modellversuches war der Stadtpark bereits in den Jahren 1999 bis 2001 durch die Polizei einer entsprechenden Überwachung unterzogen worden. Die nunmehr erfolgte Videoüberwachung geht wiederum auf die Initiative der Polizei zurück. Die Bilder laufen auf Bildschirmen im Polizeirevier auf und werden von dort überwacht.

Die Videoüberwachungstechnik wird zwischenzeitlich von der kreisfreien Stadt bereitgestellt. Da der Polizei die entsprechende Technik landesweit nur in begrenzter Anzahl zur Verfügung steht und auch andere Kriminalitätsschwerpunkte überwacht werden sollen, hat die Stadt zur Absicherung einer kontinuierlichen Überwachung eigene Überwachungstechnik angeschafft.

Auf Nachfrage des Landesbeauftragten gab die Stadt als Grund für die Wiedereinführung der Videoüberwachung an, dass die Kriminalitätsrate im Stadtpark nach dem Abbau der Videoüberwachung wieder sprunghaft angestiegen sei. In dem Zeitraum der Überwachung sei die Anzahl der Straftaten insgesamt um 65% gesunken. Zudem nehme die Attraktivität des Stadtparks als Naherholungsgebiet in dem Maße ab, in dem die Anzahl der Straftaten zunehme.

Über den bisherigen Umfang der Überwachung hinaus kann in begründeten Fällen auch eine zeitlich begrenzte **Videoaufzeichnung** erfolgen. Diese Aufzeichnungen sind nach der geltenden Rechtslage zulässig. Die Aufnahmen dienen der Gefahrenabwehr und der Kriminalitätsbekämpfung. Zu diesbezüglichen datenschutzrechtlichen Einwänden vgl. Ziff. 17.1.2.

14.3 Informantenschutz - Wer informiert, wird geschützt!

Durch Vertreter einer Tierschutzorganisation erfuhr der Landesbeauftragte, dass nach einer Anzeige von vermuteten Verstößen gegen das Tierschutzgesetz bei einem Landkreis von dort die Angaben zur anzeigenden Person an Dritte - einen Rechtsanwalt - weitergegeben worden sein sollen. In der Folge sei der anzeigenden Person eine kostenpflichtige Unterlassungserklärung von dem Rechtsanwalt übersandt worden.

Die Ermittlungen des Landesbeauftragten ergaben keine Anhaltspunkte dafür, dass die personenbezogenen Daten der anzeigenden Person durch den Landkreis weitergegeben worden waren.

Hinzuweisen ist in diesem Zusammenhang jedoch darauf, dass die personenbezogenen Daten von **Behördeninformanten** den datenschutzrechtlichen Regelungen unterliegen und nicht ohne weiteres dem Angezeigten bzw. dessen Vertreter preisgegeben werden dürfen. So hat auch das Bundesverwaltungsgericht in seiner Entscheidung vom 4. September 2003 (BVerwG 5C48.02) darauf hingewiesen, dass das **Geheimhaltungsinteresse** eines Behördeninformanten dann das Informationsinteresse des Betroffenen überwiegt, wenn keine Anhaltspunkte dafür vorliegen, dass der Informant wider besseren Wissens oder leichtfertig falsche Behauptungen aufgestellt hat.

14.4 Strafanzeigen im Internet - Keine Information für jedermann

Aufgrund der Eingabe eines Bürgers hat der Landesbeauftragte bei einem Zweckverband eine Kontrolle durchgeführt und festgestellt, dass auf dessen Internetseite eine gegen den Verbandsvorsitzenden und seinen Stell-

vertreter gerichtete Strafanzeige für jedermann zugänglich eingestellt worden war.
Rechtlich handelt es sich bei der Veröffentlichung personenbezogener Daten im Internet um eine Datenübermittlung an nicht-öffentliche Stellen in das Ausland nach den §§ 12 und 13 DSG-LSA, da diese Daten von beliebigen Orten und Personen aus der ganzen Welt abgefragt werden können. Daneben stellt die Verbreitung personenbezogener Daten über das Internet eine völlig neue Qualität der Veröffentlichung dar. Sie erreicht weltweit einen ungleich größeren Personenkreis als jede auflagenbegrenzte papierene Veröffentlichung. Eine solche globale Verfügbarkeit steht im krassen Gegensatz zu der lokalen Begrenzung des Aufgaben- und Wirkungskreises eines Zweckverbandes. Weder ist es Aufgabe eines Zweckverbandes, den Internetnutzern auf der ganzen Welt frei Haus Informationen über Vorgänge in seinem Bereich zu liefern, noch haben Internetnutzer außerhalb des lokalen Raumes und ohne Beziehung zur Kommune ein generelles berechtigtes Interesse an solchen Informationen.

Eine andere Rechtsgrundlage für diese Datenübermittlung gibt es nicht. Nach Art. 6 Abs. 1 der Verfassung des Landes Sachsen-Anhalt hat jeder Bürger das Recht auf Schutz seiner personenbezogenen Daten. In dieses Recht darf aber durch öffentliche Stellen des Landes nur durch oder aufgrund eines Gesetzes eingegriffen werden. Ein Eingriff ist vorliegend weder durch die allgemeinen datenschutzrechtlichen Bestimmungen noch aufgrund einer bereichsspezifischen Regelung zulässig.
Zwar wäre als bereichsspezifische Regelungen an das GKG-LSA und die GO LSA zu denken. Keines dieser Gesetze ermächtigt aber zu einer Veröffentlichung im Internet. Eine Datenübermittlung ist auch nach dem DSG-LSA als allgemeiner datenschutzrechtlicher Regelung nur zulässig, wenn dieses Gesetz selbst oder eine andere Rechtsvorschrift sie erlaubt bzw. anordnet oder Betroffene einwilligen.

Da die Voraussetzungen des § 13 Abs. 1 DSG-LSA nicht gegeben waren, konnte eine Veröffentlichung nur in Frage kommen, wenn der Betroffene seine Einwilligung zur Veröffentlichung im Internet erklärt hätte. Eine solche Einwilligung zur Datenübermittlung hatte in diesem Fall aber nicht vorgelegen. Die Veröffentlichung im Internet war daher unzulässig.

Der Zweckverband wurde durch den Landesbeauftragten auf die Rechtslage hingewiesen und gebeten, auch die Verbandsversammlung entsprechend zu unterrichten. Über die Unterrichtung der Verbandsversammlung wurde dem Landesbeauftragten ein Nachweis vorgelegt.

14.5 Sitzungen des Gemeinderates - Das Band läuft mit

Dem Landesbeauftragten wurde durch einen Petenten mitgeteilt, dass bei Sitzungen eines Gemeinderates **Tonbandaufzeichnungen** gefertigt wurden. Sie sollten dazu dienen, dem Protokollführer die Niederschrift zu erleichtern. Auch während des nicht-öffentlichen Teils der Sitzungen erfolgten Bandmitschnitte. Diese Aufnahmen wurden dem Bürgermeister und dem protokollierenden Verwaltungsmitarbeiter vorgespielt, die dessen In-

halt mit der entsprechenden Niederschrift abstimmten. Zudem war bei einigen Sitzungen nicht deutlich, ob Aufzeichnungen tatsächlich erfolgten oder nicht. Die anwesenden Gäste wurden weder über die Tonbandaufzeichnung informiert noch nach ihrem Einverständnis gefragt.

Im Rahmen seiner Prüfung hat der Landesbeauftragte anhand der Geschäftsordnung der Gemeinde festgestellt, dass der Protokollführer in einer Gemeinderatssitzung die Möglichkeit hat, zur Erleichterung der Aufnahme der Niederschrift Tonbandaufzeichnungen zu fertigen. Nach Fertigstellung, Unterzeichnung und Genehmigung der Niederschrift sind die Aufzeichnungen wieder zu löschen.

Der Landesbeauftragte hat gegen diese Verfahrensweise keine Bedenken, wenn die Aufzeichnung nur den für die Fertigstellung und Aufzeichnung der Niederschrift verantwortlichen Personen zugänglich ist und bis zur Löschung sicher aufbewahrt wird. Verantwortliche Personen werden im Regelfall die Protokollführenden und der Bürgermeister sein.
Die Rechte der Gemeinderatsmitglieder richten sich in diesem Fall ausschließlich nach den Vorschriften der Gemeindeordnung. Zu den Rechten gehören die Ansprüche auf richtige Wiedergabe der Beiträge und die Möglichkeit, die Aufzeichnungen der Redebeiträge im Streitfall vor Genehmigung der Niederschrift im Beisein des Protokollführers und des Bürgermeisters abzuhören. Allerdings ist bei öffentlichen Sitzungen die Sperrvorschrift in § 50 Abs. 2 GO LSA zu berücksichtigen.

Die rechtliche Situation ist grundlegend anders zu bewerten, wenn Vertreter der **Presse** Tonbandaufzeichnungen von Gemeinderatssitzungen anfertigen. Da hier eine nicht absehbare weitere Verwendung möglich ist, sind Aufzeichnungen durch Pressevertreter nicht zulässig, wenn auch nur ein Gemeinderatsmitglied einer Aufzeichnung widerspricht. Gänzlich ausgeschlossen sind Bandmitschnitte der Presse während der Bürgerfragestunden.

14.6 Einsatz von Parkkrallen bei der Verwaltungsvollstreckung

Im Berichtszeitraum konnte vielfach der Presse entnommen werden, dass einzelne Gemeinden beabsichtigten, säumige Schuldner durch den Einsatz so genannter Parkkrallen zu pflichtgemäßen Zahlungen anzuhalten. Einmal wurde eine Bürgermeisterin mit der Bemerkung zitiert, man wolle einen Erziehungseffekt erzielen.

Sicher ist die konsequente Beitreibung öffentlicher Forderungen geboten. Ob dabei das Vollstreckungsrecht ein Instrument zur Erziehung mündiger Bürger ist, kann dahinstehen. Jedenfalls hat die Vollstreckung unter Beachtung der rechtlichen und gesetzlichen Grenzen stattzufinden. Hierauf hat der Landesbeauftragte in mehreren Fällen hingewiesen.

Das Anbringen von Parkkrallen führt zu einer Prangerwirkung. Der Halter eines Kraftfahrzeuges ist zumindest Verwandten, Nachbarn und Freunden häufig bekannt. Zu dieser so bestimmbaren Person wird durch die Park-

kralle die Information übermittelt, dass sie als säumiger Schuldner angesehen wird. Die Übermittlung dieser personenbezogenen Information bedürfte einer Rechtsgrundlage (§ 4 Abs. 1 DSG-LSA).

Das bloße „Stilllegen“ eines Kraftfahrzeugs mit dem Ziel der Freigabe nach der Begleichung der Zahlungsrückstände als vollstreckungsrechtliche Motivation ist im Katalog der Vollstreckungsmaßnahmen des Verwaltungsvollstreckungsgesetzes des Landes Sachsen-Anhalt nicht vorgesehen.

Denkbar wäre lediglich eine Vollstreckung in den Pkw durch Pfändung. Dabei sind jedoch die rechtlichen Voraussetzungen zu beachten.

Zunächst ist zu berücksichtigen, dass die Ermittlung des Fahrzeughalters im Zusammenhang mit der Vollstreckung auf der Grundlage des § 39 Abs. 3 Satz 1 Nr. 1a) StVG erst dann erfolgen darf, wenn eine Forderung in Höhe von mindestens 500 € aussteht. Den Zeitungsmeldungen war jedoch zu entnehmen, dass beabsichtigt ist, bei „vergleichsweise geringen Beträgen“ mit Hilfe der Parkkralle vorzugehen. In diesen Fällen dürfte schon keine Halterauskunft erfolgen.

Selbst wenn die Eigenschaft als Kraftfahrzeughalter rechtmäßig bekannt geworden ist, ist die Pfändung eines Pkw bei geringen Schuldbeträgen grundsätzlich unzulässig. Die Pfändung eines in der Regel wesentlich höherwertigen Pkw wäre unverhältnismäßig. So gebietet § 27 Abs. 2 VwVG LSA, dass die Pfändung nicht weiter ausgedehnt werden darf, als es zur Deckung der beizutreibenden Geldbeträge und der Kosten der Vollstreckung erforderlich ist.

Der Landesbeauftragte hat darauf hingewiesen, dass die Rechtswidrigkeit der Vollstreckungsmaßnahme gleichzeitig dazu führen würde, dass die Übermittlung der Information der Schuldnereigenschaft rechtswidrig ist. Liegen jedoch die Voraussetzungen für eine rechtmäßige Pfändung grundsätzlich vor, kann eine Güterabwägung zwischen dem Interesse des Steuerschuldners am Schutz seiner persönlichen Daten einerseits und dem Interesse des Staates an der Sicherung seines Steueraufkommens durch effiziente Verfahren und an der gleichmäßigen Besteuerung der Bürger andererseits ergeben, dass die Anlegung einer Parkkralle auch aus datenschutzrechtlicher Sicht zulässig ist.

15. Landtag

15.1 Kleine Anfrage im Landtag - Eine Fortsetzung

Der Antwort auf eine Kleine Anfrage hatte die Landesregierung die Kopie der Teilnehmerliste zur Gründungsversammlung eines Vereins beigefügt. In dieser Liste wurden die Gründungsmitglieder namentlich mit Privatadresse und Unterschrift aufgeführt. Im Rahmen der Öffentlichkeitsarbeit hatte die Landtagsverwaltung die Antwort unverändert in das Internetan-

gebot des Landtages eingestellt. Der Landesbeauftragte hatte hierüber bereits im VI. Tätigkeitsbericht (Ziff. 15) berichtet.

Mit der Landtagsverwaltung wurde die rechtliche Seite besprochen. Wie diese - und auch mehrheitlich die Konferenz der Landtagsdirektoren - ist der Landesbeauftragte der Rechtsauffassung, dass jedes Verfassungsorgan die rechtliche Verantwortung für seine Handlungen trägt.
Werden also durch die Landesregierung Anfragen beantwortet, welche personenbezogene Daten Betroffener beinhalten, so prüft die Landesregierung zum einen, ob eine Information zu einzelnen Personen überhaupt erforderlich ist, um die Fragen zu beantworten. Zudem klärt sie, ob im Rahmen ihrer Auskunftspflicht u.a. Rechte Dritter betroffen sein könnten, und sie darum die Auskunft nach Art. 53 der Verfassung des Landes Sachsen-Anhalt (Verf LSA) verweigern müsste. Aufgrund der Kontrollkompetenz des Parlaments wird diesem allerdings nur selten eine Information, sei sie auch personenbezogen, verwehrt werden dürfen. Wie das Bundesverfassungsgericht (BVerfG) zuletzt in einem Beschluss vom 30. März 2004 - 2 BvK 1/01 - (vgl. ZParl 2004, 487) dargelegt hat, erfordert die Begrenzung eines parlamentarischen Informationsverlangens durch die Regierung im Einzelfall eine nachvollziehbare Begründung und Abwägung der unterschiedlichen Interessen von Regierung, eines ggf. betroffenen Dritten einerseits und des Informationsanspruchs des Parlaments andererseits.
Vor diesem Hintergrund ist es von besonderer Bedeutung, zwischen der Übermittlung von Informationen an die Abgeordneten und der weiteren Öffentlichkeitsarbeit des Landtages zu unterscheiden. Der umfassende Anspruch der Abgeordneten auf unveränderte Überlassung von Informationspapieren der Regierung ist verfassungsrechtlich verankert. Gleiches gilt bezüglich der Veröffentlichung solcher Informationen durch den Landtag nicht in entsprechender Weise.
Aus den Regelungen in § 19 Abs. 4 und § 82 Abs. 2 der Geschäftsordnung des Landtags wird deutlich, dass die Landtagsverwaltung nicht verpflichtet ist, Landtagsdrucksachen über das Internet einer weltweiten Öffentlichkeit zugänglich zu machen. Das Landesparlament hat den verfassungsrechtlichen und rechtstatsächlichen Unterschied zwischen einem Informationszugang über das Internet und einer Einsichtnahme beim Landtag gesehen und den für die Grundrechte betroffener Bürgerinnen und Bürger schonenderen Weg der Einsicht beim Landtag gewählt.
Die Verwaltung des Landtags muss in jedem Einzelfall die Entscheidung treffen, ob und ggf. welche Informationen sie auf der Internetseite des Landtags weltweit und nicht rückholbar zur Verfügung stellen will und darf. Die weitergehende Internetveröffentlichung von Landtagspapieren dient nicht der Erfüllung der verfassungsrechtlich gebotenen Informationspflicht des Landtags und seiner Mitglieder, sondern stellt einen besonderen Modus der Öffentlichkeitsarbeit dar, auf den die Persönlichkeitsrechte schützenden Regelungen anwendbar sind, insbesondere Art. 1 Abs. 1, 2 Abs. 1 GG, Art. 6 Abs. 1 Verf LSA, § 4 Abs. 2 Nr. 3 Landespressegesetz sowie die Bestimmungen des DSG-LSA. Demzufolge stellt es keinen Eingriff in die Rechte eines Verfassungsorgans dar, wenn der Landtag anlässlich der Veröffentlichung von Drucksachen, insbesondere im Internet, personen-

bezogene Daten auf das zulässige Maß begrenzt. Der Anspruch der parlamentarischen Fragesteller auf eine Antwort der Landesregierung wird in keiner Weise beschränkt, da ihnen die Antwort in der von der Landesregierung übermittelten Fassung zugeleitet wird.

Nachdem dies einhellige Meinung zu sein schien, konnte der Landesbeauftragte also davon ausgehen, dass die Landtagsverwaltung künftig in adäquater Weise verfahren würde und die schutzwürdigen Belange Betroffener bei ihrer Öffentlichkeitsarbeit, auch soweit sie dabei das Medium Internet nutzt, berücksichtigen würde.
Trotzdem kam es 2004 zur erneuten Veröffentlichung personenbezogener Daten, indem eine Liste zu Beraterverträgen auf der Internetseite des Landtages eingestellt wurde. Der Landesbeauftragte hat dies kritisiert und erneut darauf hingewiesen, dass solches ohne Einwilligung der Betroffenen grundsätzlich nicht hinnehmbar ist. Auch das Urteil des Verfassungsgerichts Mecklenburg-Vorpommerns vom 19. November 2002 (LKV 2003, 182), welches u.a. die über das Internet vorgenommene Veröffentlichung von Daten von Rechtsanwälten zum Gegenstand hat, führt nicht zu einer anderen Einschätzung, da diese Personen nach Auffassung des Gerichts nur in ihrer (öffentlichen) Rolle als Organ der Rechtspflege betroffen waren.

Zusammenfassend stellt der Landesbeauftragte klar, dass sich Öffentlichkeitsarbeit öffentlicher Stellen nur in ihrer grundsätzlichen Zulässigkeit bzw. Notwendigkeit, jedoch nicht bezüglich des gewählten Modus aus dem Demokratieprinzip rechtfertigt.
Die Öffentlichkeitsarbeit nicht nur des Landtages, sondern - wegen der Vielzahl ihrer Internetseiten - besonders auch jene der kommunalen Körperschaften, muss sich immer an der nicht einschränkbaren Menschenwürde der Betroffenen ausrichten. Das BVerfG hat mehrfach betont, dass die Menschenwürde tragendes Konstitutionsprinzip und oberster Verfassungswert ist und es mit der Würde des Menschen nicht vereinbar ist, ihn zum bloßen Objekt der Staatsgewalt zu machen. Dies geschieht jedoch, wenn die Daten Betroffener ohne deren Einwilligung bzw. schon ohne deren Kenntnis auf einer Internetseite durch öffentliche Stellen weltweit verfügbar gemacht werden.

Um eine Diskussion über eine gesetzliche Regelung zur Erweiterung der Befugnisse bei der Öffentlichkeitsarbeit zu vermeiden, weist der Landesbeauftragte klarstellend darauf hin, dass ein Bedürfnis zur normativen Zulassung von Internetveröffentlichungen personenbezogener Daten in diesem Zusammenhang verfassungsrechtlich nicht vertretbar sein dürfte.

15.2 Verwendung von personenbezogenen Daten aus Gerichtsverfahren während einer Landtagssitzung

Ein Petent wandte sich mit Folgendem an den Landesbeauftragten:
Er betreibe ein Gerichtsverfahren, welches nun beim Oberlandesgericht (OLG) des Landes Sachsen-Anhalt anhängig sei. Im Laufe dieses Verfah-

rens habe seine Bürgermeisterin, zur Schilderung der besonderen sozialen Situation des Petenten, ein Schreiben an das OLG gerichtet.
Nun seien im Laufe einer Landtagssitzung von einem Landtagsabgeordneten Informationen aus diesem Schreiben zitiert worden. Zudem sei dieser Sachverhalt in der Folge in der Presse, wenn auch ohne Namensnennung, nachzulesen gewesen.

Der Landesbeauftragte teilte nach Überprüfung der Geschehnisse dem Petenten mit, dass auch nach seiner Auffassung das Grundrecht des Petenten auf Schutz seiner personenbezogenen Daten (Artikel 6 Abs. 1 der Verfassung des Landes) beeinträchtigt worden ist.
Dies geschah zweifach; zum einen durch die Weitergabe des Briefes an den Landtagsabgeordneten. Denn hier musste eine zur Einsicht in diese Unterlagen befugte Person Dritten vorsätzlich oder fahrlässig den Zugang zu dem streitigen Schreiben verschafft und damit die Übermittlung persönlicher Informationen des Petenten ermöglicht haben. Zum anderen geschah es auch durch die Art und Weise der Verwendung. Zwar erfolgte keine namentliche Bezeichnung des Petenten, seine Identifizierung mit Hilfe der Daten, welche im Protokoll der Landtagssitzung öffentlich zugänglich sind, wäre jedoch trotzdem möglich gewesen.

Auf welchem Weg das Schreiben zu dem Landtagsabgeordneten gelangte, konnte nicht geklärt werden.

Dieser selbst berief sich auf Nachfrage auf das allen Abgeordneten nach der Verfassung des Landes Sachsen-Anhalt zustehende Recht, Auskünfte über die Herkunft ihnen zugeleiteter Informationen zu verweigern.
Das gleichfalls befragte OLG teilte dem Landesbeauftragten mit, dass das Schreiben im Rahmen der verfassungsrechtlichen Pflicht, rechtliches Gehör zu gewähren, ausschließlich den Verfahrensbeteiligten zugeleitet worden war. Auch nach einer Kontrolle, die bei einem verfahrensbeteiligten Landkreis durchgeführt wurde, ergaben sich keine weiteren Hinweise, wie das Schreiben übermittelt wurde.

Letztlich ließ sich nur feststellen, dass die Kopie des Schreibens dem Abgeordneten vermutlich nicht von einer der „beteiligten“ öffentlichen Stellen zugeleitet wurde.
Der Landesbeauftragte erklärte dem Petenten, dass er keine gesetzliche Grundlage für eine Untersuchung bei privaten Stellen hat und ihm bezüglich des Landtags lediglich ein Beratungsrecht obliegt.
Er gab ihm abschließend den Hinweis, andere Möglichkeiten, wie z.B. eine Strafanzeige wegen Verletzung der Privatsphäre, in Betracht zu ziehen.

15.3 Einsicht in Unterlagen des Petitionsausschusses

Im Rahmen eines Petitionsverfahrens begehrte ein Petent Einsicht in die Akten des Petitionsausschusses des Landtags. Nachdem ihm diese verweigert worden war, bat er den Landesbeauftragten um Unterstützung bei der Einsicht in ihn betreffende Unterlagen.

Da er davon ausging, der Landesbeauftragte könne ihm aufgrund der übertragenen Befugnisse zu einer Einsicht verhelfen, musste der Petent zunächst über die anzuwendenden gesetzlichen Regelungen ebenso informiert werden, wie über die gesetzlich festgelegten Befugnisse des Landesbeauftragten für den Datenschutz. Im Gegensatz zur Auffassung des Petenten verfügt der Landesbeauftragte bereits von Verfassungs wegen über keine Vollzugskompetenzen, schon gar nicht gegenüber dem Parlament. Dem Petenten wurde mitgeteilt, dass der Landesbeauftragte gegenüber öffentlichen Stellen keine Weisungen, etwa zur Erteilung von Akteneinsicht erteilen kann. Seine Kontrollfunktion, welche sich im schärfsten Fall in einer förmlichen Beanstandung realisieren würde, bezieht sich beim Parlament lediglich auf dessen verwaltende Tätigkeit. Im Übrigen nimmt er vornehmlich eine beratende Funktion wahr.

Da der Petent zur gleichen Thematik Akteneinsicht in Unterlagen einer Stadt begehrte, wurde er vom Landesbeauftragten auch über die wesentlichen Aspekte bezüglich des Informationszugangs zu Behörden informiert.
Neben der Möglichkeit, nach § 29 VwVfG LSA **Akteneinsicht** verlangen zu können, soweit die Verteidigung eigener rechtlicher Interessen eines **Verfahrensbeteiligten** dies erfordert, steht **Betroffenen** nach § 15 DSG-LSA die Möglichkeit offen, **Auskunft** u.a. über die Nutzung der eigenen personenbezogenen Daten zu beantragen. Diese Auskunft kann nur unter gesetzlich festgelegten Voraussetzungen verweigert werden. Diese Regelung gewährt jedoch keinen Anspruch auf Einsicht der Betroffenen in Akten oder Anspruch auf Überlassen von Aktenauszügen in Kopie. Die jeweilige Stelle ist indessen nicht gehindert, diese weitergehenden Möglichkeiten einzuräumen.

Im konkreten Fall teilte die betreffende Stadt dem Landesbeauftragten unaufgefordert mit, dass der Petent uneingeschränkt in die ihn betreffenden Vorgänge einsehen kann. Dieses Angebot wurde vom Petenten genutzt.
Von ihm vermutete Veränderungen des Akteninhalts („Säuberung“ von Akten) konnten nicht festgestellt werden.

16. Personalwesen

16.1 Aufbewahrung von Anlassbeurteilungen im Zusammenhang mit Auswahlentscheidungen

Der Landesbeauftragte für den Datenschutz Bremen befragte unter Bezugnahme auf die Entscheidung des BVerwG vom 21. August 2003 (Az. 2 C 14.02) alle Landesbeauftragten zur Verfahrensweise der Länder beim Umgang mit Anlassbeurteilungen im Zusammenhang mit einem Auswahlverfahren.
Hierzu nahm der Landesbeauftragte wie folgt Stellung:

In Sachsen-Anhalt sind Beurteilungen zur Personalakte zu nehmen. Grundlage hierfür ist der § 90 Abs. 1 Satz 2 BG LSA, in dem es heißt:

"Zur Personalakte gehören alle Unterlagen einschließlich der in Dateien gespeicherten, die den Beamten betreffen, soweit sie mit dem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen (Personalaktendaten); andere Unterlagen dürfen in die Personalakte nicht aufgenommen werden."

Da die Beurteilung, egal ob Regel- oder Anlassbeurteilung, die Eignung und Befähigung des Beamten im Beurteilungszeitraum widerspiegelt, wird ein unmittelbarer Zusammenhang mit dem Dienstverhältnis bejaht.

Ein Beurteilungsbeitrag, der von einem unmittelbaren Vorgesetzten oder von einem früheren Erstbeurteiler bei Wechsel des Unterstellungsverhältnisses im Beurteilungszeitraum abgefordert wurde, ist jedoch nach endgültiger Aufnahme der Beurteilung in die Personalakte zu vernichten.

16.2 Umsetzung der Beurteilungsrichtlinien

Der Landesbeauftragte erhielt von einigen Mitarbeitern Oberster Landesbehörden zu Beginn der Berichtsperiode Eingaben zur Umsetzung der seinerzeit gültigen Beurteilungsrichtlinien. Darin waren zunächst Quotenvorgaben im Hinblick auf die Zulässigkeit höherer Benotungen gemacht worden. Im Übrigen war die Einsetzung eines Beurteilungsgremiums mit beratender Funktion gestattet worden. Aufgrund der angedachten Verfahrensweise in den einzelnen Ressorts hatten die Petenten den Verdacht, dass die zu erstellenden Beurteilungsentwürfe zunächst zentral gesammelt und dann in größerer Runde „ausgehandelt“ werden.

Der Landesbeauftragte hat die Obersten Landesbehörden in Gesprächen und schriftlich auf Folgendes hingewiesen:

Nach Inhalt und Zweck ist die dienstliche Beurteilung eine Äußerung des Vorgesetzten über die Eignung, Befähigung und fachliche Leistung des Beamten unter Bezugnahme auf den Beurteilungszeitraum. Dabei wird in der Regel eine unbestimmte Vielzahl nicht benannter Einzeleindrücke während des Beurteilungszeitraums in einem Wert berücksichtigt.

Deshalb müssen die Beurteilungen nach der bekannten obergerichtlichen Rechtsprechung in der Regel vom unmittelbaren Dienstvorgesetzten abgegeben werden. Der höhere Dienstvorgesetzte kann Beurteilungen zur Herbeiführung möglichst einheitlicher Beurteilungsmaßstäbe überprüfen und gegebenenfalls ändern. Dabei muss er jedoch selbst in der Lage sein, Fähigkeiten und Leistungen des einzelnen Beamten abzuschätzen.

Beurteilungsdaten gehören zu den besonders vertraulichen Personalaktendaten. Eine Erörterung der Stärken und Schwächen der zu Beurteilenden ist daher nur unter den zuständigen Beurteilern zulässig. Die Schutzwürdigkeit solcher personbezogenen Daten ist auch bei Beurteilungen im Entwurfstadium gegeben.

Beurteilungsgremien dürfen sich somit, soweit sie mit Personen besetzt sind, die nicht selbst zur Beurteilung des Betroffenen berufen sind, nicht mit individuellen Bewertungen, sondern nur mit generell anzulegenden Wertmaßstäben befassen. Für eine grundrechtsrelevante Bekanntgabe von personenbeziehbaren Bewertungsdaten an solche Gremien fehlt die erforderliche Rechtsgrundlage.

16.3 Sammelverfügungen

Das im § 90 Abs. 1 Satz 1 BG LSA normierte Personalaktengeheimnis erfordert, Personakten vertraulich zu behandeln und vor unbefugter Einsicht zu schützen. Daher ist es grundsätzlich unzulässig, Personalakteninformationen zu einer Person in Personalakten von anderen Personen zu speichern. Nimmt eine der anderen Personen in ihre Personalakte Einsicht, ist der Tatbestand der Übermittlung erfüllt (§ 2 Abs. 5 Nr. 3a DSG-LSA). Hierfür gibt es keine Rechtsgrundlage. Bei Unterlagen, die parallel laufende Personalmaßnahmen zu mehreren Personen betreffen und diese Personen namentlich aufführen (so genannte Sammelverfügungen), dürfen deshalb bei der Einfügung in die Personalakte nur die personenbezogenen Informationen zu der jeweils betroffenen Person ungeschwärzt bleiben. Schwärzungen sind allerdings derart durchzuführen, dass das Ziel, die Kenntnisnahme von personenbezogenen Daten auszuschließen, auch tatsächlich erreicht wird.

Bei Prüfungen durch den Landesbeauftragten wurde häufig festgestellt, dass Sammelverfügungen achtlos als Ablichtung in die jeweilige Personalakte gegeben worden sind. Teilweise war in den Dienststellen zwar ein Problembewusstsein vorhanden. Das Schwärzen der Daten nichtbetroffener Personen wurde aber so oberflächlich durchgeführt, dass die Namen dennoch ohne weiteres erkennbar waren. Daher sieht sich der Landesbeauftragte veranlasst, noch einmal ausdrücklich auf die oben genannte Problematik der Sammelverfügungen hinzuweisen.

16.4 Amtsärztliche Gutachten

Das Personalamt eines Landkreises teilte im Rahmen einer Prüfung mit, dass bereits in drei Fällen durch das Personalamt in Auftrag gegebene amtsärztliche Gutachten zum Schutze des Mitarbeiters vor sich selbst nicht in der Personalakte, sondern gesondert aufbewahrt worden seien. Ursache seien Hinweise des jeweiligen Amtsarztes gewesen. In einem Fall hat beispielsweise das Gutachten den Befund einer unheilbaren Erkrankung ergeben.

Der Landesbeauftragte wies hierzu auf § 90 Abs. 1 und 2 BG LSA hin. Danach gehören Unterlagen, die mit dem Beschäftigungsverhältnis in einem unmittelbaren inneren Zusammenhang stehen, in die Personalakte. Dies betrifft insbesondere auch grundlegende Unterlagen über unfallbedingte Abwesenheit sowie längerfristige Erkrankungen, die die Arbeitspflicht dem Grunde nach berühren. Der Grundsatz der Einheit und Vollständigkeit der Personalakte gebietet auch die Aufnahme von amtsärztli-

chen Gutachten, die schwerwiegende medizinische Feststellungen für den Betroffenen enthalten. Das Grundrecht auf informationelle Selbstbestimmung in Gestalt des Rechts auf Einsicht in die vollständige Personalakte darf nicht durch fürsorgliches Ausgliedern schwerwiegender amtsärztlicher Gutachten auf ärztliches Anraten umgangen werden. Eine Ausnahmesituation könnte nach höchstrichterlicher Rechtsprechung allenfalls dann gegeben sein, wenn konkrete Anhaltspunkte für eine Selbstmordgefahr bzw. dafür bestünden, dass der Betroffene bei seinem Verlangen auf Akteneinsicht und damit bei der Ausübung seines Selbstbestimmungsrechtes in der Fähigkeit krankhaft eingeschränkt war, seinen Willen frei zu bestimmen.

Die Dienststelle hat aber nach § 90c Abs. 3 BG LSA die Möglichkeit, dass Einsichtsverfahren zu beeinflussen. In diesem Rahmen könnte sie darauf hinwirken, den betroffenen Mitarbeiter zur Zustimmung zu bewegen, dass ein Arzt an der Eröffnung des amtsärztlichen Gutachtens teilnimmt.

16.5 Personaldatenübermittlung an Kollegen

Das Personalamt einer Hochschule hatte eine Mitarbeiterin schriftlich gebeten, sich einer amtsärztlichen Untersuchung zu unterziehen, da sie gesundheitliche Probleme habe, nicht längere Zeit stehen, sitzen oder gehen und auch nicht über längere Zeit am PC arbeiten könne.
Eine Ablichtung des Schreibens wurde auch dem Institutsdirektor übermittelt. Damit wollte das Personalamt darauf hinweisen, dass man der Anregung des Institutsdirektors, eine Dienstfähigkeitsuntersuchung vorzunehmen, gefolgt ist. Der Institutsleiter hatte das Schreiben mit anderen Schreiben „an alle Kollegen - im Hause -“ weitergeleitet.
Die Überprüfung der Angelegenheit in der Hochschule hat ein knappes halbes Jahr gedauert. Die Institutsleitung teilte mit, dass nicht mehr nachvollziehbar sei, wie das Schreiben an andere Personen gelangen konnte. Es sei lediglich beabsichtigt gewesen, den Vorstand des Instituts zu informieren.
Die vielfältigen Informationen bezogen sich auf den Gesundheitszustand und seine Konsequenzen für das Beschäftigungsverhältnis. Sie unterliegen als Gesundheitsinformationen nach § 2 Abs. 1 Satz 2 DSG-LSA als personenbezogene Daten besonderer Art einem besonderen bundes-, landes- und europarechtlich vorgegebenen Schutz. Zudem stehen die Daten in einem unmittelbaren inneren Zusammenhang mit den Rechten und Pflichten aus dem Arbeitsverhältnis. Nach § 28 Abs. 1 DSG-LSA i.V.m. § 90 Abs. 1 Satz 2 BG LSA handelte es sich damit um Personalaktendaten, die dem Personalaktengeheimnis unterliegen. Personalaktendaten dürfen nur für Zwecke der Personalverwaltung oder Personalwirtschaft verwendet werden. Nur zu diesen Zwecken dürfen Beschäftigte Zugang haben (§ 90 Abs. 1 Satz 3, Abs. 3 BG LSA).

Eine Rechtfertigung der Weiterleitung der Informationen an einen unzuständigen, größeren Personenkreis war nicht ersichtlich. Auch die Hochschule ging von einer unzulässigen Übermittlung von Personaldaten aus.
Der Landesbeauftragte hat den Vorgang formell beanstandet.

16.6 Aufbewahrung von Dienstaufsichtsbeschwerden

Bei der Kontrolle einer Polizeidirektion wurden auch Vorgänge zu unbegründeten Dienstaufsichtsbeschwerden über Beamte überprüft.
Im Zimmer des zuständigen Sachbearbeiters fanden sich ca. 30 Aktenordner mit jeweils etwa 20 Dienstaufsichtsbeschwerdevorgängen.
Ausweislich der Auszeichnung auf dem Ordnerrücken reichten die Vorgänge bis 1991 zurück. Aus den Jahren 1993, 1994, 1995 und 1997 fanden sich teilweise mehrere Vorgänge. Einige einzelne Ordner führten gut 20 Beschwerdevorgänge eines einzelnen Beschwerdeführers aus dem letzten Jahrzehnt auf.

Die Notwendigkeit der Aufbewahrung wurde zunächst damit begründet, dass einzelne Beschwerdeführer regelmäßig über lange Jahre Beschwerden einlegen, die überwiegend auf vorherige Vorgänge Bezug nehmen.

Für die sachdienliche Beantwortung sei daher ein Rückgriff auf die vorherigen Vorgänge erforderlich. Zudem sei ein längeres Aufbewahren erforderlich, um Berichtspflichten gegenüber der obersten Landesbehörde Rechnung zu tragen. Gelegentlich seien auch Informationen für den Petitionsausschuss des Landtages zur Verfügung zu stellen.

Der Landesbeauftragte musste die Polizeidirektion darauf hinweisen, dass die Aufbewahrung von Vorgängen zu Dienstaufsichtsbeschwerden zurück bis in das Jahr 1991 datenschutzrechtlich bedenklich ist (vgl. VI. Tätigkeitsbericht, Ziff. 16.5). Die auf den betroffenen Beamten bezogenen Informationen werden in Sachakten geführt. Das Speichern in Sachakten ist nach § 10 Abs. 1 DSG-LSA nur insoweit zulässig, als es zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist und für Zwecke erfolgt, für die die Daten erhoben worden sind. Eine Datensammlung auf Vorrat für vorläufig unbestimmte Zwecke ist im Hinblick auf das betroffene Grundrecht verfassungsrechtlich unzulässig (vgl. BVerfGE 65,1). Die Erforderlichkeit der Aufbewahrung von teilweise bis zu über 10 Jahre alten Dienstaufsichtsbeschwerdevorgängen ist nicht ersichtlich. Es ist zwar der Möglichkeit Rechnung zu tragen, dass sich ein Beschwerdeführer mit der Zurückweisung seines Vorbringens evtl. nicht zufrieden gibt und weitere Beschwerden einlegt. Auch kann es im engen zeitlichen Zusammenhang vorkommen, dass der konkrete Sachvorgang Gegenstand einer Berichtspflicht oder einer Zuarbeit für den Petitionsausschuss des Landtages wird. Eine Aufbewahrung erscheint daher insoweit erforderlich, als nach realistischer Einschätzung unter Berücksichtigung der betroffenen Grundrechte und der Fürsorgepflicht gegenüber dem betroffenen Mitarbeiter die Bearbeitung des Vorgangs aus datenschutzrechtlicher Sicht noch nicht vollständig abgeschlossen ist. In ganz besonders gelagerten Einzelfällen kann ggf. berücksichtigt werden, dass ein Beschwerdeführer in regelmäßigen Abständen nach wenigen Monaten erneut Beschwerden vorbringt, wenn sich diese überwiegend inhaltlich auf vorherige Vorgänge beziehen. Grundsätzlich ist jedoch die bloße Möglichkeit, dass in der Folgezeit noch weitere Beschwerden folgen, sei es über

den betroffenen Mitarbeiter, sei es vom betroffenen Beschwerdeführer, keine Rechtfertigung für die langfristige Aufbewahrung personenbezogener Informationen.

Auch eine auf die Vorgaben der Aktenordnung abstellende 5-jährige Aufbewahrung entspricht nicht den datenschutzrechtlichen Erfordernissen. Dabei ist zu beachten, dass die Vorgänge Beschwerden enthalten, die entweder unbegründet oder zumindest nicht gerichtsfest nachweisbar sind. Wären die Beschwerden jedoch zunächst als begründet angesehen und in die Personalakte übernommen worden, wären sie bei nachträglicher Erkenntnis der Unbegründetheit unverzüglich aus der Personalakte zu entfernen und zu vernichten (§ 90e Abs. 1 Satz 1 Nr. 1 BG LSA). Selbst wenn die Beschwerden begründet gewesen wären, wären die Vorgänge nach Eingang in die Personalakte spätestens nach drei Jahren zu entfernen und zu vernichten (§ 90e Abs. 1 Satz 1 Nr. 2 BG LSA). Bedienstete, gegen die unbegründete Vorwürfe erhoben wurden bzw. denen nichts nachzuweisen war, wären also schlechter gestellt als diejenigen, die von begründeten Beschwerden betroffen sind.

16.7 Videoüberwachung während der Dienstzeit

Um Bauarbeiten in einem Dienstgebäude überwachen zu können, ließ eine Behörde in einem Dienstzimmer eine verdeckte Videokamera installieren. Von dieser Maßnahmen hatten der Leiter der Abteilung, der Installateur der Videokamera und der Mitarbeiter, dem dieses Dienstzimmer gehört, Kenntnis. Da die Baumaßnahmen über die regelmäßige Dienstzeit fortwährten, wurde die Videoüberwachung 24 Stunden täglich durchgeführt.
Aufgrund der Baumaßnahmen wurde der Kopierer im besagten videoüberwachten Dienstzimmer aufgestellt. Eine Information an alle Bediensteten, welche den Kopierer nutzen mussten, unterblieb.

Die heimliche Videoüberwachung stellt einen Eingriff in das durch Art. 2 Abs. 1 GG geschützte allgemeine Persönlichkeitsrecht eines Arbeitnehmers dar (BAG-Urteil vom 27. März 2003 - NJW 2003, S. 3436).
Dieser Eingriff in das Persönlichkeitsrecht kann zwar bei Wahrnehmung überwiegender schutzwürdiger Interessen des Arbeitgebers gerechtfertigt sein. Dies setzt aber eine Güterabwägung im Einzelfall voraus. Die heimliche Videoüberwachung eines Arbeitnehmers wäre danach zulässig, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers bestünde, weniger einschneidende Mittel zur Aufklärung des Verdachts ausgeschöpft wären, die versteckte Videoüberwachung praktisch das einzig verbleibende Mittel darstellte und insgesamt nicht unverhältnismäßig wäre.

Die Überprüfung des Sachverhaltes ergab, dass eine Rechtsgrundlage für diesen erheblichen Eingriff in die Persönlichkeitsrechte der Mitarbeiter zu keinem Zeitpunkt vorgelegen hat. Alle erfolgten Aufzeichnungen wurden aktenkundig vernichtet.

Der Vorfall wurde zum Anlass genommen, in dieser Behörde die Leitungsebene für die Einhaltung der Persönlichkeitsrechte aller Mitarbeiter zu sensibilisieren.

16.8 Personaldatenschutz bei der Benutzung von Druckern

Durch den Hinweis eines Mitarbeiters erhielt der Landesbeauftragte davon Kenntnis, dass in einer größeren Dienststelle ein Netzwerkdrucker für die Mitarbeiter des Personalamtes in der Teeküche installiert worden sein sollte und somit allen Mitarbeitern, die diese Teeküche aufsuchen, Personaldaten bekannt werden könnten.
Auf eine erste Anfrage hin wurde der Sachverhalt bestätigt. Die Dienststelle wies jedoch darauf hin, dass es eine Dienstanweisung gäbe, in der die sofortige Abholung eines Schriftstückes nach Auslösung des Druckauftrages geregelt sei. Diese Dienstanweisung würde von den Mitarbeitern der Personalabteilung auch strikt eingehalten und häufig vom Abteilungsleiter kontrolliert.

Aus Sicht des Landesbeauftragten genügen diese Sicherheitsvorkehrungen jedoch nicht. Für den Umgang mit Personaldaten gelten die Vorschriften der §§ 90 ff. BG LSA i.V.m. § 28 Abs. 1 DSG-LSA für alle Beschäftigten des öffentlichen Dienstes.
Die Daten sind vertraulich zu behandeln und vor unbefugter Einsicht zu schützen. Das bedeutet, dass gem. § 90 Abs. 3 BG LSA Zugriff auf Personaldaten nur der konkret zuständige Mitarbeiter haben darf. Der Grundsatz der informationellen Gewaltenteilung gilt auch innerhalb einer datenschutzrechtlich verantwortlichen Stelle.

Gemäß § 6 DSG-LSA hat jede öffentliche Stelle die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Einhaltung des Datenschutzes zu gewährleisten. Dazu gehört nach Abs. 2 Nr. 1 der Vorschrift auch die Gewährleistung der Vertraulichkeit. Unter Berücksichtigung des Personalaktengeheimnisses, der teilweise erfassten und besonders geschützten Gesundheitsdaten, der Anzahl der Beschäftigten, der Größe der Einrichtung und der gesunkenen Kosten für Drucktechnik ist ein angemessenes Datenschutzniveau zu erzielen.

Selbst wenn sich der Mitarbeiter sofort nach dem Absenden des Druckauftrages in die Teeküche begibt und seinen Ausdruck aus dem Drucker nimmt, besteht die Gefahr, dass sich andere Mitarbeiter in der Teeküche befinden und Kenntnis vom Inhalt des Ausdrucks erhalten. Auch sind gelegentliche Ablenkungen der zuständigen Mitarbeiter durch Telefon- oder E-Mail-Verkehr nicht ausgeschlossen. Das Risiko liegt in der grundsätzlichen Zugänglichkeit des Druckers in einem unverschlossenen, von mehreren Personen genutzten Raum. Durch das im Regelfall korrekte Verhalten der Mitarbeiter wird das Risiko nur gemindert, aber nicht hinreichend ausgeschlossen.

Aus technisch-organisatorischer Sicht war hier zu empfehlen, separate Drucker für die einzelnen Bereiche der Personalabteilung in nicht frei zu-

gänglichen Räumen zu installieren. Möglich wäre auch die Installation eines Netzwerkdruckers, bei dem die Ausführung des Druckauftrags erst nach Eingabe einer PIN vom Mitarbeiter vor Ort ausgelöst wird.

Die Dienststelle teilte abschließend mit, dass die Teeküche vorerst verschlossen und jede Mitarbeiterinnen der Personalabteilung mit einem Schlüssel ausgestattet wird. Als weiteres Vorhaben ist jedoch der Austausch des vorhandenen Druckers gegen einen PIN-Drucker geplant.

16.9 Einrichtung von Heimarbeitsplätzen (HAP)

Aufgrund der Umstrukturierung der Landesverwaltung im Berichtszeitraum wurde der Landesbeauftragte von einer Behörde gefragt, ob es im Rahmen der Einführung flexibler Arbeitszeiten in Form alternierender Heim- und Telearbeit (mit überwiegend zwei Arbeitstagen Beschäftigung am Dienstort) die Möglichkeit der Einrichtung von HAP gäbe, bei denen Sozialdaten erhoben, genutzt und verarbeitet würden.

Der Landesbeauftragte gab hierzu folgende Hinweise:

Im Allgemeinen wird der Erhebung, Nutzung und Verarbeitung von Sozialdaten an HAP sehr kritisch begegnet. Das in § 35 Abs. 1 SGB I normierte Sozialgeheimnis umfasst die Verpflichtung sicherzustellen, dass Sozialdaten nur Befugten zugänglich sind und auch nur an diese weitergegeben werden. Aufgrund der Gefährdung des Sozialgeheimnisses beim Transport der Daten zwischen Dienstort und Wohnung sowie der Gefährdungen im häuslichen Umfeld ist die Heimarbeit technisch und organisatorisch besonders abzusichern. Der Dienststellenleiter hat in besonderer Weise seinen Aufsichts-, Fürsorge- und Kontrollpflichten nachzukommen.

Die Dienststelle hat eine Vereinbarung mit dem Bediensteten abzuschließen, in welcher er verpflichtet wird, das Sozialgeheimnis zu wahren und alle erforderlichen technisch-organisatorischen Maßnahmen zur Einhaltung des Datenschutzes zu treffen (§ 6 Abs. 2 DSG-LSA; § 78a SGB X). Der Bedienstete ist zu verpflichten, Beauftragten der Dienststelle, Sicherheits- und Datenschutzbeauftragten auch kurzfristig Zugang zum häuslichen Arbeitsplatz zu gewähren. Der Bedienstete hat zu versichern, dass Personen, die mit ihm in häuslicher Gemeinschaft leben, mit diesem Zutrittsrecht einverstanden sind. Sollte der Bedienstete o.g. Vertretern seiner Dienststelle den Zutritt verweigern, so muss dies die sofortige Beendigung der Heimarbeit zur Folge haben.

Technisch-organisatorisch sind u.a. folgende Hinweise zu beachten:
Die private Nutzung des Heimarbeitsplatz-Rechners (HAP-PC) und der Datenträger ist zu untersagen.

Alle dienstlichen Unterlagen und Datenträger, die personenbezogene Daten enthalten, sind während des Transports zwischen der Dienststelle und dem häuslichen Arbeitsplatz in einem geeigneten und entsprechend gegen den Zugriff Unbefugter gesicherten Transportbehälter aufzubewahren.

Die Speicherung der personenbezogenen Daten auf dem HAP-PC sowie auf den Datenträgern hat verschlüsselt zu erfolgen. Nach jeder Arbeitssitzung sind die Daten auf einem Speichermedium zu sichern. Sobald der Zweck der Datenverarbeitung erfüllt ist, sind die personenbezogenen Daten vom HAP-PC und den Datenträgern zu löschen. Nicht mehr erforderliche Unterlagen mit personenbezogenem Inhalt sind in der Dienststelle zu vernichten. Zum Löschen der personenbezogenen Daten vom HAP-PC und den Datenträgern muss eine Software installiert werden, die verhindert, dass die Daten wiederhergestellt werden können, d.h. die Daten sind physisch zu löschen.

Eine Zugangssoftware sollte sicherstellen, dass der HAP-PC nicht von Unbefugten genutzt werden kann. Gleichzeitig sind entsprechende Passwortvorgaben erforderlich, die verhindern, dass triviale Passwörter verwendet werden, welche leicht zu erraten sind. Entsprechend der Sensibilität der Daten ist der Einsatz von Chipkarten zu empfehlen.

Ein Zugang des HAP-PC zum Internet ist abzulehnen. Um die installierte Antiviren-Software ständig zu aktualisieren, empfiehlt es sich, für den Transport der personenbezogenen Daten ein Speichermedium zu verwenden, mit dem gleichzeitig die jeweils aktuelle Virendefinitionsdatei aus dem Behördennetz kopiert und manuell auf den HAP-PC übertragen werden kann. Alternativ dazu könnte eine besonders abgesicherte Einwahlmöglichkeit vom HAP-PC in das Behördennetz eingerichtet werden. Über diese Verbindung könnten dann neben den aktuellen Virendefinitionsdateien auch die personenbezogenen Daten verschlüsselt übertragen werden, so dass ein manueller Transport der Datenträger entfällt.

Der HAP-PC ist durch entsprechende Zugriffsrechte oder Zusatztools so abzusichern, dass der jeweilige Mitarbeiter nicht in der Lage ist, Software zu installieren bzw. zu deinstallieren oder Veränderungen an der Konfiguration vorzunehmen, wie z.B. die Einrichtung eines Internetzugangs. Die Berechtigung sollte nur den dafür zuständigen Mitarbeitern der Dienststelle vorbehalten sein.

Grundsätzlich ist die Verarbeitung personenbezogener Daten auf HAP mit größeren Risiken verbunden, als dies bei dienstlichen Arbeitsplätzen der Fall ist. Die genannten Hinweise sollen den behördlichen Datenschutzbeauftragten im Rahmen der **Vorabkontrolle** gem. § 14a Abs. 4 Nr. 2 DSG-LSA bei der Bewertung der Geeignetheit eines HAP für die Erhebung, Nutzung und Verarbeitung **personenbezogener Daten besonderer Art** unterstützen.

16.10 Beteiligung der Personalvertretung

Ein Landkreis teilte im Rahmen einer Prüfung mit, dass er frühzeitig und effizient die nach dem Personalvertretungsrecht erforderliche Beteiligung der Personalvertretung angehe. In Fällen, in denen mitbestimmungspflichtige Maßnahmen wahrscheinlich erscheinen, würde ein Mitglied der Personalvertretung bereits zur ersten Anhörung des Mitarbeiters zum Sach-

verhalt hinzugezogen. Die frühzeitige Einbeziehung erleichtere die ggf. folgende Beteiligung der Personalvertretung.

Informationsgrundlage für die Personalvertretung ist die Vorschrift des § 57 Abs. 2 PersVG LSA. Die Verpflichtung zur rechtzeitigen Beteiligung dient dem Prüfungs- und Gestaltungsspielraum der Personalvertretung. Die Übermittlung von Personaldaten schon im Stadium der Anhörung des betroffenen Mitarbeiters ist jedoch in der Regel nicht erforderlich. In diesem Stadium wird noch der Sachverhalt ermittelt, der gegebenenfalls erst zur Entscheidung führen kann, eine mitbestimmungspflichtige Maßnahme durchzuführen. Zwar besteht ein nachvollziehbares Interesse der Dienststelle, die Personalvertretung vorab einzubeziehen. Gegenüber diesem Interesse überwiegt jedoch der verfassungsrechtlich garantierte Persönlichkeitsschutz des betroffenen Mitarbeiters. Dieser kann unter Umständen ein Interesse daran haben, die Anhörung ohne die Personalvertretung durchzuführen. Die Prüfungs- und Gestaltungsmöglichkeiten der Personalvertretung werden hierdurch nicht beeinträchtigt. Die generelle vorsorgliche Beteiligung der Personalvertretung ist deshalb ohne die vorherige ausdrückliche Einwilligung des Betroffenen unzulässig. Hierauf wurde der Landkreis hingewiesen.

16.11 Leseberechtigung des Personalrates im Stellenbewirtschaftungsmodul

In einer Behörde wurde ein neues Personalverwaltungssystem installiert. Da hier nun für jeden Bearbeiter bestimmte Rechte (Lese- und Bearbeitungsrechte) vergeben werden konnten, beantragte der Personalrat das Leserecht für das Stellenbewirtschaftungsmodul.
Die Behörde meinte, dass hier zu viele Daten ständig für den Personalrat bereitgestellt würden.

Grundsätzlich regelt § 57 Abs. 2 PersVG LSA den Umfang und die Art und Weise der Unterrichtung des Personalrates durch die Dienststelle. Danach besteht eine Unterrichtungspflicht nur, soweit sie zur Durchführung der Aufgaben des Personalrats erforderlich ist. § 57 Abs. 2 PersVG LSA gibt somit keine Handhabe dafür, jegliche allgemeine Vorabinformationen zum Personal losgelöst von konkreten personalrechtlichen Aufgaben zu erhalten. Auch bei der Erfüllung der allgemeinen Aufgaben des Personalrates, so z.B. bei der Überwachung, dass die zugunsten der Beschäftigten geschaffenen Bestimmungen durchgeführt werden, können dem Informationsanspruch Grenzen gesetzt sein.
Dies ist der Fall, wenn der Unterrichtung höherrangige Rechte der Beschäftigten entgegenstehen (Personalaktendatenschutz). Ebenso ist der Grundsatz der Datensparsamkeit zu beachten.
Natürlich benötigt der Personalrat die Informationen oft frühzeitig, um seine Aufgaben erfüllen zu können. Der Anspruch auf umfassende und rechtzeitige Unterrichtung erfasst sämtliche Aufgaben des Personalrates und erstreckt sich auch auf die erforderlichen personenbezogenen Daten, die in Dateien gespeichert sind. Allerdings hat der Personalrat nicht das Recht, Daten für ein künftiges Tätigwerden zu sammeln und vorzuhalten.

Die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten durch den Personalrat ist gem. §§ 9 Abs. 1, 10 Abs. 1 DSG-LSA nur zulässig, soweit dies zur Aufgabenerfüllung erforderlich ist. Infolge der umfassenden Unterrichtungsmöglichkeiten ist die eigene Verarbeitung (§ 2 Abs. 5 DSG-LSA) personenbezogener Daten beim Personalrat daher grundsätzlich unzulässig. Die Führung von Personalnebenakten und die Vorratsdatenhaltung würden gegen das Grundrecht auf informationelle Selbstbestimmung verstoßen.

In Abhängigkeit von den Gegebenheiten und auch der Größe der Dienststelle kann es aber ggf. unabhängig vom jeweiligen Einzelvorgang zur Aufgabenerfüllung des Personalrates dennoch erforderlich sein, einige Grunddaten der Beschäftigten zur Verfügung zu haben. Einzelne Grunddaten (z.B. Name, Familienstand, Dauer der Dienststellenzugehörigkeit, Beförderungsdaten, Eingruppierung) können aufgabenbedingt vorgehalten werden, wenn es dem Personalrat nicht mehr zuzumuten ist, regelmäßig benötigte Informationen jedes Mal erneut zu erfragen. Bei der Beurteilung der Zulässigkeit und des Umfanges ist aus dem o.g. Gründen ein enger Maßstab anzulegen.

Die erforderlichen Unterlagen sind dem Personalrat in geeigneter Weise zugänglich zu machen. In welcher Weise dies geschieht, hängt von der Art und dem Inhalt der Unterlagen ab und davon, wie eingehend und häufig sich der Personalrat mit den Unterlagen befassen muss, um die Aufgaben wirksam erfüllen zu können. Die Möglichkeiten reichen vom Einblick in die Papiere bis zur befristeten oder dauerhaften Überlassung einer Aufstellung.

Somit ist ein ständiges Leserecht des Personalrates im automatisiert vorgehaltenen Stellenplan nicht zwingend erforderlich, wenn die Unterlagen oder Informationen auch auf anderem Weg zur Verfügung gestellt werden können. Insbesondere ist zu vermeiden, dass der Personalrat auf personenbezogene Daten zugreifen kann, die er nicht zur Aufgabenerfüllung benötigt.

16.12 Zielnummernerfassung bei dienstlichen Telefonaten von Personalratsmitgliedern

Durch Hinweise aus verschiedenen Dienststellen wurde der Landesbeauftragte darauf aufmerksam gemacht, dass die Zielnummernerfassung bei dienstlichen Telefonaten von Personalratsmitgliedern problematisch sei, da der Kontakt und damit die Aktivitäten der Personalratsmitglieder auf einzelne Beschäftigte zurückzuführen wäre.

Grundsätzlich besteht ein allgemeines Kontrollrecht der Dienststellenleitung über die vom Personalrat geführten Telefonate nur hinsichtlich der Haushaltsverträglichkeit. Der Personalrat darf ebenso wenig außerdienstliche Gespräche über seinen Apparat auf Kosten der Dienststelle führen, wie dies auch andere Beschäftigte dürfen.

Im gemeinsamen Runderlass des MF und MI vom 9. April 1999 - Az. 22. 02614 - (MBl. LSA S. 565) "Allgemeine Richtlinien über die Errichtung und Benutzung dienstlicher Telekommunikationsanlagen in Landesbehörden und -dienststellen (TKR)", welcher auch unter der Mitwirkung des Landesbeauftragten entstand, sind unter Ziff. 8 der Anlage zur TKR (Sonderregelung) Festlegungen für Personalvertretungen in Personalratsangelegenheiten getroffen; danach ist hier nur die Speicherung von Verbindungsgebühren zulässig.

16.13 Stasiunterlagengesetz

Die Prüfung eines Landkreises ergab, dass die Auskünfte der Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (BStU), die keine Hinweise auf eine Zusammenarbeit mit dem Ministerium für Staatssicherheit (MfS) beinhalten, in die Personalakten eingefügt werden. Die Mitarbeiter bekommen keine Kopien, könnten jedoch Einsicht nehmen. Sämtliche Mitteilungen der BStU, die Hinweise auf eine Zusammenarbeit mit dem MfS enthalten, werden zentral im Rechtsamt aufbewahrt. Dort ist der Personalausschuss angesiedelt, für dessen Bewertungen die Mitteilungen ausschließlich verwendet werden. Notwendige Maßnahmen setzt dann das Personalamt um. Im Übrigen bleiben die Unterlagen im Rechtsamt.

Der Landesbeauftragte wies darauf hin, dass die Mitteilungen der BStU als Entscheidungsgrundlage für die Einstellung bzw. Weiterbeschäftigung der Mitarbeiter dienten. Sie stehen daher in unmittelbarem Zusammenhang mit dem Dienstverhältnis und sind demgemäß Bestandteil der Personalakte. Hierauf hatte der Landesbeauftragte bereits in früheren Tätigkeitsberichten aufmerksam gemacht (II. Tätigkeitsbericht, Ziff. 18.5; III. Tätigkeitsbericht, Ziff. 18.5).

Anhaltspunkte dafür, dass der Landkreis gesonderte Teilakten führte, bestanden nicht. Vielmehr sprach die Aufbewahrung der Mitteilungen ohne Hinweis auf eine Zusammenarbeit mit dem MfS in den Personalakten dafür, dass Mitteilungen mit Hinweisen auf eine Zusammenarbeit im Rechtsamt nicht als Personalaktenbestandteil aufgefasst wurden. Unbeschadet eventueller Sachvorgänge eines Personalausschusses sollten aber die Mitteilungen insgesamt in der Personalakte geführt werden. Im Einzelfall wäre dann zu prüfen, inwieweit Vorgaben der BStU im Hinblick auf das eingeschränkte Einsichtsrecht von Mitarbeitern des Staatssicherheitsdienstes nach § 16 Abs. 4 und 5 StUG und die überwiegenden Interessen von Betroffenen oder Dritten (z.B. durch Aufnahme der Anlagen der Mitteilung in verschlossenen Umschlägen) Rechnung getragen werden kann.

17. Polizei

17.1 Novellierung des SOG LSA - Neues zur Gefahrenabwehr

Im Berichtszeitraum wurde das Gesetz über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt (SOG LSA) durch das Dritte Gesetz zur Änderung des SOG LSA vom 10. Juli 2003 (GVBl. LSA S. 150) geändert und am 23. September 2003 als Neufassung bekanntgemacht. Die Änderung erstreckte sich im Wesentlichen auf die Änderung der **Vorschriften zur Rasterfahndung** und die **Einführung der Videoaufzeichnungen** von öffentlichen Flächen.

17.1.1 Rasterfahndung

Nach § 31 SOG LSA kann eine Rasterfahndung nunmehr bereits „... zur Verhütung von Straftaten von erheblicher Bedeutung ...“ eingeleitet werden, „... wenn auf Tatsachen beruhende Anhaltspunkte die Annahme rechtfertigen, dass dies zur Verhütung dieser Straftaten erforderlich und auf andere Weise nicht möglich ist.“ Mit dieser Änderung ist die Rasterfahndung nunmehr nicht mehr nur auf die Abwehr einer gegenwärtigen Gefahr ausgerichtet. Vielmehr soll sie **zur Abwehr** künftiger - und damit **lediglich wahrscheinlicher - Straftaten** dienen. Dieser Umstand und die Änderung, dass künftig die - wenn auch gerechtfertigte - Annahme zur Einleitung einer Rasterfahndung ausreicht, zeigen, dass die Zulässigkeitsschranken deutlich gesenkt worden sind.
Auch der Wegfall der richterlichen Zustimmung vor der Durchführung einer Rasterfahndung ist ein gewichtiger Kritikpunkt. Die nunmehr erforderliche bloße polizeiliche Anordnung erscheint unter Berücksichtigung des Ausmaßes der möglichen Eingriffe unzulänglich. Der richterliche Zustimmungsvorbehalt bildete allein aufgrund der Unabhängigkeit der Richterschaft einen wesentlichen Schutz der Bürgerinnen und Bürger vor unzulässigen Rasterfahndungen.

Aufgrund der dargestellten, die Rechtsposition der Einwohner ausschließlich verschlechternden Veränderungen hält der Landesbeauftragte an seinen Feststellungen aus dem VI. Tätigkeitsbericht (Ziff. 17.1.2) fest. Die Änderungen des SOG LSA in Bezug auf die Rasterfahndung sind aus Sicht des Schutzes der personenbezogenen Daten der Bürger ein weiterer Schritt auf dem Weg zur Überwachung auch rechtstreuer Bürgerinnen und Bürger.

17.1.2 Videoaufzeichnungen

Der Landesbeauftragte hat in der Vergangenheit bereits mehrfach auf die Problematik der **Videoüberwachung und Videoaufzeichnung** hingewiesen. Zuletzt stellte er in seinem VI. Tätigkeitsbericht (Ziff. 17.1.1) einen Gesetzesvorschlag der Landesregierung für eine Änderung des SOG LSA vor, künftig nicht nur Videoüberwachungen, sondern auch Videoaufzeichnungen an sog. Kriminalitätsschwerpunkten durchführen zu lassen.

Die Videoüberwachung öffentlicher Plätze ist als Instrument der Kriminalitätsbekämpfung bereits seit dem Jahr 2000 im SOG LSA verankert. 2003 kam nun auch die Möglichkeit hinzu, Videoaufzeichnungen von Kriminalitätsschwerpunkten anzufertigen (§ 16 Abs. 2). Zur Unterscheidung sei darauf hingewiesen, dass im Falle der Videoüberwachung die Bilder ausschließlich das aktuelle Geschehen auf Monitore übertragen. Eine Aufzeichnung findet dabei nicht statt.
Auf die datenschutzrechtlichen Bedenken gegen Videoaufzeichnungen hat der Landesbeauftragte ausführlich hingewiesen. Der Landesbeauftragte hält nach wie vor an seiner Einschätzung fest, dass der Nutzen von Aufzeichnungsmöglichkeiten nicht hinreichend nachgewiesen ist.

17.2 Beendigung der Rasterfahndung nach dem 11. September 2001

Aus Anlass des 11. September 2001 wurde nach Einführung der entsprechenden gesetzlichen Regelungen in den einzelnen Bundesländern eine bundesweite **Rasterfahndung** nach sogenannten Schläfern eingeleitet. In Sachsen-Anhalt wurden ca. 66.000 Personendatensätze beim Landeskriminalamt angeliefert. Nach einem automatisierten Abgleich verblieben 1.292 sogenannte Prüffälle. In der weitergehenden Bearbeitung wurden die Prüffälle einer permanenten Überprüfung hinsichtlich der Rasterkriterien unterzogen. Durch die Feststellung von Ausschlusskriterien wurde die Anzahl der Prüffälle stetig reduziert.

Durch die Koordinierungsgruppe „Internationaler Terrorismus“ beim Bundeskriminalamt wurde beschlossen, dass die Rasterfahndung unter dem Blickpunkt des internationalen **Terrorismus** am 31. März 2003 zu beenden ist.

In Sachsen-Anhalt wurden laut Darstellung des Landeskriminalamtes die im Rahmen der Rasterfahndung erhobenen Daten am 1. April 2003 vollständig gelöscht. Allerdings haben aus der Rasterfahndung gewonnene Datensätze fälschlicherweise Eingang in andere polizeiliche Datenbanken gefunden, sollen aber dort inzwischen ebenso gelöscht worden sein. Den Ablauf der Löschung wird sich der Landesbeauftragte noch vor Ort darstellen lassen.

17.3 Störungen im privaten Telefonanschluss

Im Berichtszeitraum haben sich wiederholt Bürger an den Landesbeauftragten gewandt, weil sie Störungen in ihren privaten Telefonanschlüssen auf Telekommunikationsüberwachungsmaßnahmen zurückführten. Die Bürger fühlten sich zu unrecht diesen Maßnahmen ausgesetzt.

Die Ermittlungen durch den Landesbeauftragten haben ergeben, dass von öffentlichen Stellen des Landes gegen keinen der Bürger Maßnahmen der Telekommunikationsüberwachung durchgeführt wurden.

Die geschilderten Störungen deuteten auf technische Probleme hin. Die Petenten wurden darauf verwiesen, sich zunächst an die jeweiligen Telefonnetzbetreiber zu wenden.

17.4 Die Polizei als „Freund und Helfer“

Durch die Mitteilung einer Meldebehörde wurde dem Landesbeauftragten bekannt, dass durch Polizisten eines Polizeireviers **Meldeauskünfte** kostenfrei an Privatpersonen erteilt wurden.

Im Einzelnen stellte sich der Sachverhalt so dar, dass sich eine Privatperson zur Erlangung einer Meldeauskunft telefonisch an die zuständige Meldebehörde gewandt hatte. Die Privatperson hatte vorgetragen, die Meldeauskunft zur Habhaftwerdung eines Mietschuldners zu benötigen. Durch die Meldebehörde war mitgeteilt worden, dass eine solche Meldeauskunft gebührenpflichtig ist. Daraufhin erklärte die Privatperson, dass sie sich an die Polizei wenden werde, weil sie dort jemanden kenne und die entsprechende Auskunft schneller und kostenfrei erhalten könne.

Seitens der Meldebehörde wurde nun die Protokollierung zu den Abfragen des örtlichen Polizeireviers eingesehen. Dabei wurde festgestellt, dass nur zehn Minuten nach dem Anruf bei der Meldestelle eine Abfrage zu dem betreffenden Mietschuldner durch das Polizeirevier vorgenommen wurde.

Zum technischen Hintergrund sei erläutert, dass das Polizeirevier über einen Computer direkt Abfragen im Melderegister vornehmen kann. Die Abfragen werden jedoch bei der Meldebehörde protokolliert. Allerdings konnte dort nicht festgestellt werden, wer konkret den unzulässigen Abruf ausgeführt hatte, da für das Polizeirevier nur ein Benutzername eingerichtet worden war. Durch den Landesbeauftragten wurde das örtliche Polizeirevier einer anlassbezogenen Prüfung unterzogen. Zu den dabei festgestellten Mängeln und weitergehenden technischen Einzelheiten wird auf Ziff. 12.1 verwiesen.

Verantwortlich für einen sicheren Zugriff auf das Melderegister ist jedoch die Meldebehörde, welche auch den Computer zur Verfügung stellt. Die Mängel bei der Einrichtung des Abrufverfahrens wurden durch die Meldebehörde in Abstimmung mit dem Landesbeauftragten behoben.

Unabhängig von den technischen Gegebenheiten bleibt natürlich festzustellen, dass seitens der Polizei der Zugriff auf das Melderegister unzulässig erfolgte. Die Polizei darf Abfragen nur vornehmen, wenn diese zur Erfüllung dienstlicher Belange erforderlich sind. Darauf wurden die Polizeibediensteten nochmals hingewiesen. Zudem wurde zur Nachvollziehbarkeit der Abfragen ein Nachweisbuch eingeführt, in dem jede Abfrage hinsichtlich der Person des Abfragenden protokolliert wird.

17.5 Verkehrskontrollen mit „Zuschauern“

Die Anfrage eines Mitgliedes des Landtages an den Polizeibereich gab Anlass, sich erneut zur rechtlichen Zulässigkeit der **Teilnahme von Dritten an Verkehrskontrollen** vor Schulen bzw. an Schulwegen zu äußern. An Verkehrsaktionen wie „Pro Kids“ haben bereits Pressevertreter und/ oder Schulkinder teilgenommen. Nunmehr wollte auch ein Mitglied des Landtages zum wiederholten Male bei einer solchen polizeilichen Maßnahme anwesend sein.
Aus datenschutzrechtlicher Sicht bestehen erhebliche Bedenken gegen die Teilnahme von Dritten an einer solchen Verkehrskontrolle. Darauf wurde bereits nach Bekanntwerden der Verkehrsaktion „Pro Kids“ aufmerksam gemacht. Durch die Polizei wurde damals sichergestellt, dass Dritten - einschließlich der Presse - kein Einblick in die eigentliche polizeiliche Tätigkeit möglich war. Jede Person, die im Rahmen einer polizeilichen Verkehrskontrolle zur Offenlegung personenbezogener Daten verpflichtet wird, hat das Recht, dass diese Daten nur zu dem Zweck der Erhebung verwendet und nicht Dritten bekannt gegeben werden. Wenn Pressevertreter oder auch Schulkinder einer Maßnahme wie dem Aufnehmen der Personalien beiwohnen würden, wäre dies ein unzulässiger Eingriff in das Recht des Betroffenen auf den Schutz seiner personenbezogenen Daten.

Auch ein Mitglied des Landtages ist rechtlich gesehen ein Dritter, der an einer polizeilichen Maßnahme teilnehmen und insoweit die Rechte des Betroffenen auf den Schutz seiner personenbezogenen Daten verletzen würde. Auch ihm ist die Teilnahme aus diesem Grund zu verweigern.

Das Ministerium des Innern des Landes Sachsen-Anhalt hat das betreffende Mitglied des Landtages in Abstimmung mit dem Landesbeauftragten über die bestehende Rechtslage informiert.

18. Rechtspflege

18.1 Kennzeichnung von Daten aus besonderen Erhebungsmaßnahmen

Bereits im VI. Tätigkeitsbericht (Ziff. 25) hatte der Landesbeauftragte darauf hingewiesen, dass Daten, welche aus besonders eingriffsintensiven Erhebungsmaßnahmen stammen, zur Sicherung der Zweckbindung besonders zu kennzeichnen sind.
Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat durch eine entsprechende Entschließung besonders die Pflicht zur Kennzeichnung so gewonnener Daten, wie es das Bundesverfassungsgericht in seinem Urteil zur strategischen Fernmeldeüberwachung des Bundesnachrichtendienstes dargelegt hat, betont und festgestellt, dass diese Pflicht nicht auf den Bereich der Fernmeldeüberwachung beschränkt ist **(Anlage 2).**

Auch die Entscheidung des Bundesverfassungsgerichts zur Verfassungsmäßigkeit des sog. Großen Lauschangriffs hat die bereits bisher vertrete-

ne Rechtsauffassung des Gerichts fortgeschrieben und eine entsprechende Kennzeichnung der durch diese besondere Maßnahme erlangten Daten zur Sicherung der Grundrechte des Einzelnen für erforderlich gehalten.

18.2 Urteil des Bundesverfassungsgerichts zum Großen Lauschangriff

Am 3. März 2004 hat das Bundesverfassungsgericht (BVerfG) über die Verfassungsmäßigkeit des sog. Großen Lauschangriffs entschieden (NJW 2004, 999). Die Klage war u.a. von Abgeordneten des Deutschen Bundestages eingereicht worden. Das BVerfG beteiligte den Landesbeauftragten am Verfahren; er hat eine Stellungnahme abgegeben.

Vom ersten Senat des BVerfG wurde die Regelung in Art. 13 Abs. 3 GG mehrheitlich für verfassungsgemäß erachtet.
Die Umsetzung des Gesetzgebers in entsprechende strafprozessuale Eingriffsbefugnisse sah das Gericht in weiten Teilen jedoch für verfassungswidrig an, denn durch diese werde gegen die Menschenwürde verstoßen, indem der **Kernbereich privater Lebensgestaltung** beeinträchtigt bzw. nicht respektiert werde. Dies betrifft insbesondere § 100c Strafprozessordnung (StPO), nach dessen Abs. 1 Nr. 3 das in einer Wohnung nicht öffentlich gesprochene Wort eines Beschuldigten abgehört und aufgezeichnet werden darf, wenn bestimmte Tatsachen den Verdacht begründen, dass er in einem Straftatenkatalog näher bezeichnete Straftaten begangen hat.
In seinem Urteil hat das BVerfG klargestellt, dass die Unverletzlichkeit der Wohnung einen engen Bezug zur Menschenwürde und zum Gebot der unbedingten Achtung einer Sphäre zur ausschließlich privaten Entfaltung hat. Auch wenn es um die Effektivität der staatlichen Strafrechtspflege und die Erforschung der Wahrheit gehe, dürfe dieser Kernbereich des Privaten von staatlicher Seite auch bei überwiegenden **Interessen der Allgemeinheit** nicht angetastet werden. Dabei macht das Gericht deutlich, dass nicht jeder Lauschangriff die Menschenwürde verletzt. So gehören Gespräche über begangene Straftaten nicht zum Kernbereich privater Lebensgestaltung.

Hinsichtlich der notwendigen Neuregelung der akustischen Wohnraumüberwachung hat das BVerfG u.a. darauf hingewiesen, dass

- die Überwachung von Gesprächen mit engsten Familienangehörigen oder Vertrauten sowie bestimmten Berufsgeheimnisträgern nur zulässig sei, wenn die Gesprächsinhalte keinen absoluten Schutz erfordern, was insbesondere bei Tatbeteiligung der Gesprächspartner oder bei besonderem Bezug zur jeweiligen Straftat denkbar sei. Allerdings bestehe eine **Vermutung**, dass Gespräche mit Familienangehörigen oder engsten Vertrauten in der Privatwohnung zum Kernbereich privater Lebensgestaltung gehören

- eine Regelung hinsichtlich einer **konkreten Prognose** zur Zeit der Anordnung und zu einer laufenden Überwachung der jeweiligen Abhörmaßnahme nötig sei

- es an einer ausreichend konkreten Bestimmung fehle, die, bei Rechtswidrigkeit der Erhebung, den **Abbruch** der Maßnahme, ein **Verwertungsverbot** sowie die Verpflichtung zur **Datenlöschung** regele

- nur Anlasstaten in Betracht kämen, welche bei abstrakter Betrachtung besonders schwerwiegend seien (Höchststrafe **über 5 Jahre Freiheitsstrafe**)

- gesetzliche Festlegungen zur **Konkretheit** von Inhalt und schriftlicher Begründung der Anordnungen von Wohnraumüberwachungen getroffen werden müssen

- § 101 Abs. 1 Satz 1 StPO, welcher Ausnahmen von der **Benachrichtigungspflicht** gegenüber von einem Lauschangriff Betroffenen zulässt, **zu weit** gehe, soweit die Benachrichtigung davon abhängig gemacht werde, dass sie ohne Gefährdung der öffentlichen Sicherheit oder der weiteren Verwendung eines eingesetzten, nicht offen ermittelnden Beamten nicht erfolgen könne

- Benachrichtigungen **Drittbetroffener** (z.B. Gäste, Wohnungsinhaber, Mitbewohner) grundsätzlich notwendig seien, es sei denn, der Grundrechtseingriff werde dadurch vertieft. Außerdem genüge es nicht, die Zurückstellungen der Information Drittbetroffener nur einmalig zu kontrollieren, eine Überprüfung müsse **regelmäßig** erfolgen

- eine **Kennzeichnungspflicht** für die erlangten Daten erforderlich sei

- die Verwendung der erhobenen personenbezogenen Daten in anderen Verfahren nur zur Aufklärung gleichgewichtiger Katalogtaten oder Abwehr konkreter Gefahren für hochrangige Rechtsgüter erfolgen dürfe

- **Daten,** soweit diese noch für gerichtliche Kontrollen verfügbar sein müssen, zu **sperren** seien.

Zwei weitere Aspekte ergeben sich aus dieser Entscheidung des BVerfG.
Zum einen sind die Anforderungen an die Durchführung der Wohnraumüberwachungsmaßnahmen ab dem Zeitpunkt der Entscheidung des BVerfG zu beachten. Dies bedeutet, dass z.B. aus Wohnraumüberwachungsmaßnahmen gewonnene Ermittlungsansätze hinsichtlich solcher Taten, welche mit einer Freiheitsstrafe von 5 Jahren oder weniger bedroht sind, nicht mehr verwertet werden dürfen.
Zum anderen sind die wesentlichen Festlegungen des Urteils auch für andere, in ihrer Eingriffstiefe vergleichbar gravierende strafrechtliche Ermittlungsmaßnahmen von Bedeutung. Der Gesetzgeber wird sich insbesondere mit den damit zusammenhängenden Fragen in Bezug auf die Telekommunikationsüberwachung wie auch bezüglich der Postbeschlagnahme auseinandersetzen müssen.

Nachdem das BVerfG dem Gesetzgeber zur Herstellung eines verfassungsgemäßen Rechtszustandes eine **Frist** bis 30. Juni 2005 eingeräumt

hatte, kam es zu einem **Gesetz**entwurf **zur Umsetzung des Urteils des BVerfG** aus dem mit der Vorbereitung befassten Bundesministerium, welcher eher eine Verschärfung der Eingriffsmöglichkeiten in die Rechte der Bürgerinnen und Bürger vorsah, als eine Anpassung an die Forderungen des BVerfG.
Wegen der aufkommenden heftigen Kritik wurde der Referentenentwurf nachgebessert. Dieser nun in der Diskussion befindliche Minimalentwurf, der ausschließlich die möglichst getreuliche Umsetzung des Urteils des BVerfG zum Inhalt hat, bedarf weiterer Verbesserungen. So wurde bisher keine Begriffsbestimmung zum unantastbaren Bereich privater Lebensgestaltung vorgenommen, ebenso fehlt die Festlegung des Kreises persönlich vertrauter Personen.

Unabhängig hiervon haben die Datenschutzbeauftragten des Bundes und der Länder in einer weiteren Entschließung auf die Notwendigkeit hingewiesen, dass alle verdeckten Eingriffsmaßnahmen in die Rechte von Bürgerinnen und Bürgern an den Maßstäben der verfassungsgerichtlichen Entscheidung vom 3. März 2004 gemessen werden müssen. Alle einschlägigen Bestimmungen sind daher einer Überprüfung zu unterziehen **(Anlage 21).**

Hierüber hat der Landesbeauftragte auch die zuständigen Landesminister informiert. Er erwartet, dass in Folge des Verfassungsgerichtsurteils die präventiven Regelungen im Bereich des Gesetzes über die öffentliche Sicherheit und Ordnung (SOG LSA) und des Verfassungsschutzgesetzes, u.a. hinsichtlich der Unterrichtung der Betroffenen nach Abschluss der jeweiligen verdeckten Maßnahmen, überprüft werden.

18.3 DNA-Analyse - Gewaltige Entwicklung und Ausweitungen im Strafverfahren

Die aus einigen Ländern in besonderer Weise in die Diskussion gebrachte Absenkung der rechtlichen Zulässigkeitsvoraussetzungen für genetische Untersuchungen hat die Datenschutzbeauftragten des Bundes und der Länder veranlasst, ihre Besorgnis über eine weitergehende Beeinträchtigung des Grundrechts auf informationelle Selbstbestimmung im Rahmen einer Entschließung zu verdeutlichen und Bund und Länder aufzufordern, bei der Erweiterung der DNA-Analyse Augenmaß zu bewahren **(Anlage 10).**
Wegen der sich exponentiell entwickelnden quantitativen und qualitativen Nutzungsmöglichkeiten der DNA-Analyse hatten die Datenschutzbeauftragten bereits kurz zuvor dringenden Regelungsbedarf bei Bundestag und Bundesregierung angemahnt **(Anlage 1).**

Entgegen immer wieder zu vernehmender Äußerungen ist eine **DNA-Untersuchung nicht** mit der Auswertung eines herkömmlichen **Fingerabdrucks** zu vergleichen. Die Verwendung des Begriffs „genetischer Fingerabdruck“ ist irreführend und soll offenbar den Boden für die breiteste Nutzung dieses Instruments bereiten.

Dies stellt für alle Bürgerinnen und Bürger ein nicht zu unterschätzendes Risiko dar. Denn es scheint in absehbarer Zeit möglich zu sein, wesentliche Teile des genetischen Status und der Prädisposition eines Menschen aus solchen Untersuchungen abzuleiten. Auch soweit nur die nicht-codierenden Teile der DNA untersucht werden - nur dies ist nach der Rechtsprechung des BVerfG verfassungsrechtlich zulässig -, können schon heute **weitergehende Zusatzinformationen** (wie z.B. das Geschlecht und Wahrscheinlichkeitsaussagen zu Altersabschätzungen, Zuordnung zu bestimmten Ethnien sowie Anhaltspunkte hinsichtlich einzelner Krankheiten) gewonnen werden; was zum Teil - wegen der Verwendung industriell vorgefertigter Untersuchungskits - zwangsläufig geschehen kann und geschieht. Dies ist ein deutliches Mehr an Information, als die Erfassung und Auswertung eines zwar genetisch festgelegten, aber nur äußerlich wahrnehmbaren singulären Merkmals, wie des Fingerabdrucks, ergeben kann.
Die in diesem Zusammenhang häufiger zu hörende abwehrende Äußerung, man könne den Ermittlungsbehörden nicht unterstellen, dass sie bewusst Daten aus dem codierenden Bereich des Genoms auswerteten und speicherten, ist problematisch. Es wird unzutreffend unterstellt, Kritiker würden den Ermittlern Missachtung der rechtlichen Regelungen vorwerfen. Solche Vorwürfe werden jedoch kaum erhoben. Entscheidender ist, dass im Zusammenhang mit solchen „Verteidigungsreden“ in der Regel übersehen wird, dass bereits die Abnahme von Körpersubstanz eine Erhebung aller genetischer Daten der Betroffenen bzw. die Spurenaufnahme die umfassende Erhebung personenbeziehbarer Daten und damit einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung darstellen kann. Das Genom des Menschen ist letztlich die wesentliche „Datenbank“ zu seiner Existenz als Individuum.

Ferner besteht in höherem Maße als bei Fingerabdrücken die Gefahr, dass **Daten Unbeteiligter** verarbeitet und genutzt werden. Denn deren „genetisches Material“ kann an nahezu allen Tatorten vorhanden sein - z.B. kleinste Hautpartikel oder Haare. Weitere Überprüfungen werden zeigen müssen, ob die in den Medien wiederholt zu lesende Darstellung aus dem Polizeibereich, dass die DNA-Analyse nur ein Baustein der Ermittlungsarbeit sein könne, sich in den Akten und Dateien der Ermittlungsbehörden widerspiegelt.

Die Datenschutzbeauftragten sehen die Erweiterungen des Einsatzes der DNA-Analyse daher kritisch. Sie appellieren an die Regierungen und Gesetzgeber des Bundes und der Länder, die DNA-Analyse nicht zum Routinewerkzeug jeder erkennungsdienstlichen Behandlung werden zu lassen. Sie darf nicht zum alltäglichen polizeilichen Eingriffsinstrument im Rahmen der Aufklärung und Verhütung insbesondere von Straftaten mit geringem Unrechtsgehalt werden. Auf eine Prognoseentscheidung hinsichtlich der Gefahr der Begehung weiterer erheblicher Straftaten durch den jeweiligen Täter und auf eine **richterliche Entscheidung** als Voraussetzung einer DNA-Analyse darf nicht verzichtet werden.
Auch sollte die in anderen Ländern geübte, aber rechtlich bedenkliche Praxis, DNA-Analysen ohne einen richterlichen Beschluss ausschließlich auf der Grundlage einer **Einwilligung** der Betroffenen durchzuführen, wei-

terhin ausgeschlossen bleiben. Denn es ist immer die Frage zu stellen, wie freiwillig eine Erklärung faktisch ist, die unter den besonderen Bedingungen z.B. einer Untersuchungshaftsituation oder auch nachbarschaftlicher Beobachtung erteilt wird.
Der Landesbeauftragte informierte das Ministerium der Justiz und das Ministerium des Innern über die Entschließung zur DNA-Analyse.
Er machte dabei nachdrücklich deutlich, dass - bei aller Berechtigung zum Einsatz dieser außerordentlichen Form der Datenerhebung zur Aufklärung ebenso außerordentlicher Deliktsfälle - die Schwere des Eingriffs in die Grundrechte vieler Menschen nicht außer Acht gelassen oder gar durch einen naiven Vergleich mit daktyloskopischen Untersuchungen relativiert werden darf. Dies gebietet das Menschenbild des Grundgesetzes, welches von der Würde des Einzelnen und seiner Unbescholtenheit ausgeht. Mit dieser Grundvoraussetzung ist es nicht vereinbar, dass Daten unbescholtener Bürgerinnen und Bürger in gleicher Weise wie jene von Kriminellen erhoben und in Dateien bzw. Registern der Strafverfolgungsbehörden geführt werden.
Er verband die Übersendung der Entschließung mit der Erwartung, dass die dort niedergelegten Überlegungen bei weiteren gesetzesändernden Vorhaben Berücksichtigung finden werden.

Angesichts eines im Februar 2005 im Bundesrat eingebrachten Gesetzesantrags von vier Ländern sah die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Notwendigkeit, erneut die besondere Qualität des Grundrechtseingriffs, welchen insbesondere die staatlich veranlasste Untersuchung/Ausforschung des genetischen Substrats von Menschen beim Einsatz der DNA-Analyse darstellt, in das öffentliche Bewusstsein zu rücken **(Anlage 26).** Auch wenn der Gesetzesantrag im Bundesrat keine Mehrheit fand, bleibt das Thema etwa infolge von Initiativen im Bundestag und Überlegungen innerhalb der Bundesregierung auf der Tagesordnung.

18.4 Telekommunikationsüberwachung (TKÜ), Terrorismusbekämpfung etc. - Eine Aufforderung zur Transparenz

Das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg hat im Jahr 2003 sein im Auftrag des Bundesministeriums der Justiz erstelltes Gutachten “Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b Strafprozessordnung (StPO) und anderer verdeckter Ermittlungsmaßnahmen” vorgelegt. Darin hat es festgestellt, dass sich die Zahl der Ermittlungsverfahren, in denen TKÜ-Anordnungen erfolgten, im Zeitraum von 1996 bis 2001 um 80 % erhöht hat, sich die Zahl der jährlich Betroffenen im Zeitraum von 1994 bis 2001 fast verdreifacht hat, immer mehr Gespräche abgehört worden sind und der Anteil der staatsanwaltschaftlichen Eilanordnungen im Zeitraum von 1992 bis 1999 von ca. 2 % auf 14 % angestiegen ist.
Die Datenschutzbeauftragten des Bundes und der Länder haben aus diesem Anlass eine Entschließung **(Anlage 13)** verabschiedet, mit der sie den Gesetzgeber und die zuständigen Behörden auffordern, Konsequenzen aus der Untersuchung des Max-Planck-Instituts zu ziehen.

Solche Untersuchungsergebnisse sollten eigentlich Anlass sein, die rechtliche Situation mit der tatsächlichen Entwicklung in Einklang zu bringen.
Dass dies leider nicht die Regel ist, wird im Zusammenhang mit den Bestimmungen zur Auskunft über Telekommunikationsverbindungsdaten, welche 2001 in Folge der Anschläge gegen das World Trade Center in New York in die StPO aufgenommen worden waren, deutlich.
Der Landesbeauftragte hält es für nicht akzeptabel, wenn den Bürgerinnen und Bürgern durch Begrenzung der Geltungsdauer einer freiheitsbeeinträchtigenden Regelung vorgespiegelt wird, diese Normen würden bis zum Ablauf der festgelegten Zeit einer Überprüfung unterzogen, und dann werden die neuen Befugnisse einfach prolongiert. Eine öffentliche Erklärung, warum die Verlängerung nötig, eine Überprüfung nicht möglich gewesen sei, geschweige denn eine angemessene parlamentarische Diskussion vor der Verlängerung der Geltungsdauer des freiheitsbegrenzenden Gesetzes war nicht festzustellen.
Das Vertrauen von Bürgerinnen und Bürgern in rechtsstaatliche Institutionen und Verfahren kann durch solche Unterlassungen beeinträchtigt werden.

Auch für die Datenschutzbeauftragten kann bei ähnlicher Praxis in künftigen Gesetzgebungsverfahren eine schwierige Situation entstehen. Sollten sie bereit sein, z.B. aufgrund einer besonderen, absehbar längerandauernden Gefahrensituation, Einschränkungen von Freiheitsrechten dann als tolerabel anzusehen, wenn ausgleichende Schutz- bzw. Verfahrensregelungen, wie z.B. eine befristete Geltung und/oder eine Überprüfungsverpflichtung bezüglich der belastenden Norm fixiert werden, dann dürfen Befristungen nur nach ausreichender Begründung und öffentlicher Diskussion verlängert oder aufgehoben werden.

Der nächste Prüfstein in diesem Zusammenhang wird die gesetzlich vorgesehene Evaluierung einiger nach dem Terrorismusbekämpfungsgesetz verschärften Regelungen sein. Diese, erstmalig in einem Gesetz festgeschriebene Überprüfungsverpflichtung, stellt einen beachtlichen Fortschritt im Gesetzgebungsverfahren dar. Allerdings wurde, soweit bekannt, mit einer Evaluierung noch nicht begonnen, obwohl die Zeit schon fortgeschritten ist.
In ihrer Entschließung zu „Forderungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder an Bundesgesetzgeber und Bundesregierung“ **(Anlage 1)** haben die Datenschutzbeauftragten die Notwendigkeit unabhängiger Evaluierung der neuen Befugnisse der Sicherheitsbehörden und anderer vergleichbar intensiver Eingriffsmaßnahmen bereits deutlich gemacht.

Die demokratische Kultur kann auch beeinträchtigt werden, wenn die Allgemeinheit von repressiven Überwachungsmaßnahmen, z.B. in der Telekommunikation, nicht transparent unterrichtet wird.

Ein Ansatz für solche Offenheit im Umgang mit freiheitsbeeinträchtigenden Maßnahmen ist die Veröffentlichung von Statistiken, konkret z.B. von Jah-

resstatistiken, welche die Betreiber von Telekommunikationsanlagen nach geltendem Recht (§ 110 Abs. 8 Telekommunikationsgesetz) zu erstellen haben. Da die Bundesregierung 2003 eine Abschaffung dieser Statistiken geplant zu haben schien, forderten die Datenschutzbeauftragten des Bundes und der Länder mit einer Entschließung **(Anlage 7),** diese Grunddatenerfassung keinesfalls abzuschaffen. Die Statistiken sollten darüber hinaus nicht nur beibehalten, sondern außerdem auf die Zahl der Auskünfte über Telekommunikationsverbindungsdaten erstreckt werden.
Diese Verbesserung des Informationsgehaltes erfolgte zwar nicht, jedoch wurde immerhin auf die Streichung der Statistiken verzichtet (vgl. Ziff. 23.1.2).

Zusammenfassend hält es der Landesbeauftragte für erforderlich, dass zuvörderst mit der Evaluierung der mit dem Terrorismusbekämpfungsgesetz vom 9. Januar 2002 in Kraft getretenen Neuregelungen begonnen wird, damit es nicht zum 12. Januar 2007 zu einer ungeprüften Verlängerung der Regelungen kommt.
Er bittet die Landesregierung, ihren Einfluss diesbezüglich geltend zu machen.

18.5 Kontrollen bei Staatsanwaltschaften zu Telekommunikationsüberwachungen (TKÜ)

Im Berichtszeitraum hat der Landesbeauftragte bei Staatsanwaltschaften Kontrollen zur Aktenführung im Zusammenhang mit dem Einsatz von TKÜ-Maßnahmen vorgenommen. Die in den auszugsweise geprüften und zum Teil sehr umfangreichen Vorgängen enthaltenen TKÜ-Anordnungen basierten auf § 100a Strafprozessordnung (StPO). Die Anträge waren den Anlässen überwiegend angemessen.
Nicht in jedem Fall konnte festgestellt werden, dass nach Abschluss der TKÜ-Maßnahme eine Benachrichtigung von Betroffenen veranlasst worden war. Auf Nachfrage wurde darüber informiert, dass entweder nur die Verurteilten von der Maßnahme betroffen waren bzw. die Verfahren anderer Beschuldigter nach Abtrennung an andere zuständige Staatsanwaltschaften abgegeben worden waren. Soweit im Übrigen von der kontrollierten Staatsanwaltschaft eingewandt wurde, dass die Beschuldigten anwaltlich vertreten gewesen seien, würde nur dann die Benachrichtigungspflicht erfüllt werden, wenn der Verteidiger ausdrücklich auf die durchgeführte TKÜ hingewiesen wurde. Allerdings erscheint es dem Landesbeauftragten ausreichend, wenn über die aufgezeichneten Telefonate in der Hauptverhandlung durch Inaugenscheinnahme Beweis erhoben wurde und in diesem Zusammenhang die Beschlüsse nach § 100a StPO verlesen wurden. Jedoch wäre dann zu prüfen gewesen, ob die Benachrichtigung in den einzelnen Fällen nicht früher hätte erfolgen können (vgl. § 101 Abs. 1 StPO).

Protokolle zur Vernichtung von Unterlagen über die TKÜ waren den Akten beigefügt. Schriftliche Unterlagen wurden oft vom zuständigen Staatsanwalt eigenhändig vernichtet, Datenträger jedoch auch ohne Anwesenheit eines Staatsanwalts, durch Mitarbeiter des Landeskriminalamtes. Auf die-

sen Verstoß gegen § 100b Abs. 6 StPO hat der Landesbeauftragte hingewiesen.
Trotz dokumentierter Vernichtung befinden sich in den Akten noch TKÜ-Vorgangslisten zu Ermittlungsverfahren, aus denen sich - neben den Namen der Betroffenen - auch inhaltliche Aspekte entnehmen lassen. Dies wurde damit erklärt, dass die Unterlagen für mögliche Wiederaufnahmeverfahren aufbewahrt werden müssten. Zur Wahrscheinlichkeit eines solchen Verfahrens wurde keine Aussage getroffen. Ohne tatsächliche Anhaltspunkte erscheint dem Landesbeauftragten diese Möglichkeit zumeist eher hypothetisch zu sein. Im übrigen fanden sich auf keinem Vorgang Sperrvermerke, welche die Verwendung nur für den Wiederaufnahmezweck gesichert hätten.

In einem Fall erschien dem Landesbeauftragten der Antrag der Staatsanwaltschaft auf Überwachung eines Handyanschlusses nicht ausreichend dargetan. Das Handy wurde bei der Wohnungsdurchsuchung beim Beschuldigten gefunden. Der eingetragene Anschlussinhaber des Handys war jedoch nicht Beschuldigter im Verfahren und anderweitig wohnhaft. Den Antrag begründete die Staatsanwaltschaft mit der Feststellung, der Beschuldigte solle das Handy benutzt haben, um so mit evtl. Mittätern Kontakt aufzunehmen bzw. über dieses Handy erreichbar zu sein. Der behauptete Sachverhalt war aus den Unterlagen tatsächlich und rechtlich nicht verifizierbar.
Der Landesbeauftragte hat darauf hingewiesen, dass die Staatsanwaltschaft die richterliche Anordnung zur Überwachung der Telekommunikation nach § 100a StPO nur beantragen darf, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer dort bezeichnete Straftaten begangen hat oder sich diese gegen Personen richtet, von denen aufgrund bestimmter Tatsachen anzunehmen ist, dass der Beschuldigte ihren Anschluss benutzt.

Erneut musste der Landesbeauftragte den problematischen Gebrauch von Faxgeräten feststellen. So ergab sich aus den geprüften Vorgängen, dass personenbezogene Daten per Fax zwischen Staatsanwaltschaften und Dienststellen der Polizei übermittelt wurden, ohne dass dies den in § 6 DSG-LSA festgelegten Datensicherheitszielen immer entsprochen hätte. Wie bereits mehrfach dargelegt, ist der Einsatz eines Faxgerätes zur Übermittlung personenbezogener Daten wegen hinreichend bekannter Sicherheitsmängel nur in besonders gelagerten Eilfällen vertretbar. In den geprüften Fällen waren keine Eilsituationen belegt; zum Teil befanden sich die Behörden in unmittelbarer geografischer Nähe zueinander. Eine Übersendung enthielt zudem als „VS-NfD“ (Verschlusssache - Nur für den Dienstgebrauch) eingestuften Inhalt.
Die Datensicherheitsanforderungen müssen sich zudem mit dem anfänglich bestehenden Geheimhaltungsinteresse der strafprozessual angeordneten und abgeschirmten Telefonüberwachung decken. Der für die Ermittlungen insoweit zuständige Staatsanwalt hat deshalb nach § 152 Gerichtsverfassungsgesetz auch die datenschutzrechtliche Verantwortung dafür, dass die beteiligten Polizeidienststellen und Behörden diese Sicherheitsanforderungen beachten.

Der Landesbeauftragte hat empfohlen, unbeschadet der eigenen Verantwortlichkeit der beteiligten Polizeibehörden, auch seitens der im Einzelfall zuständigen Staatsanwälte auf die Beachtung der zur Datensicherheit geltenden gesetzlichen Bestimmungen zu achten.

18.6 Presse, Funk und Fernsehen bei der Strafverfolgung

Die Strafverfolgungsbehörden sind zur Aufklärung von Straftaten gehalten, alle gesetzlich zulässigen Maßnahmen zu ergreifen. Sie dürfen dabei grundsätzlich auch **Publikationsorgane** (Presse, Rundfunk und Fernsehen) um ihre Mitwirkung bitten.

Unter welchen Voraussetzungen die Inanspruchnahme von Presse, Funk und Fernsehen erfolgen darf, regelt die Anlage B zur RiStBV - Richtlinie über die Inanspruchnahme von Publikationsorganen zur Fahndung nach Personen bei der Strafverfolgung.

Eine Änderung wurde erforderlich, weil neue Kommunikationsmittel bisher keine Berücksichtigung fanden. Die Richtlinie soll zukünftig als „Richtlinie über die Inanspruchnahme von Publikationsorganen und die Nutzung des Internets sowie anderer elektronischer Kommunikationsmittel zur Öffentlichkeitsfahndung nach Personen im Rahmen von Strafverfahren“ bezeichnet werden. In der Neufassung der Richtlinie soll in erster Linie der Umgang mit dem Internet zu Strafverfolgungszwecken geregelt werden.

In unserer hochtechnisierten Zeit, in der das Medium **Internet** längst selbstverständlich und allgegenwärtig geworden ist, kommen auch Strafverfolgungsbehörden nicht umhin, sich der Vorzüge des Internets zu bedienen. Mit einer Personenfahndung im Internet kann die Strafverfolgungsbehörde wesentlich mehr Menschen erreichen, die ggf. zur Aufklärung von Straftaten beitragen können.

Trotz dieser Vorteile kann insbesondere aus Sicht des Datenschutzes nicht deutlich genug auch auf die Nachteile eines solchen Verfahrens hingewiesen werden. Datenschutzrechtlich gesehen kommt die Veröffentlichung einer Fahndung im Internet einer Datenübermittlung in das Ausland gleich. Die Anforderungen an eine solche Übermittlung sind zu Recht sehr hoch. Auf Veröffentlichungen im Internet hat jeder Zugriff, der einen Zugang zum Internet hat. Zudem ist zu berücksichtigen, dass einmal **im Internet** veröffentlichte personenbezogene **Daten nicht rückholbar** sind. Selbst wenn die Daten von der Homepage z.B. der Polizei gelöscht werden, so können in der Zeit seit der Veröffentlichung unzählige Kopien angefertigt worden sein. Der Eingriff in die Persönlichkeitsrechte der Betroffenen ist bei einer Veröffentlichung im Internet nicht hoch genug einzuschätzen.

Unter Berücksichtigung dieser Gegebenheiten hatte der Landesbeauftragte die vorgesehenen Änderungen geprüft und dem Ministerium der Justiz des Landes Sachsen-Anhalt mitgeteilt, dass die Regelungen zur Nutzung des Internets modifiziert werden sollten.

In der Richtlinie wird zwar darauf hingewiesen, dass die Nutzung dieses Mediums nur zurückhaltend und unter Beachtung der Verhältnismäßigkeit erfolgen solle. Angesichts der praktischen Erfahrung, dass solche Vorschriften in der Regel ohne weitere Reflektion in der täglichen Arbeit genutzt werden, hatte der Landesbeauftragte die Aufnahme eines Hinweises, dass einmal im Internet zum Abruf bereitgestellte Informationen nicht rückholbar und damit über sehr lange Zeit verfügbar sind, für unbedingt erforderlich erachtet. Schließlich erschienen ihm auch die Intervalle der regelmäßigen Prüffristen zu großzügig gewählt. Die Prüfung von Internetfahndungen auf das weitere Vorliegen der Ausschreibungsvoraussetzungen in halbjährlichen Abständen beeinträchtigt die Interessen der Betroffenen in dem Fall unverhältnismäßig, in dem das weitere Vorliegen der Voraussetzungen verneint werden muss. Die Anzahl der Internetfahndungen dürfte zahlenmäßig derart begrenzt sein, dass eine Prüfung in einer erheblich kürzeren Frequenz zu gewährleisten sein dürfte. Auch wies der Landesbeauftragte darauf hin, dass es sinnvoll wäre, die Voraussetzungen für die ausnahmsweise erlaubte Inanspruchnahme privater Internetanbieter zu definieren.

18.7 Datenschutz in der Rechtsförmlichkeitsprüfung

Im Rahmen ihres Arbeitskreises Justiz haben die Datenschutzbeauftragten des Bundes und der Länder einen Prüfkatalog zur Datenschutzvereinbarkeit von Gesetzen und Verordnungen erarbeitet.
Dieser soll ggf. noch durch einen Teil zum technischen Datenschutz ergänzt werden. Angesichts anstehender Gesetzesvorhaben war es angezeigt, den Prüfkatalog bereits vorher dem Justizministerium mit der Bitte zuzuleiten, ihn bei künftigen Rechtsetzungsvorhaben zu berücksichtigen.

Der Landesbeauftragte hat mit Zufriedenheit zur Kenntnis genommen, dass der Justizminister den Fragen des Datenschutzes im Rahmen der Rechtsförmlichkeitsprüfung eine besondere Bedeutung beimisst und die übersandte Anregung im Rahmen der Überarbeitung der „Grundsätze der Rechtsförmlichkeit“ berücksichtigen will.

18.8 Justizkommunikationsgesetz

Das kurz vor Ende des Berichtszeitraums vom Bundestag am 22. März 2005 beschlossene „Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz (Justizkommunikationsgesetz)“ - BGBl. I, S. 837 - soll für alle Gerichtszweige mit Ausnahme der Strafgerichtsbarkeit die rechtliche Grundlage zur elektronischen Aktenführung einschließlich des dazu notwendigen elektronischen Postverkehrs schaffen.
Der Landesbeauftragte hatte im Rahmen einer Stellungnahme gegenüber dem Ministerium der Justiz insbesondere auf folgendes hingewiesen:

Auch wenn grundsätzlich Zweifel an der dauerhaften Überprüfbarkeit der Zertifikate selbst bei qualifizierten elektronischen Signaturen bleiben mögen, sei der für alle Verfahrensordnungen vorgesehene Ersatz der Schriftform durch die qualifizierte anstelle einer weniger sicheren Signaturform

zu begrüßen. Die qualifizierte elektronische Signatur bilde die Grundvoraussetzung, um die Anforderungen an die technischen und organisatorischen Maßnahmen gem. § 6 DSG-LSA, insbesondere die Integrität und die Authentizität personenbezogener Daten bei der automatisierten Verarbeitung (§ 6 Abs. 2 Nrn. 2 und 4 DSG-LSA) zu gewährleisten.
Der Landesbeauftragte erläuterte, dass es sowohl aus verwaltungspraktischen Gründen als auch zur Steigerung der Akzeptanz bei Bürgerinnen und Bürgern sinnvoll sein könne, keine Differenzierungen bei den Formen der Signatur vorzunehmen, soweit mit den jeweils signierten Schreiben ein Außenkontakt verbunden wäre.
Völlig zurecht wurde in der Begründung des Gesetzentwurfs wie auch zuletzt durch die Bundesjustizministerin in ihrer Rede vor dem Deutschen Bundestag am 25. Februar 2005 darauf hingewiesen, dass bei der gesetzlichen Zulassung und näheren Ausgestaltung der elektronischen Aktenführung Anforderungen an die Zuverlässigkeit der elektronisch geführten Akte besonderer Beachtung bedürfen. Diese Forderung ist um so leichter und ohne großen Aufwand zu erfüllen, wenn vermieden würde, durch Verwendung unterschiedlicher Grade an Signaturqualität die Gefahr zu erzeugen, dass Justizbeschäftigte einen qualifiziert zu signierenden Vorgang versehentlich in einfacher Form signieren.
Nicht qualifiziert zu zeichnen wäre z.B. ein Mahnbescheid, da hier in der „Papierwelt“ auf eine eigenhändige Unterschrift verzichtet werden durfte. Da aber auch eine qualifizierte Signatur verwendet werden dürfte (vgl. § 692 Abs. 2 ZPO-neu), wird zunächst die Beobachtung der Praxis ausreichen, um datenschutzrechtliche Standards zu sichern. Bei Bedarf wird der Landesbeauftragte auf Nachbesserung drängen.
Gleiches gilt bezüglich der Handhabung kombinierter elektronischer Dokumente. Es wird sich zeigen, wie künftig beispielsweise mit eingebetteten Videostreams bzw. Bilddateien verfahren wird, ob z.B. dadurch rechtliche Probleme entstehen, dass ein im Bereich der Rechtspflege erstelltes Textdokument mit einer aus dem Polizei- bzw. Verwaltungsbereich stammenden Videodatei kombiniert und anschließend digital signiert wird, ohne dass die Videodatei die gleiche rechtliche Qualität wie das erstellte Textdokument hat, jedoch die Gesamtdatei die Verbindlichkeit eines elektronischen qualifiziert signierten Dokuments erhält. Ähnliches wäre bezüglich Sachverständigengutachten denkbar. Hinzu kommt, dass der das Gutachten signierende Sachverständige nicht zwangsläufig selbst die evtl. Bildaufnahmen gefertigt haben muss.

Im Gesetz wurden zahlreiche Bestimmungen getroffenen, welche die Veröffentlichung von Daten Betroffener im Internet ermöglichen. Ob es im Einzelfall unabdingbar ist, die entsprechenden Daten tatsächlich einer internationalen Öffentlichkeit zugänglich zu machen, wird immerhin der Entscheidung des Richters unterworfen.
Wie vom Landesbeauftragten wiederholt betont, ist eine Veröffentlichung im Internet datenschutzrechtlich generell kritisch zu bewerten, da insbesondere das Kopieren von Daten und deren Weiterverbreitung nicht unterbunden werden kann.
Löschungsregelungen helfen nach einer Veröffentlichung nicht weiter, denn dann sind diese Daten "in der Welt". Da die vorgesehenen Veröffent-

lichungen nicht immer im vermutlichen Interesse des Betroffenen sein dürfte, erscheint es geboten, dass der Gesetzgeber die tatsächliche Entwicklung im Auge behält. Eine Evaluationsklausel wäre sinnvoll gewesen, ihr Fehlen hindert die Überprüfung indessen nicht.

Ursprünglich wollte der Bundesgesetzgeber der seit langem und wiederholt vorgetragenen Forderung der Datenschutzbeauftragten des Bundes und der Länder nach einer umfassenden gesetzlichen Regelung zur **Justizaktenaufbewahrung** im Rahmen des Justizkommunikationsgesetzes nachkommen. Der Landesbeauftragte begrüßte den Entwurf im Grundsatz. Da er jedoch einige notwendige Vorgaben an die Verordnungsgeber vermisste, bat er das Ministerium der Justiz im Rahmen seiner Zuständigkeit darauf hinzuwirken, dass u.a. eine differenzierte Normierung zu Aufbewahrungs-, Prüffristen etc. sichergestellt wird. Auch müsse eine Sperrungsregelung vorgesehen werden, soweit Löschungen wegen besonderer tatsächlicher Konstellationen nicht möglich sein sollten; die hinsichtlich des Löschverzichts akzeptablen Gründe sollten rechtlich fixiert werden.

Allerdings kam es nicht zu einer in Bund und Ländern gültigen Normierung. Es wurde ausschließlich eine Regelung für die Bundesgerichte und den Generalbundesanwalt getroffen, da der Bundestag - in Anschluss an das Verdikt des Bundesverfassungsgerichts zur Regelungsbefugnis des Bundes in Sachen Studiengebühren - seine Gesetzgebungskompetenz für ein einheitliches Aktenaufbewahrungsgesetz nicht mehr zweifelsfrei als gegeben ansah.
Nachdem für die Bundesgerichte und den Generalbundesanwalt nunmehr das Schriftgutaufbewahrungsgesetz geschaffen wurde, hofft der Landesbeauftragte, dass im Land Sachsen-Anhalt umgehend eine entsprechende gesetzliche Grundlage zur Justizaktenaufbewahrung initiiert wird.

18.9 Dienstanweisungen von Gerichten zum Datenschutz

Der Landesbeauftragte hatte auch im Berichtszeitraum die Gelegenheit wahrgenommen, durch Informationsbesuche bei den Gerichten bzw. im Rahmen von Beratungen an der Erstellung von Dienstanweisungen zum datenschutzgerechten Umgang mit personenbezogenen Daten bei den Gerichten mitzuwirken.
Es lagen bereits Verfügungsentwürfe vor, welche die gesetzlichen Grundlagen differenziert berücksichtigten, so dass sich die konstruktiven Gespräche im Wesentlichen auf technisch-organisatorische Fragestellungen konzentrieren konnten.
Problematisiert wurde z.B. die Speicherung von Entscheidungen vor und nach der Verkündung gerichtlicher Entscheidungen.
Der Landesbeauftragte hat darauf hingewiesen, dass dabei, soweit Entwürfe vor Verkündung von Entscheidungen gespeichert sind, durch unberechtigte Nutzung - wegen der möglichen Nachvollziehbarkeit des Entscheidungsprozesses - auch die richterliche Unabhängigkeit berührt sein kann.
Der Zugriff auf vorbereitende Überlegungen durch einen Vertreter setzt die Einwilligung des vertretenen Richters voraus.

Nach Verkündung von Entscheidungen ist es nach gesetzlich geregelten Zugangsbefugnissen in der Regel Verfahrensbeteiligten und staatlichen Institutionen gestattet, die jeweilige Entscheidung - gleich ob in Akten- oder elektronischer Form gespeichert - einzusehen. Die Dokumentation/ Speicherung für diese Zwecke ist notwendig.
Der Landesbeauftragte hält es jedoch für rechtlich fraglich, wenn daneben nicht anonymisierte Entscheidungen in Einzelrichter-, Kammer- oder Senatssammlungen (langfristig bzw. gar auf Dauer) aufbewahrt werden. Eine gesonderte Rechtsvorschrift, die gestattet, eine weitere personifizierbare Datensammlung dieser Art einzurichten und zu nutzen, gibt es weder in den Verfahrensordnungen noch dem Gerichtsverfassungsgesetz.
Das allgemeine Datenschutzrecht erlaubt die Verarbeitung und Nutzung personenbezogener Daten, wenn es zur Erfüllung der Aufgaben der öffentlichen Stelle erforderlich ist und die Nutzung für jene Zwecke erfolgt, für welche die Daten erhoben worden waren. Diese in allen Datenschutzgesetzen zu findende Regelung spiegelt das im Grundrecht nach Art. 6 der Verfassung des Landes Sachsen-Anhalt fundierte Verbot der Vorratsdatenhaltung sowie das Gebot der Zweckbindung unmittelbar wider.
Da gerichtliche Entscheidungen immer im Einzelfall ergehen, ist zunächst kein rechtlicher Grund ersichtlich, warum Entscheidungen, respektive personenbezogene Daten, aus anderen Verfahren längerfristig - und zusätzlich zur Aufbewahrung beim jeweiligen Verfahrensvorgang - gespeichert werden sollten. Dem verständlichen Interesse an Präzedenzfällen kann auch mit einer anonymisierten und nach sachlichen Aspekten differenzierten Sammlung (JURIS) genügt werden.
Sinn der Aufbewahrung der Originalentscheidungen in den Geschäftsstellen bzw. Archiven - und damit datenschutzrechtlich gesprochen, der Zweck - ist jedenfalls nicht die Rechtsfindung in einem mit dem ausgeurteilten Verfahren nicht zusammenhängenden neuen Verfahren.
Auch der Umstand, dass es in Verfahren mit Amtsermittlungsgrundsatz notwendig erscheinen kann, die Einlassungen einzelner Betroffener in unterschiedlichen Verfahren zum gleichen Sachverhalt auf Deckungsgleichheit zu prüfen, kann zumindest nicht zu einer dauernden Speicherung der nicht anonymisierten Entscheidungen an mehreren Stellen führen. Denn auch für diesen Überprüfungszweck steht der Originalvorgang grundsätzlich zur Verfügung.

Da jedoch in den vorgelegten Datenschutzbestimmungen, wenn auch mit unterschiedlicher Formulierung festgelegt wurde, dass Entscheidungen bzw. deren Entwürfe nur zu dienstlichen Zwecken aufbewahrt werden dürfen und sich die Begrifflichkeit dienstlicher Zweck und Zweckbindung semantisch entsprechen dürften, bestand kein weiterer Handlungsbedarf. Darüber hinaus werden die Entscheidungen, welche Unterlagen wann und zu welchem Zweck benötigt werden, im Laufe eines gerichtlichen Verfahrens getroffen, welches nicht der Kontrolle des Landesbeauftragten unterliegt. Davon, dass die Richterschaft dabei ihre materiellrechtliche Bindung auch an das Grundrecht auf Datenschutz beachtet, geht der Landesbeauftragte aus.

18.10 Schulhofrauferei verhindert Praktikum

Die Mühlen der Justiz mahlen langsam - manchmal auch Sachen, welche nicht zu mahlen sind.
So geschah es einem Jungen, welcher zwischen jene Mühlsteine geraten war. Wie dessen Vater dem Landesbeauftragten Mitte 2004 berichtete, habe sich sein noch nicht volljähriger Sohn um einen Praktikumsplatz bei einer Staatsanwaltschaft bemüht, weil er eine Ausbildung zum Rechtspfleger anstrebe. Das begehrte Praktikum sei jedoch nicht möglich gewesen, weil in den „Akten“ etwas gegen seinen Sohn vorgelegen haben soll. Auf seine Nachfrage sei ihm mitgeteilt worden, um Auskunft zu erhalten, müsse er einen Rechtsanwalt einschalten. Es sei ihm aber trotzdem bekannt geworden, dass es sich um eine „Strafanzeige“ im Zusammenhang mit einer tätlichen Auseinandersetzung zwischen seinem Sohn und einem etwas älteren Schüler auf einem Schulhof gehandelt habe. Sein Sohn sei damals 9 Jahre alt gewesen. Auf seine Anfrage hin habe die Staatsanwaltschaft erklärt, dass solche Vorgänge fünf Jahre lang gespeichert werden dürften. Der Petent meinte aber, dass die fünf Jahre längst abgelaufen seien.
Nach diesen Hinweisen hat der Landesbeauftragte die betreffende Staatsanwaltschaft gebeten, den einschlägigen Vorgang zu Prüfungszwecken zu sichern und ihm zu übersenden. Aus diesem ließ sich entnehmen, dass entgegen einer heranziehbaren gesetzlichen Regelung zur Datenhaltung in Dateien (§ 489 Abs. 4 Strafprozessordnung (StPO)) in der Geschäftsstelle der Staatsanwaltschaft eine sogenannte Aussonderungsprüffrist von fünf Jahren festgelegt worden war. Da der Betroffene noch nicht strafmündig war und die besonderen Bedingungen, nach denen eine Einspeicherung der Daten eines Kindes in Verfahrensdateien hätte erfolgen können, nicht ersichtlich waren, hätte nur eine Speicherung zur Vorgangsverwaltung erfolgen können bzw. der Vorgang ggf. gesperrt werden müssen.

Aus der Akte war zudem weder ersichtlich, dass, noch warum dieser Vorgang im Zusammenhang mit einer Bewerbung um einen Praktikumsplatz verwendet worden war. Selbst wenn die Aufbewahrung rechtmäßig gewesen wäre, hätte es für die zweckändernde Verwendung einer Rechtsgrundlage bedurft.

In ihrer Stellungnahme verwies die Justiz darauf, dass Strafanzeigen gegen Kinder nach § 47 der Aktenordnung für die Gerichte der ordentlichen Gerichtsbarkeit und die Staatsanwaltschaften, einer Verwaltungsvorschrift, gespeichert werden müssten und die Erfassung unter rein formalen Gesichtspunkten erfolge. Die Speicherung sei damit unabhängig von einem Anfangsverdacht bzw. einer Beschuldigteneigenschaft.
Daneben wäre eine Speicherung in einer Datei für Zwecke künftiger Strafverfahren möglich, wonach die Speicherung des Kindes nach zwei Jahren hätte geprüft werden müssen, wenn seine Daten dort gespeichert worden wären. Die Daten des Jungen wurden jedoch nach den Darlegungen der Justiz lediglich im Rahmen der Vorgangsverwaltung gespeichert und nach

den Aufbewahrungsbestimmungen (gleichfalls lediglich eine Verwaltungsvorschrift) für fünf Jahre aufbewahrt.
Die Erforderlichkeit - als Ausprägung des verfassungsrechtlichen Verhältnismäßigkeitsprinzips - einer Datennutzung kann jedoch in der Regel nicht an fixen Terminen ausgerichtet werden. Im vorliegenden Fall wäre sie zudem sachlich nicht zu begründen gewesen. Dass dies auch in der Justiz so gesehen wurde, zeigt eine problematische Formulierung ihrer Stellungnahme zum Fall. Es wird dort festgestellt, dass die Speicherung der Daten „so lange erforderlich sei, wie die Akten nach den Aufbewahrungsbestimmungen aufzubewahren sind“. Wie dargelegt, handelt es sich bei diesen Bestimmungen lediglich um eine Verwaltungsvorschrift. Dies bedeutet, dass die Erforderlichkeit entgegen dem verfassungsrechtlich und gesetzlich Notwendigen nicht aus dem Einzelfall bestimmt wird, sondern überspitzt gesagt, hätte sich - nach dieser Mitteilung - die Justizverwaltung die Erforderlichkeit zur Datenhaltung selbst geschaffen. Die gesetzliche Regelung legt jedoch fest, dass zu Zwecken der Vorgangsverwaltung gespeicherte Daten zu löschen sind, wenn sie nicht mehr erforderlich sind. Diese Forderung darf nicht durch eine extensive Festlegung von Prüffristen und Speicherungsdauern in Errichtungsanordnungen umgangen werden. Auch macht dieser Fall zudem deutlich, dass die Festlegung statischer Fristen im Rahmen rechtsstaatlicher Verfahren häufig problematisch ist.

Angesichts der gesetzlich eingeräumten Möglichkeit, die zur Vorgangsverwaltung gespeicherten personenbezogenen Daten auch für andere Zwecke verwenden zu dürfen (§ 485 S. 2 und 3 StPO), hätte sich zumindest die Heranziehung der Fristen von § 489 Abs. 4 StPO angeboten.
Neben der wiederholt geäußerten Forderung der Datenschutzbeauftragten des Bundes und der Länder (vgl. im VI. Tätigkeitsbericht Ziff. 18.10) nach einer gesetzlichen Regelung durch ein Aktenaufbewahrungsgesetz hält der Landesbeauftragte eine Überprüfung der bestehenden Prüf- und Speicherungsfristen für angezeigt.

Die Verwendung der zu Vorgangsverwaltungszwecken gespeicherten Daten des Jungen für seine Überprüfung als Praktikumbewerber war auch nach Auffassung der zuständigen Staatsanwaltschaft mangels rechtlicher Grundlage unzulässig.
Da der Leitende Oberstaatsanwalt nach Kenntnis des Vorgangs umgehend das Erforderliche veranlasst hat, u.a. um Ähnliches künftig zu verhindern, konnte auf eine förmliche Beanstandung verzichtet werden.

Eine gleichfalls erfolgte Abfrage bei der vor fünf Jahren sachbearbeitenden Dienststelle der Polizei ergab zwar, dass die Daten des Jungen versehentlich in das damals genutzte automatische Vorgangsbearbeitungssystem der Polizei übernommen worden waren. Er wurde jedoch immer als Kind und nicht als Beschuldigter geführt. Seine Befragung erfolgte zudem durch den Jugendsachbearbeiter des Polizeireviers. Das Ministerium des Innern veranlasste vorsorglich eine Überprüfung der einschlägigen Datensätze.

18.11 Online-Banking bei Gerichtsvollziehern

Nehmen Gerichtsvollzieher zur Führung eines Dienstkontos am Online-Banking-Verfahren teil, führt das häufig zur Verarbeitung personenbezogener Daten der Zahlungspartner. Das war vom Ministerium der Justiz auch so gesehen worden, als es beabsichtigte, eine Allgemeinverfügung nebst Begleiterlass zur Genehmigung der Teilnahme am Online-Banking-Verfahren für den Geschäftsbereich der Gerichtsvollzieher in Kraft zu setzen. Es beteiligte rechtzeitig den Landesbeauftragten.
Der musste feststellen, dass sich der Erlassentwurf nur auf das PIN/TAN-Verfahren (PIN = persönliche Identifikationsnummer, TAN = nur einmal verwendbare Transaktionsnummer) bezog, das unter bestimmten Umständen wesentlich sicherere HBCI-Verfahren (HBCI = Home Banking Interface) damit überhaupt keine Beachtung fand. Außerdem war beabsichtigt, dass **soweit als möglich** PIN und TAN nicht im EDV-System zu hinterlegen sind. In seiner Stellungnahme regte der Landesbeauftragte an, auch das HBCI-Verfahren zuzulassen und vor allem die Speicherung von PIN und TAN im EDV-System **ausnahmslos zu unterbinden**. Dies hätte auch einer Bestimmung des Erlasses entsprochen, nach der die Übersendung von TAN online nicht gestattet ist.
Durch die Speicherung von PIN und TAN im EDV-System besteht durchaus die Möglichkeit, dass bei nachlässiger Sicherheitskonfiguration, z.B. Fehlen einer Personal Firewall, durch einen Dritten ein Spionageprogramm auf den PC geschleust wird, das die gespeicherten Nummern unbemerkt an den Dritten sendet, der sie missbraucht.

Leider hat die Argumentation des Landesbeauftragten das Ministerium der Justiz zunächst nicht überzeugt. Zwar wurde ein Speicherverbot für PIN und TAN begrüßt, jedoch wurde dem nicht gefolgt, da dadurch einige Softwareprodukte, nämlich solche, die PIN und TAN speicherten, von der Verwendung ausgeschlossen seien, ohne dass damit eine qualitative Änderung des Sicherheitsstandards verbunden sei. Man würde als Kompromiss nun klarstellen, dass die PIN/TAN-Speicherung nur zulässig sei, wenn die Arbeitsweise des Programms dies zwingend voraussetze.
Erst als der Landesbeauftragte das Argument nachschob, bei gespeicherten PIN und TAN könne außer datenschutzrechtlich bedenklichen Situationen auch ein deutlich erhöhtes Risiko hinsichtlich böswilliger Finanztransaktionen vorliegen, konnte sich das Ministerium der Justiz dem Landesbeauftragten anschließen und die PIN/TAN-Speicherung in dem Erlass generell untersagen.

Durch den Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder wurde im Berichtszeitraum eine Arbeitsgruppe gebildet, die sich auch mit PIN- und TAN-Speicherung befasste und eine Orientierungshilfe zum datenschutzgerechten Anschluss an Internet und Online-Banking bei Gerichtsvollziehern erarbeitet hat.
Sie ist im Service-Angebot auf der Homepage des Landesbeauftragten zum Download verfügbar.

18.12 Insolvenzbekanntmachungen

Wie dem Landesbeauftragten beim Einsehen der entsprechenden Internetangebote des elektronischen Bundesanzeigers sowie von „Insolvenzbekanntmachungen.de“ (diese Seite wird von sachsen-anhaltischen Gerichten noch nicht genutzt) deutlich geworden ist, werden ohne Bedenken weiterhin Personen, u.a. mit ihrem Namen, im Internet an den (Schulden-) Pranger gestellt.

Bereits im vorherigen Tätigkeitsbericht hatte der Landesbeauftragte an mehreren Stellen darauf hingewiesen, dass die Veröffentlichung von personenbezogenen Daten im Internet im Vergleich zur Veröffentlichung in anderen Medien eine vollkommen andere Qualität erhält. Dies wird insbesondere dann deutlich, wenn die Wirksamkeit dieser öffentlichen Darstellung von Menschen zeitlich begrenzt sein soll. Es ist naiv zu glauben, man könne die Nutzung von im Internet bereitgestellten Informationen durch rechtsstaatliche Normen in ihrer Auswirkung auf die Betroffenen begrenzen oder gar rückgängig machen, als könnten die veröffentlichten Insolvenzinformationen in irgendeiner Weise zurückgeholt werden (vgl. auch VI. Tätigkeitsbericht, Ziff. 18.11).
Wenig verständlich ist auch jene durch die Nichtrückholbarkeit der personenbezogenen Informationen entstehende faktische Gleichbehandlung der von Insolvenz Betroffenen mit Verdächtigen, welche wegen schwerster Delikte unter Zuhilfenahme des Internets gesucht werden. Diese gleichartige Grundrechtsbeeinträchtigung wird den Betroffenen zugemutet, unabhängig davon, wie groß ihr eigener Anteil an ihrer wirtschaftlich kritischen Lage ist.

Nicht nachvollziehbar ist es, wenn in den entscheidenden Vorschriften der Anschein erweckt wird, man könne die Kopierbarkeit von auf diesem Weg übermittelten Informationen begrenzen. Es stellt sich die Frage, wie es zu den Regelungen von § 9 Abs. 2 Satz 3 InsO, § 2 Abs. 1 Satz 3 Insolvenzbekanntmachungsverordnung kommen konnte. In diesen Regelungen wird verlangt, dass nach dem Stand der Technik sicherzustellen sei, dass Insolvenzinformationen nicht von Dritten kopiert werden können. Angesichts der technischen Gegebenheiten scheint dies eine nicht umsetzbare Forderung zu sein.
Noch widersprüchlicher wird der Eindruck, wenn man die Tatsache berücksichtigt, dass Insolvenzveröffentlichungen selbst ohne den in diesen Bestimmungen geforderten Minimalschutz bereits erfolgen. Tatsächlich ist dies keine graue Theorie. Denn wie der „Blick“ auf die eingangs genannten Seiten zeigte, war noch nicht einmal der von Gesetzes wegen zu gewährleistende Kopierschutz in der digitalen Welt verwirklicht. Schon durch die Funktion „Kopieren/Einfügen“ war es möglich u.a. Namen und Anschrift der Betroffenen zu beschaffen. Fraglich ist nur, ob dies in irgendeiner Weise vorwerfbar ist. Bekanntlich kann im Rechtsstaat auch von ausführenden Behörden und deren Bediensteten nichts Unmögliches - wie z.B. ein verlässlicher Kopierschutz für Internetangebote - gefordert werden.

Zumindest die einfache Form der Kopierbarkeit hätte jedoch nach dem Stand der Technik ausgeschlossen werden können; z.B. durch Verwendung von Bilddateien statt Textformaten.
Konsequent wäre einzig die Rückkehr zur Papierform. Diese kann zwar gleichfalls digitalisiert werden, aber mit deutlich erhöhtem Aufwand.
Daneben besteht noch die Möglichkeit, verfahrensrechtlich u.a. die Nutzbarkeit der Informationen zu beschränken (Verwertungsverbot) und nach Abschluss des jeweiligen Verfahrens die Nutzung der Daten eindeutiger als bisher unter Strafe zu stellen. Dies könnte zumindest innerhalb Deutschlands eine gewisse Schutzwirkung entfalten.

Eine Begrenzung der weiten Verbreitung personenbezogener (Insolvenz-) Daten natürlicher Personen ist notwendig. Eine Anpassung der Regelungen des Bundesdatenschutzgesetzes zur geschäftsmäßigen Datenerhebung und -speicherung zum Zwecke der Übermittlung erscheint dem Landesbeauftragten auch bedenkenswert, wenn Gläubigerinteressen dadurch berührt werden.
Es ist kaum nachvollziehbar, warum wirtschaftliche Interessen es erlauben sollen, das nicht einschränkbare Grundrecht der Menschenwürde in seiner Wirkung zu beeinträchtigen. Auch der Schutz des Eigentums auf Seiten der Gläubiger kann den tatsächlich zeitlich nicht begrenzten Eingriff in grundrechtliche Positionen der Betroffenen nicht rechtfertigen.

Der Landesbeauftragte hält eine Überprüfung dieser Situation für geboten und fordert die Landesregierung auf, das ihr Mögliche in der Umsetzung wie auch in der Beteiligung am Gesetzgebungsverfahren zu initiieren, um weitere Beeinträchtigungen von Betroffenen zu verringern.

19. Schulen

19.1 Vortragsangebote an Gymnasien

Wie bereits im VI. Tätigkeitsbericht (Ziff. 19.5) dargestellt, bietet der Landesbeauftragte den Gymnasien Referate zum Thema „Datenschutz und seine verfassungsrechtlichen Grundlagen“ an.
Im Berichtszeitraum wurden erneut mehrere Gymnasien angeschrieben, jedoch konnte lediglich eine Rückäußerung verzeichnet werden. Das verhaltene Echo hat sich damit fortgesetzt.

19.2 Übermittlung von Schülerdaten an eine Bürgerinitiative

Eine Bürgerinitiative plante eine Befragung aller betroffenen Eltern zur Klärung von Schulstandortentscheidungen eines Landkreises. Der Vorsitzende der Bürgerinitiative, gleichzeitig auch Vorsitzender des Stadtelternrates, erhielt vom Landkreis eine Liste der betroffenen Eltern (Namen und Anschriften).
Der Landesbeauftragte wies den Landkreis darauf hin, dass eine Datenübermittlung an Elternvertretungen nach § 84 a Abs. 3 Schulgesetz möglich ist, soweit es für den Erziehungs- und Bildungsauftrag erforderlich ist. In diesem Falle war der Vorsitzende des Stadtelternrates jedoch nicht als

Elternvertretung, sondern als Leiter der Bürgerinitiative tätig gewesen. Nach Hinweis auf die fehlende Rechtsgrundlage zur Datenübermittlung wurde die Adressenliste an den Landkreis zurückgegeben.
Ein datenschutzrechtlich unbedenkliches Vorgehen wäre das sogenannte **Adressmittlungsverfahren** gewesen. Hierzu hätte es eines Schreibens der Elterninitiative bedurft, in dem auf das Problem hingewiesen wird, mit dem Zusatz, dass sich die Eltern freiwillig an die Initiative wenden können, um sich zu beteiligen. Dieses Schreiben hätte durch die Initiative kuvertiert beim Landkreis abgegeben und von diesem an die betroffenen Eltern weitergeleitet werden können.

19.3 Anmelde- und Aufnahmebögen

Leider bedürfen auch von Schulen erstellte Vordrucke immer einmal wieder einer datenschutzrechtlichen Überarbeitung. So geschehen bei den von einer Landesschule verwendeten Anmelde- und Aufnahmebögen. Diese enthielten u.a. nicht erforderliche Datenerhebungen und waren zum Teil unübersichtlich strukturiert.
Der Landesbeauftragte hat darauf hingewiesen, dass der Bewerbungs- und Anmeldebogen vom Aufnahmebogen, der erst nach erfolgter Aufnahme auszufüllen ist, getrennt werden sollte. Außerdem sollten die Pflichtangaben und die freiwilligen Angaben auch optisch voneinander getrennt abgefragt werden. Ebenso sollten die Daten „Geburtstage der Eltern“ in „Geburtsjahr“ geändert und das „Alter der Geschwister“ gestrichen werden, da diese Angaben nicht für die Aufgabenerfüllung der Schule erforderlich sind.
Die Vordrucke wurden entsprechend der datenschutzrechtlichen Hinweise umgehend überarbeitet.

20. Sozialwesen

20.1 Arbeitslosengeld II

Die Umsetzung des Vierten Gesetzes für moderne Dienstleistungen am Arbeitsmarkt („Hartz IV“) führte insbesondere für den Bereich der Grundsicherung für Arbeitssuchende (SGB II) in der zweiten Hälfte des Jahres 2004 zu öffentlichen Diskussionen. Auch in datenschutzrechtlicher Hinsicht bedurfte das Verfahren der Beratung der Datenschutzbeauftragten des Bundes und der Länder.

Die Begleitung der Datenerhebung und -verarbeitung durch die Bundesagentur für Arbeit und die Agenturen für Arbeit oblag, zumindest soweit noch keine Arbeitsgemeinschaften nach § 44b SGB II gegründet waren, dem Bundesbeauftragten für den Datenschutz. Betroffen waren vornehmlich die bisherigen Empfänger von Arbeitslosengeld bzw. -hilfe. Im Zuständigkeitsbereich der Landesbeauftragten für den Datenschutz sahen die Übergangsvorschriften der §§ 65 ff. SGB II vor, dass die kommunalen Träger, die noch keine **Arbeitsgemeinschaft** eingerichtet und noch keine Aufgaben an die Arbeitsgemeinschaft übertragen hatten, zunächst für die Personen tätig werden, die im Jahr 2004 Hilfe zum Lebensunterhalt nach

dem Bundessozialhilfegesetz erhielten. Damit waren die kommunalen Träger verantwortliche Stellen, denen die Beachtung der datenschutzrechtlichen Vorschriften oblag.
Gemäß den Vorgaben des § 44b SGB II haben die meisten Leistungsträger (Arbeitsagenturen und kommunale Träger) Arbeitsgemeinschaften gebildet. Infolge der kommunalen Beteiligung und in Anlehnung an die Zuständigkeits- und Aufsichtsregelung des § 44b Abs. 3 SGB II ist nunmehr die Kontrolle durch den Landesbeauftragten absehbar. Nach § 6a SGB II zugelassene kommunale Träger unterliegen jedenfalls der Kontrolle durch den Landesbeauftragten.

Im Juli 2004 wurde von der Bundesagentur ein Fragebogen für die Beantragung von Arbeitslosengeld II herausgegeben, der auch vielfach von kommunalen Trägern verwendet worden ist. Der massive Umfang der im Fragebogen und den Zusatzerklärungen vorgesehenen Datenerhebung führte häufig zum Empfinden bei den Betroffenen, sich unangemessen offenbaren zu müssen. Aber auch wenn die Antragsteller einer Mitwirkungspflicht unterliegen (§ 60 SGB I) und es sich um ein Massenverfahren handelt, haben die verantwortlichen Stellen den Umfang der Datenerhebung auf das zu begrenzen, was für die Aufgabenerfüllung unerlässlich ist. Demgemäß hat der Landesbeauftragte regelmäßig darauf hingewiesen, dass die Erforderlichkeit der einzelnen Abfragen des Antragsformulars für die Antragsbearbeitung stets zu prüfen ist.

Zudem hatte eine Arbeitsgruppe der Datenschutzbeauftragten des Bundes und der Länder zusammen mit der Bundesagentur und dem Bundesministerium für Wirtschaft und Arbeit daran mitgewirkt, die Fragebögen für die Bürger zu „verschlanken“.

Ein Ergebnis des Einwirkens der Datenschutzbeauftragten des Bundes und der Länder war unter anderem, dass die Bundesagentur Ausfüllhinweise zu dem Fragebogen erstellt hat, die unter anderem auf den Webseiten der Arbeitsagenturen veröffentlicht worden sind. Die Arbeitsagenturen wurden angehalten, die Ausfüllhinweise zu berücksichtigen. Ein weiteres Ergebnis ist, dass die im Jahr 2005 neu zu veröffentlichenden Fragebögen sich inhaltlich an den Hinweisen der Datenschutzbeauftragten des Bundes und der Länder orientieren. Weiterhin haben die Datenschutzbeauftragten darauf hingewirkt, dass diejenigen, die ihren Antrag frühzeitig unter Verwendung des ersten Fragebogens gestellt haben, nicht benachteiligt werden.

Ein weiteres datenschutzrechtliches Problem ist die Verwendung der von der Bundesagentur vorgegebenen Software A2 LL. Es besteht die Gefahr eines uneingeschränkten bundesweiten Zugriffs der Sachbearbeitung auf alle Daten, die im Rahmen von A2 LL erfasst worden. Erforderlich und damit datenschutzrechtlich zulässig ist jedoch nur der Zugriff auf diejenigen Daten, die für die Bearbeitung im jeweiligen Einzelfall unerlässlich sind.
Zur bisherigen Problematik ist auf die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom Oktober 2004

zu den gravierenden Datenschutzmängeln bei Hartz IV **(Anlage 22)** zu verweisen. Auch in Zukunft wird die Umsetzung der Grundsicherung für Arbeitssuchende beobachtend und beratend begleitet.

20.2 Anforderung von Kontoauszügen im Rahmen der Vermögensprüfung

Eine Sozialhilfeempfängerin wandte sich an den Landesbeauftragten, da sie im Rahmen der Vermögensprüfung regelmäßig Kontoauszüge vorlegen soll. Bereits bei der Antragstellung sollte die Petentin die aktuellen Kontoauszüge der letzten drei Monate vollständig und sortiert dem Sozialamt zur weiteren Prüfung zur Verfügung stellen. Nunmehr beabsichtigte das Sozialamt sechs Monate später eine erneute Vermögensprüfung unter Vorlage der Kontoauszüge der letzten drei Monate.

Die Erhebung personenbezogener Daten durch den Sozialleistungsträger ist ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung. Dieser ist auf der Grundlage des § 67a Abs. 1 Satz 1 SGB X nur zulässig, wenn er zur Aufgabenerfüllung erforderlich ist. Der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit gestattet lediglich unerlässliche Datenerhebungen. Daher vertritt der Landesbeauftragte in Anlehnung an andere Landesbeauftragte unter Berücksichtigung der hierzu ergangenen Rechtsprechung die Auffassung, dass grundsätzlich nach folgenden Kriterien Kontoauszüge der letzten drei bis sechs Monate von Hilfe Suchenden, die Leistungen zum Lebensunterhalt erhalten, gefordert werden können:

1. erstmalige Beantragung von laufenden Leistungen nach dem SGB XII
2. Beantragung von einmaligen Beihilfen gemäß § 31 Abs. 2 SGB XII
3. während des laufenden Hilfebezuges, nach Ablauf eines Hilfezeitraumes von mindestens zwölf Monaten
   oder
4. zwecks Klärung einer konkreten Frage zur Einkommens- und Vermögenssituation der Hilfe Suchenden, wenn diese nicht durch die Vorlage anderer Unterlagen herbeigeführt werden kann bzw. konkrete Zweifel an der Vollständigkeit oder Richtigkeit der Angaben der Hilfe Suchenden bestehen.

Der Landesbeauftragte verweist hierzu auch auf seine Darstellungen im III. Tätigkeitsbericht (Ziff. 24.6).

Das Sozialamt nahm - nach entsprechender Beratung - ohne Einsichtnahme in die Kontoauszüge der Petentin eine Prüfung der veränderten Vermögensverhältnisse vor.

20.3 Übernahme von Krankenhauskosten durch den Sozialhilfeträger

Ein Krankenhaus beklagte sich darüber, dass ein Sozialamt die Übernahme von Krankenhauskosten nach dem BSHG von der Ausfüllung eines zusätzlichen Fragebogens abhängig machte. Dieser Fragebogen umfasste u.a. neben dem Namen, Vornamen und der Anschrift auch Erschei-

nungsformen der behandelnden Erkrankung nach §§ 1 bis 5 Eingliederungshilfe-Verordnung.

Der Landesbeauftragte hatte das Sozialamt darauf hingewiesen, dass Personen, die keinen ausreichenden Krankenversicherungsschutz haben, Leistungen zur Krankenbehandlung entsprechend dem Dritten Kapitel, Fünften Abschnitt, Ersten Titel des Fünften Buches Sozialgesetzbuch (SGB V) erhalten. Daraus folgte, dass dem Sozialamt als Kostenträger grundsätzlich nicht mehr Zugriffsrechte auf Daten der Betroffenen zustehen als den Krankenkassen erlaubt sind. Damit war es unzulässig, den Vordruck "Fachärztliche Stellungnahme" in jedem Behandlungsfall den Krankenhausärzten zur Beantwortung zuzuleiten. Nur bei begründeten Hinweisen auf die sachliche Zuständigkeit des Landes als überörtlicher Träger gem. § 100 BSHG für wesentlich Behinderte oder von Behinderung Bedrohte (Personenkreis des § 39 Abs. 1 Satz 1 und Abs. 2 BSHG) sowie für Geisteskranke, Anfallskranke und Suchtkranke bestand ein gesetzlich begründetes Bedürfnis für weitere Angaben durch die Ärzte, wenn die Hilfegewährung in einer Einrichtung erforderlich ist (§ 47 BSHG i.V. mit der Eingliederungshilfe-Verordnung). Des Weiteren enthielt der verwendete Vordruck Unterteilungen und Fragen, die durch die Eingliederungshilfe-Verordnung rechtlich nicht abgedeckt werden. Die hierzu zählenden Fragen „Besteht Verdacht auf Krebs-Erkrankung?“ und „Besteht Verdacht auf TBC-Erkrankung?“ waren aus dem Vordruck zu streichen.

Der Landesbeauftragte wies das Sozialamt darauf hin, dass die stationären oder teilstationären Einrichtungsträger hinsichtlich der Prüfung der sachlichen Zuständigkeit nach § 100 BSHG durch einen Zusatz in dem zu überarbeitenden Vordruck sensibilisiert werden können. Dem Sozialamt wurde folgender Zusatz vorgeschlagen:

"Der Patient ist nicht krankenversichert. Die Behandlungskosten trägt die Sozialhilfe. Der überörtliche Träger der Sozialhilfe ist nur dann Kostenträger, wenn die Behandlung wegen einer vorhandenen oder drohenden, nicht nur vorübergehenden wesentlichen Behinderung im Sinne des § 39 BSHG oder wegen Geisteskrankheit, Anfallskrankheit oder Suchtkrankheit in einer stationären Einrichtung oder in einer Einrichtung zur teilstationären Betreuung erforderlich ist/war."

Das Sozialamt änderte sein Vorgehen.

20.4 Ausweisdokumente in der Sozialhilfeakte

Durch mehrere Eingaben von Petenten wurde dem Landesbeauftragten bekannt, dass einige Sozialämter vermehrt Ablichtungen von Ausweisdokumenten der Leistungsbezieher nach dem BSHG in der Sozialhilfeakte vorhalten.
Ein Sozialamt begründete die Vorhaltung der Ausweiskopien damit, dass anhand der kopierten Lichtbilder und dem persönlichen Erscheinen der Hilfe Suchenden eine eindeutige Identifizierung der Leistungsempfänger vorgenommen werden könne. Ein anderer Träger der Sozialhilfe sah darin

die Möglichkeit, Hilfe Suchenden, die einen Antrag auf Leistung nach dem BSHG gestellt und den hierfür vorgesehenen Formvordruck erhalten, jedoch nicht an den Träger der Sozialhilfe zurückgegeben haben, einen entsprechenden Ablehnungsbescheid zu erteilen.

Zwar trifft den Antragsteller bei Sozialhilfeleistungen nach §§ 60 ff. SGB I eine Mitwirkungspflicht (vgl. dazu VI. Tätigkeitsbericht, Ziff. 20.1). Die Pflicht zur Beantwortung bzw. zum Nachweis besteht jedoch nur, soweit dies für die Bearbeitung der beantragten Leistung erforderlich ist.
Danach reicht es grundsätzlich aus, dass zur Legitimierung der Personalausweis oder Reisepass vorgelegt und in einem Vermerk bzw. im Antragsvordruck schriftlich auf die Vorlage der Ausweisunterlagen hingewiesen wird (Handzeichen Sachbearbeiter).
Auf die Hinweise des Landesbeauftragten haben die Träger der Sozialhilfe Maßnahmen getroffen, um die unzulässige Datenerhebung künftig zu unterbinden.

20.5 Kontenklärung beim Rentenversicherungsträger

Ein Petent bat um Erläuterung, ob dem zuständigen Rentenversicherungsträger im Kontenklärungsverfahren erforderliche Urkunden (z.B. Ausweis für Arbeit und Sozialversicherung, Arbeitsbuch etc.) im Original vorgelegt werden müssen.
Die vom Petenten vorgelegten kopierten Unterlagen wurden mit der Begründung abgelehnt, dass nur die Originaldokumente vorzulegen seien und aufgrund enger Terminvorgaben das Kopieren der Originalunterlagen nicht möglich wäre.

Der Landesbeauftragte wies darauf hin, dass die im Kontenklärungsverfahren erforderlichen Unterlagen im Original, ggf. in Kopie mit amtlicher Beglaubigung oder Übereinstimmungserklärung, vorzulegen sind. Für die Vorlage des Ausweises für Arbeit und Sozialversicherung besteht u.a. die Möglichkeit von beglaubigten Abschriften des vollständigen Ausweises oder von Auszügen des Ausweises, in denen die Daten unkenntlich gemacht würden, die für den Träger der Rentenversicherung nicht erforderlich sind.

Der Rentenversicherungsträger hat auch unter dem Gesichtspunkt der Bürgerfreundlichkeit sein Verfahren geändert.

20.6 Datenerhebung bei Dritten anlässlich eines Gerichtsverfahrens

Im Rahmen eines einstweiligen Rechtsschutzverfahrens auf Übernahme von Miet- und Fernwärmekosten nach § 15a Abs. 1 BSHG hatte ein Sozialamt direkt bei der lokalen Versorgungs-GmbH Einzeldaten zum Zustandekommen der Fernwärmeschulden erhoben. Der Prozessbevollmächtigte des Antragstellers hatte sich deshalb an den Landesbeauftragten gewandt.

Das Sozialamt teilte mit, dass der Verdacht bestand, der Antragsteller hätte die Schulden missbräuchlich entstehen lassen. Der Antragsteller habe kein Telefon gehabt. Gegenüber dem Gericht hätte man aber, wegen des Eilverfahrens kurzfristig, vortragen müssen. Daher hätten die Daten direkt bei der Versorgungs-GmbH erhoben werden müssen. Dies sei im Rahmen von § 67a Abs. 2 Satz 2 Nr. 2 a) SGB X auch zulässig, da eine Rechtsvorschrift, nämlich § 9 DSG-LSA, eine Erhebung bei Dritten gestatte. Der Verdacht habe sich dann auch bestätigt.

Demgegenüber musste der Landesbeauftragte auf folgendes hinweisen:
Die §§ 9, 10 DSG-LSA stellen keine Rechtsvorschriften zur Datenerhebung bei anderen Personen im Sinne des § 67a Abs. 2 Satz 2 Nr. 2a) SGB X dar. Die spezialgesetzlichen Bundesregelungen zur Wahrung des Sozialgeheimnisses nach §§ 35 Abs. 1 SGB I, 67 Abs. 1 SGB X gehen den allgemeinen Regelungen des DSG-LSA vor (vgl. § 3 Abs. 3 Satz 1 DSG-LSA, §§ 37 Satz 1, 28 SGB I).

Zwar ist es nach § 67a Abs. 2 Nr. 2 b) aa) SGB X grundsätzlich möglich, Sozialdaten auch bei anderen Personen oder Stellen als dem Betroffenen zu erheben, wenn die Aufgabenerfüllung ihrer Art nach eine entsprechende Erhebung erforderlich macht. Dies kann u.a. dann der Fall sein, wenn die Angaben des Betroffenen zu überprüfen sind. Die Datenerhebung **ohne** Mitwirkung des Betroffenen nach § 67a Abs. 2 Satz 2 ist jedoch eine Ausnahme zum Grundsatz der Erhebung von Sozialdaten beim Betroffenen nach § 67a Abs. 2 Satz 1 SGB X und daher eng auszulegen. Zudem steht sie unter dem Vorbehalt, dass keine Anhaltspunkte dafür bestehen, dass durch die Fremdbefragung überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden können. Ein solcher Schutzfall bestand hier.

Die vom Sozialamt angenommene, durch Eile gebotene Erforderlichkeit der Nachfrage bei der Versorgungs-GmbH als Drittem bestand nicht. Zu klären war die Frage, ob es sich bei dem rückständigen Rechnungsbetrag der Fernwärmeversorgung um eine unerwartet hohe Nachforderung handelte, oder ob der Antragsteller langfristig und missbräuchlich Rechnungen hat auflaufen lassen.
Inhaltlich hätten sich die erforderlichen Informationen aus den beim Betroffenen vorhandenen Unterlagen ergeben. Der Antragsteller wäre nach § 60 Abs. 1 Nr. 3 SGB I auch zur Vorlage der entsprechenden Unterlagen (Zahlungsaufforderungen, Zahlungsdokumente) verpflichtet gewesen.
Unerheblich war, dass der Antragsteller kein Telefon hatte. Der Antragsteller war durch einen Prozessbevollmächtigten vertreten. Die Vollmacht ermächtigt grundsätzlich zu allen das Verfahren betreffenden Verfahrenshandlungen (§ 13 Abs. 1 Satz 2 SGB X). Die Abforderung von Unterlagen hätte hier daher beim Verfahrensbevollmächtigten erfolgen müssen, der gegenüber dem Landesbeauftragten erklärt hatte, dass entsprechende Unterlagen bei ihm vorgelegen haben.
Weiterhin standen der Datenerhebung auch schutzwürdige Interessen des Betroffenen entgegen. Dem Vorgang lässt sich entnehmen, dass es sich nicht um den Fall eines dauerhaften Leistungsbezuges, sondern lediglich

um die Übernahme von Schulden im Einzelfall handelte. Demgemäß bestand hier durchaus das schützenswerte Interesse des Betroffenen, den Kontakt zum Sozialleistungsträger als Sozialdatum nicht unbedingt anderen Stellen zur Kenntnis gelangen zu lassen. Auch konnte der Hinweis das Sozialamt nicht entlasten, dass Leistungen häufig direkt an den Versorger gezahlt werden. Auch bei der Bewilligung der Übernahme ist nicht notwendigerweise die direkte Zahlung erforderlich. Vielmehr hätte auch an den Antragsteller gezahlt werden können. § 15a Abs. 1 Satz 3 BSHG sieht lediglich vor, dass Hilfe an den Vermieter gezahlt werden "soll", wenn die zweckentsprechende Verwendung durch den Hilfesuchenden nicht sichergestellt ist. Anhaltspunkte hierfür lagen nicht vor.

20.7 Datenerhebung bei Sozialhilfe - Wohngeld

Empfänger von Leistungen der Sozialhilfe erhalten als Mieter einen besonderen Mietzuschuss (§ 31 Abs. 1 Wohngeldgesetz - WoGG). Das Sozialamt hat von Amts wegen die Voraussetzungen für die Leistung des besonderen Mietzuschusses zu prüfen und diesen zu bewilligen, wenn die Voraussetzungen vorliegen.

Nach § 25 Abs. 3 WoGG ist der Empfänger einer Miete verpflichtet, Auskünfte zu erteilen, wenn und soweit die Durchführung dieses Gesetzes es im Einzelfall erfordert. Im vorliegenden Fall hatte eine Petentin eine Betriebskostenabrechnung vorgelegt. Das Sozialamt hatte, ohne die Petentin einzuschalten, weitere Informationen beim Vermieter eingeholt.
Soweit noch weitere konkrete Einzelinformationen erforderlich gewesen wären, hätten diese zunächst bei der Petentin abgefragt werden müssen (§ 67a Abs. 2 Satz 1 SGB X). Erst wenn dies nicht ausreicht, kann im konkreten Einzelfall begründet die Abfrage beim Vermieter als Dritten erfolgen.

Darüber hinaus hätte das zuständige Sozialamt im vorliegenden Fall nur prüfen müssen, welche Änderungen gegenüber der letzten Betriebskostenabrechnung vorgenommen wurden. Die Petentin musste jedoch einen erneuten Vordruck vollständig ausfüllen, was eine unzulässige Doppelerhebung darstellte.
Mit Wegfall der Hilfe zum Lebensunterhalt und somit auch des Mietzuschusses können Bedürftige Wohngeld beim Wohngeldamt beantragen. Hierzu erhalten die Bedürftigen mit dem Einstellungsbescheid einen Wohngeldantrag. Auf dem Vordruck ist allerdings kein Hinweis enthalten, dass bereits Leistungen nach dem Wohngeldgesetz (hier: Mietzuschuss) geleistet wurden und damit dem Sozialamt bereits Belege zum Antrag auf Wohngeld vorliegen. Somit ist nicht ausgeschlossen, dass die Antragsteller mit dem Wohngeldantrag alle Unterlagen erneut vorlegen.

Hierbei wurde u.a. nicht berücksichtigt, dass unter Umständen beim Sozialamt eingereichte und somit bereits vorliegende Belege noch Gültigkeit haben, die vom Sozialamt an das Wohngeldamt hätten befugt übermittelt werden dürfen (§ 69 Abs. 1 Nr. 1 SGB X). Die Erhebungsbefugnis der

Wohngeldstelle und die Übermittlungsbefugnis des Sozialamtes sind im Rahmen der Erforderlichkeit der wiederholten Abfragen zu beachten.

Die zuständige Stadt wurde darauf hingewiesen, dass z.B. auf dem Wohngeldantrag eine interne Kennung klarstellen kann, dass bereits Leistungen vom Sozialamt erbracht wurden und somit Belege vorhanden sind. Anhand dieser Kennung kann das Wohngeldamt die Übermittlung der Unterlagen vom Sozialamt auslösen.

Der Stadt wurde empfohlen, ihr Verfahren im Sozial- und Wohngeldamt entsprechend umzustellen.

20.8 Sprechstunden im Sozialamt

Ein Petent teilte dem Landesbeauftragten mit, dass ein Sozialamt Sprechstunden bzw. Anträge für Sozialhilfe gleichzeitig in einem Raum mit Sprechstunden für Antragsteller von Rundfunkgebührenbefreiung durchgeführt hat.
Durch diese Verfahrensweise wurden dem Petenten Sozialdaten eines anderen Antragstellers bzw. Beratung Suchenden offenbart.

Der Landesbeauftragte hat das Sozialamt darauf hingewiesen, dass die Bedenken des Petenten gegen die gleichzeitige Beratung von Sozialhilfeangelegenheiten und von Rundfunkgebührenbefreiungen zu Recht bestanden. Nach § 35 SGB I hat jeder Anspruch darauf, dass die ihn betreffenden Sozialdaten (§ 67 Abs. 1 SGB X) von den Leistungsträgern nicht unbefugt übermittelt werden.
Eine Übermittlung der personenbezogenen Daten erfolgt bereits dann, wenn Dritte ohne Rechtsgrundlage oder Einwilligung des Betroffenen von den personenbezogenen Daten Kenntnis nehmen können (vgl. § 67 Abs. 6 Ziff. 3 SGB X). Diese Verfahrensweise gilt auch für die zuständigen Sachbearbeiter/innen, denen Sozialdaten ebenfalls offenbart werden, die gem. § 35 SGB I geheim zu halten sind.
Auf die Hinweise des Landesbeauftragten hat das Sozialamt umgehend reagiert und entsprechende Maßnahmen getroffen.

20.9 Private Sozialhilfeermittler

Eine Anfrage richtete sich auf Voraussetzungen und Rahmenbedingungen, sich als privater Sozialhilfeermittler selbständig machen zu können. Hierzu konnte der Landesbeauftragte nur mitteilen, dass diese Berufsberatung nicht in seine Zuständigkeit fällt. Im Rahmen allgemeiner Hinweise konnte er jedoch seine gegenüber den Sozialämtern dazu vertretene Auffassung mitteilen.

Der Einsatz von Sozialhilfeermittlern ist aus datenschutzrechtlicher Sicht nur zulässig, wenn dieser besondere Weg der Datenerhebung erforderlich und verhältnismäßig ist (vgl. VI. Tätigkeitsbericht, Ziff. 20.4). Die Verhältnismäßigkeit setzt voraus, dass die Erhebung der erforderlichen Informationen durch weniger eingreifende andere Ermittlungsmethoden nicht mög-

lich ist. Der Einsatz von Sozialhilfeermittlern zur Verdachtsfindung bzw. Verdachtserforschung ist mangels Erforderlichkeit unzulässig. Allenfalls ist bei konkret vorliegenden Anhaltspunkten eine Überprüfung im Einzelfall möglich.
Die Weitergabe der erforderlichen Informationen an den privaten Sozialhilfeermittler stellt eine Übermittlung von Sozialdaten dar, die einer gesetzlichen Grundlage bedarf. Diese fehlt in der Regel (vgl. dazu § 67d SGB X).

Eine Weitergabe von Sozialdaten wäre allenfalls noch denkbar, wenn es sich um eine sog. Datenverarbeitung im Auftrag handelte (§ 80 SGB X). Dabei dürfen jedoch nur Hilfstätigkeiten im Rahmen enger Vorgaben an Externe übertragen werden. Dies dürfte angesichts des überwiegend selbständigen Charakters der Ermittlungstätigkeit beim Einsatz privater Sozialhilfeermittler zu verneinen sein.

20.10 Aufhebung der Heranziehung

Eine Stadt bat den Landesbeauftragten um Klärung, ob sie die Unterlagen zur Gewährung von Sozialhilfe dem Landkreis nach Beendigung der Heranziehung auf der Grundlage des § 3 Abs. 1 des Gesetzes zur Ausführung des Bundessozialhilfegesetzes (AG-BSHG) und der Heranziehungsordnung des Landkreises übergeben durfte.

Die Heranziehung der Stadt hatte nichts an der Rechtsstellung des Landkreises als örtlicher Träger der Sozialhilfe geändert. Nach § 4 Abs. 1 AG-BSHG behielt der Landkreis den inhaltlichen Einfluss. Die Stadt entschied im Namen des Landkreises (§ 4 Abs. 1 Satz 3 AG-BSHG). Wenn nun der Landkreis die Aufgaben als örtlicher Träger der Sozialhilfe wieder selbst wahrnahm, lag die Aktenführung in seinen Händen. Es bestanden keine datenschutzrechtlichen Bedenken gegen die Übernahme der für die Aufgabenerfüllung erforderlichen personenbezogenen Unterlagen zur Gewährung von Sozialhilfe von der Stadt.

20.11 Mieterdaten beim Sozialamt

Dem Landesbeauftragten wurde durch eine Eingabe bekannt, dass ein Sozialamt einer Stadt eine Namensliste von Sozialhilfeempfängern an ihre Wohnungsbaugesellschaft übermittelte, um überprüfen zu können, ob eine rechtswidrige Inanspruchnahme von Sozialhilfe vorlag.

Grundsätzlich sind die Träger der Sozialhilfe nach § 117 Abs. 3 BSHG zur Vermeidung rechtswidriger Inanspruchnahme von Sozialhilfe befugt, Daten zu Personen, die Leistungen nach diesem Gesetz beziehen, bei anderen Stellen ihrer Verwaltung, bei ihren wirtschaftlichen Unternehmen und bei den Kreisen, Kreisverwaltungsbehörden und Gemeinden zu überprüfen, soweit sie für die Erfüllung dieser Aufgaben erforderlich sind.
Gemäß § 3 Abs. 1 AG-BSHG hatte der Landkreis zur Durchsetzung der ihm als örtlichen Träger der Sozialhilfe obliegenden Aufgaben durch Satzung die Stadt herangezogen. Da nur der Träger der Sozialhilfe befugt war, Daten von Personen, die Leistungen nach dem BSHG beziehen, bei

seinen wirtschaftlichen Unternehmen zu überprüfen, konnte die herangezogene Stadt dieses Recht nicht auf ihren eigenen Bereich erweitern. Die Stadt war nach § 117 Abs. 3 BSHG nicht berechtigt, die Daten bei der von der Stadt getragenen Wohnungsbaugesellschaft mbH zu überprüfen, da diese kein Unternehmen des Kreises war.

Die Stadt wurde aufgefordert, zur Beseitigung der Rechtsmängel und der Beeinträchtigung des Sozialdatenschutzes die ohne Rechtsgrundlage übermittelten Daten der Petentin von der Wohnungsbaugesellschaft zurückzufordern. Es wurde darauf hingewiesen, dass künftig von einer Sozialdatenübermittlung an Unternehmen privater Rechtsform in Anwendung des § 117 Abs. 3 Sätze 1 und 2 abzusehen ist.

20.12 BAföG-Datenabgleich

Im VI. Tätigkeitsbericht (Ziff. 20.8) hatte der Landesbeauftragte auf die Problematik des Datenabgleichs bei BAföG-Empfängern hingewiesen. Eine dauerhafte und vollständige Abfrage zu BAföG-Antragstellern beim Bundesamt für Finanzen sei mangels spezieller gesetzlicher Grundlage unzulässig.

Die Datenschutzbeauftragten des Bundes und der Länder haben die Problematik auf ihrer 66. Konferenz im September 2003 erörtert. Sie haben nachdrücklich gefordert, für den automatisierten Datenabgleich eine - teilweise als klarstellend empfundene - gesetzliche Regelung zu schaffen. Der Bundesbeauftragte hat die zuständigen Bundesministerien entsprechend informiert.

Mit dem 21. Gesetz zur Änderung des Bundesausbildungsförderungsgesetzes vom 2. Dezember 2004 (BGBl. I S. 3127) ist nunmehr dem § 41 ein Absatz 4 angefügt worden, der es den Ämtern für Ausbildungsförderung erlaubt, regelmäßig im Wege des automatisierten Datenabgleichs zu überprüfen, ob und welche Daten nach § 45d Abs. 1 des Einkommensteuergesetzes dem Bundesamt für Finanzen übermittelt worden sind.

20.13 Auskunftspflicht von Ärzten im Rahmen der Unfallversicherung

Ein Unfallversicherungsträger forderte von Ärzten, die einen Petenten früher behandelt hatten, pauschal vollständige Krankheitsblätter ab. Darüber hinaus sollte von einem privaten Krankenversicherungsunternehmen ein Auszug aus dem Leistungsverzeichnis über die Erkrankungen im Bereich des behandelten Organs vorgelegt werden.

Der Landesbeauftragte für den Datenschutz wies den Unfallversicherungsträger auf Folgendes hin:
Anfragen an frühere behandelnde Ärzte haben sich auf Erkrankungen bzw. Bereiche von Erkrankungen zu beschränken, die mit dem Unfall in einem ursächlichen Zusammenhang stehen könnten. Eine Datenerhebung bei nicht-öffentlichen Stellen hat unter Angabe der zur Auskunft verpflichtenden Vorschrift zu erfolgen. Werden Daten über frühere Erkrankungen

bei nicht an der Heilbehandlung beteiligten Ärzten abgefordert, hat dies unter Angabe des § 203 SGB VII zu erfolgen.

Auch die bisher erfolgte Abforderung von Informationen zu früheren Erkrankungen bei einem **privaten Krankenversicherungsunternehmen** war datenschutzrechtlich bedenklich. § 188 SGB VII begründet nur eine Auskunftspflicht **gesetzlicher** Krankenkassen gegenüber den Unfallversicherungsträgern. Für die Einholung von Informationen zu früheren Erkrankungen bei privaten Krankenversicherungsunternehmen ist daher eine Einverständniserklärung des Versicherten erforderlich.

Der Unfallversicherungsträger hat sein Verfahren umgestellt.

20.14 Arbeitspapier Outsourcing der Aufsichtsbehörden

Dem Landesbeauftragten lag ein Entwurf eines Arbeitspapiers der Aufsichtsbehörden der Sozialversicherungsträger „Outsourcing, Zulässigkeit der Auslagerung von Aufgaben, Anforderungen bei zulässigem Outsourcing“ vor. Das Papier wurde im Arbeitskreis Gesundheit und Soziales der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erörtert. Die Erstellung von Handlungsleitlinien wurde grundsätzlich begrüßt. Es wurde jedoch festgestellt, dass eine noch weitergehende Berücksichtigung einzelner datenschutzrechtlicher Aspekte wünschenswert wäre.

Inhaltlich wurde in dem Arbeitspapier überwiegend die Auslagerung von Aufgaben im Sinne einer Funktionsübertragung thematisiert. Dennoch wurde als Rechtsquelle u.a. auch der § 80 SGB X erwähnt, der die Datenverarbeitung im Auftrag regelt. Daher wären Hinweise zur oftmals nicht einfachen Abgrenzung der beiden Bereiche hilfreich, da sich erhebliche Unterschiede in den Rechtsauswirkungen ergeben. Während Datenübermittlungen im Rahmen einer Funktionsübertragung einer Rechtsgrundlage bedürfen, bleibt bei der Übertragung von reinen Hilfstätigkeiten im Rahmen der Datenverarbeitung im Auftrag der Auftraggeber die verantwortliche Stelle, so dass keine Übermittlung von Sozialdaten im Sinne des Gesetzes vorläge. Auch bei der Datenverarbeitung im Auftrag wären allerdings die gesetzlichen Rahmenbedingungen zu beachten (§ 80 SGB X).

Weiterhin ließ das Papier teilweise Interpretationsspielräume offen. Dies galt insbesondere im Bereich der fiskalischen Hilfsgeschäfte sowie der Hilfstätigkeiten im schlicht hoheitlichen Bereich. So ist beispielsweise die Auslagerung des Einkaufs von Schreibsystemen oder Aktenvernichtern datenschutzrechtlich unproblematisch. Anders zu beurteilen ist dagegen die Auslagerung von Schreibaufträgen oder Aktenvernichtung auf Dritte. Bedeutsam ist bei der Auslagerung von Aufgaben jeweils, ob Dritten ggf. Sozialdaten zur Kenntnis gelangen könnten.
Der Landesbeauftragte hatte angeraten, das Papier insoweit zu überprüfen.

20.15 Outsourcing des MDK-Schreibdienstes

Das Outsourcing gilt vielfach als Instrument kostensparender und gegebenenfalls effizienzsteigernder Aufgabenerfüllung. Auch der Medizinische Dienst der Krankenversicherung Sachsen-Anhalt (MDK) beabsichtigte, zur Kostensenkung und Sicherung von Arbeitsplätzen eine Service GmbH zu gründen, deren vorrangige Aufgabe es sein sollte, die sozialmedizinischen Gutachten für den MDK schneller und effektiver zu schreiben. Der MDK hat den Landesbeauftragten erfreulicherweise frühzeitig beteiligt und ihm die zugrunde liegenden vertraglichen Entwürfe zur Verfügung gestellt. Dies gab dem Landesbeauftragten die Gelegenheit, auf besondere datenschutzrechtliche Anforderungen hinzuweisen, um dem Persönlichkeitsrecht der betroffenen Patienten umfänglich Rechnung tragen zu können.

Für die datenschutzrechtliche Bewertung war einerseits die Frage zu erörtern, ob es sich bei dem angedachten Verfahren um eine Datenverarbeitung im Auftrag (§ 80 SGB X) handelte. Bei einer Datenverarbeitung im Auftrag nach § 80 SGB X hätte der MDK als die für Sozialdaten verantwortliche Stelle eine Vielzahl gesetzlicher Voraussetzungen zu erfüllen.

Wesentlich war jedoch der Hinweis darauf, dass die in sozialmedizinischen Gutachten des MDK enthaltenen sensiblen personenbezogenen Daten nicht nur dem Sozialdatenschutz unterliegen. Soweit die Ärzte des MDK im Rahmen ihrer Aufgabenerfüllung Daten erhoben und verarbeitet haben, war auch der besondere strafrechtliche Schutz des Patientengeheimnisses (§ 203 Abs. 1 StGB) zu berücksichtigen. Ein externer Schreibdienst kann im Unterschied zu angestellten Arzthelferinnen auch nicht als berufsmäßig tätiger Gehilfe im Sinne des § 203 Abs. 3 StGB angesehen werden. Externe Schreibdienste stehen nicht innerhalb des beruflichen Wirkungskreises des Arztes, ihre unterstützende Tätigkeit hat nicht den notwendigen inneren Zusammenhang mit der beruflichen Tätigkeit des Schweigepflichtigen.

Die Offenbarung von Patientengeheimnissen bedurfte daher einer Befugnisgrundlage. Nach Auffassung des Landesbeauftragten ergibt sich diese nicht aus allgemeinen Regelungen über die Auftragsdatenverarbeitung. Regelungen wie etwa § 8 DSG-LSA bzw. § 80 SGB X begründen als allgemeine Verwaltungsregelungen keine entsprechende Offenbarungsbefugnis. Die Einschränkung des Grundrechts auf informationelle Selbstbestimmung des Patienten über seine Gesundheitsdaten bedürfte im Hinblick auf den mehrfachen besonderen Schutz (personenbezogene Daten besonderer Art; Patientengeheimnis) einer spezifischen Rechtsgrundlage, wie sie beispielsweise in einzelnen Landeskrankenhausgesetzen vorgesehen ist. Sachsen-Anhalt hat keine solche bereichspezifische Regelung. Der Landesbeauftragte regte daher an, jeweils im Einzelfall die Einwilligung des betroffenen Patienten einzuholen. Daraufhin erarbeitete der MDK in Abstimmung mit dem Landesbeauftragten eine Einwilligungserklärung zur Übermittlung von Sozialdaten an die Service GmbH, die den An-

forderungen des Rechts auf informationelle Selbstbestimmung Rechnung trägt.

20.16 Privatisierung der Krankenhilfeabrechnung

Im Berichtszeitraum (vor der mit dem Gesundheitsmodernisierungsgesetz eingefügten Regelung des § 264 Abs. 2 SGB V) hatten Sozialhilfeempfänger einen Anspruch auf Krankenhilfe gegen den örtlichen Träger der Sozialhilfe in entsprechender Anwendung von Regelungen der gesetzlichen Krankenversicherung. Die Abrechnung mit Ärzten und anderen Leistungserbringern war Aufgabe der zuständigen Sozialämter. Zur Kostenersparung wollte ein Sozialamt die Abrechnung auf eine private Firma übertragen. Die private Firma erhielt vom Sozialamt die Information, wer anspruchberechtigter Krankenhilfeempfänger sein kann. Die Leistungserbringer reichten ihre Rechnungen bei der privaten Firma ein, die im gewissen Umfang Prüfungen durchführt und Auszahlungen vornimmt.
Zu diesbezüglichen Vertragsentwürfen konnte der Landesbeauftragte beratend Stellung nehmen.

Bei den personenbezogenen Informationen zur Krankenhilfeberechtigung handelte es sich um besonders geschützte Sozialdaten. Eine Übermittlung durch die Sozialämter hätte einer sozialgesetzlichen Grundlage bedurft, die nicht gegeben war. Die Einschaltung einer nicht-öffentlichen Stelle und die Weitergabe von Sozialdaten an diese Stelle war daher lediglich als Datenverarbeitung im Auftrag zulässig, die den besonderen Anforderungen des § 80 SGB X entsprechen muss. Die materielle und datenschutzrechtliche Verantwortlichkeit musste beim Auftraggeber, hier dem Sozialamt, verbleiben. Der Vertragsentwurf entsprach diesen Anforderungen weitestgehend. Die von der privaten Firma durchzuführenden Prüfungs- und Vergütungstätigkeiten waren begrenzt und detailliert beschrieben. Das Handeln der privaten Firma war umfänglich vom Weisungsrecht des auftraggebenden Sozialamtes abhängig. Lediglich zu einzelnen Formulierungen wurde durch den Landesbeauftragten eine Klarstellung angeregt, um das Missverständnis zu vermeiden, die private Firma könnte zu eigenständiger Recherche, Sachbearbeitung und eigenständiger Entscheidung berufen sein.

Die besonderen Anforderungen an die Verarbeitung von Sozialdaten im Auftrag durch nicht-öffentliche Stellen nach § 80 Abs. 5 SGB X waren ebenfalls erfüllt. Zunächst hatte der Sozialleistungsträger dargelegt, dass die Arbeiten bei der privaten Firma erheblich kostengünstiger realisiert werden können, da bereits im Verwaltungsbereich Einsparungen bis zu 50 % erwartet wurden. Auch verblieb der überwiegende Teil des Datenbestandes des Sozialhilfeträgers bei ihm selbst. Die Auftragsdatenverarbeitung erfolgte in Fallgruppen bei teilweise eigener Bearbeitung. Zudem wurden lediglich aufgabenorientierte Informationen übermittelt.
Zu den Archivierungsregelungen wurde auf Änderungsbedarf hingewiesen. Es ging um Vorgangsarchivierung auf Verwaltungsebene, nicht um archivrechtliche Aufbewahrung. Es erschien jedoch nicht vertretbar, der privaten Firma die Speicherung einzelner Vorgänge für die Dauer der

Laufzeit des gesamten Vertrages aufzugeben. Auf die Regelung des § 84 Abs. 2 Satz 2 SGB X wurde hingewiesen.

Nach § 80 Abs. 2 Satz 1 SGB X ist zudem eine Datenverarbeitung im Auftrag lediglich dann zulässig, wenn der Datenschutz beim Auftragnehmer den Anforderungen genügt, die für den Auftraggeber gelten. Diesbezüglich hatte der Vertragsentwurf vorgesehen, die in der Anlage zu § 78a SGB X enthaltenen Maßnahmen in das Vertragswerk zu inkorporieren. Gemäß § 80 Abs. 2 Satz 2 SGB X sind jedoch die technischen und organisatorischen Maßnahmen im Einzelnen festzulegen. Zu bestimmen wären beispielsweise Zeit, Ort und Berechtigte für die Übergabe der für die Datenverarbeitung vorgesehenen Datenbestände. Gleiches gilt für die Aufbewahrung der Datenträger, die Beseitigung von Ausschussmaterial, die Löschung von Restdaten usw. Beispielhafte Festlegungen könnten den Passwortschutz und Verschlüsselungen, jeweils nach dem Stand der Technik, betreffen. Nr. 8 der Anlage zu § 78a SGB X verlangt zudem, dass bei Rechenzentren, die für mehrere Auftraggeber arbeiten, eine Vermischung der Daten bzw. ein Zugriff eines Auftraggebers auf Daten eines anderen Auftraggebers verhindert werden.

Im Hinblick auf die Überwachungsrechte des Auftraggebers nach § 80 Abs. 2 SGB X wurde darauf hingewiesen, dass eine lediglich schriftliche Einräumung der Prüfungsrechte nicht ausreichend ist. Vielmehr hat der Auftraggeber sich vor Ort von der Einhaltung der Datensicherheitsmaßnahmen zu überzeugen.

Der Vertragsentwurf sah vor, die bei der privaten Firma Beschäftigten auf das Datengeheimnis nach § 5 BDSG zu verpflichten. Dazu wurde angeregt, die Belehrung und Verpflichtung mit einer inhaltlichen Information zu verbinden, um sicherzustellen, dass sich die Betroffenen in strafrechtlicher Hinsicht nicht auf einen Verbotsirrtum berufen können. Auch eine Verpflichtung auf der Grundlage des Verpflichtungsgesetzes wurde nahegelegt, mit dem Ziel des entsprechenden Datenschutzniveaus im Sinne des § 80 Abs. 2 Satz 1 SGB X.

20.17 Erlassanträge zu Elternbeiträgen in Kindertagesstätten

Wie im VI. Tätigkeitsbericht (Ziff. 20.9) angekündigt, hatte der Landesbeauftragte auch in diesem Berichtszeitraum Antragsformulare auf Übernahme/Erlass von Elternbeiträgen für die Benutzung von Kindertageseinrichtungen überprüft. In den besuchten Landkreisen bestand ebenfalls Beratungsbedarf. Die vom Landesbeauftragten gegebenen Hinweise wurden unverzüglich in die Fragebögen und Hinweisblätter eingearbeitet. Der Landesbeauftragte hat nunmehr in allen Landkreisen Beratungen durchgeführt und somit auf eine landesweit gleichmäßige datenschutzgerechte Handhabung hingewirkt.

20.18 Vordrucke für Kindertagesstättenanmeldung

Der Landesbeauftragte hat in einer Verwaltungsgemeinschaft die dort verwendeten Vordrucke im Kindertagesstättenbereich geprüft. Das Ergebnis der datenschutzrechtlichen Überprüfung wurde der Verwaltungsgemeinschaft im September 2003 mitgeteilt. Zur Förderung des Engagements erfolgte im November 2003 eine persönliche ausführliche Beratung vor Ort. Die weitere Überarbeitung vollzog sich schleppend, so dass mehrfach Erinnerungen erforderlich waren. Mitte Februar 2004 übersandte die Verwaltungsgemeinschaft wiederum nur teilweise überarbeitete Vordrucke mit dem Hinweis, sie schließe hiermit die Überarbeitung ab.
Da weiterhin keine datenschutzgerechten Vordrucke vorlagen, hat der Landesbeauftragte Ende Februar 2004 erneut auf die Problematik im Vordruckwesen und die damit verbundene unzulässige Datenerhebung hingewiesen, verbunden mit der Aufforderung, über das Veranlasste zu berichten. Es erfolgte keine Reaktion. Nach erneuter Erinnerung teilte die Verwaltungsgemeinschaft mit Schreiben vom Anfang April 2004 mit, dass sich die Vordrucke in der Überarbeitung befinden und zu gegebener Zeit zur Ansicht übersandt würden. Am 18. Mai 2004 wurde eine Kontrolle vor Ort durchgeführt. Dabei wurde zunächst festgestellt, dass mit der Überarbeitung der Vordrucke noch nicht einmal begonnen worden war. Eine nachvollziehbare Erklärung für ihre unwahre Darstellung konnte die Verwaltungsgemeinschaft nicht abgeben.

Zur Verfahrensweise wurde festgestellt, dass die verwendeten Vordrucke ausgefüllt von den Erziehungsberechtigten in der Verwaltung (Hauptamt, Abteilung Kindertageseinrichtungen) abzugeben waren. Von dort wurden die vollständig ausgefüllten Anträge in Kopie an die Kindertageseinrichtungen übermittelt.
Damit lagen die gesamten erhobenen Sozialdaten, die einem besonderen Schutz unterliegen (§ 61 SGB VIII), und die ebenfalls besonders geschützten Gesundheitsdaten der Kinder (personenbezogene Daten besonderer Art, § 67a Abs. 1 SGB X) sowohl im Hauptamt als auch in der Kindertageseinrichtung vor.

Nach § 35 Abs. 1 SGB I i.V.m. §§ 61 Abs. 1, 62 Abs. 1, 63 Abs. 1 und 64 Abs. 1 SGB VIII dürfen Sozialdaten nur erhoben, verarbeitet und genutzt werden, soweit sie zur Aufgabenerledigung erforderlich sind. Die Wahrung des Sozialgeheimnisses umfasst die Verpflichtung, auch **innerhalb** der Verwaltungsgemeinschaft sicherzustellen, dass die Sozialdaten nur Befugten zugänglich sind und nur an diese weitergegeben werden (Grundsatz der informationellen Gewaltenteilung). Für die Antragstellung war die Verwaltungsgemeinschaft nach § 16 Abs. 3 SGB I verpflichtet, darauf hinzuwirken, dass unverzüglich klare und sachdienliche Anträge gestellt werden.

Die Vordrucke wiesen in der Überschrift nicht aus, für welchen Bereich sie Anwendung finden (z.B. Krippe, Kindergarten, Hort). Die Angaben, an wen sie zu richten sind, waren teilweise fehlerhaft. Hierbei war zu unterscheiden zwischen der Anmeldung bei der Verwaltung (Hauptamt) und der Auf-

nahme in der Kindertageseinrichtung (Einrichtung). Der Aufnahmevordruck für die Einrichtung wäre nur im Falle der tatsächlichen Aufnahme eines Kindes in der Einrichtung auszufüllen gewesen. Nur dieser Vordruck darf die Daten enthalten, die dort zur Betreuung erforderlich sind. Zur Aufgabenerfüllung des Fachamtes sind dagegen in der Einrichtung nötige Informationen, z.B. zur Erreichbarkeit für den Notfall, nicht erforderlich.

Weiterhin war für die Geschwisterermäßigung ein Vordruckfeld vorgesehen, welches zur Eintragung des Namens veranlasste. Eine Namensnennung war jedoch nach der Satzung und der Gebührensatzung gerade nicht erforderlich. Die Erhebung bzw. Speicherung des Namens war daher unzulässig.

Bei der Prüfung wurden weitere datenschutzrechtlich bedenkliche Sachverhalte festgestellt. So entsprach die Forderung nach einer amtsärztlichen Bescheinigung nicht der Rechtslage. Gemäß § 18 Abs. 1 Kinderförderungsgesetz (KiFöG) wird nur eine ärztliche Bescheinigung über die gesundheitliche Eignung gefordert. Ein „Gesundheitsattest für Kinder“ in einer Akte enthielt zusätzlich Daten über durchgeführte Impfungen. Die Speicherung dieser Angaben ist durch § 18 Abs. 1 KiFöG nicht gedeckt und damit unzulässig. Auch die geforderte Bescheinigung des Arbeitgebers eines Vaters war nicht erforderlich, da die Anmeldung nur für 5 Stunden vorgenommen wurde. Damit ist gem. § 3 Abs. 1 Nr. 2 KiFöG keine derartige Bescheinigung notwendig. Die Daten waren unzulässig erhoben und gespeichert. Auf die Löschungspflicht wurde hingewiesen (vgl. § 84 Abs. 2 Satz 1 SGB X).

Darüber hinaus begegnete die Speicherung personenbezogener Daten in den Gruppenbüchern einer Kindertagesstätte datenschutzrechtlichen Bedenken. Auch bei freiwilligen Angaben ist die Erhebung und Speicherung an der Erforderlichkeit auszurichten. Der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit gebietet der Verwaltung auch bei der Datenerhebung mit Einwilligung der Betroffenen nur zur Aufgabenerfüllung notwendige Informationen zu erfragen. Erforderlich sind aber nur Daten zur Erreichbarkeit für Notfälle, nicht aber Angaben zum Arbeitgeber.
Es lagen damit vielfache Verstöße gegen die zu beachtenden datenschutzrechtlichen Bestimmungen vor. Über einen längeren Zeitraum wurde die Korrektur erheblicher rechtswidriger Eingriffe in das informationelle Selbstbestimmungsrecht der Kinder bzw. ihrer Eltern hartnäckig verweigert. Der Landesbeauftragte hat das Vorgehen formell beanstandet.

20.19 Verwendungsnachweisprüfung bei Kindertagesstätten

Durch eine Eingabe wurde der Landesbeauftragte darauf aufmerksam, dass ein Landkreis in einem Vordruck zum Verwendungsnachweis für Zuweisungen gem. § 25 Abs. 2 KiFöG i.V.m. § 3 Abs. 6 Nr. 7 der Verordnung über den Belastungsausgleich bei der Kinderförderung Informationen der Erzieherinnen und Erzieher in Kindertagesstätten abfragte, die weit über das Erforderliche hinausgehen. So wurden u.a. die Namen der Erzieherin/des Erziehers, die Arbeitsverträge sowie der Nachweis der monatlichen

Vergütung abgefordert. Der Landesbeauftragte wies den Landkreis darauf hin, dass es bei der Prüfung der Zuweisungsvoraussetzungen ausreicht, nur die Bezeichnung der in der jeweiligen Einrichtung eingesetzten Personen wiederzugeben. Auch die Übersendung von Kündigungen oder Aufhebungsverträgen bzw. der Arbeitsverträge wird durch § 3 Abs. 6 Nr. 7 der Verordnung über den Belastungsausgleich bei Kinderförderung nicht erfasst.

Letztendlich besteht gem. § 5 Abs. 5 Satz 1 der Betreuungsverordnung die Möglichkeit der regelmäßigen Prüfung in allen Kindertageseinrichtungen, auch bei Einrichtungen in freier Trägerschaft. Auf diese Weise kann im Rahmen einer Vor-Ort-Prüfung Einblick in alle Unterlagen (hier: Arbeitsverträge, Gehaltsabrechnungen des pädagogischen Personals etc.) genommen werden.

Der Landkreis hat die Hinweise aufgenommen und sein Verfahren geändert.

21. Statistik

21.1 Geschlechterdifferenzierte Statistiken - Gender Mainstreaming

Die Landesbeauftragte für Gleichstellung und Frauenpolitik leitete im Zusammenhang mit einem Konzept der Landesregierung zur Einführung von Gender Mainstreaming in der Landesverwaltung eine interministerielle Arbeitsgruppe, die nach dem Kabinettsbeschluss u.a. darauf hinwirken sollte, dass "alle in den Ressorts verfügbaren personenbezogenen Statistiken soweit wie möglich nach Geschlechtern getrennt erstellt" werden sollten.
Ein Mitglied der Arbeitsgruppe hatte dabei jedoch rechtliche Bedenken. Nach seiner Auffassung sei "die Erweiterung von personenbezogenen Erhebungen um das Merkmal 'Geschlecht' durch das Datenschutzgesetz des Landes Sachsen-Anhalt nicht gedeckt". Es würde schlichtweg an einer Rechtsgrundlage fehlen, nach der im Zuge einer Geschäftsstatistik Verwaltungsdaten völlig zweckfremd auch nach geschlechterspezifischen Merkmalen ausgewertet werden dürften.
Der Landesbeauftragte konnte die Bedenken jedoch zerstreuen.

Rechtsgrundlage für die amtlichen Statistiken Sachsen-Anhalts ist das Statistikgesetz des Landes Sachsen-Anhalt (StatG-LSA), ggf. in Verbindung mit einem die jeweilige Statistik anordnenden Spezialgesetz. Im StatG-LSA wird neben Kommunalstatistiken im Wesentlichen zwischen Landes- und Geschäftsstatistiken unterschieden. **Landesstatistiken** werden nach § 4 Abs. 1 StatG-LSA in der Regel durch oder aufgrund eines Gesetzes angeordnet. In einer solchen Rechtsvorschrift ist der Umfang der zu erhebenden Daten abschließend geregelt, Spielräume, diesen z.B. um geschlechterspezifische Merkmale zu erweitern, bestehen, ohne die Rechtsgrundlage zu ändern, nicht.
Geschäftsstatistiken dagegen bedürfen in der Regel nicht der Anordnung durch Rechtsvorschrift. Wesentlicher Unterschied zu Landesstatisti-

ken ist, dass Geschäftsstatistiken keine Datenerhebung zu statistischen Zwecken vorausgeht.

Nach § 1 Abs. 2 Nr. 3 StatG-LSA werden solche Statistiken als Geschäftsstatistiken bezeichnet, bei denen Daten verwendet werden, die im Geschäftsgang der Behörden und Gerichte des Landes sowie der der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts anfallen und die bei diesen oder den übergeordneten Behörden oder öffentlichen Stellen geführt werden.

Für die beiden Arten von Statistiken stellt sich also überhaupt nicht die Frage nach der Erweiterung der Erhebung um geschlechterspezifische Merkmale; entweder ist sie mangels Rechtsgrundlage unzulässig oder eine Erhebung von Daten speziell zu statistischen Zwecken ist gar nicht vorgesehen.

Außerdem wies der Landesbeauftragte noch auf § 5 Abs. 1 Satz 2 i.V.m. § 4 Abs. 5 StatG-LSA hin. Danach ist bei Geschäftsstatistiken und bei neu angeordneten Landesstatistiken zu sichern, dass Aussagen getrennt nach Geschlechtern getroffen werden können, soweit dies dem Sinn der Statistik entspricht.
Damit sind mit der z.Zt. geltenden Rechtslage die wesentlichen Voraussetzungen bereits geschaffen, die Ziele des Gender Mainstreaming zu erreichen.
Die den Geschäftsstatistiken zugrunde liegenden vorhandenen Verwaltungsdaten können, soweit dies möglich und sinnvoll ist, auch geschlechterspezifisch ausgewertet werden. Die Rechtsgrundlagen von Landesstatistiken müssen den Forderungen des § 4 Abs. 5 StatG-LSA angepasst werden, wenn dies nicht bereits erfolgt ist.
Im Übrigen bestehen gegen die Veröffentlichung auch geschlechterspezifisch aufbereiteter Statistiken - wie bei allen Personenstatistiken - dann keine datenschutzrechtlichen Bedenken, wenn nicht aus ggf. vorhandenen Tabelleneinsen und -zweien direkt auf die dahinter stehende natürliche Person geschlossen werden kann (vgl. II. Tätigkeitsbericht, Ziff. 27.2).

21.2 Unternehmensregister bei den Statistischen Ämtern

Die Statistischen Ämter der Länder, so auch das Statistische Landesamt Sachsen-Anhalt und das Statistische Bundesamt, führen das Unternehmensregister für statistische Verwendungszwecke (Statistikregister). Rechtsgrundlage sind die VO (EWG) Nr. 2186/93 des Rates vom 22. Juli 1993 über die innergemeinschaftliche Koordinierung des Aufbaus von Unternehmensregistern für statistische Verwendungszwecke sowie das zu deren Durchführung erlassene Bundesgesetz vom 16. Juni 1998, hier im Besonderen Art. 1 (Statistikregistergesetz - StatRegG). Nach dem StatRegG haben verschiedene öffentliche Stellen, z.B. die Finanzbehörden, die Berufsverbände, die Industrie- und Handelskammern oder die Handwerkskammern, für ihren Bezirk vom Gesetz genau bestimmte Datenarten der Steuerpflichtigen, Mitglieder oder Kammerzugehörigen an das zuständige Statistische Landesamt zu übermitteln. Um die DV-techni-

sche Kompatibilität zu gewährleisten, wurde dazu im November 2002 vom Statistischen Bundesamt eine Datensatzbeschreibung des Lieferdatensatzes der Industrie- und Handelskammern erarbeitet und an die Statistischen Ämter der Länder übergeben. Nach dem Muster dieser Datensatzbeschreibung wurden Anfang 2003 durch das Statistische Landesamt die von § 4 StatRegG genannten Datenarten von den Industrie- und Handelskammern des Landes angefordert.

Aufgrund seiner besonders aufmerksamen Arbeitsweise fiel dem Beauftragten für den Datenschutz einer der Kammern auf, dass insgesamt 5 angeforderte Datenfelder, darunter der „Grund der Betriebsaufgabe“, nicht vom Gesetz gedeckt waren, die Übermittlung dieser Datenarten durch seine Kammer also ebenso unzulässig wäre wie die Erhebung der übermittelten Daten durch das anfordernde Statistische Landesamt. Er bat den Landesbeauftragten um eine rechtliche Überprüfung.

In einer daraufhin veranlassten Besprechung zwischen dem Landesbeauftragten, dem Statistischen Landesamt und dem Ministerium des Innern wurde eine rechtlich einwandfreie Lösung im Sinne des Datenschutzes erarbeitet. So wurde u.a. ein Weg gefunden, der von den datenübermittelnden Kammern dann zu beschreiten ist, wenn ihnen das Datum des Beginns der angemeldeten Tätigkeit in der Gewerbeanmeldung des Kammermitglieds nicht bekannt ist. Außerdem wird die Abforderung des Grundes der Betriebsaufgabe durch das Statistische Landesamt fortan unterbleiben.

Über diese Lösung hatte der Landesbeauftragte die Datenschutzbeauftragten des Bundes und der Länder unterrichtet.
Da nun von allen Seiten eine solche Lösung bei den Statistischen Landesämtern gefordert wurde, blieb dem statistischen Bundesamt nichts anderes übrig, als die Datensatzbeschreibung für die Datenanforderung bei den Industrie- und Handelskammern zu überarbeiten und dem geltenden Recht anzupassen.
Wie es möglich war, dass zum einen im Statistischen Bundesamt solche elementaren handwerklichen Fehler bei der Umsetzung eines Gesetzes gemacht werden konnten und zum anderen das rechtswidrige Arbeitsergebnis offenbar zunächst von allen Statistischen Landesämtern unbeanstandet verwendet werden konnte, blieb dem Landesbeauftragten ein Rätsel.

21.3 Statistik Online

Dem Landesbeauftragten war bekannt geworden, dass durch das Statistische Landesamt in Sachsen-Anhalt ein auch in anderen Bundesländern verbreitetes Verfahren zur Datenerhebung für bestimmte Bundesstatistiken Anwendung findet. Es handelt sich um „Statistik Online“, mit dem die Auskunftspflichtigen dem Statistischen Landesamt online, also über das Internet, die geforderten Auskünfte erteilen können. Ziel der Einführung des Verfahrens sei die Ablösung überkommener Prozesse, wie z.B. das des manuellen Ausfüllens und Auswertens von statistischen Erhebungs-

bögen, durch zeitgemäße Arbeits- und Organisationsformen. Damit sollen auskunftsgebende Stellen entlastet und eine beschleunigte und kostengünstigere Aufbereitung der Daten im Statischen Landesamt erreicht werden. Mit „Statistik Online“ können Daten u.a. für den Monatsbericht Bauhauptgewerbe, die Monatserhebung im Tourismus oder die vierteljährliche Produktionserhebung eingegeben werden.

Auf den ersten Blick schien das Verfahren auch hinlänglich sicher zu sein, da schon bei der Anmeldung (mittels Benutzername und Passwort) am Server des Statistischen Landesamtes eine durch SSL-Verschlüsselung gesicherte Verbindung aufgebaut wird.
Allerdings lässt die Entwicklung der Angriffsmethoden und -techniken auf Web-Clients, gerade im Bereich JavaScript, diese Einschätzung inzwischen mindestens fraglich erscheinen. Zunehmende Verbreitung finden nämlich Angriffe mit sogenanntem Cross-Site- und Cross-Frame-Scripting. Hierbei besteht der Trick des Angreifers darin, dem Browser vorzugaukeln, das JavaScript stamme von einer vertrauenswürdigen Site. Das untergeschobene JavaScript, das z.B. Cookies auslesen kann, wird ohne Rückfrage im Browser ausgeführt. Das kann im schlimmsten Fall dazu führen, dass der Angreifer aus einem gestohlenen Cookie eine Session-ID extrahiert und unter falschem Namen eine Verbindung mit einem Server aufbaut.
Der Nutzer, der an seinem Web-Browser Sicherheitseinstellungen so vornimmt, wie sie ihm von der (offiziellen) Site www.statistik.sachsen-anhalt.de empfohlen wird, glaubt sich in Sicherheit, die jedoch trügt. Damit besteht nicht nur eine Gefahr für die Vertraulichkeit und Integrität der in "Statistik Online" eingegebenen Nutzerdaten (§ 6 Abs. 2 DSG-LSA), sondern für alle weiteren vertraulichen Nutzertransaktionen.

Vom Landesbeauftragten mit diesem Sachverhalt konfrontiert, gab das Statistische Landesamt zu, das Problem bereits seit 2003 zu kennen und schon gemeinsam mit anderen Statistischen Landesämtern an einer Lösung zu arbeiten. Diese bestehe aus einem Verfahren in Form eines Java-Servlets. Dieses wird nicht auf dem Client ausgeführt, sondern auf dem Server, von wo es dynamisch HTML-Seiten generiert, die dann im Browser des Nutzers angezeigt werden. Dazu, und das ist der große Vorteil des neuen Verfahrens, muss im Browser weder JavaScript noch Java aktiviert sein, auch die Installation zusätzlicher Programme ist nicht erforderlich. Selbstverständlich, so wurde dem Landesbeauftragten vom Statistischen Landesamt versichert, würde auch das neue Verfahren die Daten nur SSL-verschlüsselt durch das Internet transportieren.

Der Landesbeauftragte hofft, dass diese Lösung bald Wirklichkeit wird und verfolgt die weitere Entwicklung aufmerksam.

22. Strafvollzug und Untersuchungshaft

22.1 Videoaufzeichnungen im Strafvollzug?

Nachdem dem Landesbeauftragten bekannt geworden war, dass in Justizvollzugsanstalten eines anderen Landes Besuche bei Anstaltsinsassen per Videoaufzeichnungen festgehalten wurden, erfragte er die Praxis im Land Sachsen-Anhalt.
Da die Bestimmungen der §§ 179, 180 Strafvollzugsgesetz (StVollzG) nur allgemeine Regelungen über die Verarbeitung von Gefangenendaten und Daten Dritter enthalten, ist es fraglich, ob allein die besondere Situation im Strafvollzug es erlaubt, aufgrund dieser allgemeinen Vorschriften derartige Eingriffe in das informationelle Selbstbestimmungsrecht von Gefangenen sowie von Besuchern vorzunehmen. Dabei ist insbesondere hinsichtlich der Daten Dritter zu berücksichtigen, dass eine besonders sorgfältige Abwägung zwischen Grundrechtsgewährleistung einerseits und öffentlichen Interessen andererseits erfolgen muss. Diese allein dem Verwaltungsvollzug zu überlassen, erschien dem Landesbeauftragten nicht angemessen.
Bei dieser Überlegung spielte auch eine Rolle, dass bezüglich Eingriffen von besonderer Qualität der jeweils zuständige Gesetzgeber - mit Rücksicht auf die vom Bundesverfassungsgericht dargelegten Voraussetzungen zur Zulässigkeit eines Eingriffs in das informationelle Selbstbestimmungsrecht - in der Regel gesonderte Bestimmungen geschaffen hat (z.B. §§ 86, 86a StVollzG bzw. im allgemeinen Datenschutzrecht bestehende Videoüberwachungsregelungen).
Daher informierte der Landesbeauftragte in seiner Anfrage das zuständige Ministerium der Justiz darüber, dass er die allgemeinen Datenerhebungs- und Verarbeitungsregeln als Grundlage für eine Videoüberwachung/-aufzeichnung als nicht ausreichend ansehe.

Erfreulicherweise teilte das Ministerium der Justiz die rechtliche Einschätzung des Landesbeauftragten und informierte ihn darüber, dass - soweit dies technisch überhaupt möglich wäre - Videoaufzeichnungen nur auf richterliche Anordnung, z.B. im Rahmen strafrechtlicher Ermittlungen, erfolgen würden. Eine Prüfung, ob solche Aufzeichnungen beantragt wurden und ob die dafür notwendigen Anträge begründet waren, wird noch durchgeführt.

22.2 Untersuchungshaft - Versuch einer gesetzlichen Regelung

Der Landesbeauftragte hatte Gelegenheit, zum Referentenentwurf eines Gesetzes zur Regelung des Vollzuges der Untersuchungshaft Stellung zu nehmen. Da ein solches Gesetz bereits lange auf der Forderungsliste der Datenschutzbeauftragten des Bundes und der Länder steht, hat der Landesbeauftragte die Möglichkeit genutzt, um auch auf die von der Datenschutzkonferenz bereits 1999 verabschiedete Entschließung „Angemessener Datenschutz auch für Untersuchungsgefangene“ erneut aufmerksam zu machen.
Der Landesbeauftragte hat darüber hinaus u.a. auf Folgendes hingewiesen:

Im Entwurf ist vorgesehen, eine Mehrfertigung der Anklageschrift an die Anstalt zu übersenden. Dies ist problematisch, da es vor allem in Fällen einer Nichtverurteilung bzw. einer Teilverurteilung regelmäßig zu unnötigen und damit unzulässigen Datenübermittlungen kommen dürfte. Damit ist noch nicht gesagt, ob im Einzelfall die Notwendigkeit für eine Übermittlung gegeben sein kann.
Selbst wenn eine Regelung geschaffen wird, welche im Falle der grundsätzlichen Erforderlichkeit für die Aufgabenerfüllung der Anstalt eine Übersendung erlaubt, ist eine Begrenzung auf die im Einzelfall erforderlichen Informationen - statt der gesamten Anklageschrift - geboten. Die Begründung des vorgelegten Entwurfs gibt insoweit keine weitergehenden Erläuterungen.

Im Entwurf ist weiter vorgesehen, dass das Gericht seine Entscheidungszuständigkeit bezüglich der Ausgestaltung der Untersuchungshaft auf die Haftanstalt übertragen kann. Ob die Anstalt in diesem Fall alle Daten, auch die Dritter wie z.B. Zeugen oder Geschädigter, benötigt, erscheint insbesondere unter dem Aspekt zweifelhaft, dass nicht jeder Anklage eine Verurteilung folgt.

Der Entwurf ermöglicht die Übermittlung von Entlassungsanordnungen aus der Untersuchungshaft auch in anderer als Schriftform. Auch wenn die Regelung zur Nutzung von Telefaxdiensten - unter bestimmten Voraussetzungen - noch akzeptabel erscheint, so genügt die Nutzung elektronischer Medien nur dann den datenschutzrechtlichen Anforderungen, wenn entsprechende technisch-organisatorische Maßnahmen getroffen werden, die insbesondere die Vertraulichkeit der personenbezogenen Daten bei der Übermittlung sicherstellen.
Der Landesbeauftragte regte an, eine elektronische Übermittlung über das Internet nur auf sicherem (verschlüsseltem) Wege zuzulassen. Ein Hinweis im Gesetzestext auf § 9 BDSG und die Anlage zu § 9 BDSG bzw. die entsprechenden Landesregelungen scheint aber ausreichend zu sein.

Der Landesbeauftragte bat das Ministerium der Justiz, über die weitere Entwicklung zu informieren.

23. Telekommunikations- und Medienrecht

23.1 Novellierung des Telekommunikationsgesetzes

Am 26. Juni 2004 trat das neue Telekommunikationsgesetz (TKG) in Kraft (BGBl. I S. 1190). Es beinhaltet erstmals einen eigenen Datenschutzteil (Teil 7 Abschnitt 2). Darum konnte die Verordnungsermächtigung in § 89 TKG a. F. ersatzlos wegfallen und gleichzeitig die bisherige Telekommunikations-Datenschutzverordnung (TDSV) außer Kraft treten.
Bereits im Zuge des Gesetzgebungsverfahrens haben die Datenschutzbeauftragten des Bundes und der Länder datenschutzrechtliche Verschlechterungen in den Entwürfen zum TKG der Bundesregierung sowie dahingehende Bestrebungen des Bundesrates kritisiert. Mit drei Entschlie-

ßungen, „Transparenz bei der Telefonüberwachung“ vom März 2003 **(Anlage 7)**, „Verbesserung statt Absenkung des Datenschutzniveaus in der Telekommunikation“ vom April 2003 **(Anlage 8)** sowie „Gravierende Verschlechterungen des Datenschutzes im Entwurf des neuen Telekommunikationsgesetzes“ vom November 2003 **(Anlage 14)**, hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ihren Forderungen nach einer Verbesserung des Datenschutzniveaus bei der Telekommunikation Nachdruck verliehen.

23.1.1 Keine Vorratsdatenspeicherung

Einige der geplanten und von den Datenschutzbeauftragten kritisierten Veränderungen wurden nicht in das neue TKG übernommen. So wurde vom Bundesrat und dem Rechtsausschuss des Bundestages die Einführung einer Pflicht zur sechsmonatigen Speicherung von Verkehrsdaten (früher: Verbindungsdaten gem. TDSV) bei den Diensteanbietern gefordert. § 97 Abs. 3 Satz 3 TKG sieht jedoch weiterhin eine **Maximal**speicherfrist von sechs Monaten vor, die in der Praxis von den Diensteanbietern nicht ausgeschöpft wird. Die Diensteanbieter können somit weiterhin die Verkehrsdaten für die zur Abrechnung erforderliche Zeit - maximal jedoch sechs Monate nach Versendung der Rechnung - speichern. Eine Pflicht zur Vorratsspeicherung für die Strafverfolgungsbehörden besteht nicht.

23.1.2 Beibehaltung der Unternehmensstatistik

Die Jahresstatistik der Unternehmen über die von ihnen zu Strafverfolgungszwecken durchgeführten Überwachungsmaßnahmen sollte abgeschafft werden, um die Unternehmen - so die Begründung - von überflüssigen Arbeiten zu entlasten.
§ 110 Abs. 8 TKG sieht jedoch weiterhin die Verpflichtung für Unternehmen zur Erstellung einer Jahresstatistik vor und entspricht damit der Forderung der Datenschutzbeauftragten nach Transparenz bei der Telefonüberwachung.
Die Regulierungsbehörde ist verpflichtet die Ergebnisse dieser Unternehmensstatistiken zusammenzufassen und jährlich in ihrem Amtsblatt zu veröffentlichen.

23.1.3 Kundendateien - keine Ausweitung des automatisierten Abrufs

Die vom Bundesrat geforderte Ausweitung des automatisierten Auskunftsverfahrens auch auf nicht-öffentliche Diensteanbieter wie Hotels, Krankenhäuser oder Behörden wurde aus Gründen der Verhältnismäßigkeit abgelehnt. § 112 Abs. 1 TKG sieht vor, dass lediglich Unternehmen, die Telekommunikationsdienste für die Öffentlichkeit erbringen, Kundendateien zu führen und zum automatisierten Abruf für die Regulierungsbehörde bereitzustellen haben.

23.1.4 Ungekürzte Speicherung der Zielrufnummern

Trotz der genannten positiven Aspekte gibt es im neuen TKG auch datenschutzrechtliche Verschlechterungen. Bisher wurden die Zielrufnummern gem. § 7 Abs. 3 TDSV grundsätzlich um die letzten drei Ziffern gekürzt gespeichert. Dies stellte eine datenschutzfreundliche Lösung dar, denn der Kunde musste nur aktiv werden, wenn er eine vollständige Speicherung der Zielrufnummern bzw. eine vollständige Löschung wünschte. Gemäß § 97 Abs. 4 Satz 2 TKG werden die Zielrufnummern nunmehr **ungekürzt** gespeichert, wenn der Teilnehmer nicht von seinem Wahlrecht nach § 97 Abs. 4 Satz 1 Ziff. 1 (um die letzten drei Ziffern gekürzte Speicherung der Zielrufnummern) oder 2 (vollständige Löschung) TKG Gebrauch macht. Allerdings handelt es sich hierbei um eine **Widerspruchslösung**, da der Kunde aktiv werden muss, um eine gekürzte Speicherung bzw. Löschung seiner Daten zu erreichen.
Der Landesbeauftragte empfiehlt den Telefonkunden, zukünftig von ihrem Wahlrecht unbedingt Gebrauch zu machen.

23.1.5 Geschlossene Benutzergruppen

Eine weitere - allerdings unbeabsichtigte - Folge der unter 23.1.4 genannten Änderung betrifft Teilnehmer geschlossener Benutzergruppen. Da § 97 Abs. 4 Satz 4 TKG unverändert aus § 7 Abs. 4 Satz 3 TDSV übernommen wurde, könnten nun alle Zielrufnummern ungekürzt gespeichert werden, ohne dass dem Teilnehmer der geschlossenen Benutzergruppe (z.B. Hotelgast, Krankenhauspatient) ein Wahlrecht eingeräumt wird. Nach Aussage des Bundesministeriums für Wirtschaft und Arbeit (BMWA) war diese Regelung vom Gesetzgeber so nicht gewollt. Es wurde schlichtweg vergessen, den Satz anzupassen. Da diese Regelung auch das private Telefonieren von Mitarbeitern in öffentlichen Stellen betrifft, empfiehlt der Landesbeauftragte, die bisherige Verfahrensweise beizubehalten und die Zielrufnummern bei Privatgesprächen um die letzten drei Ziffern gekürzt zu speichern.

23.1.6 Inverssuche

Gemäß § 105 Abs. 3 TKG ist bei der Auskunftserteilung nun auch die sogenannte Inverssuche erlaubt. D.h. von einem Teilnehmer, von dem nur die Rufnummer bekannt ist, können Name und Anschrift erfragt werden, wenn dieser nicht widersprochen hat. Kritikpunkt ist hier wiederum die **Widerspruchslösung**, die von dem jeweiligen Teilnehmer aktives Handeln erfordert. Im Allgemeinen werden solche Widerspruchsrechte jedoch nur von einer Minderheit in Anspruch genommen. Datenschutzfreundlicher ist deshalb immer eine **Einwilligungslösung**, bei der der Teilnehmer der Inverssuche ausdrücklich zustimmen muss. Telefonkunden sollten deshalb beim Abschluss von Verträgen mit den Diensteanbietern auch diese Widerspruchsmöglichkeit beachten.

23.1.7 Datenerhebung beim Kauf von Prepaid-Produkten

Gemäß § 111 Abs. 1 TKG müssen Diensteanbieter nun auch von solchen Kunden den Namen, die Anschrift und das Geburtsdatum erheben, die sogenannte Prepaid-Produkte erwerben. Obwohl die Kunden die Leistung im Voraus bezahlt haben (z. B. Guthabenkarten für Prepaid-Handys) und die Diensteanbieter somit die Daten für ihre betrieblichen Abrechnungszwecke gar nicht benötigen, werden sie verpflichtet, Daten für mögliche Strafverfolgungszwecke auf Vorrat zu speichern.

In seinem Urteil vom 22. Oktober 2003 (NJW 2004, S. 1191) hatte das Bundesverwaltungsgericht entschieden, dass § 90 Abs. 1 TKG a. F. keine ausreichende, dem Gebot der Normenklarheit genügende gesetzliche Grundlage für die Erhebung personenbezogener Kundendaten beim Erwerb vertragsloser Handys darstellt. Demzufolge waren Anbieter von Mobilfunkleistungen nicht verpflichtet, beim Verkauf von Prepaid-Produkten personenbezogene Daten der Kunden zu erheben.

Fraglich bleibt nach dieser Entscheidung jedoch, ob nicht trotz nunmehr hergestellter „Normenklarheit“ durch § 111 Abs. 1 TKG ein unverhältnismäßiger Eingriff in das verfassungsrechtlich gewährte Recht des Kunden auf informationelle Selbstbestimmung vorliegt, wenn die Diensteanbieter für den Geschäftszweck nicht erforderliche Daten nur für Zwecke der Strafverfolgung erheben müssen.

23.1.8 Zugriffe auf PIN und PUK

Laut der Begründung zum TKG-Entwurf bestanden bisher bei den Diensteanbietern sehr unterschiedliche Rechtsauffassungen hinsichtlich der Rechtsgrundlagen für Auskunftsersuchen, in denen Angaben über solche Daten wie z.B. PIN, PUK und Passwörter nachgefragt wurden, mittels derer der Zugriff auf andere Daten geschützt wird, die ihrerseits wiederum dem Fernmeldegeheimnis unterliegen können. Im Interesse der Rechtssicherheit ist daher in § 113 Abs. 1 Satz 2 TKG geregelt, unter welchen Voraussetzungen derartige Auskünfte zu erteilen sind (z. B. allgemeine Ermittlungsbefugnis nach §§ 161, 163 StPO).

Aus Sicht der Datenschutzbeauftragten bleibt es jedoch fraglich und kritikwürdig, wieso ein Zugriff auf die o.g. Daten ohne Bindung an einen Straftatenkatalog und ohne Richtervorbehalt ermöglicht wird, wenn die dahinter liegenden Daten u. U. dem Fernmeldegeheimnis unterliegen. Der Zugriff auf diese Daten sollte auch weiterhin nur unter den Voraussetzungen der hierfür einschlägigen gesetzlichen Vorschriften (§§100g, 100h StPO) zulässig sein.

23.2 EU-Initiative zur Vorratsdatenspeicherung

Als Reaktion auf die Terroranschläge vom 11. März 2004 in Madrid legten die EU-Mitgliedsstaaten Frankreich, Irland, Schweden und Großbritannien am 28. April 2004 den „Entwurf für einen Rahmenbeschluss über die Vor-

ratsspeicherung von Daten, die in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, oder von Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für Zwecke der Vorbeugung, Feststellung und Verfolgung von Straftaten einschließlich Terrorismus“ vor. Dieser Entwurf sah vor, dass für einen Zeitraum von mindestens 12 und höchstens 36 Monaten **sämtliche** Verkehrs- und Standortdaten, die bei der Nutzung von Telefon, SMS und Internet (World Wide Web, E-Mail, Voice-over-IP etc.) anfallen, von den TK- und Internetdiensteanbietern **auf Vorrat** gespeichert werden sollen.

In einer gemeinsamen Presseerklärung vom 25. Juni 2004 forderten die Datenschutzbeauftragten des Bundes und der Länder daraufhin von der Bundesregierung, den Entwurf dieses Rahmenbeschlusses abzulehnen, da bereits bei der Verabschiedung des neuen TKG aus gutem Grund auf die Einführung einer Pflicht zur Vorratsdatenspeicherung verzichtet worden war. Eine flächendeckende Vorratsspeicherung von Kommunikationsdaten würde zudem die Grundrechte auf freie Meinungsäußerung und auf ungehinderte Unterrichtung aus allgemein zugänglichen Quellen verletzen, da die bei der Internetnutzung anfallenden Daten ebenfalls auf Vorrat gespeichert werden müssten. Darüber hinaus bestünden erhebliche Zweifel, ob der vorgeschlagene Rahmenbeschluss mit Art. 8 der Europäischen Menschenrechtskonvention (Recht auf Achtung des Privatlebens und der Korrespondenz) vereinbar ist. Der Europäische Gerichtshof für Menschenrechte hat betont, dass die Vertragsstaaten auch zur Bekämpfung des Terrorismus nicht jede Maßnahme beschließen dürfen, die sie für angemessen halten. Vielmehr muss es sich um Maßnahmen handeln, die in einer demokratischen Gesellschaft notwendig sind und dem Verhältnismäßigkeitsgrundsatz entsprechen.
In seiner Sitzung vom 17. Februar 2005 beschloss der Bundestag entsprechend der Beschlussempfehlung der BT-Drs. 15/4597 seine bereits bei der Novellierung des TKG zum Ausdruck gebrachte Ablehnung einer Mindestspeicherfrist für Verkehrsdaten. Er forderte die Bundesregierung auf, vorbehaltlich der Darlegung entsprechender Rechtstatsachen, die die Notwendigkeit einer solchen Regelung auf europäischer Ebene darlegen und eine neue Behandlung dieser Thematik erfordern, einen etwaigen Beschluss in den Gremien der EU nicht mitzutragen.

Freilich scheinen sich weder die Bundesjustizministerin noch der Bundesinnenminister an diesen Bundestagsbeschluss gebunden zu fühlen, da sie gemeinsam mit den anderen Justiz- und Innenministern der EU weiterhin an der Einführung der umstrittenen Maßnahme festhalten und den Rahmenbeschluss spätestens im Juni 2005 verabschieden wollen. Ein Ende Februar 2005 erstellter überarbeiteter Entwurf wurde im Internet veröffentlicht. Darin ist nun eine Speicherfrist von 12 Monaten vorgesehen. Allerdings wird einzelnen Mitgliedsstaaten im Einklang mit nationalen Kriterien auch eine Speicherfrist von bis zu 36 Monaten anheim gestellt. Eine Speicherdauer von 6 Monaten wird als noch akzeptabel angesehen, wenn eine längere Frist national nicht durchsetzbar sein sollte.

Da nach einer bestimmten Übergangszeit europäisches in nationales Recht umgesetzt werden muss, würde so eine Speicherfrist von mindestens 6 Monaten eingeführt werden müssen, obwohl das Parlament dies eindeutig und mehrfach abgelehnt hat.

Das ganze Verfahren könnte sich jedoch noch verzögern, da Presseberichten zu entnehmen ist, dass zwischen dem EU-Rat auf der einen und der EU-Kommission sowie dem EU-Parlament auf der anderen Seite Uneinigkeit über die Zuständigkeit für das Gesetzgebungsverfahren besteht. Die EU-Kommission hat sich nun der Auffassung des Parlaments angeschlossen, wonach die Vorratsdatenspeicherung kein Instrument allein der dritten Säule der Union ist. Es wird empfohlen, die Maßnahme größtenteils im Rahmen der ersten Unionssäule zu behandeln.

23.3 Private Nutzung von E-Mail und Internet am Arbeitsplatz

Bereits in seinem VI. Tätigkeitsbericht (Ziff. 23.2) hatte der Landesbeauftragte auf die datenschutzrechtlichen Probleme hingewiesen, die mit der privaten Nutzung von E-Mail und Internet am Arbeitplatz verbunden sind. Da der öffentliche Arbeitgeber damit gegenüber seinen Mitarbeitern zum Diensteanbieter wird (ähnlich wie beim privaten Telefonieren), hat er die Vorschriften des TKG, insbesondere die §§ 88 bis 115, zu beachten und ist somit gem. § 88 Abs. 2 TKG zur Einhaltung des Fernmeldegeheimnisses verpflichtet.

Gemäß § 206 Abs. 1 StGB wird die Verletzung des Fernmeldegeheimnisses durch Unternehmen, die geschäftsmäßig Telekommunikationsdienste erbringen, mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft. Allerdings war bisher unklar, ob es sich bei öffentlichen Stellen um solche Unternehmen handelt. Das OLG Karlsruhe hat in einem Beschluss vom 10. Januar 2005 (Az. 1 Ws 152/04 - MMR 2005, S. 178) klargestellt, dass auch eine Hochschule als Unternehmen zu betrachten ist, wenn sie nicht ausschließlich hoheitlich tätig wird. Das ist dann der Fall, wenn sie die EDV-Systeme ihren Mitarbeitern zum Austausch von E-Mails für private Zwecke zur Verfügung stellt.

Diese Rechtsauffassung ist auf alle öffentlichen Stellen mit hoheitlichen Aufgaben übertragbar und gilt auch hinsichtlich anderer Telekommunikationsdienste (Telefon, Telefax, Internetzugang), d.h., Mitarbeiter öffentlicher Stellen des Landes können sich strafbar machen, wenn sie im Rahmen der genehmigten privaten Nutzung von Telefon, Telefax, E-Mail und Internet das Fernmeldegeheimnis verletzen.

Der Landesbeauftragte hat in seinem letzten Tätigkeitsbericht die individuelle Einwilligung der Mitarbeiter in die Protokollierung ihrer privaten Nutzung als eine Lösungsmöglichkeit aufgezeigt. Der Beschluss des OLG Karlsruhe macht deutlich, dass die Problematik der Einhaltung des Fernmeldegeheimnisses im konkreten Einzelfall zu schwerwiegenden Konsequenzen für die öffentliche Stelle führen kann. Fraglich scheint, ob durch die Einwilligung des Betroffenen in Protokollierungen seiner privaten Nut-

zung alle Rechtsfragen bezüglich der Einhaltung des Fernmeldegeheimnisses zu lösen sind. Schließlich können an der Kommunikation **Dritte** beteiligt sein, die nicht eingewilligt haben, dass ihre durch das Fernmeldegeheimnis geschützte Kommunikation - auf die sie auch vertrauen - beim Empfänger protokolliert und unter Umständen sogar von anderen Personen zur Kenntnis genommen wird.

Gemäß § 206 Abs. 2 Ziff. 2 StGB wird ebenso bestraft, wer „... unbefugt eine einem solchen Unternehmen zur Übermittlung anvertraute Sendung unterdrückt ...“, d.h., auch das Filtern und Blocken virenverseuchter Mails oder von Spam-Mails könnte - wenn es sich um **private** E-Mails handelt - eine Verletzung des Fernmeldegeheimnisses und damit eine strafbare Handlung darstellen. Ob etwa durch § 109 Abs. 1 Nr. 2 TKG eine derartige Befugnis gegeben ist, ist fraglich, da hier nur von Maßnahmen zum Schutz gegen unerlaubte Zugriffe die Rede ist. Zwar ist es aus Gründen der Datensicherheit zwingend erforderlich, dass öffentliche Stellen geeignete Maßnahmen gegen Viren und Spam ergreifen, allerdings sollte dann aufgrund der dargestellten Problematik ganz auf die private Nutzung von E-Mail verzichtet werden, denn die rein dienstliche Nutzung von E-Mail unterliegt nicht dem Fernmeldegeheimnis.

Der Landesbeauftragte empfiehlt den öffentlichen Stellen des Landes, ihren Mitarbeitern zum Abruf und Versenden privater E-Mails die Nutzung sog. Freemail-Anbieter (oder auch kostenpflichtiger Angebote) zu gestatten. Die dienstliche E-Mail-Adresse sollte nur noch für dienstliche Zwecke verwendet werden. Da es sich bei der Bereitstellung eines Internetzugangs für private Zwecke um einen für den Mitarbeiter kostenlosen Telekommunikationsdienst handelt und somit keine Verkehrsdaten protokolliert werden dürfen, ist eine individuelle Einwilligung des Mitarbeiters erforderlich, wenn eine Protokollierung erfolgen soll. Beim Abruf privater E-Mails über das Internet wird dann lediglich protokolliert, dass der Mitarbeiter die Seite eines Freemail-Anbieters aufgerufen hat. Der Dritte ist nicht mehr betroffen, da weder die Tatsache protokolliert wird, dass er mit dem Mitarbeiter kommuniziert hat, noch eine Notwendigkeit besteht, Inhalte der Kommunikation zur Kenntnis zu nehmen. Ebenso ist es nicht mehr erforderlich, private E-Mails aufgrund von Viren oder Spam zu unterdrücken. Ein aktueller Virenscanner muss natürlich an jedem Internet-Arbeitsplatz aktiviert sein. Ebenso sollte jeder Mitarbeiter über die Möglichkeit informiert werden, nach der privaten Nutzung des Internets den Cache des Browsers zu löschen.

Aufgrund der durch den Beschluss des OLG Karlsruhe deutlich gewordenen Problematik sieht der Landesbeauftragte Bedarf, mit dem Ministerium des Innern über die im Jahr 2001 erlassene Musterdienstanweisung über die Bereitstellung und Nutzung von Internet-Zugängen, die die **ausnahmsweise** private Nutzung von E-Mail und Internet erlaubt, zu beraten und diese ggf. zu überarbeiten.

23.4 Zuständigkeiten im Bereich des Rundfunks

Da den Landesbeauftragten wiederholt Anfragen und Beschwerden von Bürgerinnen und Bürgern zur Arbeitsweise der Gebühreneinzugszentrale (GEZ) erreichen, weist der Landesbeauftragte darauf hin, dass seine unmittelbare Zuständigkeit weder im Bereich des öffentlich-rechtlichen noch des privaten Rundfunks gegeben ist.

Gemäß § 39 des Staatsvertrages über den Mitteldeutschen Rundfunk (MDR) sind für den MDR die Vorschriften des Freistaates Sachsen über den Schutz personenbezogener Daten anzuwenden. Gem. § 42 Abs. 1 MDR-Staatsvertrag tritt an die Stelle des Sächsischen Datenschutzbeauftragten ein vom Verwaltungsrat für die Dauer von vier Jahren und auf Vorschlag des Intendanten bestellter Beauftragter für den Datenschutz. Dieser überwacht gem § 42 Abs. 2 MDR-Staatsvertrag die Einhaltung der Datenschutzvorschriften des MDR-Staatsvertrages, des Datenschutzgesetzes des Freistaates Sachsen und anderer Vorschriften über den Datenschutz.

Im Bereich des privaten Rundfunks ist gem. § 11 Abs. 3 Mediengesetz LSA die zuständige Aufsichtsbehörde zur Überwachung der Einhaltung der Datenschutzbestimmungen die nach § 38 Abs. 6 BDSG zuständige Aufsichtbehörde. In Sachsen-Anhalt ist dies das Landesverwaltungsamt.

Aufgrund der genannten Zuständigkeiten muss der Landesbeauftragte die Bürgerinnen und Bürger, die Probleme mit der GEZ haben, an den Datenschutzbeauftragten des MDR verweisen.

23.5 Beteiligung der GEZ am Adresshandel

Im Rahmen des Achten Rundfunkänderungsstaatsvertrages wurde in Artikel 5 der Rundfunkgebührenstaatsvertrag geändert. Unter anderem wurde § 8 des Rundfunkgebührenstaatsvertrages um einen vierten Absatz erweitert. Der neue § 8 Abs. 4 Rundfunkgebührenstaatsvertrag erlaubt es den öffentlich-rechtlichen Rundfunkanstalten, personenbezogene Daten im Zusammenhang mit dem Einzug der Rundfunkgebühren entsprechend § 28 BDSG zu erheben, zu verarbeiten und zu nutzen. Grund für den Verweis auf das BDSG war offensichtlich, die bei der GEZ gängige Praxis der Datenerhebung beim kommerziellen Adresshandel zu legitimieren.

Allerdings wurde diese Regelung von den für die Rundfunkanstalten zuständigen Datenschutzbeauftragten stark kritisiert, da hier einer öffentlichen Stelle - nämlich der GEZ - Befugnisse erteilt werden, die laut § 27 Abs. 1 BDSG nur bei nicht-öffentlichen Stellen und öffentlichen Stellen des Bundes und der Länder, die als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, Anwendung finden. Außerdem stellt auch § 28 BDSG keine Befugnis zur Erhebung personenbezogener Daten bei Dritten (z. B. Adresshandel) ohne Kenntnis des Betroffenen dar.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat dazu zwei Entschließungen verabschiedet **(Anlage 9 und 23),** in denen sie ihre Forderung nach einer grundlegenden Neuorientierung der Rundfunkfinanzierung, bei der das Prinzip der Datenvermeidung und Datensparsamkeit in stärkerem Maße berücksichtigt wird, bekräftigt. Gegen das Votum der Datenschutzbeauftragten haben die Länder bereits vor Jahren regelmäßige Übermittlungen von Meldedaten an die Rundfunkanstalten zugelassen, weil dies für erforderlich gehalten wurde. Eine parallele Nutzung von Daten aus den Melderegistern bei gleichzeitiger Beschaffung von Adressen im privaten Adresshandel ist jedoch unverhältnismäßig.

23.6 Datenerhebung zur Rundfunkgebührenbefreiung

Anträge auf Befreiung sind nach § 5 Abs. 2 der Verordnung über die Voraussetzungen für die Befreiung von der Rundfunkgebührenpflicht (Land Sachsen-Anhalt) bis auf die Fälle des § 1 Abs. 1 Nr. 5 (Zuständigkeit des Ausgleichsamtes) an den zuständigen örtlichen Träger der Sozialhilfe bzw. an die Gemeinde zu richten.
Über den Antrag selbst entscheidet die Landesrundfunkanstalt (MDR) auf Vorschlag des Trägers der Sozialhilfe bzw. der Gemeinde.

Die mit dem Antrag auf Freistellung darzulegenden und glaubhaft zu machenden personenbezogenen Informationen werden benötigt, um die Voraussetzungen für eine Befreiung von der Rundfunkgebührenpflicht zu prüfen (§ 6 des Rundfunkgebührenstaatsvertrages vom 31. August 1991, zuletzt geändert durch den Achten Rundfunkänderungsstaatsvertrag vom 8. bis 15. Oktober 2004 i.V.m. den Bestimmungen der Verordnung für die Befreiung von der Rundfunkgebührenpflicht vom 28. April 1992). Die Übermittlung der personenbezogenen Daten an die zuständige Landesrundfunkanstalt (MDR) erfolgt auf der Grundlage des § 5 Rundfunkgebührenstaatsvertrag. Die Daten gehen somit an die für die Entscheidung zuständige Behörde. Die Befreiung von der Rundfunkgebührenpflicht erfolgt grundsätzlich für ein Jahr bzw. für den Zeitraum, für den die Voraussetzungen vorliegen.

Verfahrenstechnisch ist zu berücksichtigen, dass nach Ende der Voraussetzungen eine Neubeantragung stattfindet. Danach sind die zuständigen Behörden für die Gebührenbefreiung grundsätzlich berechtigt, die notwendigen und erforderlichen Unterlagen für eine Neubeantragung einzufordern. Zudem macht auch der lange Bewilligungszeitraum eine grundlegende Überprüfung der Voraussetzungen der Befreiung erforderlich. Die Bedenken eines Petenten gegen die Abfragen eines Sozialamtes waren daher nicht gerechtfertigt.

24. Verfassungsschutz

Datenschutzrechtlich relevante Einzelfälle gab es im Berichtszeitraum nur wenige. Soweit möglich hat der Landesbeauftragte Betroffene im Rahmen der gesetzlichen Vorgaben informiert. Sein Kontrollrecht gegenüber der Abteilung Verfassungsschutz im Ministerium des Innern konnte er im von ihm für notwendig erachteten Umfang wahrnehmen.

In Folge der Anschläge auf das World Trade Center in New York wurden im Bund mit dem Terrorismusbekämpfungsgesetz vom 9. Januar 2002 (BGBl. I S. 361) Änderungen u.a. im Bundesverfassungsschutzgesetz vorgenommen. Um u.a. diese Änderungen auf Landesebene nachzuvollziehen, beabsichtigt die Landesregierung einen Gesetzesvorschlag einzubringen.
Das vorgesehene Mantelgesetz soll Änderungen des Verfassungsschutzgesetzes des Landes und des Gesetzes zur Ausführung des Artikel 10-Gesetzes im Land Sachsen-Anhalt (Beschränkung des Brief-, Post- und Fernmeldegeheimnisses) regeln. Erstmalig wird zudem ein Gesetz geschaffen, welches die Grundlage für Sicherheitsüberprüfungen von Personen darstellt, die an sicherheitsempfindlichen Stellen von lebens- und verteidigungswichtigen Einrichtungen beschäftigt werden. Bislang wurden diese Überprüfungen aufgrund einer Verwaltungsvorschrift mit Einwilligung der Betroffenen vorgenommen.

Einige der auf Arbeitsebene eingebrachten Anregungen des Landesbeauftragten zu dem Gesetzgebungsvorhaben wurden bereits in einer Entwurfsfassung berücksichtigt. Ob es allerdings ausreichend ist, den Grundsätzen des Datenschutzes - wie es die Begründung des Gesetzentwurfs unter „Allgemeines“ formuliert - nur unter dem Aspekt der Verhältnismäßigkeit genügen zu wollen, bedarf weiterer Diskussion. Der endgültige Entwurf des Gesetzes wird erst nach Ende des Berichtszeitraums dieses Tätigkeitsberichts im Landtag eingebracht worden sein.

Der Landesbeauftragte wird das weitere Verfahren begleiten und insbesondere darauf drängen, dass - vergleichbar der Regelung zur Befristung des Terrorismusbekämpfungsgesetzes - eine Überprüfung der praktischen Umsetzung und Bedeutung, insbesondere der Änderungen im Verfassungsschutzgesetz, erfolgt, um frühzeitig einschätzen zu können, ob die erweiterte Begrenzung grundrechtlicher Gewährleistungen der Bürgerinnen und Bürger noch erforderlich ist.

25. Verkehr

Unsicherheiten bei der Ahndung von Ordnungswidrigkeiten

Eine Petentin berichtete dem Landesbeauftragten entrüstet, dass ihr vom Ordnungsamt einer größeren Stadt vorgeworfen worden sei, mit ihrem Auto eine Verkehrsordnungswidrigkeit nach § 24 StVG (sie parkte angeblich unzulässig im eingeschränkten Halteverbot) begangen zu haben. Das Ordnungsamt habe sogleich ein Verwarngeld erhoben. Solch ein Verfah-

ren wird aus den unterschiedlichsten Gründen - leider - täglich dutzendfach in jeder großen Stadt praktiziert.
Allerdings war die Situation bei der Petentin tatsächlich anders. Das Ordnungsamt warf ihr vor, die Ordnungswidrigkeit mit einem Pkw BMW begangen zu haben; nur war sie niemals Halterin eines BMW. Das Kennzeichen des BMW, mit dem die Ordnungswidrigkeit begangen worden sei, gehörte zwar zu einem auf die Petentin zugelassenen Pkw Nissan, dieses Fahrzeug wurde jedoch elf Monate vor der angeblichen Ordnungswidrigkeit vorübergehend still gelegt - und war dies noch zum Zeitpunkt der Ordnungswidrigkeit.

Das Ordnungsamt stellte das Verfahren gegen die Petentin nach der Anhörung sofort ein, was sicherlich richtig war.
Gegenüber dem Landesbeauftragten kam es allerdings aufgrund der von ihm zur Erforschung des Sachverhalts gestellten Fragen in Erklärungsnot.
Zunächst gestand es ein, dass offenbar bei der Aufnahme des ordnungswidrig geparkten Fahrzeuges das Kennzeichen fehlerhaft erfasst worden sei. Wahrscheinlich hatte der tatsächlich vorgefundene Pkw BMW ein ähnliches Kennzeichen wie der Wagen der Petentin. Bei der weiteren automatisierten Erstellung der Verwarnung/Anhörung wurde aus den vom Kraftfahrtbundesamt (KBA) bereitgestellten Daten lediglich Name und Anschrift des Halters des erfassten Pkw verwendet, alle weiteren Daten, also auch der Fahrzeugtyp, stammten aus der manuellen Erfassung. So wurde mangels einer funktionierenden Plausibilitätskontrolle unbemerkt aus dem Nissan ein BMW. Der Fehler hätte bemerkt werden können - und wohl auch müssen -, wenn das Ordnungsamt die aufgenommenen Daten des vorgefundenen Fahrzeugs und den vom KBA gelieferten Datensatz verglichen hätte. Das Ordnungsamt hat inzwischen diese Lücke erkannt und den Anbieter der von ihm zur Abwicklung der Verwarngeldverfahren verwendeten Software zur Abhilfe aufgefordert; bis diese automatisierte Plausibilitätskontrolle zur Verfügung steht, sollte das Ordnungsamt diesen Datenvergleich manuell durchführen.

Im Übrigen hätte das Ordnungsamt aus dem nach § 12 Nr. 1 Fahrzeugregisterverordnung vom KBA bereitgestellten Daten auch die Tatsache, dass es sich um ein vorübergehend stillgelegtes Fahrzeug handelt, entnehmen können. Wird mit einem solchen Fahrzeug eine Verkehrsordnungswidrigkeit begangen, kann das Anlass sein, einen Verstoß gegen das Kraftfahrzeugsteuergesetz und das Pflichtversicherungsgesetz zu vermuten und die zuständigen Behörden von dem Verdacht zu unterrichten.

26. Waffenrecht

Datenübermittlung durch Verein - Behörde muss „Angebot“ ausschlagen

Infolge des auch in der Presse ausführlich dargestellten Amoklaufes eines Schülers kam es zu umfangreichen Änderungen des Waffenrechts, die auch in Sachsen-Anhalt zu Anpassungsschwierigkeiten führten, weil man mitunter zuviel des Guten wollte.

Einerseits wandten sich Schützen an den Landesbeauftragten, die wissen wollten, warum sie dem Landesschützenverband nunmehr ihren ganzen Waffenbesitz offenbaren sollten, wenn sie die Erlaubnis für eine neue Waffe beantragen würden.

Andererseits wollte das Ministerium des Innern des Landes dem Begehren des Landesschützenverbandes, allen waffenrechtlichen Behörden „den namentlichen Mitgliederbestand in Form von Vereinslisten“ zu übersenden, einen datenschutzrechtlichen Riegel vorschieben und bat den Landesbeauftragten um Bestätigung.

Der Landesschützenverband e.V. war im Jahr 2003 mit dem „Angebot“ an das Ministerium des Innern des Landes Sachsen-Anhalt herangetreten, jährlich Auflistungen zu seinen Mitgliedern an die zuständigen Waffenbehörden zu übermitteln. Der Verband verstand sein „Angebot“ als Hilfestellung für die Behörden.

Nach Abstimmung zwischen dem Ministerium des Innern des Landes Sachsen-Anhalt und dem Landesbeauftragten wurde dem Landesschützenverband e.V. durch das Ministerium mitgeteilt, dass gegen eine Vorlage von Mitgliederlisten rechtliche - insbesondere datenschutzrechtliche - Bedenken bestehen.

Schießsportliche Vereine wie der Landesschützenverband e.V. sind nichtöffentliche Stellen im Sinne des Bundesdatenschutzgesetzes. Sie sind über bestehende gesetzliche Übermittlungspflichten hinausgehend befugt, personenbezogene Daten an die zuständigen öffentlichen Stellen zu übermitteln, wenn dies zur Abwehr einer Gefahr für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist. Bei der Übermittlung von Mitgliederlisten sind diese Voraussetzungen grundsätzlich nicht erfüllt, weil nicht generell von jedem Mitglied eine solche Gefahr ausgeht.

Selbst wenn die betroffenen Mitglieder in die Übermittlung der Daten eingewilligt haben oder die Übermittlung in der entsprechenden Satzung geregelt ist, darf die Waffenbehörde die Listen nicht verwenden. Behörden sind nicht berechtigt, den ihnen gesetzlich übertragenen Aufgaben- bzw. Tätigkeitsbereich durch die Verarbeitung oder Nutzung von Daten zu erweitern, die ihnen mit Einwilligung der Betroffenen übermittelt worden, aber für die behördliche Aufgabenerfüllung nicht erforderlich sind.

Anlage 1

Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. März 2003:

Forderungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder an Bundesgesetzgeber und Bundesregierung

Immer umfassendere Datenverarbeitungsbefugnisse, zunehmender Datenhunger, sowie immer weitergehende technische Möglichkeiten zur Beobachtung und Durchleuchtung der Bürgerinnen und Bürger zeichnen den Weg zu immer mehr Registrierung und Überwachung vor. Das Grundgesetz gebietet dem Staat, dem entgegenzutreten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, das Recht auf informationelle Selbstbestimmung der Bürger und Bürgerinnen, wie in den Verfassungen zahlreicher deutscher Länder und in den Vorschlägen des Europäischen Verfassungskonvents, als eigenständiges Grundrecht im Grundgesetz zu verankern.

Die Datenschutzbeauftragten werden Bundesgesetzgeber und Bundesregierung bei der Weiterentwicklung des Datenschutzes unterstützen. Sie erwarten, dass die in der Koalitionsvereinbarung enthaltenen Absichtserklärungen zur umfassenden Reform des Datenschutzrechtes in der laufenden Legislaturperiode zügig verwirklicht werden.
Sie sehen dabei folgende essentielle Punkte:

- Schwerpunkte für eine Modernisierung des Bundesdatenschutzgesetzes

  - Im Vordergrund muss die Stärkung der informationellen Selbstbestimmung und des Selbstdatenschutzes stehen: Jeder Mensch muss tatsächlich selbst entscheiden können, welche Datenspuren er hinterlässt und wie diese Datenspuren verwertet werden. Ausnahmen müssen so gering wie möglich gehalten und stets in einer präzise formulierten gesetzlichen Regelung festgeschrieben werden.
  - Es muss im Rahmen der gegebenen Strukturunterschiede ein weitgehend gleichmäßiges Schutzniveau für den öffentlichen und den nicht-öffentlichen Bereich gelten. Die Einwilligung in die Datenverarbeitung darf nicht zur Umgehung gesetzlicher Aufgaben- und Befugnisgrenzen missbraucht werden.
  - Die Freiwilligkeit der Einwilligung muss gewährleistet sein.
  - Vor der Nutzung von Daten für Werbezwecke muss die informierte und freie Einwilligung der Betroffenen vorliegen („opt in“ statt „opt out“).

- Technischer Datenschutz

  Wesentliche Ziele des technischen Datenschutzes müssen darin bestehen, ein hohes Maß an Transparenz bei der Datenverarbeitung zu erreichen und den System- und Selbstdatenschutz zu stärken. Hersteller und Anbieter müssen verpflichtet werden, den Nutzerinnen und Nutzern die geeigneten Mittel zur

Geltendmachung ihrer Rechte auch auf technischem Wege zur Verfügung zu stellen.

- Realisierung von Audit und Gütesiegel als marktwirtschaftliche Elemente im Datenschutz

  Bislang ist das Datenschutzrecht in Deutschland in erster Linie als Ordnungsrecht ausgestaltet. Seine Einhaltung soll durch Kontrolle, Kritik und Beanstandung durchgesetzt werden. Dagegen fehlen Anreize für Firmen und Behörden, vorbildliche Datenschutzkonzepte zu verwirklichen. Mit dem Datenschutzaudit könnte Firmen und Behörden ein gutes Datenschutzkonzept bestätigt werden und es würde ihnen die Möglichkeit eröffnen, damit zu werben. Das Gütesiegel ist ein Anreiz, IT-Produkte von vornherein datenschutzgerecht zu gestalten und damit Marktvorteile zu erringen.
  Eine datenschutzkonforme Technikgestaltung ist eine wichtige Voraussetzung für einen effizienten Datenschutz. Audit und Gütesiegel würden die Aufmerksamkeit auf das Thema Datenschutz lenken und so die stärkere Einbeziehung von Kundinnen und Kunden fördern. Deshalb müssen die noch ausstehenden gesetzlichen Regelungen zur Einführung des im Bundesdatenschutzgesetz vorgesehenen Datenschutzaudits umgehend geschaffen werden.

- Förderung von datenschutzgerechter Technik

  Die Verwirklichung des Grundrechtsschutzes hängt nicht allein von Gesetzen ab. Auch die Gestaltung der Informationstechnik hat großen Einfluss auf die Möglichkeit für alle Menschen, ihr Recht auf informationelle Selbstbestimmung auszuüben. Bislang spielt das Thema Datenschutz bei den öffentlichen IT-Entwicklungsprogrammen allenfalls eine untergeordnete Rolle. Neue IT-Produkte werden nur selten unter dem Blickwinkel entwickelt, ob sie datenschutzgerecht, datenschutzfördernd oder wenigstens nicht datenschutzgefährdend sind.
  Notwendig ist, dass Datenschutz zu einem Kernpunkt im Anforderungsprofil für öffentliche IT-Entwicklungsprogramme wird.
  Datenschutzgerechte Technik stellt sich nicht von alleine ein, sondern bedarf auch der Förderung durch Anreize. Neben der Entwicklung von Schutzprofilen und dem Angebot von Gütesiegeln kommt vor allem die staatliche Forschungs- und Entwicklungsförderung in Betracht. Die Entwicklung datenschutzgerechter Informationstechnik muss zu einem Schwerpunkt staatlicher Forschungsförderung gemacht werden.

- Anonyme Internetnutzung

  Das Surfen im World Wide Web mit seinen immensen Informationsmöglichkeiten und das Versenden von E-Mails sind heute für viele selbstverständlich. Während aber in der realen Welt jeder Mensch zum Beispiel in einem Buchladen stöbern oder ein Einkaufszentrum durchstreifen kann, ohne dass sein Verhalten registriert wird, ist dies im Internet nicht von vornherein gewährleistet.

Dort kann jeder Mausklick personenbezogene Datenspuren erzeugen, deren Summe zu einem aussagekräftigen Persönlichkeitsprofil und für vielfältige Zwecke (z.B. Marketing, Auswahl unter Stellenbewerbungen, Observation von Personen) genutzt werden kann. Das Recht auf Anonymität und der Schutz vor zwangsweiser Identifizierung sind in der realen Welt gewährleistet (in keiner Buchhandlung können Kundinnen und Kunden dazu gezwungen werden, einen Ausweis vorzulegen). Sie werden aber im Bereich des Internet durch Pläne für eine umfassende Vorratsspeicherung von Verbindungs- und Nutzungsdaten bedroht.
Das Recht jedes Menschen, das Internet grundsätzlich unbeobachtet zu nutzen, muss geschützt bleiben. Internet-Provider dürfen nicht dazu verpflichtet werden, auf Vorrat alle Verbindungs- und Nutzungsdaten über den betrieblichen Zweck hinaus für mögliche zukünftige Strafverfahren oder geheimdienstliche Observationen zu speichern.

- Unabhängige Evaluierung der Eingriffsbefugnisse der Sicherheitsbehörden

Schon vor den Terroranschlägen des 11. September 2001 standen den deutschen Sicherheitsbehörden nach einer Reihe von Antiterrorgesetzen und Gesetzen gegen die Organisierte Kriminalität weitreichende Eingriffsbefugnisse zur Verfügung, die Datenschutzbeauftragten und Bürgerrechtsorganisationen Sorgen bereiteten:
Dies zeigen Videoüberwachung, Lauschangriff, Rasterfahndung, langfristige Aufbewahrung der Daten bei der Nutzung des Internet und der Telekommunikation, Zugriff auf Kundendaten und Geldbewegungen bei den Banken.
Durch die jüngsten Gesetzesverschärfungen nach den Terroranschlägen des 11. September 2001 sind die Freiräume für unbeobachtete individuelle oder gesellschaftliche Aktivitäten und Kommunikation weiter eingeschränkt worden. Bürgerliche Freiheitsrechte und Datenschutz dürfen nicht immer weiter gefährdet werden.

Nach der Konkretisierung der Befugnisse der Sicherheitsbehörden und der Schaffung neuer Befugnisse im Terrorismusbekämpfungsgesetz sowie in anderen gegen Ende der 14. Legislaturperiode verabschiedeten Bundesgesetzen ist vermehrt eine offene Diskussion darüber notwendig, wie der gebotene Ausgleich zwischen kollektiver Sicherheit und individuellen Freiheitsrechten so gewährleistet werden kann, dass unser Rechtsstaat nicht zum Überwachungsstaat wird. Dazu ist eine umfassende und systematische Evaluierung der im Zusammenhang mit der Terrorismusbekämpfung eingefügten Eingriffsbefugnisse der Sicherheitsbehörden notwendig.
Die Datenschutzbeauftragten halten darüber hinaus eine Erweiterung der im Terrorismusbekämpfungsgesetz vorgesehenen Pflicht zur Evaluierung der neuen Befugnisse der Sicherheitsbehörden auf andere vergleichbar intensive Eingriffsmaßnahmen - wie Telefonüberwachung, großer Lauschangriff und Rasterfahndung - für geboten.
Die Evaluierung muss durch unabhängige Stellen und an Hand objektiver Kriterien erfolgen und aufzeigen, wo zurückgeschnitten werden muss, wo Instrumente untauglich sind oder wo die negativen Folgewirkungen überwiegen.

Wissenschaftliche Untersuchungsergebnisse zur Evaluation des Richtervorbehalts z.B. bei Telefonüberwachungen machen deutlich, dass der Bundesgesetzgeber Maßnahmen zur Stärkung des Richtervorbehalts - und zwar nicht nur im Bereich der Telefonüberwachung - als grundrechtssicherndes Verfahrenselement ergreifen muss.

- Stärkung des Schutzes von Gesundheitsdaten

  Zwar schützt die Jahrtausende alte ärztliche Schweigepflicht Kranke davor, dass Informationen über ihren Gesundheitszustand von denjenigen unbefugt weitergegeben werden, die sie medizinisch betreuen. Medizinische Daten werden aber zunehmend außerhalb des besonderen ärztlichen Vertrauensverhältnisses zu Patienten und Patientinnen verarbeitet. Telemedizin und High-Tech-Medizin führen zu umfangreichen automatischen Datenspeicherungen. Hinzu kommt ein zunehmender Druck, Gesundheitsdaten z.B. zur Einsparung von Kosten, zur Verhinderung von Arzneimittelnebenfolgen oder „zur Qualitätssicherung“ einzusetzen. Die Informatisierung der Medizin durch elektronische Aktenführung, Einsatz von Chipkarten, Nutzung des Internets zur Konsultation bis hin zur ferngesteuerten Behandlung mit Robotern erfordern es deshalb, dass auch die Instrumente zum Schutz von Gesundheitsdaten weiterentwickelt werden.
  Der Schutz des Patientengeheimnisses muss auch in einer computerisierten Medizin wirksam gewährleistet sein. Die Datenschutzbeauftragten begrüßen deshalb die Absichtserklärung in der Koalitionsvereinbarung, Patientenschutz und Patientenrechte auszubauen. Dabei ist insbesondere sicherzustellen, dass Gesundheitsdaten außerhalb der eigentlichen Behandlung soweit wie möglich und grundsätzlich nur anonymisiert oder pseudonymisiert verarbeitet werden dürfen, soweit die Verarbeitung im Einzelfall nicht durch ein informiertes Einverständnis gerechtfertigt ist. Das Prinzip des informierten und freiwilligen Einverständnisses ist insbesondere auch für eine Gesundheitskarte zu beachten und zwar auch für deren Verwendung im Einzelfall.
  Der Bundesgesetzgeber wird auch aufgefordert gesetzlich zu regeln, dass Patientendaten, die in Datenverarbeitungsanlagen außerhalb von Arztpraxen und Krankenhäusern verarbeitet werden, genauso geschützt sind wie die Daten in der ärztlichen Praxis.
  Geprüft werden sollte schließlich, ob und gegebenenfalls wie der Schutz von Gesundheitsdaten durch Geheimhaltungspflicht, Zeugnisverweigerungsrecht und Beschlagnahmeverbot auch dann gewährleistet werden kann, wenn diese, z.B. in der wissenschaftlichen Forschung, mit Einwilligung oder auf gesetzlicher Grundlage von anderen Einrichtungen außerhalb des Bereichs der behandelnden Ärztinnen und Ärzte verarbeitet werden.

- Datenschutz und Gentechnik

  Die Entwicklung der Gentechnik ist atemberaubend. Schon ein ausgefallenes Haar, ein Speichelrest an Besteck oder Gläsern, abgeschürfte Hautpartikel oder ein Blutstropfen - dies alles eignet sich als Untersuchungsmaterial, um den genetischen Bauplan eines Menschen entschlüsseln zu können. Inzwischen werden Gentests frei verkäuflich angeboten. Je mehr Tests gemacht

werden, desto größer wird das Risiko für jeden Menschen, dass seine genetischen Anlagen von anderen auch gegen seinen Willen analysiert werden. Versicherungen oder Arbeitgeber und Arbeitgeberinnen werden ebenfalls Testergebnisse erfahren wollen.
Niemand darf zur Untersuchung genetischer Anlagen gezwungen werden; die Durchführung eines gesetzlich nicht zugelassenen Tests ohne Wissen und Wollen der betroffenen Person und die Nutzung daraus gewonnener Ergebnisse muss unter Strafe gestellt werden.
In der Koalitionsvereinbarung ist der Erlass eines „Gen-Test-Gesetzes“ vorgesehen. Ein solches Gesetz ist dringend erforderlich, damit der datenschutzgerechte Umgang mit genetischen Daten gewährleistet wird. Die Datenschutzbeauftragten haben dazu auf ihrer 62. Konferenz in Münster vom 24. bis 26. Oktober 2001 Vorschläge vorgelegt.

- Datenschutz im Steuerrecht

  Im bisherigen Steuer- und Abgabenrecht finden sich äußerst lückenhafte datenschutzrechtliche Regelungen. Insbesondere fehlen grundlegende Rechte, wie ein Akteneinsichts- und Auskunftsrecht. Eine Pflicht zur Information der Steuerpflichtigen über Datenerhebungen bei Dritten fehlt ganz.

  Die jüngsten Gesetzesnovellen und Gesetzesentwürfe, die fortschreitende Vernetzung und multinationale Vereinbarungen verschärfen den Mangel: Immer mehr Steuerdaten sollen zentral durch das Bundesamt für Finanzen erfasst werden. Mit einheitlichen Personenidentifikationsnummern sollen Zusammenführungen und umfassende Auswertungen der Verbunddaten möglich werden. Eine erhebliche Ausweitung der Kontrollmitteilungen von Finanzbehörden und Kreditinstituten, die ungeachtet der Einführung einer pauschalen Abgeltungssteuer geplant ist, würde zweckungebundene und unverhältnismäßige Datenübermittlungen gestatten. Die zunehmende Vorratserhebung und -speicherung von Steuerdaten entspricht nicht dem datenschutzrechtlichen Grundsatz der Erforderlichkeit.

  Die Datenschutzbeauftragten fordern deshalb, die Aufnahme datenschutzrechtlicher Grundsätze in das Steuerrecht jetzt anzugehen und den Betroffenen die datenschutzrechtlichen Informations- und Auskunftsrechte zuzuerkennen.

- Arbeitnehmerdatenschutz

  Persönlichkeitsrechte und Datenschutz sind im Arbeitsverhältnis vielfältig bedroht, zum Beispiel durch
  - die Sammlung von Beschäftigtendaten in leistungsfähigen Personalinformationssystemen, die zur Erstellung von Persönlichkeitsprofilen genutzt werden,
  - die Übermittlung von Beschäftigtendaten zwischen konzernangehörigen Unternehmen, für die nicht der Datenschutzstandard der EG-Datenschutzrichtlinie gilt,
  - die Überwachung des Arbeitsverhaltens durch Videokameras, die Protokollierung der Nutzung von Internetdiensten am Arbeitsplatz,

- die Erhebung des Gesundheitszustands, Drogen-Screenings und psychologische Testverfahren bei der Einstellung.

Die hierzu von den Arbeitsgerichten entwickelten Schranken wirken unmittelbar nur im jeweils entschiedenen Einzelfall und sind auch nicht allen Betroffenen hinreichend bekannt. Das seit vielen Jahren angekündigte Arbeitnehmerdatenschutzgesetz muss hier endlich klare gesetzliche Vorgaben schaffen.

Die Datenschutzbeauftragten fordern deshalb, dass für die in der Koalitionsvereinbarung enthaltene Festlegung zur Schaffung von gesetzlichen Regelungen zum Arbeitnehmerdatenschutz nunmehr rasch ein ausformulierter Gesetzentwurf vorgelegt und anschließend zügig das Gesetzgebungsverfahren eingeleitet wird.

- Stärkung einer unabhängigen, effizienten Datenschutzkontrolle

  Die Datenschutzbeauftragten fordern gesetzliche Vorgaben, die die völlige Unabhängigkeit der Datenschutzkontrolle sichern und effektive Einwirkungsbefugnisse gewährleisten, wie dies der Art. 28 der EG-Datenschutzrichtlinie gebietet.

  Die Datenschutzkontrollstellen im privaten Bereich haben bis heute nicht die völlige Unabhängigkeit, die die Europäische Datenschutzrichtlinie vorsieht. So ist in der Mehrzahl der deutschen Länder die Kontrolle über den Datenschutz im privaten Bereich nach wie vor bei den Innenministerien und nachgeordneten Stellen angesiedelt und unterliegt damit einer Fachaufsicht. Selbst in den Ländern, in denen die Landesbeauftragten diese Aufgabe wahrnehmen, ist ihre Unabhängigkeit nicht überall richtlinienkonform ausgestaltet.

- Stellung des Bundesdatenschutzbeauftragten

  Die rechtliche Stellung des Bundesdatenschutzbeauftragten als unabhängiges Kontrollorgan muss im Grundgesetz abgesichert werden.

- Verbesserung der Informationsrechte

  Die im Bereich der Informationsfreiheit tätigen Datenschutzbeauftragten unterstützen die Absicht in der Koalitionsvereinbarung, auf Bundesebene ein Informationsfreiheitsgesetz zu schaffen. Nach ihren Erfahrungen hat sich die gemeinsame Wahrnehmung der Aufgaben zum Datenschutz und zur Informationsfreiheit bewährt, weshalb sie auch auf Bundesebene realisiert werden sollte. Zusätzlich muss ein Verbraucherinformationsgesetz alle Produkte und Dienstleistungen erfassen und einen Informationsanspruch auch gegenüber Unternehmen einführen.

Anlage 2

Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. März 2003:

Kennzeichnung von Daten aus besonders eingriffsintensiven Erhebungen

Das Bundesverfassungsgericht hat in seinem Urteil zur strategischen Fernmeldeüberwachung des Bundesnachrichtendienstes festgestellt, dass sich die Zweckbindung der bei dieser Maßnahme erlangten personenbezogenen Daten nur gewährleisten lässt, wenn auch nach ihrer Erfassung erkennbar bleibt, dass es sich um Daten handelt, die aus Eingriffen in das Fernmeldegeheimnis stammen. Eine entsprechende Kennzeichnung ist daher von Verfassungs wegen geboten. Dementsprechend wurde die Kennzeichnungspflicht in der Novellierung des G 10 Gesetzes auch allgemein für jede Datenerhebung des Bundesnachrichtendienstes und des Verfassungsschutzes im Schutzbereich des Art. 10 GG angeordnet.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die Pflicht zur Kennzeichnung aufgrund der Ausführungen des Bundesverfassungsgerichts nicht auf den Bereich der Fernmeldeüberwachung beschränkt ist. Sie gilt auch für vergleichbare Methoden der Datenerhebung, bei denen die Daten durch besonders eingriffsintensive Maßnahmen gewonnen werden und deswegen einer strikten Zweckbindung unterliegen müssen.

Deshalb müssen zumindest solche personenbezogenen Daten, die aus einer Telefon-, Wohnraum- oder Postüberwachung erlangt wurden, besonders gekennzeichnet werden.

Anlage 3

Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. März 2003:

Datenschutzrechtliche Rahmenbedingungen zur Modernisierung des Systems der gesetzlichen Krankenversicherung

In der Diskussion über eine grundlegende Reform des Rechts der gesetzlichen Krankenversicherung (GKV) werden in großem Maße datenschutzrechtliche Belange berührt. Erweiterte Befugnisse zur Verarbeitung von medizinischen Leistungs- und Abrechnungsdaten sollen eine stärkere Kontrolle der Patientinnen und Patienten sowie der sonstigen beteiligten Parteien ermöglichen. Verbesserte individuelle und statistische Informationen sollen zudem die medizinische und informationelle Selbstbestimmung der Patientinnen und Patienten verbessern sowie die Transparenz für die Beteiligten und für die Öffentlichkeit erhöhen.
So sehen Vorschläge des Bundesministeriums für Gesundheit und Soziale Sicherung zur Modernisierung des Gesundheitswesens u.a. vor, dass bis zum Jahr 2006 schrittweise eine elektronische Gesundheitskarte eingeführt wird und Leistungs- und Abrechnungsdaten zusammengeführt werden sollen. Boni für gesundheitsbewusstes Verhalten und Ausnahmen oder Mali für gesundheitsgefährdendes Verhalten sollen medizinisch rationales Verhalten der Versicherten fördern, was eine Überprüfung dieses Verhaltens voraussetzt. Derzeit werden gesetzliche Regelungen ausgearbeitet.

Die Datenschutzbeauftragten des Bundes und der Länder weisen erneut auf die datenschutzrechtlichen Chancen und Risiken einer Modernisierung des Systems der GKV hin.

Viele Vorschläge zielen darauf ab, Gesundheitskosten dadurch zu reduzieren, dass den Krankenkassen mehr Kontrollmöglichkeiten eingeräumt werden. Solche individuellen Kontrollen können indes nur ein Hilfsmittel zu angestrebten Problemlösungen, nicht aber die Problemlösung selbst sein. Sie sind auch mit dem Recht der Patientinnen und Patienten auf Selbstbestimmung und dem Schutz der Vertrauensbeziehung zwischen ärztlichem Personal und behandelten Personen nicht problemlos in Einklang zu bringen. Eingriffe müssen nach den Grundsätzen der Datenvermeidung und der Erforderlichkeit und Verhältnismäßigkeit auf ein Minimum beschränkt bleiben. Möglichkeiten der anonymisierten oder pseudonymisierten Verarbeitung von Patientendaten müssen ausgeschöpft werden. Eine umfassendere Information der Patientinnen und Patienten, die zu mehr Transparenz führt und die Verantwortlichkeiten verdeutlicht, ist ebenfalls ein geeignetes Hilfsmittel.

Sollte im Rahmen gesetzlicher Regelungen zur Qualitätssicherung und Abrechnungskontrolle für einzelne Bereiche der Zugriff auf personenbezogene Behandlungsdaten unerlässlich sein, müssen Vorgaben entwickelt werden, die

- den Zugriff auf genau festgelegte Anwendungsfälle begrenzen,
- das Prinzip der Stichprobe zugrunde legen,
- eine strikte Einhaltung der Zweckbindung gewährleisten und
- die Auswertung der Daten einer unabhängigen Stelle übertragen.

1.
Die Datenschutzbeauftragten erkennen die Notwendigkeit einer verbesserten Datenbasis zur Weiterentwicklung der gesetzlichen Krankenversicherung an. Hierzu reichen wirksam pseudonymisierte Daten grundsätzlich aus. Eine Zusammenführung von Leistungs- und Versichertendaten darf nicht dazu führen, dass über eine lückenlose zentrale Sammlung personenbeziehbarer Patientendaten mit sensiblen Diagnose- und Behandlungsangaben z.B. zur Risikoselektion geeignete medizinische Profile entstehen. Dies könnte nicht nur zur Diskriminierung einzelner Versicherter führen, sondern es würde auch die sozialstaatliche Errungenschaft des solidarischen Tragens von Krankheitsrisiken aufgegeben. Zudem wären zweckwidrige Auswertungen möglich, für die es viele Interessierte gäbe, von Privatversicherungen bis hin zu Arbeitgebern. Durch sichere technische und organisatorische Verfahren, die Pseudonymisierung der Daten und ein grundsätzliches sanktionsbewehrtes Verbot der Reidentifizierung pseudonymisierter Datenbestände kann solchen Gefahren entgegengewirkt werden.

2.
Die Einführung einer Gesundheitschipkarte kann die Transparenz des Behandlungsgeschehens für die Patientinnen und Patienten erhöhen, deren schonende und erfolgreiche medizinische Behandlung effektivieren und durch Vermeidung von Medienbrüchen und Mehrfachbehandlungen Kosten senken. Eine solche Karte kann aber auch dazu genutzt werden, die Selbstbestimmungsrechte der Patientinnen und Patienten zu verschlechtern. Dieser Effekt würde durch eine Pflichtkarte eintreten, auf der - von den Betroffenen nicht beeinflussbar - Diagnosen und Medikationen zur freien Einsicht durch Ärztinnen und Ärzte sowie sonstige Leistungserbringende gespeichert wären. Zentrales Patientenrecht ist es, selbst zu entscheiden, welchem Arzt oder welcher Ärztin welche Informationen anvertraut werden.

Die Datenschutzkonferenz fordert im Fall der Einführung einer Gesundheitschipkarte die Gewährleistung des Rechts der Patientinnen und Patienten, grds. selbst zu entscheiden,
- ob sie überhaupt verwendet wird,
- welche Daten darauf gespeichert werden oder über sie abgerufen werden können,
- welche Daten zu löschen sind und wann das zu geschehen hat,
- ob sie im Einzelfall vorgelegt wird und
- welche Daten im Einzelfall ausgelesen werden sollen.

Sicherzustellen ist weiterhin
- ein Beschlagnahmeverbot und Zeugnisverweigerungsrecht, in Bezug auf die Daten, die auf der Karte gespeichert sind,
- die Beschränkung der Nutzung auf das Patienten-Arzt/Apotheken-Verhältnis und
- die Strafbarkeit des Datenmissbrauchs.

Die Datenschutzkonferenz hat bereits zu den datenschutzrechtlichen Anforderungen an den „Arzneimittelpass“ (Medikamentenchipkarte) ausführlich Stellung genommen (Entschließung vom 26.10.2001). Die dort formulierten Anforderungen an eine elektronische Gesundheitskarte sind weiterhin gültig. Die „Gemeinsame Erklärung des

Bundesministeriums für Gesundheit und der Spitzenorganisationen zum Einsatz von Telematik im Gesundheitswesen“ vom 3. Mai 2002, wonach "der Patient Herr seiner Daten“ sein soll, enthält gute Ansatzpunkte, auf deren Basis die Einführung einer Gesundheitskarte betrieben werden kann.

3.
Die Datenschutzbeauftragten anerkennen die Förderung wirtschaftlichen und gesundheitsbewussten Verhaltens als ein wichtiges Anliegen. Dies darf aber nicht dazu führen, dass die Krankenkassen detaillierte Daten über die private Lebensführung erhalten („fährt Ski“, „raucht“, „trinkt zwei Biere pro Tag“), diese überwachen und so zur „Gesundheitspolizei“ werden. Notwendig ist deshalb die Entwicklung von Konzepten, die ohne derartige mitgliederbezogene Datensätze bei den Krankenkassen und ihre Überwachung auskommen.

4.
Die Datenschutzbeauftragten begrüßen alle Pläne, die darauf hinauslaufen, das Verfahren der GKV allgemein sowie die individuelle Behandlung und Datenverarbeitung für die Betroffenen transparenter zu machen. Maßnahmen wie die Einführung der Patientenquittung, die Information über das Leistungsverfahren und über Umfang und Qualität des Leistungsangebotes sowie eine verstärkte Einbindung der Patientinnen und Patienten durch Unterrichtungen und Einwilligungserfordernisse stärken die Patientensouveränität und die Selbstbestimmung.

Anlage 4

Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. März 2003:

Datenschutzbeauftragte fordern vertrauenswürdige Informationstechnik

Anwenderinnen und Anwender von komplexen IT-Produkten müssen unbedingt darauf vertrauen können, dass Sicherheitsfunktionen von Hard- und Software korrekt ausgeführt werden, damit die Vertraulichkeit, die Integrität und die Zurechenbarkeit der Daten gewährleistet sind. Dieses Vertrauen kann insbesondere durch eine datenschutzgerechte Gestaltung der Informationstechnik geschaffen werden. Ausbleibende Erfolge bei eCommerce und eGovernment werden mit fehlendem Vertrauen in einen angemessenen Schutz der personenbezogenen Daten und mangelnder Akzeptanz der Nutzerinnen und Nutzer erklärt. Anwenderinnen und Anwender sollten ihre Sicherheitsanforderungen präzise definieren und Anbieter ihre Sicherheitsleistungen schon vor der Produktentwicklung festlegen und für alle nachprüfbar dokumentieren. Die Datenschutzbeauftragten des Bundes und der Länder wollen Herstellerinnen und Hersteller und Anwenderinnen und Anwender von Informationstechnik unterstützen, indem sie entsprechende Werkzeuge und Hilfsmittel zur Verfügung stellen.
So bietet der Bundesbeauftragte für den Datenschutz seit dem 11. November 2002 mit zwei so genannten Schutzprofilen (Protection Profiles) Werkzeuge an, mit deren Hilfe Anwenderinnen und Anwender bereits vor der Produktentwicklung ihre datenschutzspezifischen Anforderungen für bestimmte Produkttypen beispielsweise im Gesundheitswesen oder im eGovernment detailliert beschreiben können. Kerngedanke der in diesen Schutzprofilen definierten Sicherheitsanforderungen ist die Kontrollierbarkeit aller Informationsflüsse eines Rechners gemäß einstellbarer Informationsflussregeln. Die Schutzprofile sind international anerkannt, da sie auf der Basis der “Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria)” entwickelt wurden. Herstellerinnen und Hersteller können datenschutzfreundliche Produkte somit nach international prüffähigen Vorgaben der Anwenderinnen und Anwender entwickeln. Unabhängige Prüfinstitutionen können diese Produkte dann nach Abschluss der Entwicklung nach international gültigen Kriterien prüfen. [1]

In Schleswig-Holstein bietet das Unabhängige Landeszentrum für Datenschutz ein Verfahren mit vergleichbarer Zielsetzung an, das ebenfalls zu überprüfbarer Sicherheit von IT-Produkten führt. Für nachweislich datenschutzgerechte IT-Produkte können Hersteller ein so genanntes Datenschutz-Gütesiegel erhalten. Das Landeszentrum hat auf der Grundlage landesspezifischer Rechtsvorschriften bereits im Jahr 2002 einen entsprechenden Anforderungskatalog veröffentlicht und zur CeBIT 2003 eine an die Common Criteria angepasste Version vorgestellt. [2]

[1] Die Schutzprofile mit dem Titel “BISS - Benutzerbestimmbare Informationsflusskontrolle” haben die Registrierungskennzeichen BSI-PP-0007-2002 und BSI-PTT-008-2002 und sind beim Bundesbeauftragten für den Datenschutz unter http://www.bfd.bund.de/technik/protection_profile.html abrufbar.
[2] Die Ergebnisse der bisherigen Auditierungen durch das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein sind unter http://www.datenschutzzentrum.de/guetesiegel veröffentlicht.

Die Datenschutzbeauftragten des Bundes und der Länder empfehlen die Anwendung von Schutzprofilen und Auditierungsprozeduren, damit auch der Nutzer oder die Nutzerin beurteilen kann, ob IT-Systeme und -Produkte vertrauenswürdig und datenschutzfreundlich sind. Sie appellieren an die Hersteller, entsprechende Produkte zu entwickeln bzw. vorhandene Produkte anhand bereits bestehender oder gleichwertiger Schutzprofile und Anforderungskataloge zu modifizieren. Sie treten dafür ein, dass die öffentliche Verwaltung vorrangig solche Produkte einsetzt.

Anlage 5

Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. März 2003:

TCPA darf nicht zur Aushebelung des Datenschutzes missbraucht werden

Mit großer Skepsis sehen die Datenschutzbeauftragten des Bundes und der Länder die Pläne zur Entwicklung zentraler Kontrollmechanismen und -infrastrukturen auf der Basis der Spezifikationen der Industrie-Allianz “Trusted Computing Platform Alliance” (TCPA).

Die TCPA hat sich zum Ziel gesetzt, vertrauenswürdige Personalcomputer zu entwickeln. Dazu bedarf es spezieller Hard- und Software. In den bisher bekannt gewordenen Szenarien soll die Vertrauenswürdigkeit dadurch gewährleistet werden, dass zunächst ein spezieller Kryptoprozessor nach dem Einschalten des PC überprüft, ob die installierte Hardware und das Betriebssystem mit den von der TCPA zertifizierten und auf zentralen Servern hinterlegten Konfigurationsangaben übereinstimmen. Danach übergibt der Prozessor die Steuerung an ein TCPA-konformes Betriebssystem. Beim Start einer beliebigen Anwendersoftware prüft das Betriebssystem dann deren TCPA-Konformität, beispielsweise durch Kontrolle der Lizenz oder der Seriennummer, und kontrolliert weiterhin, ob Dokumente in zulässiger Form genutzt werden. Sollte eine der Prüfungen Abweichungen zur hinterlegten, zertifizierten Konfiguration ergeben, lässt sich der PC nicht booten bzw. das entsprechende Programm wird gelöscht oder lässt sich nicht starten.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen alle Aktivitäten, die der Verbesserung des Datenschutzes dienen und insbesondere zu einer manipulations- und missbrauchssicheren sowie transparenten IT-Infrastruktur führen. Sie erkennen auch die berechtigten Forderungen der Softwarehersteller an, dass kostenpflichtige Software nur nach Bezahlung genutzt werden darf.

Wenn aber zentrale Server einer externen Kontrollinstanz genutzt werden, um mit entsprechend modifizierten Client-Betriebssystemen Prüf- und Kontrollfunktionen zu steuern, müssten sich Anwenderinnen und Anwender beim Schutz sensibler Daten uneingeschränkt auf die Vertrauenswürdigkeit der externen Instanz verlassen können. Die Datenschutzbeauftragten erachten es für unzumutbar, wenn

- Anwenderinnen und Anwender die alleinige Kontrolle über die Funktionen des eigenen Computers verlieren, falls eine externe Kontrollinstanz Hardware, Software und Daten kontrollieren und manipulieren kann,

- die Verfügbarkeit aller TCPA-konformen Personalcomputer und der darauf verarbeiteten Daten gefährdet wäre, da sowohl Fehler in der Kontrollinfrastruktur als auch Angriffe auf die zentralen TCPA-Server die Funktionsfähigkeit einzelner Rechner sofort massiv einschränken würden,

- andere Institutionen oder Personen sich vertrauliche Informationen von zentralen Servern beschaffen würden, ohne dass der Anwender dies bemerkt,

- die Nutzung von Servern oder PC davon abhängig gemacht würde, dass ein Zugang zum Internet geöffnet wird,

- der Zugang zum Internet und E-Mail-Verkehr durch Softwarerestriktionen behindert würde,

- der Umgang mit Dokumenten ausschließlich gemäß den Vorgaben der externen Kontrollinstanz zulässig sein würde und somit eine sehr weitgehende Zensur ermöglicht wird,

- auf diese Weise der Zugriff auf Dokumente von Konkurrenzprodukten verhindert und somit auch die Verbreitung datenschutzfreundlicher Open-Source-Software eingeschränkt werden kann und

- Programmergänzungen (Updates) ohne vorherige Einwilligung im Einzelfall aufgespielt werden könnten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb Hersteller von Informations- und Kommunikationstechnik auf, Hard- und Software so zu entwickeln und herzustellen, dass

- Anwenderinnen und Anwender die ausschließliche und vollständige Kontrolle über die von ihnen genutzte Informationstechnik haben, insbesondere dadurch, dass Zugriffe und Änderungen nur nach vorheriger Information und Einwilligung im Einzelfall erfolgen,

- alle zur Verfügung stehenden Sicherheitsfunktionen für Anwenderinnen und Anwender transparent sind und

- die Nutzung von Hard- und Software und der Zugriff auf Dokumente auch weiterhin möglich ist, ohne dass Dritte davon Kenntnis erhalten und Nutzungsprofile angelegt werden können.

Auf diese Weise können auch künftig die in den Datenschutzgesetzen des Bundes und der Länder geforderte Vertraulichkeit und Verfügbarkeit der zu verarbeitenden personenbezogenen Daten sichergestellt und die Transparenz bei der Verarbeitung dieser Daten gewährleistet werden.

Anlage 6

Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. März 2003:

Elektronische Signatur im Finanzbereich

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass mit dem Signaturgesetz und der Anpassung von mehr als 3.000 Rechtsvorschriften in Deutschland die rechtlichen Voraussetzungen geschaffen wurden, um die „qualifizierte elektronische Signatur“ der eigenhändigen Unterschrift gleichzustellen. Die administrativen und technischen Voraussetzungen sind inzwischen weitgehend vorhanden. Mehr als zwanzig freiwillig akkreditierte Zertifizierungsdiensteanbieter nach dem Signaturgesetz sind von der Regulierungsbehörde für Telekommunikation und Post (RegTP) zugelassen. Sowohl Chipkarten, die für die qualifizierte elektronische Signatur zugelassen sind, als auch die dafür erforderlichen Lesegeräte sind verfügbar.

Für die elektronische Kommunikation zwischen der Finanzverwaltung und den Bürgerinnen und Bürgern ist die „qualifizierte elektronische Signatur“ gesetzlich vorgeschrieben. Die Finanzverwaltung will eine Übergangsbestimmung in der Steuerdatenübermittlungsverordnung vom 28.1.2003 nutzen, nach der bis Ende 2005 eine lediglich fortgeschrittene, die so genannte „qualifizierte elektronische Signatur mit Einschränkungen„ eingesetzt werden kann. Aus folgenden Gründen lehnen die Datenschutzbeauftragten dieses Vorgehen ab:

- Die „qualifizierte elektronische Signatur mit Einschränkungen“ bietet im Gegensatz zur „qualifizierten elektronischen Signatur“ und der „qualifizierten elektronischen Signatur mit Anbieterakkreditierung“ keine umfassend nachgewiesene Sicherheit, vor allem aber keine langfristige Überprüfbarkeit. Die mit ihr unterzeichneten elektronischen Dokumente sind unerkannt manipulierbar. Die „qualifizierte elektronische Signatur mit Einschränkungen“ hat geringeren Beweiswert als die eigenhändige Unterschrift.

- Die technische Infrastruktur, die die Finanzverwaltung für die „qualifizierte elektronische Signatur mit Einschränkungen“ vorgesehen hat, kann sie verwenden, um elektronische, fortgeschritten oder qualifiziert signierte Dokumente von Bürgerinnen und Bürgern und Steuerberaterinnen und Steuerberatern zu prüfen und selbst fortgeschrittene Signaturen zu erzeugen.
  Damit die Finanzverwaltung selbst qualifiziert signieren kann, reicht eine Ergänzung mit einem qualifizierten Zertifikat aus.

- Für die elektronische Steuererklärung ELSTER sollen Zertifizierungsdienste im außereuropäischen Ausland zugelassen werden, für die weder eine freiwillige Akkreditierung noch eine Kontrolle durch deutsche Datenschutzbehörden möglich ist, anstatt Zertifizierungsdienste einzuschalten, die der Europäischen Datenschutzrichtlinie entsprechen. Damit sind erhebliche Gefahren verbunden, die vermeidbar sind.

- Die elektronische Signatur soll auch zur Authentisierung der Steuerpflichtigen und Steuerberater gegenüber ELSTER genutzt werden, obwohl die Trennung der Schlüsselpaare für Signatur und Authentisierung unerlässlich und bereits Stand der Technik ist.

Die Datenschutzbeauftragten des Bundes und der Länder befürchten, dass bei Schaffung weiterer Signaturverfahren mit geringerer Sicherheit die Transparenz für die Anwenderinnen und Anwender verloren geht und der sichere und verlässliche elektronische Rechts- und Geschäftsverkehr in Frage gestellt werden könnte.
Abweichend vom Vorgehen der Finanzverwaltung hat sich die Bundesregierung sowohl im Rahmen der Initiative „Bund Online 2005“ als auch im so genannten Signaturbündnis für sichere Signaturverfahren eingesetzt. Das Verfahren ELSTER sollte genutzt werden, um sogleich qualifizierten und damit sicheren Signaturen zum Durchbruch zu verhelfen.

Vor diesem Hintergrund empfiehlt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder der Bundesregierung,

- dass die Finanzbehörden Steuerbescheide und sonstige Dokumente ausschließlich qualifiziert signiert versenden,

- den Bürgerinnen und Bürgern eine sichere, zuverlässige, leicht einsetzbare und transparente Technologie zur Verfügung zu stellen,

- unterschiedliche Ausstattungen für abgestufte Qualitäten und Anwendungsverfahren zu vermeiden,

- die Anschaffung von Signaturerstellungseinheiten mit zugehörigen Zertifikaten und ggf. Signaturanwendungskomponenten für „qualifizierte elektronische Signaturen mit Anbieterakkreditierung“ staatlich zu fördern,

- die vorhandenen Angebote der deutschen und sonstigen europäischen Anbieter vornehmlich heranzuziehen, um die qualifizierte elektronische Signatur und den Einsatz entsprechender Produkte zu fördern,

- e-Government- und e-Commerce-Projekte zu fördern, die qualifizierte elektronische Signaturen unterhalb der Wurzelzertifizierungsinstanz der RegTP einsetzen und somit Multifunktionalität und Interoperabilität gewährleisten,

- die Entwicklung von technischen Standards für die umfassende Einbindung der qualifizierten elektronischen Signatur zu fördern,

- die Weiterentwicklung der entsprechenden Chipkartentechnik voranzutreiben.

Anlage 7

Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. März 2003:

Transparenz bei der Telefonüberwachung

Nach derzeitigem Recht haben die Betreiber von Telekommunikationsanlagen eine Jahresstatistik über die von ihnen zu Strafverfolgungszwecken durchgeführten Überwachungsmaßnahmen zu erstellen. Diese Zahlen werden von der Regulierungsbehörde für Telekommunikation und Post veröffentlicht. Auf diese Weise wird die Allgemeinheit über Ausmaß und Entwicklung der Telekommunikationsüberwachung in Deutschland informiert.

Nach aktuellen Plänen der Bundesregierung soll diese Statistik abgeschafft werden. Begründet wird dies mit einer Entlastung der Telekommunikationsunternehmen von überflüssigen Arbeiten. Zudem wird darauf verwiesen, dass das Bundesjustizministerium eine ähnliche Statistik führt, die sich auf Zahlen der Landesjustizbehörden stützt. Dabei wird verkannt, das die beiden Statistiken unterschiedliches Zahlenmaterial berücksichtigen. So zählen die Telekommunikationsunternehmen jede Überwachungsmaßnahme getrennt nach den einzelnen Anschlüssen, während von den Landesjustizverwaltungen nur die Anzahl der Strafverfahren erfasst wird.

In den vergangenen Jahren ist die Zahl der überwachten Anschlüsse um jährlich etwa 25 Prozent gestiegen. Gab es im Jahr 1998 noch 9.802 Anordnungen, waren es im Jahr 2001 bereits 19.896. Diese stetige Zunahme von Eingriffen in das Fernmeldegeheimnis sehen die Datenschutzbeauftragten des Bundes und der Länder mit großer Sorge. Eine fundierte und objektive Diskussion in Politik und Öffentlichkeit ist nur möglich, wenn die tatsächliche Anzahl von Telefonüberwachungsmaßnahmen bekannt ist. Allein eine Aussage über die Anzahl der Strafverfahren, in denen eine Überwachungsmaßnahme stattgefunden hat, reicht nicht aus. Nur die detaillierten Zahlen, die derzeit von den Telekommunikationsunternehmen erhoben werden, sind aussagekräftig genug.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine Beibehaltung der Unternehmensstatistik nach § 88 Absatz 5 Telekommunikationsgesetz sowie ihre Erstreckung auf die Zahl der Auskünfte über Telekommunikationsverbindungen, um auf diesem Wege bessere Transparenz bei der Telefonüberwachung zu schaffen.

Anlage 8

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28. April 2003:

Verbesserung statt Absenkung des Datenschutzniveaus in der Telekommunikation

Im Zuge der bevorstehenden Novellierung des Telekommunikationsgesetzes plant die Bundesregierung neben der Abschaffung der Unternehmensstatistik (vgl. dazu Entschließung der 65. Konferenz v. 28.3.2003 zur Transparenz bei der Telefonüberwachung) eine Reihe weiterer Änderungen, die zu einer Absenkung des gegenwärtigen Datenschutzniveaus führen würden.
Zum einen ist vorgesehen, die Zweckentfremdung von Bestandsdaten der Telekommunikation (z.B. Art des Anschlusses, Kontoverbindung, Befreiung vom Telefonentgelt aus sozialen oder gesundheitlichen Gründen) für Werbezwecke weitergehend als bisher schon dann zuzulassen, wenn der Betroffene dem nicht widerspricht. Dies muss - wie bisher - die informierte Einwilligung des Betroffenen voraussetzen.
Außerdem plant die Bundesregierung, Daten, die den Zugriff auf Inhalte oder Informationen über die näheren Umstände der Telekommunikation schützen (wie z.B. PINs und PUKs - Personal Unblocking Keys -), in Zukunft der Beschlagnahme für die Verfolgung beliebiger Straftaten zugänglich zu machen. Bisher kann der Zugriff auf solche Daten nur angeordnet werden, wenn es um die Aufklärung bestimmter schwerer Straftaten geht. Diese Absenkung oder gar Aufhebung der verfassungsmäßig gebotenen Schutzschwelle für Daten, die dem Telekommunikationsgeheimnis unterliegen, wäre nicht gerechtfertigt; dies ergibt sich auch aus dem Urteil des Bundesverfassungsgerichts vom 12.3.2003.
Aus der Sicht des Datenschutzes ist auch die Versagung eines anonymen Zugangs zum Mobilfunk problematisch. Die beabsichtigte Gesetzesänderung führt dazu, dass z.B. der Erwerb eines „vertragslosen“ Handys, das mit einer entsprechenden - im Prepaid-Verfahren mit Guthaben aufladbaren - SIM-Karte ausgestattet ist, einem Identifikationszwang unterliegt. Dies hat zur Folge, dass die Anbieter von Prepaid-Verfahren eine Reihe von Daten wegen eines möglichen Zugriffs der Sicherheitsbehörden auf Vorrat speichern müssen, die sie für ihre Betriebszwecke nicht benötigen. Die verdachtslose routinemäßige Speicherung zu Zwecken der Verfolgung eventueller, noch gar nicht absehbarer künftiger Straftaten würde auch zur Entstehung von selbst für die Sicherheitsbehörden sinn- und nutzlosen Datenhalden führen. So sind erfahrungsgemäß z.B. die Erwerber häufig nicht mit den tatsächlichen Nutzern der Prepaid-Angebote identisch.
Insgesamt fordern die Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber auf, das gegenwärtige Datenschutzniveau bei der Telekommunikation zu verbessern, statt es weiter abzusenken. Hierzu sollte jetzt ein eigenes Telekommunikations-Datenschutzgesetz verabschiedet werden, das den Anforderungen einer freiheitlichen Informationsgesellschaft genügt und später im Zuge der noch ausstehenden zweiten Stufe der Modernisierung des Bundesdatenschutzgesetzes mit diesem zusammengeführt werden könnte.

Anlage 9

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 30. April 2003:

Neuordnung der Rundfunkfinanzierung

Die Länder bereiten gegenwärtig eine Neuordnung der Rundfunkfinanzierung vor, die im neuen Rundfunkgebührenstaatsvertrag geregelt werden soll. Die dazu bekannt gewordenen Vorschläge der Rundfunkanstalten lassen befürchten, dass bei ihrer Umsetzung die bestehenden datenschutzrechtlichen Defizite nicht nur beibehalten werden, sondern dass mit zum Teil gravierenden Verschlechterungen des Datenschutzes gerechnet werden muss:

* Insbesondere ist geplant, alle Meldebehörden zu verpflichten, der GEZ zum In-Kraft-Treten des neuen Staatsvertrages die Daten aller Personen in Deutschland zu übermitteln, die älter als 16 Jahre sind . Dadurch entstünde bei der GEZ faktisch ein bundesweites zentrales Register aller über 16-jährigen Personen mit Informationen über ihre sozialen Verhältnisse (wie Partnerschaften, gesetzliche Vertretungen, Haushaltszugehörigkeit und Empfang von Sozialleistungen), obwohl ein großer Teil dieser Daten zu keinem Zeitpunkt für den Einzug der Rundfunkgebühren erforderlich ist.

* Auch wenn in Zukunft nur noch für ein Rundfunkgerät pro Wohnung Gebühren gezahlt werden, sollen alle dort gemeldeten erwachsenen Bewohner von vornherein zur Auskunft verpflichtet sein, selbst wenn keine Anhaltspunkte für eine Gebührenpflicht bestehen. Für die Auskunftspflicht reicht es demgegenüber aus, dass zunächst - wie bei den amtlichen Statistiken erfolgreich praktiziert - nur die Meldedaten für eine Person übermittelt werden, die dazu befragt wird.

* Zudem soll die regelmäßige Übermittlung aller Zu- und Wegzüge aus den Meldedaten nun um Übermittlungen aus weiteren staatlichen bzw. sonstigen öffentlichen Dateien wie den Registern von berufsständischen Kammern, den Schuldnerverzeichnissen und dem Gewerbezentralregister erweitert werden. Auf alle diese Daten will die GEZ künftig auch online zugreifen.

* Gleichzeitig soll die von den zuständigen Landesdatenschutzbeauftragten als unzulässig bezeichnete Praxis der GEZ, ohne Wissen der Bürgerinnen und Bürger deren personenbezogene Daten bei Dritten - wie beispielsweise in der Nachbarschaft oder bei privaten Adresshändlern - zu erheben, ausdrücklich erlaubt werden.

* Schließlich sollen die bisher bestehenden Möglichkeiten der Aufsicht durch die Landesbeauftragten für den Datenschutz ausgeschlossen werden, sodass für die Rundfunkanstalten und die GEZ insoweit nur noch eine interne Datenschutzkontrolle beim Rundfunkgebühreneinzug bestünde.

Diese Vorstellungen der Rundfunkanstalten widersprechen dem Verhältnismäßigkeitsprinzip und sind daher nicht akzeptabel.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen ihre Forderung nach einer grundlegenden Neuorientierung der Rundfunkfinanzierung, bei der datenschutzfreundliche Modelle zu bevorzugen sind. Sie haben hierzu bereits praktikable Vorschläge vorgelegt.

Anlage 10

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. Juli 2003:

Bei der Erweiterung der DNA-Analyse Augenmaß bewahren

Derzeit gibt es mehrere politische Absichtserklärungen und Gesetzesinitiativen mit dem Ziel, die rechtlichen Schranken in § 81 g StPO für die Entnahme und Untersuchung von Körperzellen und für die Speicherung der dabei gewonnenen DNA-Identifizierungsmuster (sog. genetischer Fingerabdruck) in der zentralen DNA-Analyse-Datei des BKA abzusenken.

Die Vorschläge gehen dahin,

- zum einen als Anlasstat zur Anordnung einer DNA-Analyse künftig nicht mehr - wie vom geltenden Recht gefordert - in jedem Fall eine Straftat von erheblicher Bedeutung oder - wie jüngst vom Bundestag beschlossen - eine Straftat gegen die sexuelle Selbstbestimmung zu verlangen, sondern auch jede andere Straftat mit sexuellem Hintergrund oder sogar jedwede Straftat ausreichen zu lassen,
- zum anderen die auf einer eigenständigen, auf den jeweiligen Einzelfall bezogenen Gefahrenprognose beruhende Anordnung durch Richterinnen und Richter entfallen zu lassen und alle Entscheidungen der Polizei zu übertragen.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass die Anordnung der Entnahme und Untersuchung von Körperzellen zur Erstellung und Speicherung eines genetischen Fingerabdrucks einen tiefgreifenden und nachhaltigen Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen darstellt; dies hat auch das Bundesverfassungsgericht in seinen Beschlüssen vom Dezember 2000 und März 2001 bestätigt.

Selbst wenn bei der DNA-Analyse nach der derzeitigen Rechtslage nur die nichtcodierenden Teile untersucht werden: Schon daraus können Zusatzinformationen gewonnen werden (Geschlecht, Altersabschätzung, Zuordnung zu bestimmten Ethnien, möglicherweise einzelne Krankheiten wie Diabetes, Klinefelter-Syndrom). Auch deshalb lässt sich ein genetischer Fingerabdruck mit einem herkömmlichen Fingerabdruck nicht vergleichen. Zudem ist immerhin technisch auch eine Untersuchung des codierenden Materials denkbar, so dass zumindest die abstrakte Eignung für viel tiefer gehende Erkenntnisse gegeben ist. Dies bedingt unabhängig von den gesetzlichen Einschränkungen ein höheres abstraktes Gefährdungspotential.

Ferner ist zu bedenken, dass das Ausstreuen von Referenzmaterial (z.B. kleinste Hautpartikel oder Haare), das mit dem gespeicherten Identifizierungsmuster abgeglichen werden kann, letztlich nicht zu steuern ist, so dass in höherem Maß als bei Fingerabdrücken die Gefahr besteht, dass genetisches Material einer Nichttäterin oder eines Nichttäters an Tatorten auch zufällig, durch nicht wahrnehmbare Kontamination mit Zwischenträgern oder durch bewusste Manipulation platziert wird. Dies kann für Betroffene im Ergebnis zu einer Art Umkehr der Beweislast führen.

Angesichts dieser Wirkungen und Gefahrenpotentiale sehen die Datenschutzbeauftragten Erweiterungen des Einsatzes der DNA-Analyse kritisch und appellieren an die Regierungen und Gesetzgeber des Bundes und der Länder, die Diskussion dazu mit Augenmaß und unter Beachtung der wertsetzenden Bedeutung des Rechts auf informationelle Selbstbestimmung zu führen. Die DNA-Analyse darf nicht zum Routinewerkzeug jeder erkennungsdienstlichen Behandlung und damit zum alltäglichen polizeilichen Eingriffsinstrument im Rahmen der Aufklärung und Verhütung von Straftaten jeder Art werden. Auf das Erfordernis der Prognose erheblicher Straftaten als Voraussetzung einer DNA-Analyse darf nicht verzichtet werden.

Im Hinblick auf die Eingriffsschwere ist auch der Richtervorbehalt für die Anordnung der DNA-Analyse unverzichtbar. Es ist deshalb auch zu begrüßen, dass zur Stärkung dieser grundrechtssichernden Verfahrensvorgabe für die Anordnungsentscheidung die Anforderungen an die Begründung des Gerichts gesetzlich präzisiert wurden. Zudem sollte die weit verbreitete Praxis, DNA-Analysen ohne richterliche Entscheidung auf der Grundlage der Einwilligung der Betroffenen durchzuführen, gesetzlich ausgeschlossen werden.

Anlage 11

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7. August 2003:

Automatisches Software-Update

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die zunehmenden Bestrebungen von Softwareherstellern, über das Internet unbemerkt auf die Personalcomputer der Nutzerinnen und Nutzer zuzugreifen.
Zur Gewährleistung der Sicherheit und der Aktualität von System- und Anwendungssoftware ist es notwendig, regelmäßig Updates vorzunehmen. Weltweit agierende Softwarehersteller bieten in zunehmendem Maße an, im Rahmen so genannter Online-Updates komplette Softwarepakete oder einzelne Updates über das Internet auf die Rechner ihrer Kunden zu laden und automatisch zu installieren. Diese Verfahren bergen erhebliche Datenschutzrisiken in sich:

- Immer öfter werden dabei - oftmals vom Nutzer unbemerkt oder zumindest nicht transparent - Konfigurationsinformationen mit personenbeziehbaren Daten aus dem Zielrechner ausgelesen und an die Softwarehersteller übermittelt, ohne dass dies im derzeit praktizierten Umfang aus technischen Gründen erforderlich ist.
- Darüber hinaus bewirken Online-Updates vielfach Änderungen an der Software der Zielrechner, die dann in der Regel ohne die erforderlichen Tests und Freigabeverfahren genutzt werden.
- Ferner ist nicht immer sichergestellt, dass andere Anwendungen problemlos weiter funktionieren. Das - unbemerkte - Update wird dann nicht als Fehlerursache erkannt.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass Änderungen an automatisierten Verfahren zur Verarbeitung personenbezogener Daten oder an den zugrunde liegenden Betriebssystemen Wartungstätigkeiten im datenschutzrechtlichen Sinn sind, und daher nur den dazu ausdrücklich ermächtigten Personen möglich sein dürfen. Sollen im Zusammenhang mit derartigen Wartungstätigkeiten personenbezogene Daten von Nutzerinnen und Nutzern übermittelt und verarbeitet werden, ist die ausdrückliche Zustimmung der für die Daten verantwortlichen Stelle erforderlich.

Die meisten der derzeit angebotenen Verfahren zum automatischen Software-Update werden diesen aus dem deutschen Datenschutzrecht folgenden Anforderungen nicht gerecht. Insbesondere fehlt vielfach die Möglichkeit, dem Update-Vorgang ausdrücklich zuzustimmen. Die Daten verarbeitenden Stellen dürfen daher derartige Online-Updates nicht nutzen, um Softwarekomponenten ohne separate Tests und formelle Freigabe auf Produktionssysteme einzuspielen.

Auch für private Nutzerinnen und Nutzer sind die automatischen Update-Funktionen mit erheblichen Risiken für den Schutz der Privatsphäre verbunden. Den Erfordernissen des Datenschutzes kann nicht ausreichend Rechnung getragen werden, wenn unbemerkt Daten an Softwarehersteller übermittelt werden und somit die Anonymität der Nutzerinnen und Nutzer gefährdet wird.

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

Anlage 12

Entschließung der 66. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. September 2003:

Gesundheitsmodernisierungsgesetz

Die Datenschutzkonferenz begrüßt, dass mit den gesetzlichen Regelungen zur Gesundheitskarte und zu dem bei den Spitzenverbänden der Krankenkassen und der Kassenärztlichen Bundesvereinigung gebildeten zentralen Datenpool datenschutzfreundliche Lösungen erreicht werden konnten. Die Gesundheitskarte unterliegt auch künftig der Verfügungsgewalt der Patientinnen und Patienten. Für den quartals- und sektorenübergreifenden Datenpool dürfen nur pseudonymisierte Daten gespeichert werden.
Die Datenschutzkonferenz wendet sich nicht grundsätzlich gegen zusätzliche Kontrollmechanismen der Krankenkassen.
Die Datenschutzbeauftragten kritisieren, dass sie zu wesentlichen, erst in letzter Minute eingeführten und im Schnellverfahren realisierten Änderungen nicht rechtzeitig und ausreichend beteiligt wurden. Diese Änderungen bedingen erhebliche Risiken für die Versicherten:

- Für das neue Vergütungssystem werden künftig auch die Abrechnungen der ambulanten Behandlungen mit versichertenbezogener Diagnose an die Krankenkassen übermittelt. Mit der vorgesehenen Neuregelung könnten die Krankenkassen rein tatsächlich umfassende und intime Kenntnisse über 60 Millionen Versicherte erhalten. Die Gefahr gläserner Patientinnen und Patienten rückt damit näher. Diese datenschutzrechtlichen Risiken hätten durch die Verwendung moderner und datenschutzfreundlicher Technologien einschließlich der Pseudonymisierung vermieden werden können. Leider sind diese Möglichkeiten überhaupt nicht berücksichtigt worden.
- Ohne strenge Zweckbindungsregelungen könnten die Krankenkassen diese Daten nach den verschiedensten Gesichtspunkten auswerten (z.B. mit data-warehouse-Systemen).

Die Datenschutzkonferenz nimmt anerkennend zur Kenntnis, dass vor diesem Hintergrund durch Beschlussfassung des Ausschusses für Gesundheit und Soziale Sicherheit eine Klarstellung dahingehend erfolgt ist, dass durch technische und organisatorische Maßnahmen sicherzustellen ist, dass zur Verhinderung von Versichertenprofilen bei den Krankenkassen

- eine sektorenübergreifende Zusammenführung der Abrechnungs- und Leistungsdaten unzulässig ist, und dass

- die Krankenkassen die Daten nur für Abrechnungs- und Prüfzwecke nutzen dürfen.

Darüber hinaus trägt eine Entschließung des Deutschen Bundestages der Forderung der Datenschutzkonferenz Rechnung, durch eine Evaluierung der Neuregelung in bezug auf den Grundsatz der Datenvermeidung und Datensparsamkeit unter Einbeziehung der Möglichkeit von Pseudonymisierungsverfahren sicherzustellen, dass Fehlentwicklungen vermieden werden.
Die Datenschutzkonferenz hält eine frühestmögliche Pseudonymisierung der Abrechnungsdaten für notwendig, auch damit verhindert wird, dass eine Vielzahl von Bediensteten personenbezogene Gesundheitsdaten zur Kenntnis nehmen kann.

Anlage 13

Entschließung der 66. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. September 2003:

Konsequenzen aus der Untersuchung des Max-Planck-Instituts über Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation

Das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg hat im Mai dieses Jahres sein im Auftrag des Bundesministeriums der Justiz erstelltes Gutachten “Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100 a, 100 b StPO und anderer verdeckter Ermittlungsmaßnahmen” vorgelegt. Darin hat es festgestellt, dass

- die Zahl der Ermittlungsverfahren, in denen TKÜ-Anordnungen erfolgten, sich im Zeitraum von 1996 bis 2001 um 80 % erhöht (1996: 2149; 2001; 3868) hat,

- die Gesamtzahl der TKÜ-Anordnungen pro Jahr im Zeitraum von 1990 bis 2000 von 2.494 um das Sechsfache auf 15.741 gestiegen ist,

- sich die Zahl der jährlich davon Betroffenen im Zeitraum von 1994 bis 2001 von 3.730 auf 9.122 fast verdreifacht hat,

- in 21 % der Anordnungen zwischen 1.000 und 5.000 Gespräche, in 8 % der Anordnungen mehr als 5.000 Gespräche abgehört worden sind,

- der Anteil der staatsanwaltschaftlichen Eilanordnungen im Zeitraum von 1992 bis 1999 von ca. 2 % auf ca. 14 % angestiegen ist,

- die Beschlüsse in ca. ¾ aller Fälle das gesetzliche Maximum von 3 Monaten umfassen, ¾ aller Maßnahmen tatsächlich aber nur bis zu 2 Monaten andauern,

- lediglich 24 % der Beschlüsse substanziell begründet werden,

- es nur in 17 % der Fälle Ermittlungserfolge gegeben hat, die sich direkt auf den die Telefonüberwachung begründenden Verdacht bezogen,

- 73 % der betroffenen Anschlussinhaberinnen und -inhaber nicht über die Maßnahme unterrichtet wurden.

Die Telefonüberwachung stellt wegen ihrer Heimlichkeit und wegen der Bedeutung des Rechts auf unbeobachtete Kommunikation einen gravierenden Eingriff in das Persönlichkeitsrecht der Betroffenen dar, zu denen auch unbeteiligte Dritte gehören. Dieser Eingriff kann nur durch ein legitimes höherwertiges Interesse gerechtfertigt werden.

Nur die Verfolgung schwerwiegender Straftaten kann ein solches Interesse begründen. Vor diesem Hintergrund ist der Anstieg der Zahl der Verfahren, in denen Telefonüberwachungen angeordnet werden, kritisch zu bewerten. Dieser kann - entgegen häufig gegebener Deutung - nämlich nicht allein mit dem Zuwachs der Anschlüsse erklärt werden. Telefonüberwachungen müssen ultima ratio bleiben. Außerdem sind die im Gutachten des Max-Planck-Instituts zum Ausdruck kommenden strukturellen Mängel zu beseitigen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert den Gesetzgeber und die zuständigen Behörden auf, aus den Ergebnissen der Untersuchung daher folgende Konsequenzen zu ziehen:

- Der gesetzliche Richtervorbehalt darf nicht aufgelockert werden. Die Verwertung der angefertigten Aufzeichnungen sollte in Fällen staatsanwaltschaftlicher Eilanordnungen davon abhängig gemacht werden, dass ein Gericht rückwirkend deren Rechtmäßigkeit feststellt.

- Um die Qualität der Entscheidungen zu verbessern, sollte die Regelung des § 100b StPO dahin gehend ergänzt werden, dass die gesetzlichen Voraussetzungen der Anordnung einzelfallbezogen darzulegen sind. Die Rechtsfolgen für erhebliche Verstöße gegen die Begründungsanforderungen sollten gesetzlich geregelt werden (z.B. Beweisverwertungsverbote).

- Um die spezifische Sachkunde zu fördern, sollten die Aufgaben der Ermittlungsrichterinnen und -richter auf möglichst wenige Personen konzentriert werden. Die Verlagerung auf ein Kollegialgericht ist zu erwägen.

- Der Umfang des - seit Einführung der Vorschrift regelmäßig erweiterten - Straftatenkataloges des § 100 a StPO muss reduziert werden.

- Um eine umfassende Kontrolle der Entwicklung von TKÜ-Maßnahmen zu ermöglichen, muss in der StPO eine Pflicht zur zeitnahen Erstellung aussagekräftiger Berichte geschaffen werden. Jedenfalls bis dahin muss auch die in § 88 Abs. 5 TKG festgelegte Berichtspflicht der Betreiber von Telekommunikationsanlagen und der Regulierungsbehörde beibehalten werden.

- Der Umfang der Benachrichtigungspflichten, insbesondere der Begriff der Beteiligten, ist im Gesetz näher zu definieren, um die Rechte, zumindest aller bekannten Geprächsteilnehmerinnen und -teilnehmer zu sichern. Für eine längerfristige Zurückstellung der Benachrichtigung ist zumindest eine richterliche Zustimmung entsprechend § 101 Abs. 1 Satz 2 StPO vorzusehen. Darüber hinaus müssen die Strafverfolgungsbehörden beispielsweise durch Berichtspflichten angehalten werden, diesen gesetzlich festgeschriebenen Pflichten nachzukommen.

- Zum Schutz persönlicher Vertrauensverhältnisse ist eine Regelung zu schaffen, nach der Gespräche zwischen den Beschuldigten und zeugnisverweigerungsberechtigten Personen grundsätzlich nicht verwertet werden dürfen.

- Zur Sicherung der Zweckbindung nach § 100 b Abs. 5 StPO und 477 Abs. 2 Satz 2 StPO muss eine gesetzliche Verpflichtung zur Kennzeichnung der aus TKÜ-Maßnahmen erlangten Daten geschaffen werden.

- Die Höchstdauer der Maßnahmen sollte von drei auf zwei Monate reduziert werden.

- Auch aufgrund der Weiterentwicklung der Technik zur Telekommunikationsüberwachung (z.B. IMSI-Catcher, stille SMS, Überwachung des Internetverkehrs) ist eine Fortführung der wissenschaftlichen Evaluation dieser Maßnahmen unabdingbar. Die gesetzlichen Regelungen sind erforderlichenfalls deren Ergebnissen anzupassen.

Anlage 14

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 21. November 2003:

Gravierende Verschlechterungen des Datenschutzes im Entwurf des neuen Telekommunikationsgesetzes

Die Bundesregierung hat am 15. Oktober 2003 den Entwurf für ein neues Telekommunikationsgesetz beschlossen. Dieser Entwurf sieht jetzt zwar - entsprechend der Forderung der Datenschutzbeauftragten - die vorläufige Beibehaltung der Unternehmensstatistik zu Überwachungsmaßnahmen vor; im Übrigen enthält er aber gravierende Verschlechterungen des Datenschutzniveaus.

Insbesondere berechtigt der Gesetzentwurf die Diensteanbieter, grundsätzlich alle entstehenden Verkehrsdaten (also auch alle Zielrufnummern) unverkürzt bis zu sechs Monate nach Versendung der Rechnung zu speichern. Damit wird ohne Not und ohne überzeugende Begründung eine Regelung aufgegeben, die bisher die Speicherung von verkürzten Zielrufnummern vorsieht, wenn die Kundinnen und Kunden sich nicht für die vollständige Speicherung oder vollständige Löschung entscheiden. Die bisherige Regelung berücksichtigt in ausgewogener Weise sowohl die Datenschutz- als auch die Verbraucherschutzinteressen der beteiligten Personen und hat sich in der Praxis bewährt. Vollends inakzeptabel ist die inzwischen vom Rechtsausschuss des Bundesrates vorgeschlagene Pflicht zur Vorratsdatenspeicherung für sechs Monate. Gegen eine solche Regelung bestehen erhebliche verfassungsrechtliche Bedenken.

Schon die von der Bundesregierung vorgeschlagene Regelung würde dazu führen, dass Millionen von Verkehrsdatensätzen selbst dann noch unverkürzt gespeichert bleiben und dem Zugriff anderer Stellen ausgesetzt sind, wenn die Diensteanbieter sie für ihre Abrechnungszwecke nicht mehr benötigen. Das im Entwurf weiterhin vorgesehene Recht der Kundinnen und Kunden, die Speicherung gekürzter Zielrufnummern oder ihre vollständige Löschung nach Rechnungsversand zu verlangen, wird daran wenig ändern, weil nur eine Minderheit es wahrnehmen wird. Die Beibehaltung des bisherigen angemessenen Datenschutzstandards sollte nicht von der Initiative der Betroffenen abhängig gemacht werden, sondern allen zugute kommen, die nicht ausdrücklich einer weitergehenden Speicherung zustimmen. Zudem sind die Rechte der angerufenen Teilnehmerinnen und Teilnehmer zu berücksichtigen, in die durch eine Speicherung der unverkürzten Verkehrsdaten zusätzlich eingegriffen wird.

Die Datenschutzbeauftragten haben zudem stets die Zwangsidentifizierung beim Erwerb von vertragslosen (prepaid) Handys als gesetzwidrig kritisiert und sehen sich jetzt in dieser Auffassung durch das Urteil des Bundesverwaltungsgerichts vom 22. Oktober 2003 (Az.: 6 C 23.02) bestätigt. Zugleich wenden sie sich gegen die mit der TKG-Novelle geplante Einführung einer derartigen Identifikationspflicht, die zu einer verdachtslosen Datenspeicherung auf Vorrat führen würde. Wer ein solches Handy kauft, gibt es häufig ab oder verschenkt es, und ist deshalb nicht identisch mit

der Person, die das Handy nutzt. Deshalb bringen diese Daten keinen nennenswerten Informationsgewinn für die Sicherheitsbehörden.

Schließlich soll den Strafverfolgungsbehörden, der Polizei und den Nachrichtendiensten ohne Bindung an einen Straftatenkatalog oder einen Richtervorbehalt der Zugriff auf Passwörter, PINs, PUKs usw. eröffnet werden, mit denen die Inhalte oder nähere Umstände einer Telekommunikation geschützt werden. Dies würde die Möglichkeit eröffnen, von dieser Befugnis unkontrolliert Gebrauch zu machen. Die Befugnis dürfte zudem häufig ins Leere laufen, da die Anbieter diese Daten aus Gründen der Datensicherheit für sie selbst unlesbar verschlüsselt speichern.

Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber auf, den Entwurf bei den bevorstehenden Beratungen in diesen sensiblen Punkten zu korrigieren und den gebotenen Schutz des Telekommunikationsgeheimnisses sicherzustellen.

Anlage 15

Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 2004:

Personennummern

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

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

Anlage 16

Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 2004:

Einführung eines Forschungsgeheimnisses für medizinische Daten

In vielen Bereichen der Forschung werden sensible medizinische Daten der Bürgerinnern und Bürger verarbeitet. Dabei ist häufig eine Verarbeitung auch personenbezogener Daten erforderlich. Diese Daten können mit Einwilligung der Betroffenen insbesondere von Ärztinnen und Ärzten, aber auch von Angehörigen anderer Heilberufe an Forscher und Forscherinnen übermittelt werden. Dies ist im Interesse der Forschung zwar grundsätzlich zu begrüßen. Mit der Übermittlung verlieren die Daten aber regelmäßig den strafrechtlichen Schutz vor Offenbarung und den Beschlagnahmeschutz im Strafverfahren. Auch ein Zeugnisverweigerungsrecht bezüglich dieser Daten steht den Forschenden - anders als insbesondere den behandelnden Ärztinnen und Ärzten - nicht zu. Zum Schutze der Forschung, vor allem aber zum Schutz der durch die Datenübermittlung und -verarbeitung Betroffenen, sollte vom Gesetzgeber deshalb sichergestellt werden, dass die bei den übermittelnden Stellen geschützten personenbezogenen medizinischen Daten auch nach ihrer Übermittlung zu Forschungszwecken den gleichen Schutz genießen.

Die Datenschutzbeauftragten fordern daher den Bundesgesetzgeber auf,

- in § 203 StGB die unbefugte Offenbarung von personenbezogenen medizinischen Forschungsdaten unter Strafe zu stellen,
- in §§ 53, 53 a StPO für personenbezogene medizinische Daten ein Zeugnisverweigerungsrecht für Forscher und ihre Berufshelfer zu schaffen,
- in § 97 StPO ein Verbot der Beschlagnahme personenbezogener medizinischer Forschungsdaten zu schaffen.

Die Datenschutzbeauftragten sehen in diesen Vorschlägen einen ersten Schritt zu einer generellen Regelung des besonderen Schutzes personenbezogener Daten in der Forschung.

Anlage 17

Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 2004:

Automatische Kfz-Kennzeichenerfassung durch die Polizei

Die Datenschutzbeauftragten des Bundes und der Länder betrachten einen anlassfreien und lageunabhängigen Einsatz von automatischen Kfz-Kennzeichen-Lesesystemen im Straßenverkehr mit Sorge, weil sich diese Maßnahmen zu einem weiteren Schritt zur Überwachung aller Bürgerinnen und Bürger entwickeln können.
Es ist zu befürchten, dass mit dem Einsatz der automatischen Kfz-Kennzeichenerfassung eine neue Infrastruktur geschaffen wird, die künftig noch weit tiefergehende Eingriffe in das Persönlichkeitsrecht ermöglicht.

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

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

Anlage 18

Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 2004:

Übermittlung von Flugpassagierdaten an die US-Behörden

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

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

Die US-Zollbehörden wollen alle Reservierungsdaten mindestens 3,5 Jahre speichern ungeachtet der Tatsache, ob gegen eine Person ein Verdachtsmoment vorlag oder nicht. Passagierdaten, die im Einzelfall überprüft wurden, sollen zudem weitere 8 Jahre gespeichert werden.

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

Mit dem Zugriff ist wegen der teilweise hohen Sensibilität der Daten ein tiefer Eingriff in die Persönlichkeitsrechte der Betroffenen verbunden. Besonders hervorzuheben ist in diesem Zusammenhang, dass die US-Behörden hier aufgrund US-amerikanischen Rechts auf Datenbanken außerhalb ihres Hoheitsbereichs zugreifen.

Die betroffenen Personen werden gegenüber dem Zugriff auf ihre Daten durch eine ausländische Stelle in ihren Datenschutzrechten weitgehend schutzlos gelassen. Ein vergleichbares Ansinnen deutscher Sicherheitsbehörden wäre schwerlich mit unserer Verfassung vereinbar.

Die Problematik kann sich weiter verschärfen, wenn die USA die Passagierdaten zukünftig auch im sog. CAPPS II - System einsetzen wollen. Dieses System ermöglicht sowohl einen automatisierten Abgleich mit Fahndungslisten als auch mit Informationen aus dem privaten Sektor. Insbesondere sollen Kreditkarten- und Adressdaten mit Informationen aus der Kreditwirtschaft abgeglichen werden.

Die Europäische Kommission bemüht sich seit über einem Jahr in Verhandlungen darum, den Datenzugang der US-Behörden auf ein angemessenes Maß zu beschränken. Leider führten die Verhandlungen nur in Teilbereichen zum Erfolg. Die erzielten Ergebnisse in ihrer Gesamtheit gewähren den Reisenden keinen angemessenen Schutz ihrer Persönlichkeitsrechte. Dies hat die Gruppe nach Art. 29 der europäischen Datenschutzrichtlinie (EG-DSRL) in ihrer Stellungnahme vom 29.01.2004 deutlich herausgearbeitet:
(http://www.europa.eu.int/comm/internal_market/privacy/workingroup/wp2004/wpdocs04_de.htm)
Die darin vertretenen Positionen werden von den Datenschutzbeauftragten ausdrücklich unterstützt. Dennoch beabsichtigt die Europäische Kommission das Ergebnis ihrer Verhandlungen als einen angemessenen Datenschutzstandard förmlich anzuerkennen. Die Datenschutzbeauftragten appellieren an die Bundesregierung, sich gegen diese Entscheidung der Kommission zu wenden. Wenn die Kommission diesen unbefriedigenden Verhandlungsergebnissen ein angemessenes Datenschutzniveau attestiert, setzt sie damit Maßstäbe sowohl für die Auslegung der EU-Datenschutzrichtlinie als auch für Verhandlungen mit anderen Staaten über die Anerkennung des dortigen Datenschutzniveaus. Die Bundesregierung sollte sich demgegenüber für eine Lösung einsetzen, die Sicherheitsaspekte und den Schutz der Persönlichkeitsrechte in ein angemessenes Verhältnis setzt. Insbesondere sind die Informationen ausdrücklich zu benennen, die für die Passagieridentifikation benötigt werden. Diese Daten können zu einem angemessenen Zeitpunkt vor dem Abflug bereitgestellt werden. Ein unmittelbarer pauschaler Zugriff auf europäische Datenbanken, wie er zurzeit praktiziert wird, muss ausgeschlossen werden.

Anlage 19

Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 2004:

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder schließt sich voll inhaltlich der folgenden Entschließung an:

Entschließung der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre

Radio-Frequency Identification

vom 20. November 2003
(Übersetzung)

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

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

a. sollte jeder Datenverarbeiter vor der Einführung von RFID-Etiketten, die mit personenbezogenen Daten verknüpfbar sind oder die zur Bildung von Konsumprofilen führen, zunächst Alternativen in Betracht ziehen, die das gleiche Ziel ohne die Erhebung von personenbezogenen Informationen oder die Bildung von Kundenprofilen erreichen;
b. wenn der Datenverarbeiter darlegen kann, dass personenbezogene Daten unverzichtbar sind, müssen diese offen und transparent erhoben werden;
c. dürfen personenbezogene Daten nur für den speziellen Zweck verwendet werden, für den sie ursprünglich erhoben wurden und sie dürfen nur solange aufbewahrt werden, wie es zu Erreichung dieses Zwecks erforderlich ist und
d. soweit RFID-Etiketten im Besitz von Personen sind, sollten diese die Möglichkeit zur Löschung der gespeicherten Daten oder zur Deaktivierung oder Zerstörung der Etiketten haben.

Diese Grundsätze sollten bei der Gestaltung und bei der Verwendung von Produkten mit RFID berücksichtigt werden.

Das Auslesen und die Aktivierung von RFID-Etiketten aus der Ferne ohne vernünftige Gelegenheit für den Besitzer des etikettierten Gegenstandes, diesen Vorgang zu beeinflussen, würde zusätzliche Datenschutzrisiken auslösen.

Die Konferenz und die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation wird die technischen Entwicklungen in diesem Bereich genau und detaillierter verfolgen, um die Achtung des Datenschutzes und der Privatsphäre in einer Umgebung allgegenwärtiger Datenverarbeitung sicherzustellen.

Anlage 20

Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 2004:

Entscheidungen des Bundesverfassungsgerichts vom 3. März 2004 zum Großen Lauschangriff und zur präventiven Telekommunikationsüberwachung

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

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

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

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

Anlage 21

Entschließung der 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28./29. Oktober 2004:

Gesetzentwurf der Bundesregierung zur Neuregelung der akustischen Wohnraumüberwachung

Die Bundesregierung hat einen Gesetzentwurf zur Neuregelung der akustischen Wohnraumüberwachung vorgelegt. Sie setzt damit in großen Teilen das Urteil des Bundesverfassungsgerichts vom 3. März 2004 um, wonach die Vorschriften der Strafprozessordnung zum „großen Lauschangriff" in wesentlichen Teilen verfassungswidrig sind. Allerdings sind zentrale Punkte, wie die Begriffsbestimmung des „unantastbaren Kernbereichs der privaten Lebensgestaltung" und die Bestimmung des Kreises der Menschen „des persönlichen Vertrauens" offen geblieben.

Ungeachtet dessen drohen im weiteren Verlauf des Gesetzgebungsverfahrens schwerwiegende Verschlechterungen: So wird diskutiert, die Vorgaben des Bundesverfassungsgerichts dadurch zu unterlaufen, dass auch bei erkannten Eingriffen in den absolut geschützten Kernbereich die technische Aufzeichnung fortgesetzt wird. Dies steht in eklatantem Widerspruch zur eindeutigen Vorgabe des Bundesverfassungsgerichts, die Aufzeichnung in derartigen Fällen sofort zu beenden. Darüber hinaus wird versucht, den Anwendungsbereich der akustischen Wohnraumüberwachung dadurch auszuweiten, dass auch nicht strafbare Vorbereitungshandlungen einbezogen werden. Auch dies widerspricht den verfassungsgerichtlichen Vorgaben und verwischt die Grenzen zwischen Strafverfolgung und Gefahrenabwehr.

Die Datenschutzbeauftragten bekräftigen im Übrigen ihre Forderung, dass es im Hinblick auf die Heimlichkeit der Überwachung und ihrer zwangsläufigen Berührung mit dem Kernbereich privater Lebensgestaltung erforderlich ist, alle Formen der verdeckten Datenerhebung an den Maßstäben der verfassungsgerichtlichen Entscheidung vom 3. März 2004 zu messen und auszurichten sowie die einschlägigen gesetzlichen Befugnisregelungen des Bundes und der Länder auf den Prüfstand zu stellen und gegebenenfalls neu zu fassen. Dies gilt etwa für die präventive Telekommunikationsüberwachung, die längerfristige Observation, den verdeckten Einsatz technischer Mittel, den Einsatz nachrichtendienstlicher Mittel und von verdeckten Ermittlern. Dabei sind insbesondere Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung und zum Schutz vertraulicher Kommunikation mit engsten Familienangehörigen und andern engsten Vertrauten sowie mit Personen, die einem Berufsgeheimnis unterliegen, zur Einhaltung der Zweckbindung bei Weiterverwendung der durch die Eingriffsmaßnahmen erlangten Daten, zu der dazu erforderlichen Kennzeichnungspflicht und zur Benachrichtigung aller von der Eingriffsmaßnahme Betroffenen sowie zur detaillierten Ausgestaltung von Berichtspflichten gegenüber den Parlamenten vorzusehen.

Anlage 22

Entschließung der 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28./29. Oktober 2004:

Gravierende Datenschutzmängel bei Hartz IV

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass es bei der praktischen Umsetzung der Zusammenlegung von Arbeitslosen- und Sozialhilfe zu erheblichen datenschutzrechtlichen Mängeln gekommen ist. Diese bestehen sowohl bei den Verfahren der Datenerhebung durch die verwendeten Antragsformulare als auch bei der Leistungsberechnungs-Software (A2LL). Die Datenschutzdefizite wären vermeidbar gewesen, wenn datenschutzrechtliche Belange von Anfang an angemessen berücksichtigt und umgesetzt worden wären.
Zwar stellt die Bundesagentur für Arbeit (BA) seit dem 20.09.2004 sog. "Ausfüllhinweise zum Antragsvordruck Arbeitslosengeld II" zur Verfügung, in denen viele Bedenken der Datenschutzbeauftragten aufgegriffen werden. Allerdings ist hierbei zu berücksichtigen, dass durch die Ausfüllhinweise nicht mehr alle antragstellenden Personen erreicht werden können. Umso wichtiger ist es, dass die örtlich zuständigen Leistungsträger die verbindlichen Ausfüllhinweise beachten und die antragstellenden Personen, die ihren Antrag noch nicht eingereicht haben, vor der Abgabe auf diese hingewiesen werden. Personen, die ihren Antrag früher gestellt haben, dürfen nicht benachteiligt werden. Überschussinformationen, die vorhanden sind und weiterhin erhoben werden, sind zu löschen.

Darüber hinaus will die BA die in den Antragsformularen nachgewiesenen Datenschutzmängel in vielen Bereichen in der nächsten Druckauflage korrigieren und für das laufende Erhebungsverfahren zur Verfügung stellen. Gleichwohl ist zu befürchten, dass die Formulare nicht das erforderliche Datenschutzniveau erreichen.
Hinsichtlich der Software A2LL bestehen immer noch wesentliche Datenschutzmängel, die zu erheblichen Sicherheitsrisiken führen. Insbesondere besteht für die Sachbearbeitung ein uneingeschränkter bundesweiter Zugriff auf alle Daten, die im Rahmen von A2LL erfasst wurden, auch soweit diese Daten für die Sachbearbeitung nicht erforderlich sind. Dieser Mangel wird dadurch verschärft, dass noch nicht einmal eine Protokollierung der lesenden Zugriffe erfolgt und damit missbräuchliche Zugriffe nicht verfolgt werden können. Das Verfahren muss über ein klar definiertes Zugriffsberechtigungskonzept verfügen. Die Beschäftigten der zuständigen Leistungsträger dürfen nur den zur Aufgabenerfüllung erforderlichen Zugriff auf die Sozialdaten haben.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die BA auf, die notwendigen Schritte unverzüglich einzuleiten und nähere Auskunft über den Stand des Verfahrens zu erteilen.

Anlage 23

Entschließung der 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28./29. Oktober 2004:

Beteiligung der GEZ am Adresshandel (8. Rundfunkänderungsstaatsvertrag)

Die für die Rundfunkanstalten zuständigen Datenschutzbeauftragten haben im Rahmen der 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu dem 8. Rundfunkänderungsstaatsvertrag nachstehende Feststellung getroffen.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich wiederholt dafür eingesetzt, bei der Finanzierung des öffentlich-rechtlichen Rundfunks in Deutschland das Prinzip von Datenvermeidung und Datensparsamkeit in stärkerem Maße zu berücksichtigen. In der Kritik steht dabei im Besonderen die Beschaffung von jährlich mehreren Millionen Adressen hinter dem Rücken der Betroffenen beim kommerziellen Adresshandel durch die von den Rundfunkanstalten beauftragte Gebühreneinzugszentrale (GEZ), die diese Adressen für flächendeckende Mailing-Aktionen nutzt. Zahlreiche Beschwerden und Anfragen von Bürgerinnen und Bürgern beziehen sich auf diese Praxis der GEZ, die die zuständigen Landesdatenschutzbeauftragten als rechtswidrig bezeichnet haben.

Anstatt gemeinsam mit den Datenschutzbeauftragten datenschutzfreundliche Varianten einer gerechten Finanzierung des öffentlich-rechtlichen Rundfunks ernsthaft zu prüfen, haben die Ministerpräsidenten der Länder mit dem Entwurf eines 8. Rundfunkänderungsstaatsvertrages neben der Erhöhung der Rundfunkgebühren und deren Erstreckung auf Computer weitgehend ohne die gebotene Beteiligung der zuständigen Landesdatenschutzbeauftragten eine weitere Verschlechterung des Datenschutzes beschlossen:

Um die Beschaffung von Daten beim kommerziellen Adresshandel gesetzlich zu legitimieren, soll der Rundfunkgebührenstaatsvertrag um eine Befugnis erweitert werden, nach der die Rundfunkanstalten und die GEZ personenbezogene Daten unter den gleichen Bedingungen verarbeiten dürfen wie privatwirtschaftliche Unternehmen. Die vorgesehene Befugnis ist mit datenschutzrechtlichen Grundsätzen nicht zu vereinbaren. Während öffentlich-rechtliche Institutionen personenbezogene Daten nur verarbeiten dürfen, wenn dies zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist, ist die Datenverarbeitung der im Wettbewerb stehenden Privatwirtschaft vom Prinzip der Vertragsfreiheit geprägt. Die öffentlich-rechtlichen Rundfunkanstalten stehen hinsichtlich des Gebühreneinzugs in keinem Wettbewerb zu anderen Rundfunkveranstaltern. Schließlich haben die Länder gegen das Votum der Datenschutzbeauftragten bereits vor Jahren regelmäßige Übermittlungen von Meldedaten an die Rundfunkanstalten zugelassen, weil dies für erforderlich gehalten wurde. Eine parallele Nutzung von Daten aus den Melderegistern bei gleichzeitiger Beschaffung von Adressen im privaten Adresshandel ist jedoch unverhältnismäßig.

Zudem wird durch die ohnehin fragwürdige Befugnis das Ziel der Rundfunkanstalten nicht erreicht. Auch bei einem Inkrafttreten der vorgesehenen Regelung bliebe die Beschaffung von Adressen beim kommerziellen Adresshandel durch die GEZ rechtswidrig, da sich die Erhebung von personenbezogenen Daten bei Dritten ohne Kenntnis der Betroffenen weiterhin nach dem maßgeblichen Landesrecht richtet.

Die Konferenz hat davon Kenntnis genommen.

Anlage 24

Entschließung der 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28./29. Oktober 2004:

Datensparsamkeit bei der Verwaltungsmodernisierung

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen die Bemühungen, Dienstleistungen der öffentlichen Verwaltung bürgernäher und effizienter zu erbringen. Sie fordern, dass im Zuge von Maßnahmen der Verwaltungsreform die sich dadurch bietenden Möglichkeiten genutzt werden, um das Datenschutzniveau zu verbessern. Verwaltungsvereinfachung muss auch dazu genutzt werden, weniger personenbezogene Daten zu verarbeiten. Künftig müssen Verfahren und Datenflüsse wesentlich besser überschaubar und nachvollziehbar sein. Besonders sollen die Möglichkeiten der Technik genutzt werden, Risiken zu minimieren, die mit der Zentralisierung von Datenbeständen verbunden sind.

Werden Rechtsvorschriften, etwa im Steuerrecht oder im Arbeits- und Sozialrecht und hier insbesondere bei Änderungen in den Systemen der sozialen Sicherung, mit dem Ziel der Verwaltungsvereinfachung erlassen, sind die Auswirkungen auf den Datenschutz frühzeitig zu prüfen. Im Ergebnis müssen die Normen den gesetzlich verankerten Grundsatz der Datenvermeidung umsetzen und somit das Recht auf informationelle Selbstbestimmung gewährleisten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deswegen, bei Vorschlägen zur Verwaltungsvereinfachung und darüber hinaus bei allen Regelungsvorhaben darauf zu achten, dass das damit verbundene Potential an Datensparsamkeit und Transparenz ausgeschöpft wird.

Hierzu ist eine Folgenabschätzung auf mögliche Beeinträchtigungen der informationellen Selbstbestimmung vorzunehmen. Die Ergebnisse sind in geeigneter Form zu dokumentieren.

Anlage 25

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26. November 2004:

Staatliche Kontenkontrolle muss auf den Prüfstand!

Das „Gesetz zur Förderung der Steuerehrlichkeit“ vom 23.12.2003 (BGBl. I 2003, S. 2928) enthält mit den §§ 93 Abs. 7, 8 und 93b der Abgabenordnung Regelungen, die das Grundrecht auf informationelle Selbstbestimmung aller Bürgerinnen und Bürger im Bereich ihrer finanziellen und wirtschaftlichen Betätigung in erheblichem Maße beschränken. Die neuen Regelungen treten am 1. April 2005 in Kraft. Sie sehen vor, dass nicht nur Finanzbehörden, sondern auch eine unbestimmte Vielzahl weiterer Behörden Zugriff auf Bankdaten erhalten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, diese Regelungen mit dem Ziel zu überarbeiten, das Recht auf informationelle Selbstbestimmung zu gewährleisten. Insbesondere das verfassungsrechtliche Gebot der Normenklarheit und die Transparenz des Verfahrens müssen beachtet werden.

Die Neuregelung erlaubt einen Zugriff auf Bankdaten, die von den Kreditinstituten bereits seit April 2003 zur Aufdeckung illegaler Finanztransaktionen vor allem zur Terrorismusbekämpfung nach § 24 c des Kreditwesengesetzes vorgehalten werden müssen. Dabei handelt es sich um die Kontenstammdaten der Bankkundinnen und Bankkunden und sonstigen Verfügungsberechtigten, wie z.B. Name, Geburtsdatum, Kontonummern. Mit der neuen Regelung einher geht bereits eine von den Datenschutzbeauftragten des Bundes und der Länder im Gesetzgebungsverfahren Ende 2003 kritisierte Zweckänderung der Verwendung der von den Kreditinstituten vorzuhaltenden Daten.
Nunmehr sollen neben Finanzbehörden auch andere Behörden, z.B. die zahlreichen Stellen der Sozialleistungsträger, Auskunft erhalten, wenn die anfragende Behörde ein Gesetz anwendet, das „an Begriffe des Einkommensteuergesetzes“ anknüpft und eigene Ermittlungen dieser Behörde ihrer Versicherung nach nicht zum Ziel geführt haben oder keinen Erfolg versprechen. Welche Behörden dies sein sollen, geht aus dem Gesetz nicht eindeutig hervor. Da das Einkommensteuerrecht eine Vielzahl von „Begriffen“ verwendet (neben den Begriffen „Einkommen“ und „Einkünfte“ etwa auch „Wohnung“, „Kindergeld“, „Arbeitnehmer“), ist wegen fehlender Begriffsbestimmungen nicht abschließend bestimmbar, welche Behörden die Auskunftsersuchen stellen dürfen. Dies jedoch ist nach dem verfassungsrechtlichen Bestimmtheitsgebot unverzichtbar. Zudem wird nicht deutlich, welche Zwecke ein Auskunftsersuchen rechtfertigen und nach welchen Regeln sie erfolgen sollen.

Von der Tatsache des Datenabrufs erfahren Kreditinstitute und Betroffene zunächst nichts. Die Betroffenen erhalten hiervon allenfalls bei einer Diskrepanz zwischen ihren Angaben (z.B. anlässlich Steuererklärung, BAföG-Antrag) und den Ergebnissen der Kontenabfragen Kenntnis, nicht jedoch bei einer Bestätigung ihrer Angaben durch die Kontenabfragen.

Die Auskunft erstreckt sich zwar nicht auf die Kontostände; auf Grund der durch den Abruf erlangten Erkenntnisse können jedoch in einem zweiten Schritt weitere Überprüfungen, dann auch im Hinblick auf die Guthaben direkt beim Kreditinstitut erfolgen.

Dass Betroffene von Abfragen, die zu keiner weiteren Überprüfung führen, nichts erfahren, widerspricht dem verfassungsrechtlichen Transparenzgebot. Danach sind sie von der Speicherung und über die Identität der verantwortlichen Stelle sowie über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung zu unterrichten. Geschieht dies nicht, hat das zur Konsequenz, dass die Rechtsschutzgarantie des Art. 19 Abs. 4 Grundgesetz verletzt wird. Die Bürgerinnen und Bürger haben einen substantiellen Anspruch auf eine tatsächlich wirksame gerichtliche Kontrolle (s. Volkszählungsurteil, BVerfGE 65, 1, 70).

Anlage 26

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Bundesratsinitiative mehrerer Länder zur Ausweitung der DNA-Analyse vom 17.02.2005:

Keine Gleichsetzung der DNA-Analyse mit dem Fingerabdruck

Die strafprozessuale DNA-Analyse ist - insbesondere in Fällen der Schwerstkriminalität wie bei Tötungsdelikten - ein effektives Fahndungsmittel. Dies hat zu Forderungen nach der Ausweitung ihres Anwendungsbereichs zur Identitätsfeststellung in künftigen Strafverfahren geführt. So sieht ein Gesetzesantrag mehrerer Bundesländer zum Bundesratsplenum vom 18. Februar 2005 die Streichung des Richtervorbehalts und der materiellen Erfordernisse einer Anlasstat von erheblicher Bedeutung sowie der Prognose weiterer schwerer Straftaten vor.

Das zur Begründung derartiger Vorschläge herangezogene Argument, die DNA-Analyse könne mit dem herkömmlichen Fingerabdruck gleichgesetzt werden, trifft jedoch nicht zu:

Zum einen hinterlässt jeder Mensch permanent Spurenmaterial z.B. in Form von Hautschuppen oder Haaren. Dies ist ein Grund für den Erfolg des Fahndungsinstruments „DNA-Analyse“, weil sich Täter vor dem Hinterlassen von Spuren nicht so einfach schützen können, wie dies bei Fingerabdrücken möglich ist. Es birgt aber - auch unter Berücksichtigung der gebotenen vorsichtigen Beweiswürdigung - in erhöhtem Maße die Gefahr, dass Unbeteiligte aufgrund zufällig hinterlassener Spuren am Tatort unberechtigten Verdächtigungen ausgesetzt werden oder dass sogar bewusst DNA-Material Dritter am Tatort ausgestreut wird.

Zum anderen lassen sich bereits nach dem derzeitigen Stand der Technik aus den sog. nicht-codierenden Abschnitten der DNA über die Identitätsfeststellung hinaus Zusatzinformationen entnehmen (Verwandtschaftsbeziehungen, wahrscheinliche Zugehörigkeit zu ethnischen Gruppen, aufgrund der räumlichen Nähe einzelner nicht-codierender Abschnitte zu codierenden Abschnitten möglicherweise Hinweise auf bestimmte Krankheiten). Die Feststellung des Geschlechts ist bereits nach geltendem Recht zugelassen. Nicht absehbar ist schließlich, welche zusätzlichen Erkenntnisse aufgrund des zu erwartenden Fortschritts der Analysetechniken zukünftig möglich sein werden.

Mit gutem Grund hat daher das Bundesverfassungsgericht in zwei Entscheidungen aus den Jahren 2000 und 2001 die Verfassungsmäßigkeit der DNA-Analyse zu Zwecken der Strafverfolgung nur im Hinblick auf die derzeitigen Voraussetzungen einer vorangegangenen Straftat von erheblicher Bedeutung, einer Prognose weiterer schwerer Straftaten und einer richterlichen Anordnung bejaht. Es hat besonders gefordert, dass diese Voraussetzungen auch nach den Umständen des Einzelfalls gegeben sein müssen und von der Richterin oder dem Richter genau zu prüfen sind.

Eine Prognose schwerer Straftaten und eine richterliche Anordnung müssen im Hinblick auf diese Rechtsprechung und den schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung, den die DNA-Analyse darstellt, auch zukünftig Voraussetzung einer derartigen Maßnahme bleiben.

Die besondere Qualität dieses Grundrechtseingriffs muss auch im Übrigen bei allen Überlegungen, die derzeit zu einer möglichen Erweiterung des Anwendungsbereichs der DNA-Analyse angestellt werden, den Maßstab bilden; dies schließt eine Gleichsetzung in der Anwendung dieses besonderen Ermittlungswerkzeugs mit dem klassischen Fingerabdruckverfahren aus.

Anlage 27

Entschließung der 69. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 10./11. März 2005:

Einführung der elektronischen Gesundheitskarte

Die Datenschutzbeauftragten des Bundes und der Länder begleiten aufmerksam die Einführung der elektronischen Gesundheitskarte. Sie weisen darauf hin, dass die über die Karte erfolgende Datenverarbeitung nach den gesetzlichen Vorgaben weitgehend auf Grund der Einwilligung der Versicherten erfolgen muss. Um die hierfür nötige Akzeptanz bei den Versicherten zu erlangen, sind neben den rechtlichen auch die tatsächlichen - technischen wie organisatorischen - Voraussetzungen zu schaffen, dass sowohl das Patientengeheimnis als auch die Wahlfreiheit bei der Datenspeicherung und -übermittlung gewahrt sind.

Die Versicherten müssen darüber informiert werden, welche Datenverarbeitungsprozesse mit der Karte durchgeführt werden können, wer hierfür verantwortlich ist und welche Bestimmungsmöglichkeiten sie hierbei haben. Das Zugriffskonzept auf medizinische Daten muss technisch so realisiert werden, dass in der Grundeinstellung das Patientengeheimnis auch gegenüber und zwischen Angehörigen der Heilberufe umfassend gewahrt bleibt. Die Verfügungsbefugnis der Versicherten über ihre Daten, wie sie bereits in den Entschließungen zur 47. und 50. Datenschutzkonferenz gefordert wurde, muss durch geeignete Maßnahmen sichergestellt werden, um die Vertraulichkeit der konkreten elektronischen Kommunikationsbeziehungen unter Kontrolle der Betroffenen entsprechend dem gegenwärtigen technischen Stand zu gewährleisten.

Vor der obligatorischen flächendeckenden Einführung der elektronischen Gesundheitskarte sind die Verfahren und Komponenten auf ihre Funktionalität, ihre Patientenfreundlichkeit und ihre Datenschutzkonformität hin zu erproben und zu prüfen. Die Tests und Pilotversuche müssen ergebnisoffen ausgestaltet werden, damit die datenschutzfreundlichste Lösung gefunden werden kann. Eine vorzeitige Festlegung auf bestimmte Verfahren sollte deshalb unterbleiben.

Für die Bewertung der Gesundheitskarte und der neuen Telematikinfrastruktur können unabhängige Gutachten und Zertifizierungen förderlich sein, wie sie ein Datenschutz-Gütesiegel und ein Datenschutz-Audit vorsehen. Vorgesehene Einführungstermine dürfen kein Anlass dafür sein, dass von den bestehenden Datenschutzanforderungen Abstriche gemacht werden.

Anlage 28

Entschließung der 69. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 10./11. März 2005:

Datenschutzbeauftragte plädieren für Eingrenzung der Datenverarbeitung bei der Fußball-Weltmeisterschaft 2006

Die Datenschutzbeauftragten des Bundes und der Länder betrachten das Vergabeverfahren für die Eintrittskarten zur Fußball-Weltmeisterschaft 2006 mit großer Sorge. Bei der Bestellung von Tickets müssen die Karteninteressentinnen und -interessenten ihre persönlichen Daten wie Name, Geburtsdatum, Adresse, Nationalität sowie ihre Ausweisdaten angeben, um bei der Ticketvergabe berücksichtigt zu werden. Die Datenschutzbeauftragten befürchten, dass mit der Personalisierung der Eintrittskarten eine Entwicklung angestoßen wird, in deren Folge die Bürgerinnen und Bürger nur nach Preisgabe ihrer persönlichen Daten an Veranstaltungen teilnehmen können.

Es wird deshalb gefordert, dass nur die personenbezogenen Daten erhoben werden, die für die Vergabe unbedingt erforderlich sind. Rechtlich problematisch ist insbesondere die vorgesehene Erhebung und Verarbeitung der Pass- bzw. Personalausweisnummer der Karteninteressentinnen und -interessenten. Der Gesetzgeber wollte die Gefahr einer Nutzung der Ausweis-Seriennummer als eindeutige Personenkennziffer ausschließen. Die Seriennummer darf damit beim Ticketverkauf nicht als Ordnungsmerkmal gespeichert werden. Zur Legitimation der Ticketinhaberin bzw. -inhabers beim Zutritt zu den Stadien ist sie nicht erforderlich. Das Konzept der Ticket-Vergabe sollte daher überarbeitet werden. Eine solche Vergabepraxis darf nicht zum Vorbild für den Ticketverkauf auf Großveranstaltungen werden. Solche Veranstaltungen müssen grundsätzlich ohne Identifizierungszwang besucht werden können.

Anlage 29

Organisationsplan

Landesbeauftragter für den Datenschutz Sachsen-Anhalt
Herr Dr. von Bose

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, Kammern	Grundsatzfragen der Technik und Organisation des Datenschutzes und der Informationstechnik, Wirtschaft, Verkehr, Raumordnung und Landesplanung
Polizei, Gefahrenabwehr, Finanzen	Sozialwesen, Personenstandswesen	Vermessungs- und Katasterwesen, Statistik, Handwerk und Gewerbe, Wohnungswesen
Kommunalrecht, Verwaltungsverfahren, Ausländer, Aussiedler, Staatsangehörigkeit, Pass- und Ausweiswesen, EUROPOL und Schengen, Internationaler Datenschutz	Gesundheitswesen, Kinder- und Jugendhilfe, Kultur, Denkmalschutz, Archivwesen, Wissenschaft und Forschung, Schulen	Betriebs- und Datenbanksysteme, Telekommunikation, Netze, Neue Medien --- Gleichstellungsfragen
Verwaltungsangelegenheiten der Geschäftsstelle	Meldewesen, 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: 16.03.2005

Abkürzungsverzeichnis

A

AbfG LSA	Abfallgesetz des Landes Sachsen-Anhalt
Abs.	Absatz
a.F.	alter Fassung
AG-BSHG	Gesetz zur Ausführung des Bundessozialhilfegesetzes
AO	Abgabenordnung
ArchG	Archivgesetz

B

BA	Bundesagentur für Arbeit
BAföG	Bundesausbildungsförderungsgesetz
BAG	Bundesarbeitsgericht
BDSG	Bundesdatenschutzgesetz
BG LSA	Beamtengesetz Sachsen-Anhalt
BGBl. I	Bundesgesetzblatt, Teil I
BIDS	Basic Input Output System
BKA	Bundeskriminalamt
BMWA	Bundesministerium für Wirtschaft und Arbeit
BSHG	Bundessozialhilfegesetz
BStU	Bundesbeauftragte für die Unterlagen des Staatssicherheits-dienstes der ehemaligen DDR
BT-Drs.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungssammlung des Bundesverfassungsgerichts
BVerwG	Bundesverwaltungsgericht

D

DNA	Deoxyribonucleic acid (Desoxyribonukleinsäure)
DSG-LSA	Gesetz zum Schutz personenbezogener Daten der Bürger des Landes Sachsen-Anhalt
DV	Datenverarbeitung

E

EG	Europäische Gemeinschaften
EG-DSRL	Europäische Datenschutzrichtlinie
ELSTER	Elektronische Steuererklärung
E-Mail	Electronic Mail
EU	Europäische Union
Europol	Europäisches Polizeiamt
EWG	Europäische Wirtschaftsgemeinschaft

G

GewO	Gewerbeordnung
GEZ	Gebühreneinzugszentrale
GG	Grundgesetz
GKG	Gesetz über kommunale Gemeinschaftsarbeit
GKI	Gemeinsame Kontrollinstanz für Europol
GKV	Gesetzliche Krankenversicherung
GmbH	Gesellschaft mit beschränkter Haftung
GO LSA	Gemeindeordnung für das Land Sachsen-Anhalt
GVBl. LSA	Gesetz- und Verordnungsblatt für das Land Sachsen-Anhalt
GVU-E	Entwurf eines Gesetzes zur Regelung des Vollzuges der Untersuchungshaft

H

HAP	Heimarbeitsplatz
HAP-PC	Heimarbeitsplatzrechner
HBCI	Home Banking Interface
HTML	Hyper Text Markup Language

I

IMSI	International Mobil Subscriber Identity
InsO	Insolvenzordnung
ISDN	Integrated Services Digital Network
IT	Informationstechnik
ITN-LSA	Informationstechnisches Netz Sachsen-Anhalt
IuK	Informations- und Kommunikationstechnik

J

JURIS	Juristisches Informationssystem

K

KAG-LSA	Kommunalabgabengesetz des Landes Sachsen-Anhalt
KBA	Kraftfahrt-Bundesamt
KiFöG	Kinderförderungsgesetz des Landes Sachsen-Anhalt
KNSA	Kommunale Nachrichten Sachsen-Anhalt

L

LAN	Local Area Network
LIT	Landesleitstelle Informationstechnik
LKV	Landes- und Kommunalverwaltung, Verwaltungs-Zeitschrift
LT-Drs.	Landtagsdrucksache
LVerfG	Landesverfassungsgericht

M

MBl.	Ministerialblatt
MDK	Medizinischer Dienst der Krankenversicherung
MDR	Mitteldeutscher Rundfunk
MF	Ministerium der Finanzen
MfS	Ministerium für Staatssicherheit
MI	Ministerium des Innern
MJ	Ministerium der Justiz
MLU	Ministerium für Landwirtschaft und Umwelt
MMR	MultiMedia und Recht
MRRG	Melderechtsrahmengesetz

N

NJW	Neue Juristische Wochenschrift
NVwZ	Neue Zeitschrift für Verwaltungsrecht

O

OLG	Oberlandesgericht

P

PC	Personal Computer
PersVG LSA	Landespersonalvertretungsgesetz Sachsen-Anhalt
PIN	Personal Identification Number/Persönliche Identifikationsnummer
PKI	Public Key Infrastrucure
PS/2	Personal System 2 (Bezeichnung einer Schnittstelle für eine 1987 von IBM eingeführte PC-Familie gleichen Namens)
PUK	Personal Unblocking Key

R

RegTP	Regulierungsbehörde für Telekommunikation und Post
RFID	Radio Frequency Identification
RiStBV	Richtlinien für das Straf- und Bußgeldverfahren

S

SGB	Sozialgesetzbuch
SMS	Short Message Service
SOG LSA	Gesetz über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt
SSL	Secure Socket Layer
StatG-LSA	Statistikgesetz des Landes Sachsen-Anhalt
StatRegG	Statistikregistergesetz
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StUG	Stasiunterlagengesetz
StVG	Straßenverkehrsgesetz
StVollzG	Strafvollzugsgesetz

T

TAN	einmal verwendbare Transaktionsnummer
TBC	Tuberkulose
TCPA	Trusted Computing Platform Alliance
TDSV	Telekommunikations-Datenschutzverordnung
TESTA	Trans-European Services for Telematics between Administrations
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikationsüberwachung

U

USB	Universal Serial Bus

V

Verf LSA	Verfassung des Landes Sachsen-Anhalt
VO	Verordnung
VS-NfD	Verschlusssache - Nur für den Dienstgebrauch
VV-DSG-LSA	Verwaltungsvorschriften zum Gesetz zum Schutz personenbezogener Daten der Bürger
VwVfG LSA	Verwaltungsverfahrensgesetz des Landes Sachsen-Anhalt
VwVG LSA	Verwaltungsvollstreckungsgesetz des Landes Sachsen-Anhalt

W

WoGG	Wohngeldgesetz

Z

ZParl	Zeitschrift für Parlamentsfragen
ZPO	Zivilprozessordnung

Stichwortverzeichnis

(Fundstelle zitiert nach Tätigkeitsbericht und Seite, ab VI. Tätigkeitsbericht nach Tätigkeitsbericht und Ziffer)

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

X

Z