

Unterrichtung

Der Präsident des Landtages
von Sachsen-Anhalt

Magdeburg, 27. November 2001

Stellungnahme der Landesregierung zum Fünften Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Sachsen-Anhalt

Sehr geehrte Damen und Herren,

mit Schreiben vom 20. November 2001, hier eingegangen am 21. November 2001, übersandte der Chef der Staatskanzlei des Landes Sachsen-Anhalt gemäß § 22 Abs. 4 Satz 4 des Gesetzes zum Schutz personenbezogener Daten der Bürger vom 12. März 1992 (GVBl. LSA S. 152), zuletzt geändert durch das Gesetz zur Änderung datenschutzrechtlicher Vorschriften vom 21. August 2001 (GVBl. LSA S. 348), die Stellungnahme der Landesregierung zum Fünften Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Sachsen-Anhalt.

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

Wolfgang Schaefer

Stellungnahme der Landesregierung zum Fünften Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Sachsen-Anhalt (Drs. 3/4565 vom 16.05.2001)

Mit seinem Fünften Tätigkeitsbericht gibt der Landesbeauftragte für den Datenschutz (Landesbeauftragter) eine Übersicht über von ihm und seinen Mitarbeitern vom 1. April 1999 bis 31. März 2001 durchgeführte Beratungen und Kontrollen sowie während dieser Zeit aufgetretene Fragen und Probleme beim Umgang mit personenbezogenen Daten.

Der Landesbeauftragte hat auch im letzten Berichtszeitraum nur vereinzelt Defizite beim Datenschutz festgestellt. Er musste nur eine formelle Beanstandung aussprechen. Die wenigen sonst aufgedeckten Mängel wurden von den betroffenen Stellen unverzüglich behoben. Soweit dies noch nicht möglich war, wird an Lösungen gearbeitet. Der Tätigkeitsbericht zeigt: Die Achtung datenschutzrechtlicher Belange ist zu einer Selbstverständlichkeit der Arbeit der öffentlichen Stellen geworden.

Die Landesregierung beschränkt sich in ihrer Stellungnahme nach bewährtem Muster auf einzelne wesentliche Kritikpunkte des Landesbeauftragten. Zudem gibt sie Hinweise auf rechtliche Entwicklungen und den aktuellen Sachstand zu bestimmten Einzelfragen.

Der Landesbeauftragte ist neuerdings mit einem eigenen Angebot im Internet vertreten (vgl. Nr. 2.3.1. – Die Homepage des Landesbeauftragten im Internet). Er hat damit einen Schritt zu mehr Bürgernähe und –information getan. Seine Tätigkeitsberichte und andere grundsätzliche Informationen zum Datenschutz sind so für die interessierte Öffentlichkeit, aber auch für die Verwaltung schnell und einfach recherchierbar. Die Landesregierung sieht darin einen wichtigen Beitrag, den Bürgerinnen und Bürgern deutlich zu machen, wie öffentliche Stellen unter Beachtung des Grundrechts auf informationelle Selbstbestimmung mit ihren personenbezogenen Daten umgehen.

Zu 1. Entwicklung des Datenschutzes

Zu 2.2 Zusammenarbeit mit anderen Aufsichts- und Kontrollinstitutionen

Zu 5.1 Richtlinie der Europäischen Union

Der Landesbeauftragte weist auf die Möglichkeiten der rasant fortschreitenden Informationstechnik hin. Er zeigt aber auch die daraus erwachsenden Risiken für das Recht auf informationelle Selbstbestimmung auf.

Niemand kann und will den technischen Fortschritt auf diesem Gebiet beschränken. Auch die Entwicklung hin zu einer weltweit verknüpften Informationsgesellschaft in Folge der Globalisierung der Wirtschaft ist nicht umkehrbar. Die Landesregierung sieht in diesen Faktoren ein wesentliches Potenzial für die Entwicklung der Wirtschaft im Lande und für die Schaffung zusätzlicher Arbeitsplätze.

Die moderne Informationstechnik macht das Leben und Arbeiten einfacher. Erst durch das Internet ist auch der Einzelne in der Lage, sich jederzeit ohne Rücksicht auf Entfernungen und in Sekundenschnelle abrufbar mit all den Informationen zu versorgen, die er für die Teilnahme an der Gemeinschaft benötigt. Der informierte

und mündige Bürger wird so in die Lage versetzt, seine aus dem Demokratieprinzip folgenden Teilhaberechte an der staatlichen Gemeinschaft wahrzunehmen.

Die Landesregierung stimmt dem Landesbeauftragten zu, dass sich aus dem technischen Fortschritt und der weltweit verknüpften Informationsgesellschaft ständig neue Herausforderungen ergeben, den Belangen des Einzelnen auf Wahrung seines Rechts auf informationelle Selbstbestimmung ausreichend zu entsprechen. Schon im Jahr 1983 hat daher das Bundesverfassungsgericht aus der Menschenwürde und dem Recht auf freie Entfaltung der Persönlichkeit das Recht auf informationelle Selbstbestimmung abgeleitet. Dieses Recht ist in der Landesverfassung als eigenständiges Grundrecht garantiert. Der Sicherung dieses Rechts dient das allgemeine und das spezielle – „bereichsspezifische“ - Datenschutzrecht. Es gewährleistet, dass öffentliche Stellen unter strikter Wahrung des Verhältnismäßigkeitsprinzips nur insoweit personenbezogene Daten erheben, verarbeiten oder nutzen, als dies zur Aufgabenerledigung erforderlich ist. Es garantiert auch, dass Daten nicht zweckentfremdet werden und dass technische oder organisatorische Vorkehrungen zu ihrem Schutz getroffen werden. Trotz der Fülle der vorhandenen Daten und ihrer theoretischen Kombinierbarkeit ist damit der vom Landesbeauftragten aufgezeigten Gefahr eines totalen Überwachungsstaates effektiv entgegengewirkt.

Den „gläsernen Bürger“ - in diesem Fall wäre der Einzelne in seiner gesamten Persönlichkeit und in allen Einzelheiten seines Handelns durch öffentliche oder nicht öffentliche Stellen dokumentiert und wären diese Informationen einer mehr oder weniger breiten Öffentlichkeit zugänglich - wird es nicht geben. Nicht jede technisch realisierbare Forderung aus dem politischen Raum nach umfassender Erhebung, Verarbeitung und Nutzung sensibler personenbezogener Daten wird tatsächlich umgesetzt. So berechtigt die Bestürzung über Sexualmorde an Kindern und das öffentliche Interesse an der unverzüglichen Ermittlung und Bestrafung der Täter ist, wird es doch nicht die Vorraterfassung des genetischen Fingerabdrucks eines jeden Bürgers schon im Säuglingsalter geben - für Fälle möglicher späterer Strafverfolgung oder zu sonstigen noch nicht vorhersehbaren Zwecken. Eine solche Totalerfassung wäre zur Zweckerreichung zwar geeignet, aber nicht verhältnismäßig. Der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit zwingt dazu, bei der Schaffung und Anwendung von Regelungen zum Umgang mit personenbezogenen Daten das öffentliche Interesse hieran und das entgegenstehende Interesse der Betroffenen an Privatheit zu einem gerechten Ausgleich zu bringen. An dieser Abwägung wirken der Bundesbeauftragte für den Datenschutz und die Landesbeauftragten für den Datenschutz mit. Darüber hinaus erfolgt eine Kontrolle durch die zuständigen Gerichte und Verfassungsgerichte.

Es steht außer Frage, dass den neuartigen und aktuellen Bedrohungen durch den internationalen Terrorismus wirksam begegnet werden muss. Dieses ist jedermann durch die schrecklichen Ereignisse des 11. September 2001 bewusst geworden. Der Datenschutz kann und will der Bekämpfung des Terrorismus nicht entgegenstehen. Die Landesregierung ist der Auffassung, dass schon heute Instrumente, wie z. B. die Rasterfahndung, die Vorgaben des Geldwäschegesetzes und der europäischen und internationalen Zusammenarbeit auf dem Gebiet der Gefahrenabwehr und der Strafverfolgung vorhanden sind, um einen Beitrag zur Terrorismusbekämpfung zu leisten.

Diese Befugnisse und ihre Voraussetzungen müssen ständig daraufhin überprüft werden, ob sie den Erfordernissen der jeweils aktuellen Sicherheitslage noch ent-

sprechen. Bei notwendigen Veränderungen wird die Landesregierung darauf achten, dass in die Persönlichkeitssphäre Einzelner nicht stärker als unbedingt erforderlich eingegriffen wird. Andererseits muss gerade bei drohenden Gefahren für allerhöchste Rechtsgüter einer Vielzahl von Menschen die Gewichtigkeit des Rechts auf informationelle Selbstbestimmung des Einzelnen gegenüber den Sicherheitsinteressen der Bürgerinnen und Bürger auf den Prüfstand gestellt werden.

Ein Beispiel für den verantwortungsvollen Umgang mit den Möglichkeiten der modernen Informationstechnik sind die jüngsten Regelungen zur Beobachtung mit optisch-elektronischen Einrichtungen. Der Landesgesetzgeber hat im Jahr 2000 mit dem Zweiten Gesetz zur Änderung des Gesetzes über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt strenge Regelungen zur Zulässigkeit der Erhebung, Verarbeitung und Nutzung von Daten mittels Videobeobachtung für Zwecke der Gefahrenabwehr getroffen. In diesem Jahr folgten vergleichbar strenge Regelungen zur Zulässigkeit der optisch-elektronischen Beobachtung zu anderen Zwecken als der Gefahrenabwehr im Gesetz zur Änderung datenschutzrechtlicher Vorschriften.

Mit dem Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze sowie auf Landesebene mit dem Gesetz zur Änderung datenschutzrechtlicher Vorschriften sind in diesem Jahr die Vorgaben der EG-Datenschutzrichtlinie umgesetzt worden. Weil der Bund und nahezu alle Länder nunmehr der Pflicht zur Umsetzung nachgekommen sind, hat die Kommission die Klage gegen die Bundesregierung wegen Nichtumsetzung der EG-Datenschutzrichtlinie im August 2001 zurückgenommen. Damit ist das Vertragsverletzungsverfahren beendet.

Das nunmehr bestehende gleichwertige Datenschutzniveau gewährleistet den im Binnenverkehr unverzichtbaren freien und ungehinderten Datenverkehr innerhalb der Europäischen Union. Durch die Stärkung der Rechte der Bürgerinnen und Bürger sind ihre Möglichkeiten, auf den Umgang mit ihren Daten durch Dritte Einfluss zu nehmen, weiter gefestigt worden.

Das war aber nur der erste Schritt. Die Fortentwicklung des Datenschutzrechts ist noch nicht abgeschlossen. So gibt es auf Bundesebene eine Initiative zur weiteren Modernisierung des Datenschutzrechtes. Dabei werden noch intensiver als bisher Instrumente zum Schutz personenbezogener Daten durch den Betroffenen selbst geschaffen werden müssen, z. B. durch die selbstbestimmte Nutzung von technischen und organisatorischen Schutzinstrumenten oder die verbesserte Möglichkeit, Dienste anonym oder pseudonym in Anspruch zu nehmen. Die Landesregierung unterstützt diese Initiative. Sie wird Wege aufzeigen, das künftige Datenschutzrecht an die Gegebenheiten der sich grundlegend verändernden Informationslandschaft anzupassen. Ziel ist nicht, die fortschreitende Entwicklung der Technik zu verhindern, sondern für ihre Anwendung einen Rahmen aufzuzeigen, der den Interessen aller Beteiligten gerecht wird. Es wird verstärkt darum gehen, Möglichkeiten der modernen Informationstechnik selbst auszuschöpfen, um dem aus ihr erwachsenden Gefahrenpotenzial für die Bürgerinnen und Bürger zu begegnen.

Um den Interessen der Bürger gerecht zu werden, steht die Landesregierung bei der Vorbereitung neuer Regelungen mit datenschutzrechtlichem Bezug in ständigem Dialog mit dem Landesbeauftragten. Auch im Berichtszeitraum war die Zusammenarbeit mit dem Landesbeauftragten kooperativ und konstruktiv. Sie hat dazu beige-

tragen, dass stets Lösungen gefunden werden konnten, die den Belangen des Datenschutzes in besonderer Weise entsprechen.

Zu 3.1 Prüfung von Ausländerbehörden

Der Landesbeauftragte empfiehlt, eingezogene Pässe nicht zur Ausländerakte zu nehmen, sondern in verschlossenen Safes aufzubewahren. Bereits mit Erlass vom 05.11.1992 (MBI. LSA S. 1951) hat das Ministerium des Innern Regelungen über die gesicherte Aufbewahrung von Vordrucken für Urkunden, von Pässen, Dienstsiegeln und sonstigen Dokumenten getroffen. Die Regierungspräsidien wurden zuletzt im Juni 2001 angewiesen, die Ausländerbehörden auf die Beachtung der Regelung hinzuweisen.

Zu 3.2 Fehlerhafte Ausschreibungen im Schengener Informationssystem

Nachdem das Ministerium des Innern Kenntnis von fehlerhaften Ausschreibungen von Ausländern im Schengener Informationssystem (SIS) erlangt hatte, wurden die Regierungspräsidien im Februar 2000 in einem ausführlichen Erlass auf die Rechtslage hingewiesen. Soweit durch Ausländerbehörden unzulässige Ausschreibungen erfolgt waren, wurden diese gelöscht. Da der Landesbeauftragte noch nach Herausgabe des Erlasses Fehler bei Ausschreibungen festgestellt hat, wurden die Regierungspräsidien im Juni 2001 erneut angewiesen, bei den Ausländerbehörden für die Beachtung der einschlägigen Vorschriften für Ausschreibungen im Inpol-System, im Ausländerzentralregister und im SIS zu sorgen.

Zu 6.1 Automatisierte Datenverarbeitung in der Landesverwaltung (Seite 17, Abs. 2 und 3)

Immer mehr Menschen wünschen, ihre Behördenangelegenheiten über das Internet zu erledigen. Sie wollen staatliche Dienstleistungen schnell und unkompliziert in Anspruch nehmen. Derzeit konzentrieren sich die Internetangebote öffentlicher Stellen auf das Angebot von Informationen. Darüber hinaus wird der e-mail-Kontakt rege genutzt. Echte Transaktionen, „e-Government“ im eigentlichen Sinne, sind noch die Ausnahme. Erst dann, wenn die Verwaltungsabläufe den veränderten Bedingungen der Technik angepasst sind und die rechtlichen Rahmenbedingungen vorliegen, wird auch im öffentlichen Bereich elektronische Dienstleistung zur Alltäglichkeit werden. Die von den Datenschutzbeauftragten des Bundes und der Länder vorgelegte Broschüre „Vom Bürgerbüro zum Internet – Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung“ gibt Hinweise, wie bei der Realisierung der einzelnen (Pilot-)Projekte den Anforderungen des Datenschutzes genügt werden kann. Nur Dienste, deren Sicherheit die Bürgerinnen und Bürger vertrauen, werden letztlich von ihnen auch angenommen.

Der Landkreistag Sachsen-Anhalt weist darauf hin, dass sich neben dem Land, den Städten und den Gemeinden auch die Landkreise mit dem Thema e-Government befassen. Über die Pilotprojekte „Bürgernahe Verwaltung im Jerichower Land“ und „Zukunftsregion Wernigerode“ werden unter Federführung dieser Landkreise zukunftsweisende Lösungen für alle Landkreise erarbeitet.

Zu 6.2 Das IT-Leitbild der Landesregierung

Das IT-Leitbild widmet sich den Potenzialen des Einsatzes der Informationstechnik aus Sicht der Landesregierung. Das IT-Leitbild hat einen hohen Abstraktionsgrad. Es befasst sich nicht mit einzelnen Ausprägungen des IT-Einsatzes. Daher wird nur allgemein bestimmt, dass die Verfügbarkeit, Vertraulichkeit und Integrität der Informationen zu gewährleisten sind. Insoweit ist eine Differenzierung nach personenbezogenen und nicht personenbezogenen Daten nicht vorgenommen worden.

Dagegen müssen sich IT-Konzepte oder -Maßnahmen, die das IT-Leitbild konkretisieren oder ausfüllen, am Schutzbedarf der einzelnen Datenbestände bzw. Informationen orientieren. Soweit personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ist den Anforderungen des Datenschutzes zu genügen.

Im Rahmen des Projektes „IT-Organisationsstruktur“ sollen eine Landesleitstelle IT und ein Landesinformationszentrum eingerichtet werden. Eine der ersten Aufgaben dieser Einrichtungen wird die Neufassung der IT-Grundsätze sein.

Zu 6.3 Fehlendes Sicherheitskonzept für das Landesnetz (ITN-LSA)

Das Ministerium des Innern lässt das Sicherheitskonzept für das ITN-LSA und seine Außenübergänge durch eine externe Stelle erstellen, da weder bei ihm selbst noch beim Landesrechenzentrum ausreichende Ressourcen vorhanden sind. Mit diesem Sicherheitskonzept wird ein Beitrag zur Verbesserung des Datenschutzes und der Datensicherheit geleistet. Auch wird dem Ziel Rechnung getragen, datenschutzfreundliche Produkte auf dem Markt sowie deren Anschaffung und Nutzung durch öffentliche Stellen zu fördern. Nach Abschluss der Arbeiten - im Laufe dieses Jahres - wird der Landesbeauftragte über das Ergebnis unterrichtet. Eine ständige Fortschreibung des ITN-Sicherheitskonzeptes ist vorgesehen.

Auch wenn bisher ein nachlesbares Gesamtsicherheitskonzept nicht vorliegt, besteht gleichwohl für das Landesnetz ein hoher Sicherheitsstandard. Dies ergibt sich schon daraus, dass das Technische Polizeiamt (TPA) Netzbetreiber ist. Die Grundsicherheit dieses Netzes ist insbesondere deshalb als hoch einzustufen, weil es den polizeilichen Sicherheitsanforderungen entspricht.

Die Grundsicherheit des Netzes ist auch deshalb gegeben, weil es sich um ein geschlossenes Netzwerk mit ausschließlich gesicherten und durch Firewall kontrollierten Übergängen in Fremdnetze handelt. Der Übergang ITN-LSA - TESTA wird im Sicherheitskonzept ebenfalls betrachtet (vgl. Nr. 6.2 - Das IT-Leitbild der Landesregierung).

Die Auffassung des Landesbeauftragten, dass in dem nur der Landesverwaltung zugänglichen Intranet zu viele sicherheitsrelevante Informationen bereitgestellt werden, wird nicht geteilt. Im Rahmen des Sicherheitskonzeptes wird aber geprüft, ob der Zugriff auf das Intranet gegebenenfalls über gesonderte Zugangsrechte geregelt werden kann.

Der Forderung des Landesbeauftragten nach dem Erlass von Vorschriften zur Grundsicherheit, zur Nutzung von Internet und E-Mail wird nach Vorlage des Sicherheitskonzepts entsprochen. Mit der geplanten Errichtung der neuen IT-Organisationsstruktur kann auch der Forderung nach einem ständigen Gremium für die IT-Sicherheit nachgekommen werden.

Bei Errichtung der Landesleitstelle IT könnte auch dadurch der Forderung des Landesbeauftragten nach einem ständigen Gremium für die IT-Sicherheit entsprochen werden.

Zu 6.4 Projekt TESTA Deutschland

Das Projekt „transeuropean services for telematics between public administrations“ – TESTA Europa - ist ein europäisches Projekt, um innereuropäische Verwaltungen zu vernetzen. Es handelt sich um ein geschlossenes Verwaltungsnetz. Die Technologie TESTA Europa wurde für TESTA Deutschland übernommen. TESTA Deutschland bedeutet einen ersten Schritt zur Schaffung der technischen Voraussetzungen für eine Vernetzung der Verwaltungen in Deutschland und später in Europa. Ob und in welchem Umfang Daten, insbesondere personenbezogene Daten, in diesem Netz übermittelt oder weitergegeben werden dürfen, bestimmt sich nach materiellem Recht. Sicherheitsmerkmal in TESTA Deutschland ist die Leitungsverchlüsselung. Der Übergang zu TESTA Deutschland ist mit der Network Address Translation und Paketfiltern abgesichert. Auch wenn eine offizielle und ausdrückliche Unterrichtung über den bisher erreichten Sicherheitsstandard des Anschlusses des Landesverwaltungsnetzes an TESTA Deutschland noch nicht stattgefunden hat, ist der Landesbeauftragte über den Sicherheitsstandard von TESTA Deutschland stets informiert worden, insbesondere durch die Mitarbeit im IMA-IT. Darüber hinaus wird eine umfassende Unterrichtung über alle größeren IT-Vorhaben in der Landesverwaltung – noch intensiver als bisher – für die Zukunft ausdrücklich zugesagt.

Zu 8. Forschung

Der Landesbeauftragte bemerkt zu Recht, dass auch bei Forschungsvorhaben der Grundsatz der Datensparsamkeit gilt. Dieses Prinzip lag dem Datenschutzrecht von Anfang an zu Grunde; es ist jetzt aber in § 1 Abs. 2 DSGVO ausdrücklich genannt. Danach dürfen personenbezogene Daten nur erhoben werden, soweit sie zur Erreichung des Forschungszwecks erforderlich sind. Reicht etwa für die Zuordnung zu einer Gruppe die Angabe des Lebensalters aus, ist auf die Erhebung des vollständigen Geburtsdatums zu verzichten.

Soweit der Landesbeauftragte die Freiwilligkeit von Angaben und die Einwilligung zur weiteren Verarbeitung und Nutzung der Daten gleichsetzt, mag dies im Bereich der Forschung regelmäßig zutreffen. Ansonsten gilt: Es handelt sich um unterschiedliche Anforderungen, die das DSGVO in § 4 Abs. 1 und § 9 Abs. 2 getrennt voneinander regelt. Die nachfolgende Verarbeitung und Nutzung freiwilliger Angaben, z. B. für die amtliche Statistik, kann sich durchaus auf einen anderen Erlaubnistatbestand als die Einwilligung der betroffenen Person stützen.

Zu 8.2 Begleitforschung zur Umsetzung der Kindschaftsrechtsreform

Das Ministerium der Justiz hat – wie andere Landesjustizverwaltungen - seinen Geschäftsbereich gebeten, das Forschungsvorhaben zu unterstützen. Dem Landesbeauftragten für den Datenschutz ist zuzustimmen, dass es in dieser Forschungsangelegenheit zu einer verzögerten Beteiligung seiner Behörde gekommen ist. Zu der im Bericht beanstandeten Reaktionszeit des Ministeriums haben allerdings auch Missverständnisse auf Seiten des Forschungsinstituts beigetragen. Den Fall hat das Ministerium zum Anlass genommen, auf die rechtzeitige Beteiligung des Landesbeauftragten für den Datenschutz hinzuwirken.

Zu 10.1 Industrie- und Handelskammern

Gemäß § 9 Abs. 6 des Gesetzes zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern (IHK-G) in Verbindung mit § 11 DSGVO dürfen die Kammern die Daten ihrer Kammerzugehörigen an andere öffentliche Stellen - überwiegend sind das die Industrie- und Handelskammern in den anderen Bundesländern - zur Erfüllung ihrer Aufgaben übermitteln. Dabei bedienen sich die Kammern Sach-Anhalts eines automatisierten Abrufverfahrens, das von der Gemeinschaftseinrichtung der Kammern, der IHK-GfI, vorgehalten wird.

Unter Einbindung des Deutschen Industrie- und Handelstages e. V. (DIHT) wurde Anfang des Jahres 2000 ein Arbeitskreis eingesetzt, der die Notwendigkeit einer bundeseinheitlichen gesetzlichen Grundlage für dieses Abrufverfahren prüfen sollte. Das Ergebnis dieser Prüfung wurde dem Bundesministerium für Wirtschaft und Technologie Ende 2000 zugeleitet. Der Landesbeauftragte wurde zeitgleich unterrichtet.

Aus Sicht des Landes Sachsen-Anhalt ist eine bundeseinheitliche Rechtsgrundlage nicht zwingend erforderlich, weil sich die Befugnis zur Teilnahme an dem Verfahren unmittelbar aus dem geänderten § 7 Abs. 1 DSGVO ergibt. Die bisherige Anforderung einer besonderen materiell-rechtlichen Regelung ist mit dem In-Kraft-Treten des Gesetzes zur Änderung datenschutzrechtlicher Vorschriften entfallen.

Die Arbeitsgemeinschaft Kammerleitstelle für Bemessungsgrundlagen e. V. (AKB e. V.) wird als gemeinsame Leitstelle der Industrie- und Handelskammern bei der Ermittlung der Bemessungsgrundlagen für die Beitragserhebung tätig. Mit der Ausführung dieser Aufgabe ist die AKG mbH betraut. Sie betreibt Auftragsdatenverarbeitung. Hierzu hat der Landesbeauftragte für den Datenschutz Nordrhein-Westfalen unter Beteiligung des DIHT mit der AKB e. V. Musterverträge für die Vertragsverhältnisse zwischen den IHK/HWK und AKB e. V. bzw. zwischen AKB e. V. und AKG mbH erarbeitet.

Entsprechende Verträge zwischen den Kammern Sachsen-Anhalts und dem AKB e. V. sind abgeschlossen worden. Damit ist die Angelegenheit, wie der Landesbeauftragte in seinem Schreiben vom 16.07.2001 mitgeteilt hat, erledigt.

Zu 10.6 Korruptionsregister

Nach wie vor hält das Ministerium des Innern als in der Sache zuständiges Ressort an seiner Auffassung fest, dass es zur Einrichtung eines bundesweiten Korruptionsregisters einer bundesrechtlichen Regelung bedarf. Die Bundesregierung erarbeitet gegenwärtig einen Gesetzentwurf, mit dem u. a. auch die Rechtsgrundlage für ein bundesweites Korruptionsregister geschaffen werden soll. Sobald ein diskussionsfähiger Gesetzentwurf vorliegt, werden die Länder – noch vor dem Bundesratsverfahren - beteiligt werden.

Es ist weiterhin nicht beabsichtigt, in Sachsen-Anhalt vorab ein (Landes-) Korruptionsregister einzurichten. Mit der Verwaltungsvorschrift zur Vermeidung und Bekämpfung der Korruption sind 1998 Regelungen zum Umgang mit unzuverlässigen Bewerbern bei der Vergabe öffentlicher Aufträge getroffen worden. Bewerber und Unternehmen sind im Einzelfall dann von der Teilnahme am Wettbewerb auszuschließen, wenn ihnen eine schwere Verfehlung nachgewiesen wurde und dadurch ihre Zuverlässigkeit für den zur Vergabe anstehenden Auftrag in Frage gestellt ist.

Zu 11.3 E-Mail/

11.3.1 Generelle Sicherheitsprobleme

Der Austausch von E-Mail zwischen den Landesbehörden erfolgt grundsätzlich nur über das Intranet des Landes (ITN-LSA), mit öffentlichen Stellen des Bundes und anderen Ländern vorrangig über TESTA Deutschland. Damit kann der Großteil des E-Mail-Verkehrs - anders als im Internet - nicht ohne weiteres weltweit zur Kenntnis genommen werden. Die Sicherheit der E-Mails erhöht sich bei der Einführung digitaler Signaturen. Es fällt in die Eigenverantwortung jeder übermittelnden Stelle und jedes einzelnen Bediensteten, dafür zu sorgen, dass beim Datentransport Vertraulichkeit gewahrt ist. Dies schließt den ungesicherten Transport sensibler Daten per E-Mail aus.

MI hat für seine Behörde den Entwurf einer Dienstanweisung zur Nutzung des Internet, des Intranet, der Hausdienste und der E-Mail erarbeitet. Ob hieraus eine Musterdienstanweisung für die Landesverwaltung abgeleitet werden kann, wird geprüft. Darüber hinaus wurde eine Musterdienstanweisung zur privaten und dienstlichen Nutzung von Internet und E-Mail zwischen den Ressorts abgestimmt und dem Landesbeauftragten zur Stellungnahme zugeleitet. Diese Musterdienstanweisung soll in Kürze in Kraft gesetzt werden.

Zu 11.4 PC-Diebstähle, Jahr-2000-Problem und die unangenehmen Folgen

Nach dem vom Landesbeauftragten geschilderten Einbruchdiebstahl im Jahr 1996 zog das betroffene Dezernat des Regierungspräsidiums Magdeburg in ein vermeintlich sichereres Gebäude in der gleichen Liegenschaft um. Allerdings liegt dieses Gebäude abseits der Straße und kann nur unzureichend bewacht werden. Nach einem erneuten Einbruchversuch im Januar 1998 wurde in Zusammenarbeit mit der kriminalpolizeilichen Beratungsstelle Magdeburg ein Bewegungsmelder installiert, da eine

regelmäßige Überwachung durch Polizeistreifen auf Dauer nicht gewährleistet werden konnte.

Bei einem weiteren Einbruchsdiebstahl im Februar 2000 in dieselbe Liegenschaft wurde erneut PC-Technik gestohlen. Dabei gelangten auch personenbezogene Daten lesbar in den Besitz Unbefugter. Der Landesbeauftragte hat dies beanstandet, weil keine ausreichenden und angemessenen technischen und organisatorischen Maßnahmen nach § 6 DSGVO getroffen worden waren.

Zum Zeitpunkt des letzten Diebstahls arbeitete das betroffene Dezernat mit Arbeitsplatzcomputern, die nur bedingt "Jahr-2000-fähig" waren. Zusätzlich traten Probleme mit der eingesetzten Datenschutzsoftware auf, die deshalb deinstalliert wurde. Ein beabsichtigter Austausch der Altgeräte und die Neuinstallation geeigneter Datenschutzsoftware wurde zunächst wegen des für Anfang des Jahres vorgesehenen Umzugs des Dezernats in das Hauptgebäude zurückgestellt. Danach konnten beide Maßnahmen wegen der am 01.10.1999 kurzfristig verhängten Haushaltssperre nicht mehr realisiert werden. Die Dringlichkeit der Beschaffung, die trotz der Haushaltssperre hätte realisiert werden müssen, ist nicht erkannt worden.

Die Beanstandung ist auf Grund der vom Regierungspräsidium Magdeburg veranlassten technischen und organisatorischen Sofortmaßnahmen ausgeräumt. Die jetzt eingesetzte Hard- und Software gewährleistet die geforderte Sicherheit. Außerdem wird die bisher in der Außenstelle untergebrachte Organisationseinheit nach Abschluss von Renovierungsarbeiten in ausreichend gesicherte Räume des Hauptgebäudes des Regierungspräsidiums Magdeburg umziehen. Das Risiko eines Einbruchsdiebstahls ist dann deutlich geringer.

Auf Grund der Vorfälle ist durch die IT-Stelle des Regierungspräsidiums eine nochmalige Belehrung und Einweisung der Mitarbeiterinnen und Mitarbeiter des betroffenen Dezernats hinsichtlich der Einhaltung der Bestimmungen des DSGVO vorgenommen worden. Zur Sensibilisierung aller Beschäftigten in Fragen des Datenschutzes hat das Regierungspräsidium Magdeburg zudem einen entsprechenden Workshop durchgeführt.

Einen wichtigen Beitrag zur Verbesserung der Datensicherheit in den Behörden hat der Gesetzgeber kürzlich mit dem Gesetz zur Änderung der datenschutzrechtlichen Vorschriften getroffen. Danach haben künftig alle öffentlichen Stellen einen Beauftragten für den Datenschutz einzusetzen. Diese Beauftragten werden Garant dafür sein, dass die verantwortlichen Stellen auch intern zur Beachtung des Datenschutzes angehalten werden.

Zu 14.4 Personaldaten in Verzeichnisdiensten

Werden über Angehörige des öffentlichen Dienstes Angaben zur dienstlichen Erreichbarkeit, zur Funktion oder zum jeweiligen Aufgabenbereich in Verzeichnisdienste eingestellt, handelt es sich dabei nicht um Personalaktendaten. Daher kommen die für Personalaktendaten einschlägigen Vorschriften der §§ 90 bis 90g BGG LSA nicht zur Anwendung. Zu beachten ist aber § 90 Abs. 4 Satz 1 BGG LSA, der nach § 28 Abs. 1 DSGVO auch für Tarifpersonal gilt. Danach darf der Dienstherr bzw. Arbeitgeber über Bedienstete personenbezogene Daten nur erheben, soweit

dies zur Begründung, Durchführung, Beendigung oder Abwicklung des Dienst- bzw. Arbeitsverhältnisses oder zur Durchführung organisatorischer, personeller oder sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist.

Die Zulässigkeit der Verarbeitung und Nutzung von Personaldaten in Verzeichnisdiensten bestimmt sich nach §§ 10 ff DSGVO. Aus § 10 Abs. 1 DSGVO folgt die Bindung an den Erhebungszweck. Danach dürfen entsprechende Verzeichnisse in behördeninterne Netze, in das Intranet des Landes und im bundesweiten TESTA Deutschland nur eingestellt werden, wenn der Dienstverkehr es erfordert. Die Eröffnung des Zugriffs auf solche Verzeichnisse innerhalb der jeweiligen verantwortlichen Stelle und für über- und nachgeordnete Behörden ist danach stets zulässig. Darüber hinaus lässt sich die Öffnung des Zugriffs für öffentliche Stellen insoweit rechtfertigen, als eine Notwendigkeit zur Zusammenarbeit besteht. In diesem Umfang sind auch Abrufverfahren zulässig.

Beizupflichten ist dem Landesbeauftragten, dass Verzeichnisdienste mit personenbezogenen Angaben zu Bediensteten grundsätzlich nur mit deren Einwilligung ins Internet eingestellt werden dürfen. Die Einwilligung ist nur dann entbehrlich, wenn es sich um allgemein zugängliche Daten über Personen in herausgehobenen Positionen handelt. Dies können Angaben über Behördenleiter (in Ausnahmefällen über deren Stellvertreter) oder über solche Personen sein, die als Ansprechpartner für die Öffentlichkeit benannt sind (z. B. Pressesprecher), nicht aber Angaben über jeden Leiter von Organisationseinheiten.

Dementsprechend sind in das bundesweite, aber nur öffentlichen Stellen zugängliche Netz „TESTA Deutschland“ ausschließlich Daten über Behörden eingestellt, nicht aber über einzelne Mitarbeiter.

Sofern in Zukunft auch Daten zur dienstlichen Erreichbarkeit einzelner Bediensteter in TESTA Deutschland eingestellt werden sollten, wird dies grundsätzlich nicht ohne Einwilligung der Betroffenen erfolgen. Der Landesbeauftragte wird über entsprechende Planungen rechtzeitig in Kenntnis gesetzt.

Sonderregelungen des Signaturrechts, die z. B. die Prüfung elektronischer Signaturen regeln, bleiben unberührt. Sie kommen zur Anwendung, sobald elektronische Signaturen in der Verwaltung eingesetzt werden. Über konkrete Vorhaben wird der Landesbeauftragte frühzeitig informiert.

Zu 15.4 INPOL-Neukonzeption

Die Ständige Konferenz der Innenminister der Länder (IMK) hat auf ihrer Sitzung im November 2000 das vom Bundesministerium des Innern (BMI) unterbreitete Angebot, im Rahmen der von INPOL - neu vorgegebenen Funktionen eine dauerhafte Auftragsdatenverarbeitung (von polizeilichen Landesdaten) beim Bundeskriminalamt (BKA) vertraglich abschließen zu können, zur Kenntnis genommen. Ebenfalls hat sie die im Oktober 2000 gefasste Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Auftragsdatenverarbeitung durch das BKA zur Kenntnis genommen. Danach halten die Datenschutzbeauftragten eine dauerhafte Speicherung von Landesdaten beim BKA für unzulässig. Diese Ansicht vertritt

die IMK nicht. Vielmehr teilt sie die Auffassung des BMI, wonach eine dauerhafte Auftragsdatenverarbeitung von Landesdaten beim BKA mit § 2 Abs. 5 BKA-Gesetz (BKAG) vereinbar ist.

Gemäß § 2 Abs. 5 BKAG kann das BKA die Länder auf Ersuchen bei deren Datenverarbeitung unterstützen. Die Verarbeitung und Nutzung der Daten erfolgt nach den Weisungen der Länder und gemäß den jeweiligen landesspezifischen Vorschriften über die Auftragsdatenverarbeitung. Die Verarbeitung der polizeilichen Landesdaten bleibt dabei eine originär den Ländern obliegende Aufgabe. Die in § 2 Abs. 1 BKAG statuierten Schranken, wonach das BKA als Zentralstelle grundsätzlich nur bei Straftaten mit länderübergreifender, internationaler oder sonst erheblicher Bedeutung tätig wird, greifen hier gerade nicht. In diesem Fall werden die Länder lediglich „bei deren Datenverarbeitung“ unterstützt; das Verfahren liegt ausschließlich in ihrer Kompetenz.

Die erforderliche Trennung der Datenbestände von Bund und Ländern beim BKA ist technisch möglich. Infolgedessen kann bei entsprechender Ausgestaltung der zwischen dem jeweiligen Land und dem BKA abzuschließenden Vereinbarung die vom Landesbeauftragten befürchtete „Machtverschiebung zu Lasten der Länder und ihrer Bürger“ verhindert werden.

Das Ministerium des Innern hat sich deshalb und darüber hinaus aus Kostengründen grundsätzlich für die Auftragsdatenverarbeitung beim BKA entschieden.

Zu 16. Rechtspflege

Der Tätigkeitsbericht des Landesbeauftragten belegt den hohen Stellenwert, den der Schutz des Rechts der Bürgerinnen und Bürger auf informationelle Selbstbestimmung im Land Sachsen-Anhalt auch für den Bereich der Justiz einnimmt. Das gilt für die Gerichte selbstverständlich auch dann, wenn sie nicht in Verwaltungsangelegenheiten tätig werden und insoweit nicht der Prüfkompetenz des Landesbeauftragten unterliegen.

Zu 16.2.2 Parlamentarische Kontrolle von Lauschangriffen auf Landesebene

Der Landesbeauftragte für den Datenschutz vertritt die Ansicht, dass es im Land Sachsen-Anhalt eine der Regelung des Art. 13 Abs. 6 GG gleichwertige parlamentarische Kontrolle von Lauschangriffen nicht gibt. Er bemängelt dabei einerseits, dass eine gesetzliche Regelung dazu nicht existiert, und fordert andererseits, dass der Landtag die Möglichkeit haben muss, die anonymisierten Berichte der Landesregierung öffentlich zu erörtern.

Dem Landesbeauftragten für den Datenschutz ist zuzustimmen, dass in Sachsen-Anhalt eine gesetzliche Grundlage für die parlamentarische Kontrolle nicht existiert.

Auf Grund einer Einigung zwischen der Landesregierung und dem Ältestenrat des Landtages erstattet die Landesregierung den Fachausschüssen ihren Bericht in nicht öffentlicher Sitzung. Dieses Verfahren soll einem Antrag der Fraktionen der SPD, der

CDU und der PDS zufolge in der Geschäftsordnung des Landtages verankert werden (vgl. LT-Drs. 3/4690).

Nach Art. 13 Abs. 6 GG übt ein vom Bundestag gewähltes Gremium auf der Grundlage eines von der Bundesregierung an den Bundestag jährlich zu erstattenden Berichts die parlamentarische Kontrolle aus. Die Länder haben danach lediglich eine gleichwertige parlamentarische Kontrolle zu gewährleisten. Eine öffentliche Erörterung der Berichte sieht Art. 13 Abs. 6 GG nicht vor. Die Regelung des Verfahrens der Kontrolle obliegt dem jeweiligen Landesparlament. Nach Auffassung der Landesregierung entspricht das derzeitige Verfahren der parlamentarischen Kontrolle in Sachsen-Anhalt den Anforderungen von Art. 13 Abs. 6 GG.

Zu 16.4 DNA-Identitätsfeststellung

Hinsichtlich der Aussage des Landesbeauftragten, in Fällen der Anordnung molekulargenetischer Untersuchungen in laufenden Ermittlungsverfahren erfolge häufig die Prüfung des § 81g StPO durch die Polizei und nicht durch den gesetzlich vorgesehenen Richter, ist festzustellen, dass in Sachsen-Anhalt molekulargenetische Untersuchungen ausnahmslos auf Grund richterlicher Anordnungen durchgeführt werden und diese stets richterlich begründet sind.

Zu 16.5 Der gläserne Internetbürger?

Die IMK hat am 24. November 2000 folgenden Beschluss gefasst:

- „1. Die Innenminister und –senatoren der Länder betrachten die konsequente Bekämpfung der Kriminalität in den Datennetzen als eine zentrale Herausforderung.
2. Die Innenministerkonferenz bittet den Bundesminister des Innern, sich bei der Bundesregierung dafür einzusetzen, dass den Providern und Betreibern von Servern eine Protokollierungspflicht hinsichtlich der IP-Adresse und des Nutzungszeitraums sowie eine angemessene Aufbewahrungszeit der Daten vorgeschrieben wird.“

Aus dem Wortlaut des Beschlusses ergibt sich, dass sich die IMK entgegen der Darstellung des Landesbeauftragten weder für eine Datenspeicherung noch für eine „Beobachtung“ der Internetsurfer durch staatliche Stellen ausgesprochen hat. An der bisherigen Rechtslage, nach der staatliche Stellen auf gespeicherte Daten nur im Einzelfall und unter bestimmten Voraussetzungen auf Grund richterlichen Beschlusses oder – bei Gefahr im Verzuge – einer staatsanwaltschaftlichen Anordnung zugreifen können, soll nichts geändert werden.

Zu 19.1 Hochbaustatistik

Die Landesregierung wird in Kürze die Erhebung von Angaben für die Hochbaustatistik durch Verordnung regeln. Dabei wird der Tatsache Rechnung getragen, dass für bestimmte Angaben der Bauherr und die Bauaufsichtsbehörde nebeneinander

auskunftspflichtig sind. In Abstimmung mit dem Landesbeauftragten wird geregelt, dass der Bauherr seine Angaben – wie bisher – grundsätzlich über die Bauaufsichtsbehörde dem Statistischen Landesamt zuleitet. Dies entspricht den Kernprinzipien des allgemeinen Datenschutzrechts und des Statistikrechts in besonderem Maße. Der Grundsatz der vorrangigen Erhebung beim Betroffenen wird beachtet. Das Statistikgeheimnis wird in keinem Fall tangiert. Die Bauaufsichtsbehörde kennt die Daten bereits aus dem Verwaltungsverfahren. Statistikdaten gelangen nicht in den Verwaltungsvollzug.

Zu 19.2 Bevölkerungstatistik

Die bei der Durchführung der Erhebung der Geburten, Sterbefälle und Eheschließungen von den Standesämtern verwendeten Zählkarten sind entsprechend dem Vorschlag des Landesbeauftragten überarbeitet worden. Hilfsmerkmale sind gesondert gekennzeichnet und mit Erläuterungen zu deren Verwendung und Löschung versehen.