Landtag von Sachsen-Anhalt **Drucksache 4/1257**
Vierte Wahlperiode **15.12.2003**

Unterrichtung

Der Präsident des Landtages von Sachsen-Anhalt

Magdeburg, 12. Dezember 2003

Stellungnahme der Landesregierung zum Sechsten Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

Sehr geehrte Damen und Herren,

mit Schreiben vom 5. Dezember 2003, hier eingegangen am 9. Dezember 2003, übersandte der Chef der Staatskanzlei des Landes Sachsen-Anhalt gemäß § 22 Abs. 4a Satz 2 des Gesetzes zum Schutz personenbezogener Daten der Bürger (DSG-LSA) die Stellungnahme der Landesregierung zum Sechsten Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Sachsen-Anhalt für die Zeit vom 1. April 2001 bis 31. März 2003.

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

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

Mit freundlichen Grüßen

Prof. Dr. Adolf Spotka

(Ausgegeben am 16.12.2003)

Stellungnahme der Landesregierung zum Sechsten Tätigkeitsbericht des Landesbeauftragten für den Datenschutz des Landes Sachsen-Anhalt (Drs. 4/839 vom 18. Juni 2003)

Der Sechste Tätigkeitsbericht des Landesbeauftragten für den Datenschutz (Landesbeauftragter), der Mitte Juni 2003 vorgelegt wurde, bezieht sich auf den Zeitraum vom 1. April 2001 bis 31. März 2003. Mit ihm gibt der Landesbeauftragte einen exemplarischen Einblick in seine Arbeit.

Neben der Abhandlung datenschutzrechtlicher Einzelfragen befasst sich der Bericht schwerpunktmäßig mit technischen und rechtlichen Aspekten der neuen, aber immer gebräuchlicher werdenden elektronischen Verfahren und deren Gefahren für das Persönlichkeitsrecht.

Der Landesbeauftragte konnte während des Berichtszeitraums auf formelle Beanstandungen verzichten. Auch für die Landesregierung ist das ein Zeichen dafür, dass bei den Mitarbeitern im öffentlichen Dienst mittlerweile ein hohes Maß an Fachwissen und Problembewusstsein im Umgang mit dem allgemeinen Persönlichkeitsrecht erreicht ist.

Wie schon in der Vergangenheit beschränkt sich die Landesregierung in ihrer Stellungnahme im Wesentlichen auf Themen, bei denen Auffassungsunterschiede zwischen dem Landesbeauftragten und der Landesregierung bestehen. Daneben nutzt sie die Möglichkeit, über Sachstände zu informieren. Aus Achtung vor dem Gesetzgeber sieht sie davon ab, sich zu gesetzlichen Regelungen zu äußern, die von den gesetzgebenden Gremien im Bund oder vom Landtag Sachsen-Anhalt bereits verabschiedet wurden.

Zu 1. Entwicklung des Datenschutzes

Der Landesbeauftragte gibt in seiner Einleitung zum Tätigkeitsbericht allgemeine Erkenntnisse wieder, die er beim Umgang mit personenbezogenen Daten im öffentlichen wie im nicht-öffentlichen Bereich gewonnen hat. Danach sei die Tendenz ungebrochen, die einzelne Person mehr als früher zum Objekt der Beobachtung zu machen. Ihr Verhalten in der Öffentlichkeit werde umfassend dokumentiert. Um in den Genuss von Leistungen zu kommen, sei es für den Einzelnen unumgänglich, immer mehr Daten über die jeweilige individuelle Lebenssituation preiszugeben.

Zur Untermauerung dieser Einschätzung führt der Landesbeauftragte unter anderem für den öffentlichen Bereich Regelungen des Terrorismusbekämpfungsgesetzes vom 9. Januar 2002 an. Diese sind geschaffen worden, weil sich der Staat - gemeinsam mit den anderen Staaten der zivilisierten Welt - in seiner Schutzfunktion den aktuellen Bedrohungen durch den internationalen Terrorismus zu stellen hat. Er hat Vorsorge zu treffen, der Bedrohungslage, die aus der logistischen Vernetzung des internationalen Terrorismus und seinem extrem hohen Gewaltpotential gegenüber einem nicht eingrenzbaren Personenkreis hervorgeht, nicht nur im akuten Ernstfall, sondern schon prophylaktisch begegnen zu können. Dieses Ziel lässt sich leider nicht immer erreichen, ohne in die Sphäre Unbeteiligter einzudringen. Beim Terrorismusbekämpfungsgesetz sah sich der Bundesgesetzgeber in besonderem Maße verpflichtet, die widerstreitenden Interessen des Staates an einer wirksamen Gefahrenabwehr und Strafverfolgung einerseits und dem Interesse des Einzelnen, in seinem

Verhalten und Handeln frei von staatlicher Beobachtung zu sein andererseits, zu einem gerechten Ausgleich zu bringen. Aus diesem Grund gelten viele Regelungen des Gesetzes nur befristet bis zum 10. Januar 2007 und sind vor diesem Zeitpunkt zu überprüfen. Regelmäßig ist die Ausübung neuer Befugnisse zur Informationsbeschaffung durch die Sicherheitsbehörden an die Einhaltung verfahrensmäßiger Vorkehrungen gekoppelt. Auch bestehen strenge Regelungen zur Zweckbindung der erhobenen Daten.

Der Landesbeauftragte weist darauf hin, dass Pässe bzw. Personalausweise neben dem Lichtbild künftig auch biometrische Angaben von Fingern, Händen oder Gesicht des Inhabers enthalten dürfen. Hierdurch werden die Papiere deutlich fälschungssicherer und die Identitätsprüfung wird erleichtert. Der Missbrauch von Ausweisen wird insgesamt erschwert, was zu einem erheblichen Sicherheitsgewinn führen wird. Ausfüllende Regelungen, auch zum Schutz des Persönlichkeitsrechts der Betroffenen, sind einem künftigen Bundesgesetz vorbehalten. Konkrete Planungen hierzu bestehen noch nicht. Schon jetzt ist aber gesetzlich festgelegt, dass die zusätzlichen Merkmale nicht zentral gespeichert werden, sondern nur auf dem im Besitz des Ausweisinhabers befindlichen Identitätspapier. Auch hier sind enge Zweckbindungsregelungen getroffen worden.

Gegenwärtig erarbeitet das Büro für Technikfolgenabschätzung (TAB) für den Deutschen Bundestag ein Gutachten zu datenschutzrechtlichen Anforderungen hinsichtlich der Verwendung biometrischer Merkmale auf Ausweispapieren. Mit einem Ergebnis ist nicht vor Ende dieses Jahres zu rechnen.

Mit der Novellierung des Bundes- und Landesdatenschutzgesetzes im Jahr 2001 sind erstmals allgemeine Regelungen zur Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen in die Datenschutzgesetze aufgenommen worden. Damit wurde dem - vereinzelt zu beobachtenden - Wildwuchs auf dem Gebiet der Videoüberwachung entgegengetreten. Die Videoüberwachung ist nur für festgelegte Zwecke zulässig. Sie muss für den Betroffnen erkennbar sein. Erhobene Daten dürfen nur für bestimmte Zwecke verwendet und allenfalls kurzfristig gespeichert werden.

Die Landesregierung pflichtet dem Landesbeauftragten bei, dass die nahezu unbegrenzte Speicherkapazität und die hohe Auswertgeschwindigkeit moderner Informationstechnik das Risiko bergen, im Interesse der Einzelfallgerechtigkeit den Bezug öffentlicher Leistungen von immer spezifizierteren Angaben und dem Abgleich mit anderen Datenbeständen abhängig zu machen. Das kann nach Ansicht des Landesbeauftragten – wenn man es übertreibt - so weit gehen, dass die kostenmäßigen Vorteile der automatisierten Verarbeitung gegenüber der herkömmlichen Informationsverarbeitung in Akten aufgewogen werden. Solchen Tendenzen tritt die Landesregierung entschieden entgegen. Sie steht in der Pflicht, öffentliche Aufgaben sachgerecht, aber mit dem geringst möglichen Aufwand zu erledigen. Die strikte Beachtung des in § 1 Abs. 2 Satz 1 DSG-LSA niedergelegten Grundsatzes, Verfahren zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten an dem Ziel auszurichten, so wenig Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen, wirkt überflüssigem Verwaltungsaufwand entgegen - angesichts der knappen Haushaltlage ein probates Mittel, Sach- und Personalkosten einzusparen.

Die Verwendung moderner Informationstechnik einschließlich weltweiter Nutzung des Internets ist inzwischen zur Selbstverständlichkeit in allen Lebensbereichen geworden. Die Landesregierung ist der Auffassung, dass den aus dem Einsatz der Technik herrührenden Risiken für das Persönlichkeitsrecht, z. B. durch das bewusste, aber auch unbewusste Setzen elektronischer Spuren, mit klaren, praxisorientierten Regelungen im Kommunikationsrecht allgemein und im Datenschutzrecht im besonderen begegnet werden muss. Erster Schritt in diese Richtung sind Überlegungen auf Bund-/Länderebene zur Zusammenführung des Teledienstedatenschutzgesetzes und des Mediendienste-Staatsvertrages zu einem Elektronische-Medien-Datenschutzgesetz. Zweiter Schritt wird eine Modernisierung des Datenschutzrechts gemeinsam in Bund und Ländern sein. Hierzu liegt bereits ein Gutachten vor; dieses ist vom Bundesministerium des Innern unter *www.bmi.bund.de* in das Internet eingestellt worden. Der Bund beabsichtigt, noch in dieser Legislaturperiode das Bundesdatenschutzgesetz grundlegend zu novellieren.

Ein wichtiges Ziel hierbei ist es, dem Einzelnen die Möglichkeit zu geben, als gleichwertiger Partner am Informationsprozess teilzunehmen. Er muss, wenn möglich, anonym oder pseudonym auftreten können. Er darf nicht zum Objekt umfassender Überwachung durch öffentliche oder nicht-öffentliche Stellen werden. Er muss durch aktive Teilnahme am Verarbeitungsprozess grundsätzlich selbst entscheiden können, inwieweit sein Verhalten in der Öffentlichkeit oder im Netz für andere nachvollziehbar sein soll. Dies lässt sich nur durch ein Recht erreichen, das den Realitäten der modernen Technik ausreichend gerecht wird. Wichtig ist es, die Anwendung von Informationstechnik mehr als bisher zum Schutz des Einzelnen vor einer Beeinträchtigung seiner Privatsphäre einzusetzen. Die Zielvorgabe heißt: Nicht Datenschutz gegen Technik, sondern Datenschutz durch Technik.

Erreicht werden muss auch die Vereinfachung des Datenschutzrechts. Hierzu bedarf es eines radikalen Abbaus bereichsspezifischen Datenschutzrechts, ohne hierbei den Datenschutz substanziell abzusenken. Die verbleibenden Normen müssen verständlicher werden. Nicht nur die Verarbeitungsprozesse selbst, sondern auch die für sie geltenden Rechtsvorschriften müssen transparent sein.

Zu 2.1 Tätigkeit im Berichtszeitraum

Erfreulicherweise konnte der Landesbeauftragte im Berichtszeitraum von formellen Beanstandungen absehen. Diese positive Entwicklung ist vor allem auf die zielgerichtete Aus- und Fortbildung der Bediensteten zurückzuführen, an der auch der Landesbeauftragte maßgeblich beteiligt ist. Die Landesregierung wird auch weiterhin dem Datenschutz den ihm gebührenden Platz in der Aus- und Fortbildung einräumen. Gleichwohl hat der Datenschutzbeauftragte in etwa 30 Fällen Defizite beim Datenschutz festgestellt. Die Mängel konnten aber in Abstimmung mit den betroffenen Stellen und ihren Aufsichtsbehörden kurzfristig beseitigt werden.

Besondere Bedeutung für die Wahrung des Datenschutzes, auch bei der Aus- und Fortbildung von Bediensteten, kommt den „internen“ Beauftragten für den Datenschutz zu. Diese sind grundsätzlich für jede öffentliche Stelle einzusetzen, die personenbezogene Daten in automatisierten Verfahren erhebt, verarbeitet oder nutzt. Die Beauftragten haben auf die Einhaltung des DSG-LSA und anderer Datenschutzvorschriften hinzuwirken. Hierfür müssen sie die erforderliche Fachkunde und Zuverlässigkeit besitzen; dazu zählt neben der Kenntnis der rechtlichen Grundlagen ein all-

gemeines technisches Verständnis rund um die Informationsverarbeitung genauso wie die Kenntnis des Aufbaus und der Organisationsabläufe der öffentlichen Stelle, für die sie zuständig sind. Die Beauftragten sind auch Multiplikatoren, die die Bediensteten der jeweiligen öffentlichen Stelle mit den einschlägigen Datenschutzvorschriften vertraut machen. Sie können als das „Datenschutzgewissen“ einer öffentlichen Stelle bezeichnet werden, die deren Leitung Hinweise zur datenschutzgerechten Ausgestaltung des Umgangs mit personenbezogenen Daten geben und darauf dringen, erkannte Defizite zu beseitigen.

Zu 4.1 Datenübermittlungen im Kostenabrechnungsverfahren

Der Landesbeauftragte problematisiert erneut das Verfahren für die von der Kostenerstattung betroffenen Personen nach dem Aufnahmegesetz. Er weist darauf hin, dass zur Erfüllung der Aufgabe eine generelle Übermittlung personenbezogener Daten der Landkreise bzw. kreisfreien Städte an die Regierungspräsidien nicht zulässig ist, und mahnt an, Datenübermittlungen künftig nur für den Einzelfall vorzunehmen.

Gemäß Beschluss der Landesregierung vom 12. August 2003 sollen die Haushaltsmittel für das Kostenabrechnungsverfahren in das Finanzausgleichsgesetz (FAG) überführt werden. Ein entsprechendes Gesetz ist in Vorbereitung. Da die Mittelzuweisungen an die Landkreise und kreisfreien Städte künftig im Rahmen der allgemeinen Zuweisungen im FAG erfolgen, werden Einzelabrechnungen überflüssig.

Losgelöst vom Einzelfall ist die Landesregierung der Auffassung, dass Zahlungen des Landes, die von persönlichen Verhältnissen Einzelner abhängen, ausreichend belegt sein müssen. Die Landesregierung schlägt dem Landesbeauftragten daher vor, unter Beteiligung aller Ressorts und des Landesrechnungshofs eine allgemeingültige Position zu der Frage zu entwickeln, welche Angaben zur Person Verwendungsnachweise und ähnliche Unterlagen enthalten müssen, mit denen Personalkostenzuschüsse usw. abgerechnet werden.

Zu 7.1 Automatisierte Datenverarbeitung in der Landesverwaltung

Der Landesbeauftragte weist auf die Verantwortung der obersten Landesbehörden und der übrigen in § 14 Abs. 1 DSG-LSA genannten Stellen für eine datenschutzgerechte Gestaltung des eGovernment-Konzepts und der Ausgestaltung des Landesportals hin.

Unter Elektronic Government – eGovernment – wird gemäß „Grundkonzept eGovernment in Sachsen-Anhalt“ die Durchführung von Prozessen der öffentlichen Willensbildung, der Entscheidung und der Leistungserstellung in Politik, Staat und Verwaltung unter intensiver Nutzung der Informationstechnik verstanden. Die Nutzungsmöglichkeiten sind vielfältig; sie bestehen unter anderem in der Bereitstellung elektronischer Kommunikationsmöglichkeiten zwischen Verwaltung und Bürgern bzw. Wirtschaftsunternehmen, aber auch von Verwaltungsbehörden untereinander.

EGovernment fängt an bei der Verwaltungsmodernisierung durch elektronische Vorgangsbearbeitung, reicht von der Bereitstellung von Verwaltungsinformationen auf Behörden-Portalen im Internet bis hin zu komplexen Transaktionsdiensten (z. B. Stellung von Anträgen) und echten Teilhabediensten (vollelektronische Abwicklung

von Verwaltungsverfahren im Netz). Ziel ist es, für jedermann möglichst viele Dienstleistungen der Verwaltung elektronisch zugänglich zu machen. Verwaltungsintern wird ein ganzheitliches Informationsmanagement angestrebt. Darüber hinaus ist eGovernment ein Mittel, den Bürgern mehr Transparenz zu bieten und sie von Behördengängen zu entlasten.

Über das Landesportal *www.sachsen-anhalt.de* kann jedermann auf das eGovernment-Grundkonzept unter dem Stichwort „eGovernment“ zugreifen. Im Grundkonzept werden Wesen, Ausrichtung, Ziel und Leitthesen für eine eGovernment-Strategie in Sachsen-Anhalt formuliert und Plattformen sowie künftige Dienste und Anwendungen beschrieben. Auf dem Grundkonzept wird der ressortübergreifende Aktionsplan aufbauen; in ihm werden abgestimmte Vorhaben und Projekte erfasst. Die so fixierten Projekte und Vorhaben werden dann von den Ressorts in Abstimmung mit der eGovernment-Koordinierungsstelle ausgestaltet und umgesetzt (eGovernment-Anwendungen).

Die technische Ausgestaltung von eGovernment in Sachsen-Anhalt wird sich auf Standards und Aufbaukonzepte für eGovernment-Anwendungen des Bundesministeriums des Innern ebenso stützen wie auf im Kooperationsausschuss ADV (KoopA ADV) getroffene Festlegungen. Die Kommunikationsplattformen bilden das Landesdatennetz (ITN-LSA), TESTA Deutschland und das Internet. Hierfür wird ITN-LSA zum gemeinsamen und einheitlichen Landes- und Kommunalnetz ausgebaut. ITN-LSA und TESTA Deutschland sind geschlossene, ausschließlich für öffentliche Stellen bestimmte Netze. Diese Netze bieten daher einen Sicherheitsstandard, der den Grundanforderungen des § 6 DSG-LSA an ausreichende technische Vorkehrungen zur Gewährleistung des Datenschutzes genügt.

Allen Beteiligten ist bewusst, dass vor dem Hintergrund aktueller technischer Entwicklungen die Sicherheitsbedingungen für eGovernment zu verbessern sind. Beim künftigen Einsatz von Kommunikations-, Transaktions- und Partizipationsdiensten ist von besonderer Bedeutung die Realisierung der in § 6 DSG-LSA genannten sechs Schutzziele, nämlich der Wahrung der Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz. Dabei handelt es sich zwar auch um Anforderungen an den Datenschutz, vorrangig aber um solche an die Datensicherheit. Hierzu werden die Beteiligten vermehrt digitale Signaturen einsetzen müssen. Der Bund hat nach Erlass des Signaturgesetzes und der hierzu ergangenen Signaturverordnung den rechtlichen Rahmen für die rechtsverbindliche Kommunikation zwischen Verwaltung und Bürger unter anderem durch das Dritte Gesetz zur Änderung verwaltungsverfahrensrechtlicher Vorschriften vom 21. August 2002 (BGBl. I S. 3222) geschaffen; eine entsprechende Änderung des Landesrechts ist in Vorbereitung.

Bei der Realisierung von eGovernment im Land werden die Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI), des KoopA ADV sowie die Handlungsempfehlungen "Datenschutzgerechtes eGovernment" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder berücksichtigt. So werden bei Anwendungen, bei denen auch Netze genutzt werden, die wie das Internet nicht ausschließlich für öffentliche Stellen bestimmt sind, Vorkehrungen (z. B. durch Firewalls) getroffen, die den allgemeinen Sicherheitsanforderungen des ITN-LSA genügen.

Wichtige Hinweise zum Einsatz von Verschlüsselungsverfahren in der Verwaltung geben der Handlungsleitfaden für die Einführung der elektronischen Signatur und Verschlüsselung in der Verwaltung sowie die Orientierungshilfe zum Einsatz kryptografischer Verfahren, die der Landesbeauftragte in das Internet eingestellt hat.

Es wird darauf geachtet, dass die Anforderungen, die das Telekommunikations,- Tele- und Medienrecht stellen, eingehalten werden. Hierbei sind auch die „internen“ Beauftragten für den Datenschutz nach § 14a DSG-LSA in der Pflicht.

Nach Realisierung der letzten Ausbaustufe stehen über eGovernment Dienste und Leistungen zur Verfügung, die mehr als ein automatisiertes Informationssystem im Sinne des § 22 Abs. 4 Satz 2 DSG-LSA sind. Einen solchen Charakter haben nur die Informations- und Kommunikationsdienste. Ungeachtet dessen wird der Landesbeauftragte auch weiterhin uneingeschränkt und umfassend entsprechend § 22 Abs. 4 Satz 2 DSG-LSA in die Planungen für eGovernment eingebunden. Dazu gehört die rechtzeitige Unterrichtung durch die fachlich zuständigen Ressorts über einzelne Anwendungen. Die Landesregierung ist der Auffassung, dass die Unterrichtung des Landesbeauftragten nach § 22 Abs. 4 Satz 2 DSG-LSA nicht an eine besondere Form gebunden ist. Die Unterrichtung kann auch durch das zur Verfügungstellen erforderlicher Unterlagen für den Koordinierungsausschuss Informationstechnik (IT-KA), in dem der Landesbeauftragte als ständiger Gast vertreten ist, erfolgen. Eine gesonderte und damit doppelte Unterrichtung, die der Landesbeauftragte zu befürworten scheint, brächte unnötigen Verwaltungsaufwand mit sich.

Zu 7.2 Neuordnung der IT-Organisation des Landes

Der Landesbeauftragte geht in seinem Tätigkeitsbericht auf grundlegende Änderungen in der IT-Organisationsstruktur der Landesverwaltung seit dem Jahr 2002 ein. Neben der Bildung des Landesinformationszentrums Sachsen-Anhalt (LIZ) als Landesbetrieb nach § 26 LHO nennt er die Einrichtung des Referates *Landesleitstelle Informationstechnik (LIT)* beim Ministerium des Innern.

Schon in der Vergangenheit war die Auseinandersetzung mit Vorschlägen und Empfehlungen des Landesbeauftragten eine selbstverständliche Pflicht der zuständigen IT-Gremien. Die Landeregierung begrüßt, dass der Landesbeauftragte an den Beratungen des IT-KA teilnimmt und durch die Mitarbeit in diesem Gremium seinem Beratungsauftrag nach § 22 Abs. 4 Satz 1 DSG-LSA frühzeitig und intensiv nachkommen kann.

Soweit der Landesbeauftragte Regelungen und Normierungen für Sicherheitsstandards fordert, ist auf Folgendes hinzuweisen: Die Landesregierung ist durch die Mitarbeit des Ministeriums des Innern in bundesweiten Gremien, insbesondere dem KoopA ADV, an der Fortschreibung von Standards intensiv beteiligt. Vor dem Hintergrund der unter eGovernment zusammengefassten Aktivitäten (vgl. Nr. 7.1) gewinnt die Interoperabilität auf der Grundlage sicherer Mechanismen zunehmende Bedeutung. Die Landesregierung wird die unter ihrer Beteiligung entwickelten Rahmenbedingungen für das Land Sachsen-Anhalt für verbindlich erklären und damit den Datenschutz innerhalb der strategischen IT-Entwicklung des Landes weiter festigen. Hierbei ist zu beachten, dass eine stärkere Kooperation von Landes- und Kommunalverwaltungen zu verzeichnen ist, die durch einheitliche Infrastrukturen unterstützt werden soll. Dadurch werden potenzielle Sicherheitslücken vermieden.

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

Der Landesbeauftragte weist darauf hin, dass das ITN LSA auf der Grundlage einer internen Richtlinie von T-Systems ISS GmbH in Bonn erstmals am 29.11.2001 auf seine Sicherheit überprüft worden ist. Das Zertifikat gilt bis zum 31.12.2003. Darin festgestellte Defizite wurden inzwischen ausgeräumt. Ohne Mängel der bisherigen Zertifizierung aufzuzeigen, regt der Landesbeauftragte an, das Sicherheitskonzept künftig nach den strengen Regelungen der international gültigen Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (1999 angepasst an den internationalen Standard ISO/IEC 15408) durch das BSI prüfen zu lassen. Damit voraussichtlich verbundene wesentliche Mehrkosten müssten im Interesse der Sicherheit in Kauf genommen werden.

Dem Landesbeauftragten ist zuzustimmen, dass die Sicherheit in der Kommunikationstechnik nicht aus Kostengründen vernachlässigt werden darf. Die Landesregierung erinnert an dieser Stelle daran, dass die öffentliche Hand zum wirtschaftlichen und sparsamen Umgang mit öffentlichen Mitteln verpflichtet ist. Dieser Gedanke liegt auch § 6 Abs. 1 DSG-LSA zu Grunde, wonach nur solche technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit zu treffen sind, deren Aufwand in einem angemessenen Verhältnis zum Schutzzweck stehen. Das ITN-LSA bedient sich im Wesentlichen der Leitungen und Übertragungstechnik von T-Systems. Zudem existiert ein Wartungsvertrag mit T-Systems, der die Verantwortlichen darin unterstützt, eine hohe Betriebsbereitschaft der Netzknotentechnik zu gewährleisten. Die hierauf abgestimmte Zertifizierung des Landesnetzes durch die T-Systems ISS GmbH hält die Landesregierung weiterhin für angemessen und inhaltlich ausreichend.

Der Landesbeauftragte weist zu Recht darauf hin, dass das ITN-LSA als informationstechnisches Netz nur ein Transportsystem darstellt. Das LIZ als Betreiber gewährleistet zusammen mit dem Technischen Polizeiamt die Grundsicherheit des Netzes. Insoweit trägt das Ministerium des Innern nach § 14 Abs. 1 DSG-LSA die Ressortverantwortung. Sollte nach Art der transportierten Daten ein höheres Schutzniveau erforderlich sein, um den Zielvorgaben des § 6 DSG-LSA zu genügen, hat hierfür die jeweils verantwortliche Stelle zu sorgen. Diese Schutzvorkehrungen fallen in die Ressortzuständigkeit der für die einzelnen Verfahren fachlich zuständigen Ministerien. Die Sicherheitskomponenten variieren also von Fall zu Fall. Dementsprechend gibt es kein einheitliches Gesamt-Sicherheitskonzept dergestalt, dass alle Einzelheiten verfahrensübergreifend in einem Papier fixiert sind.

Die IT-Grundsätze vom 01.06.1992 (MBl. LSA S. 805) sowie der sog. Netz-Erlass zum ITN-LSA vom 07.02.1994 (MBl. LSA S. 1251) werden gegenwärtig überarbeitet. Im Netz-Erlass soll klargestellt werden, dass der jeweilige Fachanwender die Verantwortung für ausreichende verfahrensspezifische Schutzvorkehrungen trägt.

Der Landesbeauftragte erhält Gelegenheit, an der Neufassung der Regelungen mitzuwirken, die als gemeinsamer Runderlass ergehen sollen.

Zu 7.5 Neues IP- und Routingkonzept im ITN-LSA

Der Landesbeauftragte hat dargelegt, aus welchen Gründen beim weiteren Ausbau des ITN-LSA von der bisherigen Netzknotentechnik und der Vergabe fester IP-Adressen abgegangen wurde. Nunmehr erfolgt die Kommunikation über Vermittlungsrechner, die die Hauptverbindungsrouten (Backbone) des Netzes verbinden. Dazu sind sechs Sektoren gebildet worden, die nach dem OSPF-Prinzip (Open Shortest Path Prinzip – „kürzester Weg zuerst“) miteinander verbunden sind und damit schnelle, aber auch sichere Übertragungswege schaffen.

Es ist richtig, dass durch das dynamische Routing (vgl. Nr. 7.5 des Tätigkeitsberichts) alle Rechner im ITN-LSA leichter erreichbar geworden sind und damit ein geringerer Schutz gegen technikkundige Innentäter besteht. Die Änderung des Routings war aber erforderlich, um die Adressierungsprozesse im Netz, die zunehmend ressortübergreifend erfolgen, auch in Zukunft bewältigen zu können.

Der Landesbeauftragte bestätigt gleichwohl, dass die Änderungen der Kommunikationsstrukturen ein wesentlicher Beitrag sind, um die Sicherheitsziele des § 6 Abs. 2 DSG-LSA zu erreichen. Die Landesregierung teilt die Auffassung des Landesbeauftragten, dass nur bei konsequenter Nutzung der mit der Neuordnung des Routingkonzepts zusätzlich geschaffenen Sicherheitsmechanismen den vom Landesbeauftragten aufgezeigten Gefahren bei der Kommunikation der Teilnehmer im Netz begegnet werden kann. Der vom Landesbeauftragten angesprochene ausreichende Passwortschutz ist nur eines der Instrumente. Bei der Neufassung der Regelungen zum ITN-LSA wird den Sicherheitsbelangen gebührend Rechnung getragen werden. Für die LIT ist bei entsprechendem Schutzbedürfnis die Verschlüsselung von Daten ein wesentliches Kriterium, das sie auch in die länderübergreifende Normsetzung eingebracht hat. Damit sind die Grundlagen dafür geschaffen, dass auch im Netzverbund der Bundesrepublik Deutschland die gleichen Ansätze verfolgt werden.

Zu 8.2 Prüfung der Finanzämter (Seite 31 Absatz 3)

Das vom Landesbeauftragten angemahnte zentrale Verfahrensverzeichnis wird gegenwärtig von der Oberfinanzdirektion Magdeburg erarbeitet. Es ist vorgesehen, den Finanzämtern das Verfahrensverzeichnis nach seiner Fertigstellung in geeigneter Form zur Verfügung zu stellen.

(Seite 31 Absätze 4 und 5) und (Seite 32 Absatz 1)

Der Landesbeauftragte bemängelt die nicht ausreichende Kontrolle von Fremdfirmen durch Mitarbeiter der Finanzämter bei der Reinigung der Diensträume außerhalb der Dienstzeiten. Er sieht darin einen Verstoß gegen das Steuergeheimnis nach § 30 der Abgabenordnung (AO) und auch gegen die Anforderungen des § 6 DSG-LSA, der die technischen und organisatorischen Sicherheitsmaßnahmen regelt, um Daten vor dem Zugriff Unbeteiligter zu schützen. Im geschilderten Fall sind das Daten, die in Akten oder manuellen Karteien aufbewahrt werden.

Die Feststellungen des Landesbeauftragten wurden zum Anlass genommen, die Verträge mit den beauftragten Firmen umgehend zu ändern Eine Reinigung der

Diensträume erfolgt nur noch während der Dienstzeiten. Die Regelungen hinsichtlich der Reinigungszeiten wurden auch in die Dienstanweisung zum Datenschutz aufgenommen. Sollte in Ausnahmefällen eine Reinigung der Diensträume während der Dienstzeiten nicht möglich sein, wird das Reinigungspersonal durch einen Bediensteten des Finanzamtes beaufsichtigt oder stichprobenartig kontrolliert.

Den Anforderungen an das Steuergeheimnis und auch an die technischen und organisatorischen Maßnahmen ist somit Genüge getan.

Ein Abdruck der Dienstanweisung zum Datenschutz ist dem Landesbeauftragten am 28. April 2003 zugeleitet worden.

Zu 8.3 Änderung des Kraftfahrzeugsteuergesetzes

Bei der Kraftfahrzeugsteuer (KraftSt) kommt es in den Ländern zu überdurchschnittlich hohen Rückständen. Die Rückstandsfälle beruhen im Vergleich zu anderen Stauerarten auf einer Vielzahl von Fällen mit vergleichsweise geringen Beträgen. In Sachsen-Anhalt betreffen 44 % der Rückstandsfälle die KraftSt, wobei die durchschnittliche Höhe weniger als 200 € pro Fall beträgt.

Auf Initiative der Länder wurde das KraftStG dahingehend geändert, dass die Zulassungsbehörde bei Anmeldung eines Kraftfahrzeuges den Fahrzeugschein erst aushändigen darf, wenn nachgewiesen ist, dass den Vorschriften über die KraftSt genügt ist. Hierzu dürfen die Landesregierungen die Aushändigung des Fahrzeugscheins durch Rechtsverordnung davon abhängig machen, dass die KraftSt für den ersten Zeitraum entrichtet ist, eine Einzugsermächtigung erteilt wird oder eine Bescheinigung vorgelegt wird, dass das Finanzamt wegen einer erheblichen Härte für den Fahrzeughalter darauf verzichtet. Ferner darf durch Rechtsverordnung geregelt werden, dass die Aushändigung des Fahrzeugscheins davon abhängig gemacht wird, dass keine KraftSt-Rückstände bestehen. Zu diesem Zweck dürfen die Finanzämter den Zulassungsbehörden Auskünfte über KraftSt-Rückstände des Fahrzeughalters erteilen. Wird das Fahrzeug nicht durch den Fahrzeughalter, sondern durch einen Dritten zugelassen, so muss dieser eine Einverständniserklärung des Steuerpflichtigen mit der Bekanntgabe seiner kraftfahrzeugsteuerlichen Verhältnisse vorlegen.

Diese Regelungen dienen dazu, die fristgerechte Zahlung der KraftSt sicherzustellen. Es soll ein spürbarer Rückgang der Rückstandsfälle erreicht werden.

Der Bundesgesetzgeber hat sich trotz der Vorbehalte der Datenschutzbeauftragten in Bund und Ländern entschieden, die oben ausgeführten Regelungen in das KraftStG aufzunehmen. Ob das Land Sachsen-Anhalt von der Ermächtigung zum Erlass einer Rechtsverordnung Gebrauch macht, wird derzeit geprüft. Der Landesbeauftragte wird zu gegebener Zeit über die Planungen der Landesregierung unterrichtet.

Zu 12.4 Unsicherheiten in Bürosoftware

Der Landesbeauftragte macht im Anschluss an seine Ausführungen im IV. Tätigkeitsbericht darauf aufmerksam, dass bei der Benutzung simpler Menüfunktionen wie „Datei, speichern unter“ temporäre Dateien auf dem jeweiligen Nutzer-PC angelegt

werden. Temporäre Dateien sind Hilfsdateien, die vom Betriebssystem automatisch und vom Nutzer unbemerkt im Ordner „Temp-Dateien“ abgespeichert werden. Sie stellen lediglich Sicherungskopien aktueller Anwendungen vor akuten Störungen (wie z. B. Stromausfall) dar. Ihre Anlage erfolgt selbst dann, wenn wegen der besonderen Sensibilität von Daten festgelegt ist, dass diese auf besonders abgeschirmten Servern zu speichern sind. Der Landesbeauftragte empfiehlt, in diesem Fall auch für die einzelnen Nutzer-PC - und mithin für Temp-Dateien - erhöhte Sicherheitsvorkehrungen zu treffen.

PC-Sicherheit bedeutet die Einhaltung bestimmter Sicherheitsstandards, die den Schutz der Verfügbarkeit, der Integrität und der Vertraulichkeit von Informationen und Funktionen betreffen. Die Entscheidung darüber, in welchem Umfang Sicherheitsmaßnahmen notwendig sind, obliegt der jeweiligen verantwortlichen Stelle; umgesetzt werden sie durch die zuständigen Administratoren. Darüber hinaus ist es erforderlich, dass die einzelnen Nutzer für die IT-Sicherheit sensibilisiert sind.

Die Festlegung von angemessenen Sicherheitsmaßnahmen ergibt sich aus dem Schutzbedarf der gespeicherten Daten. Bei geringem oder weniger hohem Schutzbedarf genügt es, Standardsicherheitsmaßnahmen zu ergreifen. Bei hohem Schutzbedarf geht der Festlegung von Sicherheitsvorkehrungen eine Analyse der Sicherheitsrisiken voraus. Grundsätzlich ist aber auch hier der Aufwand der Maßnahmen gegen deren Wirtschaftlichkeit abzuwägen.

Die Landesregierung wird ihrem Gesetzesauftrag nach § 6 Abs. 2 DSG-LSA gerecht: Neben allgemeinen Schutzmaßnahmen - wie dem regelmäßigen Wechseln von Passwörtern, der Verschließbarkeit von bestimmten Büros oder der Verwendung von Bildschirmschonern mit Passwortschutz - werden sensible Daten auf speziell abgeschirmten Servern gespeichert. Administratoren kontrollieren und löschen gegebenenfalls jede Festplatte, die eine Behörde verlässt, z. B. bei Wartung oder Verkauf von Hardware. Durch diese Vorgehensweise können Manipulationen erkannt und Zugriffe durch Unbefugte verhindert werden.

Die Anlage von Sicherungskopien ist dann sinnvoll, wenn im Bedarfsfall darauf zurückgegriffen werden muss. Grundsätzlich ist es jedem Nutzer selbst überlassen, wann die Löschung solcher temporären Dateien vorgenommen wird. Die Landesregierung nimmt die Ausführungen des Landesbeauftragten zum Anlass, für die Landesverwaltung auf einer der nächsten Sitzungen des IT-KA verbindliche Festlegungen zu Löschungsfristen für temporäre Dateien zu treffen. Die Löschung sollte nach kurzer Zeit auch automatisch erfolgen.

Zu 12.5 Sichere Kommunikation im Internet

Der Landesbeauftragte meint, dass öffentliche Stellen beim Umgang mit dem Medium „Internet“ nicht immer die erforderliche Sorgfalt und Zurückhaltung walten lassen. Dies gelte sowohl für das Einstellen personenbezogener Daten ins Netz als auch für die Nutzung spezieller Kommunikationswege. Wegen tatsächlicher und rechtlicher Unsicherheiten dürften öffentliche Stellen nur unter besonderen und engen Voraussetzungen das Internet nutzen.

Dem ist entgegenzuhalten, dass sich die Landesregierung und alle in § 14 Abs. 1 DSG-LSA genannten Stellen, die für die Einhaltung des Datenschutzes in ihrem Or-

ganisationsbereich verantwortlich sind, der Risiken des Einsatzes des Internets bewusst sind und diesen in gebührender Weise begegnen. Es wird sorgfältig geprüft, ob personenbezogene Daten im Internet veröffentlicht werden dürfen. Es kann aber keinen Verzicht auf Technik geben. Der Abbau von Bürokratie ist erklärtes Ziel der Landesregierung, und auch das der Kommunen und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts. Dieses Ziel ist nur bei konsequenter Nutzung der modernen Informationstechnik und im Wege der Informationsübertragung zu erreichen. Für den Bürger und die Wirtschaft eröffnet das Internet als „Portal“ für den Kontakt mit öffentlichen Stellen die Möglichkeit, ohne Zeitverzug erforderliche Informationen einzuholen, Erklärungen abzugeben usw. und gleichzeitig eine Entlastung von unnützen Wegen zu erreichen.

Unverändert fortfahren wird die Landesregierung daher in ihrem Bestreben, immer mehr Dienstleistungen der Verwaltung dem Bürger online zur Verfügung zu stellen. Ihr ist dabei bewusst, dass solche Dienste, sofern es um den Transport sensibler Daten geht, nur dann von den Bürgern und der Wirtschaft angenommen werden, wenn durch ausreichende technische und organisatorische Maßnahmen sichergestellt ist, dass Unbefugte von den Daten nicht Kenntnis nehmen können (z. B. durch ausreichende Verschlüsselungen oder Verwendung von Signaturen u.s.w.). Im Einzelnen wird auf die Ausführungen zu Nr. 7.1 verwiesen.

Der Landesbeauftragte hat sowohl in seinem Tätigkeitsbericht als auch auf seiner Internet-Seite ausgeführt, dass er aufgrund bekannter Sicherheitsprobleme des Internets seine E-Mail-Adresse für den Dienstgebrauch, nicht aber für jedermann zur Verfügung stellt. Hierzu darf angemerkt werden, dass Diensteanbieter - um einen solchen handelt es sich beim Landesbeauftragten - gemäß § 6 Nr. 2 Teledienstegesetz und auch § 10 Abs. 2 Nr. 2 Mediendienstestaatsvertrag solche Angaben leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten haben, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation mit ihnen ermöglichen, einschließlich der Adresse der elektronischen Post. Hierzu gehört nach der Gesetzesbegründung zu § 6 Nr. 2 Teledienstegesetz zumindest die Angabe einer Telefonnummer und die Angabe einer E-Mail-Adresse.

Zu 14.3 Daten von Stadtratsmitgliedern und Schiedsleuten auf der Homepage einer Stadt

Auch Städte und Gemeinden nutzen zunehmend die sich durch das Internet bietenden Möglichkeiten und präsentieren sich über ihre örtlichen Grenzen hinaus im WorldWideWeb. Solange sich die Informationen auf allgemeine Serviceleistungen beschränken, sind diese datenschutzrechtlich unproblematisch. Im Gegensatz zum Landesbeauftragten hält es die Landesregierung für datenschutzrechtlich unbedenklich, wenn Kommunen die Namen ihrer Mandatsträger neben der Angabe, welchen Ausschüssen sie angehören, in das Internet einstellen. Sie befindet sich hier in Übereinstimmung mit der Auffassung vieler Landesbeauftragter für den Datenschutz in anderen Ländern. Der Landesregierung ist bewusst, dass öffentliche Stellen eine Befugnis zur Veröffentlichung personenbezogener Daten nur aufgrund entsprechender gesetzlicher Ermächtigung haben. Aber auch die allgemeinen Übermittlungsbefugnisse nach dem DSG-LSA können zur Veröffentlichung personenbezogener Daten berechtigen, wenn nicht wegen der Schwere des Eingriffs eine spezialgesetzliche Regelung erforderlich ist. Aufgabe der öffentlichen Stellen ist auch ihre allgemeine Öffentlichkeitsarbeit. Diese Aufgabe erwächst letztlich aus dem Demokratiegrundsatz

und den darauf fußenden Prinzipien der Transparenz und Publizität des staatlichen Handelns. Auch wenn man die strengen Übermittlungskriterien des § 13 Abs. 2 DSG-LSA für Übermittlungen an ausländische Stellen ohne ausreichendes Datenschutzniveau zu Grunde legt, muss man eine solche Übermittlung als zur Aufgabenerfüllung der übermittelnden Stelle erforderlich im Sinne des § 12 Abs. 1 Nr. 1 DSG-LSA ansehen. Das öffentliche Interesse an der Veröffentlichung überwiegt nach § 13 Abs. 2 Satz 3 Nr. 3 DSG-LSA. Hinnehmbar ist auch, dass bei der Veröffentlichung die Einhaltung der Zweckbindung nicht gewährleistet werden kann. Bei Mandatsträgern tritt insoweit die Privatperson hinter ihrem öffentlichen Amt zurück, zumal die Zugehörigkeit zu kommunalen Vertretungskörperschaften nach Kommunalwahlrecht öffentlich bekannt gemacht worden ist.

Die Landesregierung stimmt mit dem Landesbeauftragten jedoch darin überein, dass eine Veröffentlichung der Privatadressen oder privaten Telefonnummern von kommunalen Mandatsträgern nur möglich ist, wenn die Betroffenen vorher in eine Veröffentlichung eingewilligt haben. Der Vorschlag, im Vorfeld eine entsprechende Entscheidung aller Mitglieder des betroffenen Gremiums herbeizuführen, wird als zweckmäßig begrüßt.

Uneingeschränkt geteilt wird auch die Empfehlung des Landesbeauftragten, Veröffentlichungen über Mandatsträger im Internet nur als Bilddateien vorzunehmen, um so direkte Recherchen durch Suchmaschinen auszuschließen.

Die vorstehenden Ausführungen gelten für die Veröffentlichung von Angaben über Schiedspersonen im Internet grundsätzlich entsprechend. In bestimmten Rechtsstreitigkeiten ist die Durchführung eines Einigungsversuchs vor einer außergerichtlichen Schlichtungsstelle nicht freiwillig, sondern sogar gesetzlich vorgeschrieben, bevor eine Klage eingereicht werden kann. Nach dem Schiedsstellen- und Schlichtungsgesetz (SchStG) richtet jede Gemeinde eine oder mehrere Schiedsstellen ein. Daneben sind auch alle Notare sowie bestimmte - in einer im Ministerialblatt für das Land Sachsen-Anhalt veröffentlichten Liste aufgeführte - Rechtsanwälte zur obligatorischen Streitschlichtung berufen. Die Aufgaben der Schiedsstelle werden in der Regel von einer Schiedsfrau oder einem Schiedsmann (Schiedsperson) wahrgenommen. Die Schiedsperson ist ehrenamtlich tätig. Im Interesse einer funktionierenden Rechtspflege gehört es zur Öffentlichkeitsarbeit der Kommunen, jedem Interessierten Informationen darüber zu geben, wie er die zuständige Schiedsstelle erreichen kann. Dies kann auch durch Veröffentlichung im Internet geschehen. § 22 Abs. 1 SchStG bestimmt, dass ein Antrag auf Durchführung des Schlichtungsverfahrens sowie dessen Rücknahme bei der Schiedsstelle schriftlich einzureichen oder mündlich zu Protokoll zu erklären sind. Ist eine Schiedsstelle nur mit einer Person besetzt und dient als Büro *ausnahmsweise* die Privatwohnung, sind deren Anschrift und wohl auch der Name der Schiedsperson unverzichtbare Adressierungszusätze.

Schiedsleute werden aber häufig auch außerhalb von Schlichtungsverfahren in sogenannten „Tür-und-Angel-Fällen“ vermittelnd tätig, weswegen auch hier die Erreichbarkeit durch die Mitteilung der Anschrift der Schiedsperson notwendig sein kann. Die Landesregierung stimmt mit dem Landesbeauftragten überein, dass auch die Veröffentlichung von Daten über Schiedspersonen nur als Bilddatei erfolgen sollte.

Zu 14.5 Übertragung von Ratssitzungen und anderen Veranstaltungen in das Internet

Die Ausführungen des Landesbeauftragten für den Datenschutz zur Zulässigkeit der Übertragung von Sitzungen des Gemeinderates und anderer, insbesondere öffentlicher Veranstaltungen in der Gemeinde im Internet werden nicht uneingeschränkt geteilt. Sofern die ausdrückliche Einwilligung der Betroffenen vorliegt, ist die Übertragung ins Internet unbedenklich.

Bisher besteht keine besondere Regelung, die die Übertragung öffentlicher Sitzungen kommunaler Gremien im Internet gestattet; allerdings gibt es auch kein Verbot. Öffentlichkeit von Sitzungen bedeutet, dass jedermann als Zuschauer persönlich an Sitzungen teilnehmen kann, fraglich ist aber, ob das Öffentlichkeitsgebot auch eine „weltweite“ Veröffentlichung im Internet deckt. Diese wird gleichwohl als zulässig angesehen, wenn alle anwesenden Mitglieder des jeweiligen Gremiums hierin eingewilligt haben. Besucher sollten darauf hingewiesen werden, dass die Sitzung ins Internet eingestellt wird. Der Besucherbereich sollte nicht von Kameras erfasst werden; zumindest müssen Besucher die Möglichkeit haben, sich außerhalb des Aufnahmebereichs zu platzieren.

Die Übertragung öffentlicher Sitzungen im Internet ist jedoch mit Risiken behaftet. Dies gilt z. B., wenn Angelegenheiten erörtert werden, deren Behandlung in öffentlicher Sitzung hinzunehmen ist, der Betroffene aber auf eine „lokale“ Öffentlichkeit vertrauen kann und nicht mit einer „weltweiten“ Öffentlichkeit rechnen muss. In diesem Zusammenhang wird auf § 56 Abs. 3 der Gemeindeordnung hingewiesen, wonach nur Einwohner ein Recht auf Einsicht in Niederschriften über öffentliche Sitzungen haben.

Die Landesregierung nimmt die Feststellungen des Landesbeauftragten zu Nrn. 14.3 und 14.5 zum Anlass, gelegentlich einer der nächsten Dienstbesprechungen mit den Vertretern der kommunalen Spitzenverbände die Gefahren beim Umgang mit personenbezogenen Daten bei Internetpräsentationen und auch bei Übertragung von Ratssitzungen im Internet zu thematisieren. Das Ministerium des Innern wird anregen, die Kommunen in einem der kommunalen Mitteilungsblätter auf die datenschutzrechtlichen Anforderungen hinzuweisen.

Zu 16.2 Zeiterfassung

Der Landesregierung ist bewusst, dass Daten, die von automatisierten Zeiterfassungssystemen gespeichert werden, sehr sensible Informationen enthalten können, soweit sie mit Daten aus anderen Systemen (z. B. aus der Kontrolle von Zugangsberechtigungen für die Dienstgebäude) kombiniert werden. Die Landesregierung legt deshalb besonderen Wert darauf, dass für solche Verfahren die organisatorischen und verfahrensmäßigen Voraussetzungen der Nutzung möglichst umfassend festgelegt werden. Hierbei erfolgt regelmäßig die Beteiligung der jeweils zuständigen Personalräte.

Bei der automatisierten Zeiterfassung werden den Bediensteten die monatlichen Buchungsübersichten in der Regel über die Dienstvorgesetzten zugeleitet und stichprobenartig, ggf. anlassbezogen, kontrolliert. Sofern in der Vergangenheit vereinzelt Buchungslisten über die unmittelbaren Vorgesetzten an die Beschäftigten gelangt sind,

werden die obersten Landesbehörden für ihren Zuständigkeitsbereich organisatorische Maßnahmen einleiten, die gewährleisten, dass die Buchungsübersichten den Beschäftigten künftig direkt zugeleitet werden.

Zu 16.3 Schutz von Personaldaten bei Privatisierung der Reinigung

Die Auffassung des Landesbeauftragten, wonach die Übermittlung personenbezogener Daten im Vorfeld einer Privatisierung öffentlicher Aufgaben datenschutzrechtlichen Bedenken begegnet, wird von der Landesregierung geteilt. Eine Übermittlung anonymisierter Daten erscheint für den vorgesehenen Zweck völlig ausreichend. Die Landesregierung geht davon aus, dass es sich bei dem beschriebenen Vorgang um einen Einzelfall handelt.

Zu 18.1 „Personalaktenführung in der Justiz“ oder „Jeder will alles im eigenen Hause haben“

Auf die vom Landesbeauftragten angesprochene Entwicklung, wonach auf mehreren Ebenen des Gerichts- bzw. Behördenaufbaus inhaltlich identische Personalakten geführt werden, hat das Ministerium der Justiz durch Erlass der AV vom 09.12.2002 (JMBl. LSA S. 348 ff.) reagiert. Die AV zur „Führung und Verwaltung der Personalakten im Geschäftsbereich des Ministeriums der Justiz des Landes Sachsen-Anhalt“ wirkt der zum Teil doppelten und dreifachen Führung vollständiger Personalakten auf mehreren Hierarchieebenen zum Zwecke der Reduzierung des Verwaltungsaufwands entgegen und stellt sicher, dass Daten nur in dem zur Aufgabenerfüllung erforderlichen Maß erhoben, verarbeitet und genutzt werden. Auch wahrt die AV den vom Landesbeauftragten angesprochenen Grundsatz der Einheit der Personalakte.

Dem Umstand, dass in manchen der vom Landesbeauftragten stichprobenartig eingesehenen Personalakten Angaben zu der Existenz von Teil- und Nebenakten fehlten, wurde durch die Regelung in Abschnitt II Nr. 2 der AV begegnet. Demnach ist jeder Personalgrundakte ein vollständiges Verzeichnis aller Teil- und Nebenakten vorzuheften. Teil- und nebenaktenführende Stellen haben die Anlegung der Teil- und Nebenakten der grundaktenführenden Stelle mitzuteilen (Abschnitt III Nr. 1 Satz 3 und Abschnitt IV Nr. 2 der AV).

Den Bericht des Landesbeauftragten über die Existenz von Sammelverfügungen und Berichten in Personalakten, in denen personenbezogene Daten über andere Bedienstete nicht geschwärzt worden waren, hat das Ministerium der Justiz zum Anlass genommen, den Geschäftsbereich an die datenschutzrechtlich gebotene Anonymisierung der personenbezogenen Daten Dritter zu erinnern.

Zu 18.2 Fehlende Anonymisierung bei Beschlüssen zur DNA-Untersuchung

Es ist bedauerlich, dass in den von dem Landesbeauftragten genannten Fällen eine Anonymisierung unterblieben ist. Anlass zur Besorgnis, man könne aus den vorgefundenen Fällen auf einen grundsätzlichen Mangel im Verfahren schließen, besteht indessen nicht. Die von den Ministerien des Innern und der Justiz entwickelte Konzeption zur Umsetzung des DNA-Identitätsfeststellungsgesetzes (Gem. RdErl. des MJ und MI vom 28.10.2002) ist unter anderem auch zur Wahrung der Belange des Datenschutzes geschaffen worden.

Hierneben wird das Ministerium der Justiz angesichts der Bedeutung des Themas die Bemerkungen des Landesbeauftragten zum Gegenstand der nächsten Dienstbesprechungen mit den Staatsanwaltschaften machen.

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

Die Landesregierung unterstützt die Bestrebungen des Datenschutzbeauftragten auf Ergänzung der Regelungen der Nr. 2.1 Abs. 3 DB-PKHG. Nordrhein-Westfalen hat hierzu eine Formulierung vorgeschlagen, zu welcher die Länder um Stellungnahme bis zum 20. Oktober 2003 gebeten worden waren. Da insoweit keine Bedenken erhoben worden sind, ist davon auszugehen, dass der Text demnächst festgestellt werden wird.

Zu 18.11 Insolvenz und Zwangsversteigerungen im Internet

Die Gesetzgebungskompetenz für die Insolvenzordnung und das Zwangsversteigerungsgesetz liegt beim Bund.

Nach § 9 InsO erfolgt die öffentliche Bekanntmachung durch Veröffentlichung in dem für amtliche Bekanntmachungen des Gerichts bestimmten Blatt oder in einem für das Gericht bestimmten elektronischen Informations- und Kommunikationssystem. Dabei ist der Schuldner genau zu bezeichnen; insbesondere sind seine Anschrift und sein Geschäftszweig anzugeben. § 9 Abs. 2 InsO ermächtigt das Bundesministerium der Justiz, durch Rechtsverordnung mit Zustimmung des Bundesrates die Einzelheiten der Veröffentlichung in einem elektronischen Informations- und Kommunikationssystem zu regeln. Das Bundesministerium der Justiz hat aufgrund dieser Ermächtigung die Verordnung zu öffentlichen Bekanntmachungen in Insolvenzverfahren im Internet erlassen.

Nach § 38 ZVG soll die Terminsbestimmung, die veröffentlicht wird, unter anderem die Bezeichnung des zurzeit der Eintragung des Versteigerungsvermerks eingetragenen Eigentümers enthalten. Artikel 10 des Entwurfs eines Justizmodernisierungsgesetzes sieht eine Änderung des § 38 ZVG dahingehend vor, dass die Wörter „die Bezeichnung des zur Zeit der Eintragung des Versteigerungsvermerks eingetragenen Eigentümers sowie“ gestrichen werden. Tritt dieses Gesetz in Kraft, gehört die Bezeichnung des eingetragenen Eigentümers nicht mehr zu den Angaben, die die zu veröffentlichende Terminsbestimmung enthalten soll.

Zu 19.6 Nutzung des Internets

Das Kultusministerium wird die Anmerkungen des Landesbeauftragten zur Nutzung des Internets in den Schulen zum Anlass nehmen, diese über die Schulaufsichtsverwaltung auf die einschlägigen gesetzlichen Bestimmungen bei der Veröffentlichung eines Internetangebots (Homepage) und bei der schulischen und privaten Nutzung des Internets durch Lehrer und Schüler hinzuweisen. Zudem werden die Schulen gebeten, die Nutzung des Internets sowie die Veröffentlichung eigener Angebote im Internet entsprechend den Empfehlungen des Landesbeauftragten zu gestalten.

Zu 22.1 Gefangene erhalten Behördenpost offen

Das Ministerium der Justiz wird die Feststellungen des Landesbeauftragten zum Anlass nehmen, erneut darauf hinzuweisen, Schreiben an Gefangene in einem geschlossenen Umschlag zur Sammelpost zu geben.

Zu 23.1 Informationsangebote öffentlicher Stellen im Internet

Die Landesregierung hat *www.sachsen-anhalt.de* als das einheitliche Internetportal der Verwaltungen in Sachsen-Anhalt ausgestaltet. Über dieses Internet-Portal können schon jetzt viele im Internet verfügbare Dienstleistungen der unmittelbaren und mittelbaren Landesverwaltung, z. B. durch das Herunterladen von Formularen, erreicht werden. Für den Bürger umständliche Amtsgänge können durch einen Internet-Dialog abgekürzt oder ersetzt werden. Die Internet-Präsenz der öffentlichen Verwaltung und das damit verbundene Service-Angebot für die Nutzer ist – bundesweit – nicht mehr wegzudenken (vgl. hierzu auch Nr. 7.1).

Bei der Einrichtung des Landesportals wurden die einschlägigen Rechtsvorschriften von der Landesregierung beachtet; auch die übrigen Anbieter sind sich ihrer rechtlichen Verpflichtung bewusst. Die vom Landesbeauftragten geforderten Maßnahmen hinsichtlich Anbieterkennzeichnung, datenschutzrechtlicher Unterrichtung und automatischer Datenspeicherung wurden umgesetzt. Um einen umfassenden Konsens zu erreichen, fanden im Vorfeld der Planungen mehrere Besprechungen mit dem Landesbeauftragten statt.

Zu 23.2 Internet und E-Mail am Arbeitsplatz

Zutreffend ist die Feststellung des Landesbeauftragten, dass immer mehr öffentliche Stellen ihren Beschäftigten die Nutzung des Internets zur schnellen Informationsbeschaffung und zum Informationsaustausch per E-Mail zur Verfügung stellen. Dieser Trend wird sich noch verstärken. Der Zugang zum Internet wird in naher Zukunft unverzichtbares Arbeitsmittel sein – nicht zuletzt durch die Entscheidung für eGovernment.

Der Landesbeauftragte hat in seinem Tätigkeitsbericht Kernaussagen der vom Arbeitskreis „Medien“ der Konferenz der Datenschutzbeauftragten erarbeiteten Orientierungshilfe „Datenschutzgerechte Nutzung von E-Mail und anderen Diensten am Arbeitsplatz“ dargestellt. Die Landesregierung sieht diese Ausarbeitung als Beitrag für die datenschutzgerechte Gestaltung des Internetzugangs am Arbeitsplatz an.

Besteht am Arbeitsplatz ein Internetzugang, kann dieser – rein technisch gesehen – auch privat genutzt werden. Ist ausschließlich die dienstliche Nutzung von Internet und E-Mail erlaubt, besteht zwischen dem Dienstherrn/Arbeitgeber und den Beschäftigten kein „Anbieter-Nutzer-Verhältnis“; der Dienstherr/Arbeitgeber ist in diesem Falle nicht Diensteanbieter im Sinne der einschlägigen Vorschriften. Hier richtet sich die Verarbeitung personenbezogener Daten nach § 28 DSG-LSA. Erlaubt der Dienstherr/Arbeitgeber auch nur gelegentlich die private Nutzung des Internets, wird er zum Diensteanbieter. Als solcher har er das Fernmeldegeheimnis nach § 85 TKG zu beachten. Ferner darf die private Nutzung des Internets grundsätzlich nur zu Abrechnungszwecken protokolliert werden.

Je nachdem, ob das Internet am Arbeitsplatz ausschließlich dienstlich oder auch privat genutzt werden darf, kommen unterschiedliche Vorschriften zur Anwendung. Diese könnte der Dienstherr/Arbeitgeber erfüllen, wenn er bei der technischen Ausgestaltung zwischen dienstlicher und privater Nutzung des Internets strikt trennen würde. Dies wäre aber mit erheblichem Aufwand verbunden, der schon deshalb nicht gerechtfertigt ist, weil in der Praxis die private Nutzung nicht abgerechnet wird.

Keine öffentliche Stelle ist verpflichtet, ihren Bediensteten die private Nutzung des Internets zu gestatten. Deshalb kann sie die Erlaubnis der privaten Nutzung an Bedingungen, z. B. an einen Zeitrahmen oder an zugelassene Bereiche, knüpfen. Der Landesbeauftragte weist zu Recht darauf hin, dass Daten über die private Nutzung nicht anders als solche über die dienstliche Nutzung des Internets behandelt werden müssen, wenn der Betroffene hierin ausdrücklich und in Kenntnis aller Umstände eingewilligt hat. Genaueres hierzu ergibt sich aus der Musterdienstanweisung über die Bereitstellung und Nutzung von Internet-Zugängen des Ministeriums des Innern (vgl. Seite 93 des Tätigkeitsberichts).

Diese Musterdienstanweisung wurde mit dem Landesbeauftragten abgestimmt und auch von anderen Ressorts übernommen. Die Musterdienstanweisung und die vorgenannte Orientierungshilfe hat der Landesbeauftragte ins Internet eingestellt.

Zu 26.3 Fahrzeug- und Halterdaten nicht „offenkundig“

Der Bundesgerichtshof hat mit Urteil vom 8. Oktober 2002 entschieden, dass die unbefugte Weitergabe der Anschriften von Fahrzeughaltern durch einen Polizeibeamten den Straftatbestand des § 203 Abs. 2 Satz 2 des Strafgesetzbuches erfüllt und auch nach allgemeinem Datenschutzrecht strafbewehrt ist. Die Tatsache, dass über diese Daten bei Darlegung eines berechtigten Interesses jedermann eine einfache Halterauskunft erteilt wird, macht die Daten noch nicht offenkundig.

Bereits vor dieser Entscheidung hatten der Bundes- und der Landesgesetzgeber die Bußgeld- und Strafvorschriften in §§ 43 und 44 BDSG und in §§ 31 und 31a DSG-LSA grundlegend geändert. Mit Rücksicht auf von der späteren Position des Bundesgerichthofs abweichende Rechtsprechung zum Merkmal der Offenkundigkeit wurde dieser Begriff durch „nicht allgemein zugänglich“ ersetzt. Darüber hinaus wurden bisherige Straftatbestände in § 43 BDSG bzw. § 31 DSG-LSA zu Ordnungswidrigkeitentatbeständen herabgestuft. Nur wenn der Täter in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, verbleibt es bei der – im Strafmaß unveränderten – Strafbewehrung.