Landtag von Sachsen-Anhalt

Drucksache 6/997
03.04.2012

Unterrichtung

Chef der Staatskanzlei Magdeburg, 28. März 2012

Stellungnahme der Landesregierung zum Zehnten Tätigkeitsbericht des Landesbeauftragten für den Datenschutz für die Zeit vom 1. April 2009 bis 31. März 2011

Sehr geehrter Herr Präsident,

als Anlage übersende ich gemäß § 22 Abs. 4a Satz 2 des Gesetzes zum Schutz personenbezogener Daten der Bürger (DSG-LSA) die

> Stellungnahme der Landesregierung zum Zehnten Tätigkeitsbericht des Landesbeauftragten für den Datenschutz für die Zeit vom 1. April 2009 bis 31. März 2011 (Drs. 6/398)

mit der Bitte um Kenntnisnahme.

Mit freundlichen Grüßen
In Vertretung

Olmes

Verfügung des Präsidenten des Landtages von Sachsen-Anhalt:

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

Gemäß § 40 Abs. 1 GO.LT überweise ich die Unterrichtung an die Ausschüsse für Inneres (federführend), für Recht, Verfassung und Gleichstellung, für Bundes- und Europaangelegenheiten sowie Medien und für Bildung und Kultur.

Hinweis: *Die Drucksache steht vollständig digital im Internet/Intranet zur Verfügung. Die Anlage ist in Word als Objekt beigefügt und öffnet durch Doppelklick den Acrobat Reader.*
Bei Bedarf kann Einsichtnahme in der Bibliothek des Landtages von Sachsen-Anhalt erfolgen oder die gedruckte Form abgefordert werden.

(Ausgegeben am 03.04.2012)

Stellungnahme der Landesregierung zum
X. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz für die Zeit vom 1. April 2009 bis 31. März 2011
(Drs. 6/398)

Gliederung

Vorbemerkung

Die Landesregierung nimmt zum X. Tätigkeitsbericht des LfD (zu Abkürzungen vgl. das Abkürzungsverzeichnis, S. 41 ff) gemäß § 22 Abs. 4a Satz 2 des Gesetzes zum Schutz personenbezogener Daten der Bürger (Datenschutzgesetz Sachsen-Anhalt - DSG LSA) Stellung. Eine Befassung mit den Ausführungen des LfD erfolgt insbesondere zu solchen Themen, bei denen auf aktuelle Entwicklungen im Recht oder in der Praxis einzugehen ist, bei denen eine Positionsbestimmung der Landesregierung noch ausstand oder bei denen zwischen dem LfD und der Landesregierung Auffassungsunterschiede bestehen. Verzichtet wird generell auf Ausführungen zu Punkten, die der LfD abschließend dargestellt hat und bei denen erkennbar kein Anlass für ergänzende Äußerungen oder weiteres Handeln der Landesregierung oder der betroffenen öffentlichen Stellen besteht. Aus Achtung vor den Parlamenten unterbleibt grundsätzlich auch eine Auseinandersetzung mit kritischen Aussagen des LfD zu verabschiedeten Bundes- oder Landesgesetzen.

Zu 1. Entwicklung und Situation des Datenschutzes

Zu 1.1 Sicherheit und Freiheit

Zu Beginn seines Tätigkeitsberichtes weist der LfD darauf hin, dass die Planungen und Maßnahmen zur Gewährleistung des Datenschutzes auf vier Eckpfeilern ruhen. Erstens auf dem Recht, zweitens auf der Technik, drittens auf der Kontrolle und viertens auf der Vermittlung von Medienkompetenz.

Zum Recht:

Das nationale Datenschutzrecht wird zunehmend durch europäisches Recht und internationale Übereinkommen geprägt. Dieser Trend ist insoweit zu begrüßen, als er dazu beiträgt, anzuwendendes Recht zu harmonisieren und Lösungen für solche datenschutzrechtlichen Probleme zu finden, die von den nationalen Gesetzgebern wegen der weltweiten Vernetzung von Informationen nicht befriedigend beantwortet werden können. Diese Tendenz birgt aber zugleich die Gefahr, dass mit Rücksicht auf internationale Verflechtungen und wirtschaftliche Beziehungen zu anderen Staaten Kompromisse eingegangen werden, die den Belangen des Datenschutzes nicht optimal gerecht werden. In diesem Zusammenhang sei an die Diskussion über Regelungen zum Austausch von Fluggastdaten zwischen der EU und den USA erinnert. (Zu den Vorstellungen der KOM für die Neuordnung des Datenschutzrechts in der EU und den sich daraus ergebenden Folgen für das nationale Recht siehe im Einzelnen unten bei 3.1.).

Es zeigt sich, dass der EuGH in Ausfüllung der Europäischen Grundrechtscharta zunehmend die Auslegung des Datenschutzrechts bestimmt. Seine jüngste Entscheidung erging am 24. November 2011 – C-468/10 und C 469/10. Bemerkenswert in ihrer Schärfe war die Feststellung des Gerichtshofes, dass bestimmte materielle Vorgaben der EG-Datenschutzrichtlinie unmittelbar geltendes Recht sind und so gesetzte Standards des europäischen Rechts weder von nationalen Gesetzgebern über- noch unterschritten werden dürfen. Welche Konsequenzen sich aus der Entscheidung für die Gesetzgebung in Deutschland ergeben, bedarf noch intensiver Prüfung. Es wäre bedauerlich, wenn der Standard nationalen Datenschutzrechts, der in bestimmten Bereichen über dem des europäischen Rechts liegt, selbst dort abgesenkt werden müsste, wo dies für das Funktionieren des europäischen Binnenmarktes nicht erforderlich ist.

Von besonderer Bedeutung für den datenschutzgerechten Umgang mit personenbezogenen Daten ist die Rechtsprechung des Bundesverfassungsgerichts. Sie zielt darauf ab, dem Recht des Einzelnen auf Schutz der informationellen Selbstbestimmung (u. a. Urteil vom 15. Dezember 1983, BVerfGE 65,1) bestmöglich Rechnung zu tragen. Der Einzelne soll in seinem privaten Bereich grundsätzlich unbeobachtet bleiben (BVerfGE 120, 274 - Anerkennung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme). Um die Verhältnismäßigkeit staatlicher Überwachungssysteme und -maßnahmen zu gewährleisten, ist – wie vom LfD ausgeführt - eine Überwachungsgesamtrechung (Urteil des BVerfG vom 2. März 2010, NJW 2010, 833) anzustellen. Die Landesregierung sieht sich den Zielvorgaben der Verfassungsrechtsprechung verpflichtet und wird weiterhin im Rahmen der Rechtsanwendung und der Rechtssetzung darauf achten, dass der Einzelne nicht mehr Einschränkungen seiner Rechte hinnehmen muss, als es die Teilhabe an der Gesellschaft zwingend erfordert. Die Landesregierung stimmt mit dem LfD überein, dass zur Erreichung des Ziels die Evaluierung von Eingriffsgesetzen nötig ist.

Zur Technik:

Aus dem immer komplexer werdenden Einsatz von Informationstechnik und ihrer weltweiten Vernetzung rühren gegenwärtig die größten Risiken für den Einzelnen im Umgang mit seinen personenbezogenen Daten her. So ermöglichen einerseits neue Techniken, wie z.B. der RFID-Einsatz und das Smartmetering, Verhaltens- und Bewegungsprofile des Einzelnen zu erzeugen. Andererseits kann die moderne Informationstechnik aber auch Hilfen zur Gewährleistung von Datenschutz bieten, z. B. durch datenschutzfreundliche Grundeinstellungen von Verfahren, frühzeitige Pseudonymisierung oder Anonymisierung

personenbezogener Daten oder durch die Unterstützung technischer und organisatorischer Maßnahmen im Sinne des § 6 DSG LSA.

Der Landesregierung ist bewusst, dass der Einzelne die Möglichkeiten des eGovernment nur dann nutzen wird, wenn er von den jeweiligen Angeboten einerseits einfach, andererseits aber auch in sicherer Weise Gebrauch machen kann. Er muss darauf vertrauen können, dass bei elektronischer Kommunikation seine Daten in mindestens gleicher Weise vor dem Zugriff durch Unbefugte und vor unzulässiger Zweckänderung geschützt sind wie bei herkömmlicher Informationsverarbeitung in Akten. Hierauf achtet die Landesregierung besonders.

Zur Kontrolle:

Wirksamer Datenschutz erfordert effektive Kontrolle. Dabei ist die Tätigkeit des LfD nur eine, wenn auch tragende Säule. Wichtiger als repressive Kontrolle ist die im DSG LSA an mehreren Stellen verankerte Beratungsfunktion des LfD, die von den Adressaten des Gesetzes und insbesondere der Landesregierung bei der Setzung neuen Rechts und bei den Planungen zum Umgang mit personenbezogenen Daten genutzt wird. Die Beratungsaufgabe ist deshalb so wichtig, weil eine permanente allumfassende Kontrolle durch den LfD vom Gesetzgeber nicht gewollt ist und in der Praxis auch nicht zu leisten wäre. Dementsprechend weist das Gesetz den verantwortlichen Stellen die Verantwortung für die Beachtung datenschutzrechtlicher Vorgaben selbst zu und verpflichtet sie, als Instrument der Eigenkontrolle Beauftragte für den Datenschutz einzusetzen. Daneben verpflichtet das Gesetz die obersten Landesbehörden und die übrigen juristischen Personen des öffentlichen Rechts, die Beachtung datenschutzrechtlicher Vorschriften in ihrem Organisationsbereich sicherzustellen. Darüber hinaus geben die gesetzlichen Rechte, z. B. auf Auskunft, Berichtigung, Sperrung oder Löschung, auch dem Betroffenen selbst die Möglichkeit, auf den ordnungsgemäßen Umgang mit seinen personenbezogenen Daten hinzuwirken.

Zur Medienkompetenz:

Von seinen Rechten kann der Einzelne nur wirksam Gebrauch machen, wenn er über diese Rechte hinreichend informiert ist und sie daher zielgerichtet einsetzen kann. Ebenso muss der Einzelne wissen, welche Vorkehrungen rechtlicher, aber auch technischer Art er selbst treffen kann und sollte, damit mit seinen Daten sicher und datensparsam umgegangen wird. Dies setzt Medienkompetenz voraus (siehe hierzu im Einzelnen unten bei 1.2 und 21.2).

Zu 1.2 Nicht-öffentlicher Bereich

Übermittlungen in Drittstaaten:

Soweit personenbezogene Daten aus der EU oder dem EWR in Drittländer übermittelt werden, muss gewährleistet sein, dass bei den Stellen, an die übermittelt wird, ein angemessenes Datenschutzniveau besteht. Hierzu kann es bilaterale Abkommen und internationale Übereinkommen geben. Andere Möglichkeiten sind die Einhaltung von Standardvertragsklauseln i. S. des Art. 26 Abs. 4 der EG-Datenschutzrichtlinie oder verbindliche Unternehmensregelungen. Es ist davon auszugehen, dass die anstehende Neuregelung des Datenschutzes in der EU weitere Konkretisierungen und Verbesserungen im grenzüberschreitenden Datenverkehr bringen wird. Ergänzend bedarf es der Verständigung auf internationale Mindeststandards im Umgang mit personenbezogenen Daten, speziell im Internet.

Der Europarat hat angekündigt, im Jahr 2012 das Übereinkommen zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention 108) vom 28. Januar 1981 zu überarbeiten. Die Konvention soll stärker als bisher als globales Instrument fungieren, um Mindeststandards für grenzüberschreitende Datenströme zu gewährleisten. Dabei dürfte als Bedingung für die Kommunikation über Grenzen hinweg gefordert werden, dass Strafverfolger oder Behörden in den Nicht-Europarats-Ländern ein ausreichendes Datenschutzniveau garantieren. Entsprechende Vorgaben enthält das deutsche Datenschutzrecht in Umsetzung der EG-Datenschutzrichtlinie schon jetzt; vgl. § 13 Abs. 2 DSG LSA.

Selbstverpflichtung der Wirtschaft und Selbstdatenschutz:

Der LfD geht auf die Frage ein, inwieweit Selbstverpflichtungen der Wirtschaft und der Selbstdatenschutz durch Betroffene Möglichkeiten bieten, die Einzelnen vor dem ungewollten oder unzulässigen Umgang mit ihren personenbezogenen Daten zu schützen. Dem liegt die Erkenntnis zugrunde, dass ein einzelner Staat nicht allein mit Rechtsvorschriften und durch die Kontrolle der Beachtung der Normen all den Risiken begegnen kann, die in einer freien Informationsgesellschaft mit weltweiter Vernetzung über das Internet für den Einzelnen aus dem Umgang mit seinen personenbezogenen Daten herrühren.

Zu Selbstverpflichtungen der Wirtschaft:

Selbstverpflichtungen der Wirtschaft sind durchaus geeignet, den gesetzlichen Regelungsbedarf zu minimieren und die zuständigen Aufsichtsbehörden zu entlasten. Sie können sich darauf beziehen, vereinbarte Standards im Umgang mit personenbezogenen

Daten zu beachten, den Grundsätzen der Datensparsamkeit und Datenvermeidung Rechnung tragende Verfahren einzusetzen, die Datenverarbeitung für die Betroffenen transparent zu gestalten usw. Das BMI hat in einer Pressemitteilung vom 1. Dezember 2011 wichtige Anforderungen an Selbstverpflichtungen aufgeführt. Sie müssen auf den bestehenden Gesetzen aufbauen, also diese ergänzen oder konkretisieren. Keinesfalls dürfen Selbstverpflichtungen hinter gesetzlichen Anforderungen zurückbleiben. Auch muss es wirksame Kontroll- und Sanktionsmechanismen geben.

Die Bundesregierung setzt verstärkt auf ein funktionierendes System von Selbstverpflichtungen; beispielhaft wird auf die Diskussion über eine Änderung des BDSG zu Geodatendiensten, wie z. B. Google Street View, verwiesen (vgl. Gesetzentwurf des Bundesrates und die Gegenäußerung der Bundesregierung - BT-Drs. 17/2765). Die Bundesregierung will danach gesetzliche Regelungen zur Veröffentlichung personenbezogener Daten im Internet darauf beschränken, dass ehrverletzende Äußerungen unterbleiben und umfassende Persönlichkeits- oder Bewegungsprofile Einzelner nicht erstellt werden dürfen.

Selbstverpflichtungen sind dem Grunde nach bereits im geltenden Datenschutzrecht mit den in § 38a BDSG geregelten Verhaltensregeln zur Förderung der Durchführung datenschutzrechtlicher Regelungen vorgesehen. Bei einer Überprüfung der Selbstverpflichtungen durch die Datenschutzaufsichtsbehörden gemäß § 38 Abs. 2 BDSG kann festgestellt werden, ob die Selbstverpflichtungen den Anforderungen des Datenschutzrechts genügen.

Auf Bundesebene ist die Einrichtung einer Stiftung Datenschutz geplant, die im Jahr 2012 ihre Arbeit aufnehmen soll. Es wird eine rechtsfähige Stiftung des privaten Rechts errichtet. Stifterin ist die Bundesrepublik Deutschland, vertreten durch das BMI. Die Stiftung soll Instrumente der Selbstverpflichtung der Wirtschaft auf dem Gebiet des Datenschutzes, die Entwicklung eines Datenschutzaudits und die Prüfung von Produkten und Dienstleistungen auf ihre Datenschutzfreundlichkeit fördern. Der Einsatz von nach Vorgaben der Stiftung auditierter bzw. geprüfter Produkte und Dienstleistungen dürfte als Indiz zu werten sein, dass sich die jeweils verantwortliche öffentliche oder nicht-öffentliche Stelle datenschutzgerecht verhält. Ob hierdurch in der Praxis eine Entlastung der Datenschutzkontrollinstitutionen (BfD, LfD, Aufsichtsbehörden nach § 38 BDSG) eintritt, wird die Zukunft zeigen. Rechtliche Bindungswirkung käme einer Auditierung oder Prüfung nach den Maßstäben der Stiftung allerdings nicht zu; dies wäre mit der Unabhängigkeit der Datenschutzkontrollinstitutionen nach Art. 28 Abs. 1 Satz 2 der EG-Datenschutzrichtlinie auch nicht vereinbar.

Zum Selbstdatenschutz:

Selbstdatenschutz erfordert Medienkompetenz. Diese besteht bei der Nutzung des Internets nicht schon in der Kenntnis von Bedienungsmöglichkeiten der Informationstechnik, sondern setzt darüber hinaus voraus, dass dem Einzelnen bekannt ist, welche Risiken für die Gewährleistung des Rechts auf informationelle Selbstbestimmung etwa bei der Teilnahme an sozialen Netzwerken und bei der Einstellung eigener oder fremder personenbezogener Daten ins Internet bestehen und wie man diesen Risiken begegnen kann. Die Vermittlung von Medienkompetenz ist zum einen Aufgabe der Schulen (siehe Ausführungen zu 21.2), zum anderen wird es aber auch Zweck der Stiftung Datenschutz sein, die Bildung im Bereich des Datenschutzes zu stärken sowie den Selbstdatenschutz durch Aufklärung zu verbessern.

Zu 1.3 IuK-Technik und Organisation – Grundsatzthemen

Zu 2.1 Tätigkeit im Berichtszeitraum

Zu 2.2 Schwerpunkte – Empfehlungen

Die Anregungen und Empfehlungen des LfD zur Umsetzung des Datenschutzrechts bzw. zur Anpassung der Datenschutzpraxis an die stetig fortschreitenden technischen Entwicklungen sind für die Arbeit der Ministerien konstruktiv. Dies gilt in besonderem Maße für das MF als das für die Informations- und Kommunikationstechnologie federführend zuständige Ressort. Die bewährte Zusammenarbeit mit dem LfD wird fortgesetzt.

Ein Datenschutzmanagement kann dazu beitragen, das Datenschutzbewusstsein der Bediensteten zu verbessern und den Datenschutz in den Verwaltungsabläufen zu verankern. Auf Fortbildungsangebote, Veröffentlichungen und Beratungen durch den LfD werden die Ressorts weiterhin gern zurückgreifen.

Zu 3.1 Novellierung des Datenschutzrechts

Zu 3.1.1 BDSG-Novelle 2009 – Novellierung des Landesrechts?

Zu 3.1.2 Arbeitnehmerdatenschutz

Das DSG LSA ist zuletzt durch das Zweite Gesetz zur Änderung datenschutzrechtlicher Vorschriften vom 27. September 2011 (GVBl. LSA S. 648) geändert worden. Die Änderung beschränkte sich - um Terminvorgaben der Europäischen Kommission zur Umsetzung eines Urteils des Europäischen Gerichtshofes vom 9. März 2010 nachzukommen - weitgehend auf Regelungen zur Übertragung der Aufgabe der Datenschutzkontrolle im nicht-öffentlichen Bereich zum 1. Oktober 2011 auf den LfD. In diesem Zusammenhang fasste der Landtag am 8. September 2011 eine Entschließung (LT-Drs. 6/388), nach der die LReg aufgefordert ist, bis spätestens Ende 2012 einen Gesetzentwurf zur Änderung des DSG LSA vorzulegen, der die nötige Anpassung der landesgesetzlichen Regelungen im Datenschutz an den Stand von Wissenschaft und Technik gewährleistet. Gleichzeitig ist beabsichtigt, die Transparenz von Datenverarbeitungsprozessen zu verbessern und das Recht auf informationelle Selbstbestimmung zu stärken. Die weitere Änderung des DSG LSA sagte der Minister für Inneres und Sport bei der abschließenden Beratung des Zweiten Gesetzes zur Änderung datenschutzrechtlicher Vorschriften zu. Die Ankündigung wurde in der Mitteilung der LReg vom November 2011 zur LT-Drs. 6/388 wiederholt. Gegenwärtig finden auf Arbeitsebene Abstimmungen zwischen dem LfD und dem MI statt, wie das DSG LSA geändert werden soll. Bei der Neuregelung ist das Urteil des EuGH vom 24. November 2011[1] zu berücksichtigen und sicherzustellen, dass keine Regelungen getroffen werden, die den Datenschutz abweichend von zwingenden Vorgaben der EG-Datenschutzrichtlinie regeln.

Gegenstand der Rechtsänderung wird auch die Umsetzung der im Bundesrecht seit 2009 geltenden Regelungen zur Stärkung der Rechtsstellung behördlicher Datenschutzbeauftragter und zur Verschärfung des Rechts der Auftragsdatenverarbeitung sein.

Ein zentraler Punkt soll die Neuregelung des Beschäftigtendatenschutzes für Bedienstete der unmittelbaren und mittelbaren Landesverwaltung sein, die sich an der bevorstehenden Neuregelung des Beschäftigtendatenschutzes im BDSG orientieren soll; (vgl. BT-Drs. 17/4230). Es bleibt zu hoffen, dass das Gesetzgebungsverfahren auf Bundesebene zügig fortgesetzt wird und nicht mit Rücksicht auf zu erwartende Regelungen im EU-Recht zum Stillstand kommt. Im Interesse der Rechtseinheitlichkeit darf der Beschäftigtendatenschutz in

[1] siehe http://curia.europa.eu/juris/document/document.jsf?text=&docid=115205&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=711512

Bund und Ländern nicht auseinanderfallen. Unterschiede im Beschäftigtendatenschutz für Bedienstete öffentlicher und nicht-öffentlicher Stellen müssen die Ausnahme und sachlich geboten sein.

Geprüft wird, inwieweit als Reaktion auf veränderte Gegebenheiten und Nutzungen der modernen Informations- und Kommunikationstechnologie bereits Vorstellungen der KOM zur Neuordnung des Datenschutz in der Europäischen Union Eingang in die anstehende Novelle des DSG LSA finden können. Gegenwärtig neigt die Landesregierung dazu, davon abzusehen. Der Anwendungsbereich des Landesdatenschutzrechts ist anders als das europäische Datenschutzrecht und das BDSG auf öffentliche Stellen beschränkt. Auch wären derartige Landesregelungen mit dem Risiko behaftet, nach relativ kurzer Zeit einer Anpassung an künftiges EU-Datenschutzrecht und Bundesrecht zu bedürfen. Das widerspräche der Gesetzesökonomie und würde die Gesetzesanwender und die Betroffenen zusätzlich irritieren.

Die KOM hat ihr Gesamtkonzept für den Datenschutz in der Europäischen Union Ende 2010 vorgestellt (BR-Drs. 707/10). Hierzu hat der Bundesrat am 11. Februar 2011 (BR-Drs. 707/10 (Beschluss)) Stellung genommen. Danach besteht hinsichtlich der Regelungsziele weitgehend, nicht aber bezüglich des Regelungsrahmens, Übereinstimmung. Am 25. Januar 2012 hat die KOM Entwürfe für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutzgrundverordnung – BR-Drs. 52/12) sowie für eine Richtlinie über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr (BR-Drs. 51/12) vorgelegt. Beide Entwürfe bedürfen einer kritischen Begleitung, besteht doch die Gefahr, dass sie die Regelungskompetenzen der nationalen Gesetzgeber massiv beschränken.

Von allen an der europäischen Rechtsetzung beteiligten deutschen Stellen wird eingehend zu prüfen sein, inwieweit beide Regelungswerke dem von der EU zu beachtenden Subsidiaritätsprinzip nach Art. 5 Abs. 3 EUV Rechnung tragen.

Das vorstehend angeführte Urteil des EuGH vom 24. November 2011 zeigt, dass schon die EG-Datenschutzrichtlinie, die durch die Verordnung abgelöst werden soll, nationale Gesetzgeber weitgehend daran hindert, von der Richtlinie abweichendes, den Datenschutz strenger normierendes nationales Recht, zu schaffen.

Problematisch erscheint ferner, dass die KOM – gestützt auf Art. 16 Abs. 2 Satz 1 AEUV - die für die Bereich der justiziellen und polizeilichen Zusammenarbeit vorgesehene Richtlinie auch auf die Zusammenarbeit von Polizei und Justiz auf nationaler Ebene und weitere innerstaatliche Datenverarbeitungsvorgänge erstrecken und damit über Art. 82 bis 89 AEUV hinausgehen will.

Einheitliches Datenschutzrecht innerhalb der EU und des EWR hat in vielen Bereichen seine Berechtigung. Dies gilt vor allem dann, wenn der Einzelne so effektiver als durch nationales Recht vor den Risiken geschützt werden kann, die seinen Persönlichkeitsrechten in der vernetzten Informationsgesellschaft drohen. Auch ist einheitliches Recht in vielen Bereichen für das Funktionieren des Binnenmarktes und die reibungslose Zusammenarbeit der Organe der EU mit Behörden der Mitgliedsstaaten unverzichtbar. Es muss aber darauf geachtet werden, dass die EU ihren Kompetenzrahmen nicht überschreitet. Das Hinnehmen von Kompetenzüberschreitungen wäre faktisch der Verzicht der Mitgliedsstaaten, innerhalb ihrer Kompetenzen an der Fortentwicklung des Datenschutzrechts eigenständig mitzuwirken. Es sei daran erinnert, dass das Datenschutzrecht, wie wir es heute weltweit kennen, maßgeblich durch die Rechtsentwicklung in Deutschland in den letzten 40 Jahren beeinflusst worden ist. Auch wäre es bedenklich, wenn die angekündigte EU-Datenschutzverordnung zur Konsequenz hätte, dass sie die Grundrechte nach deutschem Verfassungsrecht zurückdrängt und die deutschen Verfassungsgerichte, insbesondere das BVerfG, hindern würde, Verfassungsbeschwerden mit datenschutzrechtlichem Inhalt nachzugehen.

Zu 3.1.4 Stiftung Datenschutz

Auf die Ausführungen unter 1.2 wird Bezug genommen.

Zu 4.1. IT-Strategie – Landesleitlinie Informationssicherheit

Die Regelungen zum IT-Sicherheitsmanagement in der Landesverwaltung aus dem Jahre 2002 nehmen Bezug auf entsprechende Regelungen des Bundes. IT-Sicherheitskonzepte sind an den Vorgaben des BSI auszurichten. Mit dem Beschluss der IT-Strategie wurden 2008 die Planungen zum Aufbau einer IT-Sicherheitsorganisation in der Landesverwaltung festgelegt.

Zur Umsetzung der Maßnahmen der IT-Strategie und in Ausrichtung auf eine umfassende Informationssicherheit wurde in einer Arbeitsgruppe unter Beteiligung der Datenschutzbeauftragten des Bundes und der Länder der Entwurf einer Landesleitlinie

Informationssicherheit (LL IS) erarbeitet. Aufgrund der aktuellen Gefährdungslage plant der IT-Planungsrat eine verbindliche Leitlinie für Informationssicherheit für den Bund und die Länder zu erstellen. Sobald die Planungen abgeschlossen sind, wird die Beschlussfassung der Landesregierung über eine LL IS herbeigeführt.

Der erfolgte Wechsel der Zuständigkeit für die IT-Strategie zum MF wird zum Anlass genommen, die IT-Strategie neu zu justieren und mit der E-Government-Strategie zusammenzuführen.

Die gute Zusammenarbeit mit dem LfD in den IKT-Gremien wird fortgesetzt.

Zu 4.3. Zentraler IT-Dienstleister – Sachstand zum Landesrechenzentrum

Die kritischen Anmerkungen des LfD zur Art und Weise sowie zum Umfang seiner Einbeziehung in die Migration der IT-Querschnittsdienste bzw. der Übernahme der Fachverfahren werden bei den künftigen Ressort-Migrationen - zusätzlich zur erfolgten Einbeziehung der Datenschutzbeauftragten in den Ressorts - berücksichtigt.

Die Themen Auftragsdatenverarbeitung, Wartung von Datenverarbeitungsanlagen oder –verfahren durch externe Dritte sowie automatisierte Abrufverfahren werden intensiv und vertrauensvoll mit dem LfD erörtert. Die Fortführung der guten Zusammenarbeit in Vorbereitung der Sitzungen des IT-Planungsrats ist ebenso selbstverständlich, wie die frühzeitige und umfassende Einbeziehung im Rahmen der AG IT-Architektur, z. B. bei der Konzipierung des IAM-Systems.

Angestrebt wird auch, die Zusammenarbeit mit dem LfD im Projekt ITN-XT, für dessen Betrieb das LRZ nach der Entscheidung der Landesregierung vom September 2009 zuständig ist, zu intensivieren.

Zu 4.4 E-Government-Maßnahmeplan 2010 – Fehlanzeige

Die Erfahrungen der letzten Jahre haben gezeigt, dass Belange des Datenschutzes und der Datensicherheit nicht erst bei der tatsächlichen Realisierung der einzelnen E-Government-Projekte berücksichtigt, sondern bereits bei den strategischen Überlegungen und Zielsetzungen für solche Projekte bedacht werden müssen. Deshalb wurde der LfD frühzeitig in die Erstellung des ersten Entwurfs der E-Government-Strategie Sachsen-Anhalts einbezogen.

Wie vom LfD dargestellt, liegt die wesentliche Ursache für die Nichteinbringung des Entwurfs in der vom IT-Planungsrat am 24. Juni 2010 verabschiedeten Nationalen E-Government-Strategie (NEGS). Die strategischen Überlegungen für das weitere Vorgehen in Sachsen-Anhalt müssen sich daran orientieren.

Zu 4.5 Landesportal Sachsen-Anhalt

SSL-Verschlüsselung:

Die Einrichtung der Verschlüsselung für das Landesportal und das damit zusammenhängende Redaktionssystem ist vom LRZ vorgesehen und bereits eingeplant. Allerdings besteht derzeit keine (vertragliche) Möglichkeit zur Beschaffung eines Zertifikates mit einer dem Webbrowser bekannten Zertifizierungsstelle (CA – Certificate-Authority; "Vertrauenswürdige" Zertifikate). Sobald die Möglichkeit der Beschaffung von Zertifikaten besteht, werden folgende Dienste verschlüsselt angeboten:

- LPSA,
- LPSA Redaktion,
- Statistik LPSA (SAWMILL),
- E-Mail-Service (wird derzeit portiert).

Nutzung aktueller Web-Standards:

Die Definition und die Prüfung von Webstandards sowie eine Syntaxüberprüfung des Portals ohne datenschutzrechtlichen Bezug gehören nicht zu den Aufgaben des LfD im engeren Sinne. Das Portal ist weitgehend CSS-basiert. Der Anteil der Nutzung des Browsers IE 6 in der Landesverwaltung ist mit Sicherheit deutlich höher als dessen Weltmarktanteil; man muss derzeit noch von 25 bis 50% ausgehen.

Die Nutzung der technischen Webstandards ist grundsätzlich durch den ältesten zu unterstützenden Browser (in diesem Fall der Internet Explorer 6) limitiert. Eine Überprüfung der Webseite hat ergeben, dass einige Fehler, die durch die Nichteinhaltung des Standards erzeugt werden, enthalten sind. Diese Fehler haben aber keine praktische Relevanz für die Darstellung und Nutzbarkeit der Seite.

Aus der Kritik des LfD am Editor *"Derzeit erzeugt der automatische Editor sehr viele Formatanweisungen selbst. Damit ist leider keine einfache Wiederverwendbarkeit von Daten des Landesportals realisierbar."* lässt sich nicht der Schluss "fehlende Wiederverwendbarkeit

von Daten" ziehen, da zwischen Editor und Datenverwendung kein Zusammenhang besteht. Die Wiederverwendbarkeit demonstriert z.B. der Sachsen-Anhalt-App.

Die Aktualisierung der Templatetechnologie ist Bestandteil der Arbeit der AG Templates; Aktivitäten für 2012 sind geplant. Die mit der Setzung von Templates verbundenen datenschutzrechtlichen Folgen werden überprüft. Templates sind Formatvorlagen im Redaktionsbereich des Contentmanagementsystems Typo3 des Landesportals incl. des Bürger- und Unternehmensservices (BUS).

Datenübermittlung an YouTube, (Twitter, Facebook)
Im Landesportal findet keine Einbindung von Facebook und Twitter statt.

Das Abspielen der YouTube-Videos im Landesportal, zum Beispiel auf der Seite der Videobotschaften des Ministerpräsidenten, erfordert aus technischen Gründen die Übermittlung der IP-Adresse des Nutzers beim Aufruf der Seite. Weitere Daten werden durch den Seitenaufruf nicht an YouTube übermittelt.

Zu 4.6 EU-Dienstleistungsrichtlinie

Die EU-Dienstleistungsrichtlinie verpflichtet die Mitgliedstaaten zur grenzüberschreitenden Verwaltungszusammenarbeit über das Binnenmarktinformationssystem IMI, ein elektronisches System der KOM zur Unterstützung der Verwaltungszusammenarbeit im Bereich der Binnenmarktvorschriften. Das IMI hilft den zuständigen Behörden in den Mitgliedstaaten, praktische Hemmnisse zu überwinden, wie sie insbesondere durch unterschiedliche Verwaltungsweisen, Sprachschwierigkeiten oder fehlende Informationen über die Ansprechpartner in anderen Mitgliedstaaten entstehen. Neben unmittelbar zuständigen Stellen (z. B. den berufsständischen Kammern) wurden die Landkreise als IMI-Behörden im IMI-Basismodul „Dienstleistungsrichtlinie“ registriert. Die Landkreise nehmen koordinierende Aufgaben wahr, sofern kreisangehörige Gemeinden an IMI-Anfragen beteiligt sind. Dieses Koordinierungsmodell hat sich für Sachsen-Anhalt nicht zuletzt wegen des geringen Aufkommens an IMI-Anfragen bewährt.

Die Aufgaben für das IMI-Zusatzmodul „Vorwarnmechanismus“ und der Verbindungsstelle sowie die koordinierende Aufgabe für IMI-Anfragen aus anderen Mitgliedstaaten ohne konkrete Bezeichnung der zuständigen Stelle werden im Landesverwaltungsamt wahrgenommen, jedoch nicht vom Einheitlichen Ansprechpartner (§ 10 EAG LSA). Es liegt eine klare Aufgabentrennung vor.

Die IT-Umsetzung der elektronischen Verfahrensabwicklung erfolgt über das EA-Portal. Das EA-Portal bietet den Dienstleistern ein umfangreiches Informationsangebot zu Verwaltungsverfahren, die für die Aufnahme bzw. Ausübung ihrer Tätigkeit erforderlich sind. Gleichzeitig ist es Dienstleistern im Portal möglich, über den EA Genehmigungen und Erlaubnisse elektronisch zu beantragen oder Anzeigeverfahren elektronisch abzuwickeln. Die zuständigen Behörden sind an das EA-Portal angeschlossen, so dass eine elektronische Verfahrensabwicklung zwischen dem Dienstleister und der zuständigen Stelle über den EA gewährleistet ist.

Die vom LfD angeführte Statistik der zunehmenden Seitenaufrufe des EA-Portals (2009: 2649; 2010: 26392; 2011(1. Q.): 7987) zeigt das wachsende Interesse an dem EA und seinen Angeboten besteht. Gegenwärtig bedient sich der größte Teil der Nutzer nur der Informationsbereitstellung des EA-Portals und der elektronischen Vorhabensklärung, um sich ggf. anschließend doch selbstständig mit Hilfe der gesammelten Informationen mit den zuständigen Stellen vor Ort in Verbindung setzen.

§ 6 Abs. 2 EAG LSA enthält eine Verordnungsermächtigung zur Regelung von Einzelheiten der Zusammenarbeit zwischen dem EA und den zuständigen Behörden. Die Verordnung steht in Zusammenhang mit dem derzeit in der Gesetzgebung befindlichen E-Government-Gesetzes des Bundes, der Nationalen E-Government-Strategie sowie der sich daran anlehnenden E-Government-Strategie des Landes Sachsen-Anhalt. Deshalb und in Anbetracht der geringen Inanspruchnahme des EA sowie wegen der für 2012 angekündigten Evaluierung der Verortungsentscheidung, ist der Erlass der Verordnung bisher zurückgestellt worden. Parallel zu der ab dem 3. Quartal 2012 anstehenden Evaluierung der Verortungsentscheidung, über deren Ergebnis im 2. Quartal 2013 berichtet werden soll, werden unter anderem im Rahmen der Bund-Länder-AG „Optimierung der Einheitlichen Ansprechpartner“ Überlegungen angestellt, wie die EA künftig attraktiver für die Dienstleister werden können.

Der Entwurf des Sicherheitskonzeptes wird auf Arbeitsebene abgestimmt und anschließend dem LfD zur Stellungnahme zugeleitet.

Zu 4.8. De-Mail

Immer mehr Bürger wünschen ihre Behördenangelegenheiten über das Internet zu erledigen. Sie wollen staatliche Dienstleistungen schnell und unkompliziert in Anspruch nehmen. Hierfür ist - wie vom LfD festgestellt - die rechtliche Verbindlichkeit von E-Mails das wichtigste Element.

Die Internetangebote der öffentlichen Stellen bieten derzeit mehr Informationen als tatsächliche verbindliche Kommunikationsmöglichkeiten. Aufgrund des De-Mail-Gesetzes könnte künftig auch im öffentlichen Bereich die elektronische verbindliche Kommunikation zur Alltäglichkeit werden. Dies setzt voraus, dass die Verwaltungsabläufe den veränderten Bedingungen der Technik angepasst werden.

Um die Datensicherheit zu gewährleisten, empfiehlt der LfD den Stellen, die einen De-Mail-Zugang anbieten, einen Ende-zu-Ende verschlüsselten Zugang vorzusehen. Die Landesregierung nimmt die Empfehlungen des LfD, wie bei der Realisierung des De-Mail-Projektes den Anforderungen des Datenschutzes Rechnung getragen werden sollte, zur Kenntnis. Sie wird diese Empfehlungen bei ihren Vorhabenplanungen berücksichtigen. Um die Akzeptanz und Verbreitung der De-Mail zu unterstützen, sollte dem Nutzer die Entscheidung überlassen bleiben, auf welchem Sicherheitsniveau er die Kommunikation führen möchte. Nur Dienste, die anwenderfreundlich sind und deren Sicherheit die Bürger und Bürgerinnen vertrauen, werden letztlich von ihnen auch angenommen.

Zu 5.2 Gesetzentwurf zur Änderung des Gesetzes über das Ausländerzentralregister

Der Bitte des LfD, ihn in seinen Bemühungen zur datenschutzgerechten Umsetzung des EuGH-Urteils vom 16. Dezember 2008 (NVwZ 2009, 379) zu unterstützen, wurde gefolgt. Sein Votum zum Referentenentwurf eines Gesetzes zur Änderung des Gesetzes über das Ausländerzentralregister wurde dem BMI zugeleitet.

Zu 7.2 Neues Abkommen zu Swift

SWIFT (Society for Worldwide Interbank Financial Telecommunication) ist eine international tätige Organisation der Geldinstitute, die zur Abwicklung des weltweiten Zahlungsverkehrs ein Telekommunikationsnetz für den Nachrichtenaustausch zwischen den Mitgliedern betreibt. In der Vergangenheit konnten US-Ermittlungsbehörden unmittelbar auf innereuropäische Finanztransaktionsdaten, die auf einem in den USA gelegenen

Rechenzentrum von SWIFT gespiegelt gespeichert waren, zugreifen. Dies ist nicht mehr möglich, seit die Daten in Europa verarbeitet werden. Nunmehr haben US-Sicherheitsbehörden nur noch auf Antrag Zugang zu Daten von Swift. Geregelt ist dies in einem im August 2010 abgeschlossenen Abkommen (TFTP-Abkommen) zwischen der EU und den USA über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der EU an die USA für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus (Abl L. 195/5). Vor einer Übermittlung wird die Zulässigkeit durch Europol geprüft. Zu Mängeln[2] in der Umsetzung des Abkommens hat sich zuletzt die Bundesregierung in ihrer Antwort vom 3. August 2011 auf eine Kleine Anfrage (BT-Drs. 17/675) geäußert.

Die KOM wurde mit Ratsbeschluss zum TFTP-Abkommen aufgefordert, zwecks Prüfung der Errichtung eines Terrorist Finance Tracking Systems für die EU einen rechtlichen und technischen Rahmen für die Überprüfung von Zahlungsverkehrsdaten auf dem Gebiet der EU vorzulegen. Nach den Vorstellungen der KOM ist vorgesehen, die an die USA zu übermittelnden Daten zu reduzieren und Finanztransaktionsdaten für Strafverfolgungsbehörden der EU und ihrer Mitgliedsstaaten nutzbar zu machen. Einzelheiten stehen noch nicht fest.

Zu 8.1 Auskunftsrechte für Betroffene im Steuerverfahren

Das MF teilt nicht die Ansicht des LfD, dass mangels spezialgesetzlicher Regelung in der Abgabenordung die allgemeinen Regelungen zum Auskunftsrecht im § 19 BDSG – und somit auch § 15 DSG-LSA – anwendbar sind. Für die Landesfinanzbehörden gelten weder die im BDSG noch die im DSG LSA vorgesehenen Auskunftsrechte. Das BDSG gilt grundsätzlich nur für Bundesbehörden. Im Anwendungsbereich der Abgabenordnung kann der Landesgesetzgeber keine landesgesetzlichen Verfahrensregeln treffen. Nach Art. 105 Abs. 2 GG steht dem Bund die konkurrierende Gesetzgebung für Steuern zu. Art. 108 Abs. 5 Satz 2 GG gibt dem Bund darüber hinaus die Gesetzgebungskompetenz, das steuerliche Verfahrensrecht zu regeln. Zur Wahrung der Rechtseinheit des Besteuerungsverfahrens ist es unzulässig, im Anwendungsbereich der Abgabenordung in den Ländern unterschiedliche steuerliche Verfahrensrechte zu gewähren. Daher kann § 15 DSG LSA im Besteuerungsverfahren nicht gelten.

[2] Siehe hierzu:
http://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/PMGKIzuSWIFT.pdf?__blob=publicationFile

Zwischenzeitlich ist der überarbeitete Entwurf einer Regelung zum Auskunftsanspruch in der Abgabenordnung dem BfDI vom BMF zur Stellungnahme übersandt worden. In absehbarer Zeit ist mit einer bundesrechtlichen Lösung des Problems zu rechnen.

Zu 10.1 Kontrolle des Hunderegisters (letzter Satz)

Die dem LfD bei einer Vor-Ort-Kontrolle in einer Kommune aufgefallenen „zunächst unerklärlichen Zahlen im Rahmen der statistischen Auswertung“ wurden seitens der betroffenen Behörde bereinigt, so dass nunmehr plausible Daten im Verhältnis Hund/Halter im zentralen Hunderegister hinterlegt sind.

Zu 11. Geoinformation und Vermessung

Der Aufbau der nationalen und die Schaffung der europäischen Geodateninfrastruktur umfasst als wesentliche Aufgabe die Identifizierung der von beiden Infrastrukturvorhaben betroffenen Geodaten. Die Identifizierung der betroffenen Geodaten ist ein gegenwärtig noch laufender Prozess. Sie erfolgt durch die jeweils sachlich zuständigen Geodaten haltenden Stellen unter koordinierender Begleitung durch das MLV, unter anderem im Zuge der Umsetzung der Entscheidung der Kommission vom 5. Juni 2009 zur Durchführung der Richtlinie 2007/2/EG des Europäischen Parlaments und des Rates hinsichtlich Überwachung und Berichterstattung (ABl. EU Nr. L 148 vom 11. Juni 2009).

Der Stand der Sichtung, Identifizierung und Bewertung des Bestandes kommunaler Geodaten ist in den Berichten der Landesregierung an den Landtag zu den kostenmäßigen Auswirkungen des GDIG LSA auf die Kommunen dargestellt (LT-Drs. 5/2579 vom 30. April 2010, LT-Drs. 5/2912 vom 14. Oktober 2010 und LT-Drs. 6/231 vom 14. Juli 2011). Bei den unter Punkt 11.1 des Tätigkeitsberichts des LfD angesprochenen Geodatenbeständen hat sich bisher keine sachliche Betroffenheit der Kommunen nach § 4 GDIG LSA gezeigt. Die Geodatenbestände der Kommunen sind bisher nicht vom GDIG LSA erfasst. Dementsprechend sind die Kommunen nicht verpflichtet, diese Datenbestände öffentlich verfügbar bereit zu stellen. Daher war eine generelle Bewertung hinsichtlich der Beachtung datenschutzrechtlicher Übermittlungs- und Veröffentlichungsvorschriften entbehrlich. Sofern jedoch Kommunen ihre Geodatenbestände im Rahmen eines freiwilligen Engagements und zur Aktivierung der Nutzungs- und Wertschöpfungspotenziale dieser Daten über die Geodateninfrastruktur Sachsen-Anhalt öffentlich verfügbar bereitstellen wollen, müsste eine datenschutzrechtliche Bewertung unter Beteiligung des LfD erfolgen.

Zu 12.3 Einschulungsuntersuchung/schulärztliche Untersuchungen

Die Thematik wird auf der Amtsärztedienstberatung 2012 nochmals angesprochen werden. Die Hinweise des LfD zu Einschulungsuntersuchungen wurden umgesetzt.

Zu 12.7 Landeskrebsregister

Die Datenbestände der drei klinischen Krebsregister der Tumorzentren im Land werden zu einem Krebsregister zusammengefasst. Die Umsetzung erfolgt unter Einbeziehung des LfD.

Zu 12.8 Neugeborenenscreening

Von der Universitätskinderklinik wird die Beanstandung des LfD als erledigt betrachtet. Die Probenbestände wurden vernichtet; die Aufbewahrungsfristen wurden entsprechend den Hinweisen des LfD angepasst. Der LfD wurde von den ergriffenen Maßnahmen in Kenntnis gesetzt und hat sich damit einverstanden erklärt.

Zu 13.2 Bekämpfung von Schwarzarbeit und illegaler Beschäftigung

Die Bedenken des LfD gegen die Verwaltungsvereinbarung zwischen Niedersachsen und Sachsen-Anhalt zur gemeinsamen Nutzung einer Webanwendung mit zentraler Datenbankanbindung zur Erfassung von Ordnungswidrigkeiten nach dem Schwarzarbeitsbekämpfungsgesetz und der Handwerksordnung hatte das MW zum Anlass genommen, die Verwaltungsvereinbarung nochmals zu überarbeiten und mit dem LfD abzustimmen.

Ergebnis dieser Abstimmung im Oktober 2011 war, dass die Bedenken des LfD ausgeräumt werden konnten. Weitere vom LfD gegebene datenschutzrechtliche Hinweise werden in einer Dienstanweisung für die zuständigen Behörden (Landkreise und kreisfreie Städte) berücksichtigt. Mit Kabinettsbeschluss vom 13. Dezember 2011 wurde das MW beauftragt, die Verwaltungsvereinbarung abzuschließen und nach Ablauf von zwei Jahren dem Kabinett über den Nutzen der Webanwendung zu berichten.

Zu 14.1 Cloud Computing und Datenschutz

Cloud Computing ist regelmäßig ein Fall der Auftragsdatenverarbeitung. Die Landesregierung teilt die Auffassung des LfD, dass öffentliche Stellen beim Umgang mit personenbezogenen Daten regelmäßig Cloud Computing nur in Hybrid Clouds betreiben

können. Dabei kennen sich Anbieter (Auftragnehmer i. S. des Datenschutzrechts) und Nutzer (Auftraggeber im Sinne des Datenschutzrechts). Datenverarbeitungskapazitäten werden dem Nutzer exklusiv zur Verfügung gestellt. Nur bei Hybrid Clouds können regelmäßig alle Vorgaben erfüllt werden, die § 8 DSG LSA bzw. bereichsspezifische Vorschriften (z. B. § 80 SGB X) an die Zulässigkeit von Auftragsdatenverarbeitung stellen. Voraussetzung ist allerdings nicht, dass Anbieter und Nutzer derselben Organisation angehören. Dies ist auch in anderen Fällen der Auftragsdatenverarbeitung nicht die Regel.

Die von den Arbeitskreisen Technik und Medien der DSB-Konferenz erarbeitete Orientierungshilfe „Cloud Computing“ – Version 1.0, Stand 26. September 2011 – hat der LfD inzwischen auf seiner Homepage eingestellt. Sie ist eine geeignete Arbeitshilfe zur datenschutzgerechten Ausgestaltung von Cloud Computing durch öffentliche Stellen, auch wenn sie nicht speziell auf Regelungen des DSG LSA abstellt, sondern sich an den Vorgaben des § 11 BDSG zur Auftragsdatenverarbeitung orientiert.

Für die Einrichtung einer „Private Cloud“ im LRZ wurden erste Überlegungen in einem Positionspapier zusammengetragen. Dabei wurde der Blick auf die Bereiche IT-Architektur, IT-Servicemanagement sowie Datenschutz und Informationssicherheit gerichtet. Die Integration von Cloud Computing Technologien und der Wandel in der Serviceerbringung bedingt die Anpassung vorhandener bzw. die Modellierung und Einführung neuer Geschäftsprozesse im LRZ. Bei den weiteren Planungen werden auch die datenschutzrechtlichen Belange umfassend zu berücksichtigen sein. In die Planungen wird der LfD rechtzeitig eingebunden.

Zu 14.3 Mobile Computing und Datenschutz (vom iPhone bis zum BlackBerry)

Beim Einsatz mobiler Endgeräte in der Landesverwaltung wurden und werden Belange der Datensicherheit und des Datenschutzes beachtet. Hierbei geeignet ist die Einbindung über SALSA in das ITN-LSA. Die Sicherheitskonzepte werden im Einzelnen mit dem LfD abgestimmt.

Zu 14.4 Datenschutz durch Einsatz von IPv6

Es trifft zu, dass sich das LRZ mit der Thematik befasst hat. Erforderlich ist ein koordiniertes Vorgehen im Zusammenhang mit dem Aufbau des ITN-XT. Das IPv6-Adresskonzept wird vom LRZ erarbeitet und mit den Kommunen abgestimmt. Das Thema „Privacy Extension“

wird dabei ebenso eine Rolle spielen wie die Absicherung durch DNSSEC und RPKI. Der LfD wird in die Planungen einbezogen.

Zu 14.5 Veraltete Software ist kein „Stand der Technik“

Der Einsatz aktueller Softwareversionen, insbesondere beim Zugriff auf das Internet, ist geeignet die Sicherheit zu erhöhen. Mit Fragen der Verwendung alternativer Software befasst sich die AG Standards. Um aktuelle Software bereitstellen zu können, wird an einem Konzept für einen Standard-Arbeitsplatz gearbeitet, das auch das Softwaremanagement betrachtet. Eine zentrale Bereitstellung von MSI-Archiven kann eine sinnvolle Alternative vor der Migration zum zentralen IT-Dienstleister sein.

Zu 14.6 Datenschutzgerechtes Web-Tracking

Adressaten des DSG LSA dürfen, wenn sie zur bedarfsgerechten Ausgestaltung ihres Angebotes das Surfverhalten der Nutzer analysieren, nur datenschutzkonforme Verfahren zur Reichweitenmessung bei Internetangeboten einsetzen. Hierzu hat der LfD dem MF mit Schreiben vom 11. November 2011 unter Bezugnahme auf die in einem Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 26./27. November 2009 (**Anlage 24** zum 10. TB des LfD) angeführten Anforderungen aktuelle Hinweise gegeben. Das Schreiben wurde allen in Betracht kommenden Stellen zur Kenntnis gegeben.

Zu 14.8 Kontaktformular im Landesportal

Das LRZ hat der bei der Staatskanzlei eingerichteten Zentralredaktion des Landesportals vorgeschlagen, den Redakteuren zu ermöglichen, eigene Kontaktformulare für ihre Portalbereiche einzurichten. Die technischen Gegebenheiten sind vorhanden und lassen sich mit vergleichsweise wenig Aufwand für den Einzelfall aktivieren. Die Zentralredaktion hat von dem Angebot keinen Gebrauch gemacht. Eingehende Anfragen über das Kontaktformular sollen in der Staatskanzlei auch weiterhin gebündelt und von dort an die zuständigen Ressorts weitergeleitet werden.

Zu 16.1 Datenübermittlung bei der Nutzung von Ratsinformationssystemen

Dem LfD ist beizupflichten, dass Daten, die für die Erfüllung der Aufgaben nicht mehr benötigt werden, zu löschen sind.

Zu dem Hinweis, dass für die Nutzung personenbezogener Daten in Sitzungsunterlagen im ratsinternen Verkehr die Voraussetzungen des § 10 DSG LSA erfüllt sein müssen, ist festzustellen, dass zur Gewährleistung der Ratsarbeit der interne Informationsaustausch und damit im Rahmen des Zulässigen auch der Austausch von personenbezogenen Daten erforderlich ist.

Zur Veröffentlichung von Sitzungsunterlagen im Internet ist darauf hinzuweisen, dass nach § 56 Abs. 3 GO LSA den Einwohnern die Einsichtnahme in die Niederschriften über die öffentlichen Sitzungen gestattet ist. Darüber hinausgehende Ansprüche der Einwohner, etwa Anspruch auf Aushändigung von Abschriften bzw. Kopien der Sitzungsprotokolle, sind gesetzlich nicht normiert. Die GO LSA enthält auch keine Norm, auf deren Grundlage und nach deren Maßgabe eine öffentliche oder ortsübliche Bekanntmachung der Niederschriften vorzunehmen ist. Die GO LSA trifft aber auch kein ausdrückliches Veröffentlichungsverbot. Sofern in Verantwortung der Kommunen Sitzungsunterlagen der öffentlichen Sitzungen und die jeweiligen Protokolle in das Internet eingestellt werden, muss sichergestellt sein, dass nicht unbefugt personenbezogene Daten veröffentlicht werden. Dies kann ggf. durch die Schwärzung einzelner Passagen in Sitzungsprotokollen geschehen.

Zu 16.2 Übertragung von Gemeinderatssitzungen im Internet

Gegen die Ausführungen des LfD bestehen keine Bedenken. Da die Übertragung der Sitzungen der kommunalen Vertretungen im Internet grundsätzlich die Einwilligung der Betroffenen voraussetzt, sind drei verschiedene Handlungsalternativen möglich:

a) Soweit alle Ratsmitglieder mit der Übertragung einverstanden und Beeinträchtigungen der Ratsarbeit nicht zu erwarten sind, müssen die Fernsehübertragungen gestattet werden.

b) Sofern einzelne Ratsmitglieder sich gegen eine Übertragung im Internet wenden, kann diese unter der Auflage gestattet werden, dass die Redebeiträge betroffener Ratsmitglieder nicht aufgenommen werden.

c) Lehnt eine größere Anzahl der Ratsmitglieder Filmaufnahmen ab, können diese vollständig untersagt werden, wenn zu erwarten ist, dass das Überwachen der Auflagen den Sitzungsverlauf insgesamt stören würde.

Zu 18.2 Personalmanagement

Bei der Entwicklung des Systems wird weiterhin ein hoher Stellenwert auf den Datenschutz gelegt. Dies gilt insbesondere für das Rollen- und Berechtigungskonzept. Zwischen der

entwickelnden Firma und der Projektleitung wurde vereinbart, zu den Themen Datenaufbewahrung, Datenlöschung und Verschlüsselung von Daten/Datensätzen datenschutzkonforme Lösungen zu entwickeln, die im Anschluss mit dem LfD abgestimmt werden.

Ein weiteres wichtiges Thema ist die Anpassung des Verfahrensverzeichnisses an den fortentwickelten Systemstand. Dazu soll eine Masterdatenbank aufgebaut werden, mit deren Hilfe jederzeit Übersichten über die im System implementierten Strukturen (u. a. Felder, Masken, Menüs, Kataloge, Plausibilitäten und Auswertungen) erstellt werden können. Über den Projektfortschritt wird zeitnah der LfD informiert.

Zu 18.3 Erweiterte Zentralregisterauskunft für Polizeibewerberauswahlverfahren

Der LfD weist darauf hin, dass die Einholung von unbeschränkten Auskünften gemäß § 41 BZRG durch das MI keiner gesetzlichen Zweckbindung unterliegt, gleichwohl aber der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit aber zu berücksichtigen ist.

Es steht außer Frage, dass die Verwendung der unbeschränkten Auskunft bei der Einstellung von Polizeibeamten ein ähnlich gewichtiges öffentliches Interesse wie die im BZRG aufgeführten Zwecke darstellt. Wenn schon Waffenbehörden befugt sind, zur Erteilung waffenrechtlicher Erlaubnisse unbeschränkte Auskünfte einzuholen, muss dies erst recht bei der Einstellung von Polizeibeamten möglich sein. Die Verhinderung sowie Verfolgung von Straftaten und Ordnungswidrigkeiten gehört zu den Kernaufgaben des Polizeivollzugsdienstes. Eigene Verstöße in diesem Bereich können Zweifel an der persönlichen Eignung des Bewerbers begründen. Zu bedenken sind die weitreichenden Befugnisse von Polizeibeamten, denen innerhalb der gesetzlichen Grenzen die Anwendung unmittelbarer Gewalt durch unmittelbaren Zwang erlaubt ist.

In den Einstellungsvoraussetzungen des § 4 PolLVO LSA ist geregelt, dass nur der Bewerber in den Vorbereitungsdienst eingestellt werden kann, der gerichtlich nicht bestraft ist.

Zweck des Eignungsauswahlverfahrens ist es, aus einem Bewerberkreis auf Grundlage von Eignung, Befähigung und Leistung die besten Bewerber auszuwählen. Dazu muss auch das Vorliegen der Einstellungsvoraussetzungen geprüft werden.

Auf die Einholung der unbeschränkten Auskunft kann nicht deshalb verzichtet werden, weil die überwiegende Zahl der Bewerber die Voraussetzungen erfüllt.

Die Bedenken des LfD hinsichtlich der Anwendbarkeit des § 84 Abs. 1 LBG LSA werden vom MI nicht geteilt. § 84 Abs. 1 LBG LSA ermächtigt den Dienstherrn zur Erhebung personenbezogener Daten über Bewerberinnen und Bewerber, soweit diese zur Begründung des Dienstverhältnisses erforderlich ist. Das LBG LSA differenziert insoweit gerade nicht zwischen personalverwaltender Dienststelle und oberster Dienstbehörde. Der Zweck der Datenerhebung besteht im Übrigen nicht in der Weiterleitung der unbeschränkten Auskünfte, sondern nur in der Prüfung des Vorliegens einer Einstellungsvoraussetzung. Das MI wertet die Auskünfte aus und vernichtet diese nach Abschluss des Einstellungsverfahrens. Der Fachhochschule Polizei wird lediglich mitgeteilt, ob die Einstellungsvoraussetzung vorliegt.

Das MI hält es auch nicht für problematisch, dass es zum Zweck der Überprüfung der Einstellungsvoraussetzungen diesen Teil des Eignungsauswahlverfahrens an sich zieht. Nach Artikel 70 der Verfassung des Landes Sachsen-Anhalt ernennt der Ministerpräsident die Beamten. Diese Befugnisse hat der Ministerpräsident mit Anordnung vom 7. Juni 1994 (MBl. LSA S. 1487), zuletzt geändert durch Verwaltungsvorschrift vom 5. Januar 2005 (MBl. LSA S. 5), für Beamte des einfachen, mittleren und gehobenen Dienstes den Ministern für deren Geschäftsbereich übertragen. Das MI hat mit Runderlass vom 7. Januar 2008 (MBl. LSA S. 66) den nachgeordneten Polizeibehörden und –einrichtungen die Ausübung des Rechts der Ernennung bis einschließlich Besoldungsgruppe A 14 übertragen. Dabei hat sich das MI die personalrechtlichen Befugnisse im Einzelfall vorbehalten. Die Fachhochschule Polizei ist gemäß § 81 Abs. 2 Nr. 1 SOG LSA eine Einrichtung der Polizei und unterliegt als solche der Dienst- und Fachaufsicht des MI. Aus diesem Grund hat das MI auch die Möglichkeit, die personalrechtlichen Befugnisse hinsichtlich der Überprüfung der Einstellungsvoraussetzungen des § 4 Nr. 1 PolLVO LSA an sich zu ziehen.

Das MI wird gegenüber dem Bewerber nicht Verfahrensbeteiligter. Falls ein Bewerber gegen einen auf der Grundlage einer Mitteilung des MI durch die Fachhochschule Polizei vorgenommenen Abbruch des Eignungsauswahlverfahrens vorgeht, übermittelt das MI die unbeschränkte Auskunft an die Fachhochschule mit Einverständnis des Bewerbers. Erklärt der Bewerber sein Einverständnis nicht, zieht das MI das Einstellungsverfahren in Gänze an sich und wird damit auch Verfahrensgegner.

Das MI wird zukünftig in den Fällen, in denen eine unbeschränkte Auskunft eine Eintragung über eine gerichtliche Bestrafung zum Inhalt hat, zu einer Einzelfallprüfung übergehen. Im Rahmen dieser Prüfung erfolgt eine Abwägung zwischen der Schwere der gerichtlichen Bestrafung und den Anforderungen an die charakterliche Eignung von Polizeibeamten, so dass nicht jede gerichtliche Bestrafung automatisch zum Ausschluss aus dem Bewerberkreis führt.

Zu 18.4 Eingliederungsmanagement und Personalvertretung

Eine Einschränkung der Informationsrechte des Personalrats auf Vorlage sämtlicher Hinweisschreiben an Beschäftigte im Rahmen des betrieblichen Eingliederungsmanagements ist nicht gerechtfertigt. Die Übersendung von Musteranschreiben ohne Namensnennung reicht nicht aus. Die Schreiben sind auch nicht nur im Einzelfall auf Anforderung des Personalrats zu übersenden. Eine Begrenzung auf einzelne Personalratsmitglieder ist ebenfalls nicht zulässig. Der Personalrat hat einen Informationsanspruch nach § 84 Abs. 2 Satz 7 SGB IX in Verbindung mit § 57 Abs. 2 Satz 1 und 2 PersVG LSA. Auf die Entscheidungen des BVerwG vom 23. Juni 2010 - Az.: 6 P 8.09 - sowie des VG Oldenburg vom 03. Mai 2011 - Az.: 8 A 2967/10 - (veröffentlicht in Der Personalrat 2011, S. 486 ff.) wird hingewiesen. Die Berücksichtigung datenschutzrechtlicher Belange erfolgt vielmehr dergestalt, dass die Schreiben inhaltlich auf die Gesichtspunkte zu begrenzen sind, die für eine ordnungsgemäße Belehrung nach § 84 Abs. 2 Satz 3 SGB IX unumgänglich sind. Außerdem dürfen Antwortschreiben der Beschäftigten nur mit deren Zustimmung weitergegeben werden.

Zu 18.5 Irrweg einer Lohndaten-CD

Das Universitätsklinikum Halle hatte unverzüglich nach dem scheinbaren Verlust einer Lohndaten-CD angeordnet, Datenträger solcher Brisanz mit Boten gegen Quittung zu transportieren.

Vor Abschluss einer Vereinbarung zwischen der Finanzbehörde und dem Universitätsklinikum Halle/S. mussten zunächst die konkreten Abläufe ermittelt werden, um Schwachstellen aufzudecken. Bei der anschließenden Ausgestaltung des Konzepts mussten unterschiedliche Vorstellungen über den Regelungsinhalt zum Ausgleich gebracht werden. Dies betraf z. B. das Kontrollrecht des Arbeitgebers und die Haftung sowie den Umgang mit den Daten nach Beendigung des Vertrags. Nachdem über alle strittigen Punkte eine Einigung erzielt worden war, musste das Konzept erneut ergänzt werden. Vor dem

Hintergrund, dass die Oberfinanzdirektion zugleich die Bezügeunterlagen des Universitätsklinikums Halle/S. verwahrt, erschien es angezeigt, über die Regelungen des reinen Datentransfers hinaus verbindliche Vorgaben zur Aufbewahrung und zum Schutz der Unterlagen vor Ort vertraglich zu regeln.

Die Vereinbarung soll die bisherige Vereinbarung über die Bezügeabrechnung vom 11. April 2007 ergänzen. Ein Entwurf ist unter Einbeziehung des Datenschutzbeauftragten der OFD Magdeburg erarbeitet worden. Er beruht zum großen Teil auf den Vorgaben im Mustervertrag zu Auftragsverhältnissen nach § 8 DSG LSA. Allerdings ist aufgrund ausfüllungsbedürftiger Formulierungen im Mustervertrag ein umfangreicher und zeitintensiver Abstimmungsprozess im Detail erforderlich. Der Abschluss der Abstimmungen wird von der OFD im ersten Quartal 2012 angestrebt. Vom Universitätsklinikum Halle/S. ist noch einen weitere Ergänzung vorgeschlagen worden, die noch inhaltlich ausgestaltet werden muss.

Zu 18.7 E-Mail-Verkehr des Personalrates

Auch bei der genannten Polizeidirektion haben Personalratsmitglieder ausreichende technische und organisatorische Möglichkeiten, bei der Teilnahme am E-Mail-Verkehr ihren Verschwiegenheitspflichten zu genügen. Zum einen verfügt der Personalrat über eine Funktionsadresse. Zum anderen versendet die Systemadministration bei Abwesenheit des E-Mail-Postfachinhabers an die Absender Abwesenheitsnotizen. Eine Umleitung von E-Mails erfolgt nur noch mit vorherigem schriftlichen Einverständnis des E-Mail-Postfachinhabers.

Zu 19.2 Änderung des SOG LSA

Für das Vorhaben „Novellierung des SOG LSA“ ist nach derzeitigem Stand folgender Zeitplan vorgesehen:

-ab Januar 2012: Beteiligung des LfD und der betroffenen Ressorts auf Arbeitsebene,
-März 2012: 1. Kabinettsbefassung,
-Juni 2012: 2. Kabinettsbefassung,
-September 2012: 1. Lesung im Landtag,
-Januar 2013: 2. und 3. Lesung im Landtag,
-März 2013: geplantes Inkrafttreten.

Ein erster Referentenentwurf ist dem LfD zur Stellungnahme zugeleitet worden.

Zu 20.2 Quellen-Telekommunikationsüberwachung

Im VerfSchG-LSA sind ergänzende landesrechtliche Regelungen zur Durchführung von Maßnahmen der Quellen-TKÜ derzeit nicht geplant.

Zu 20.3 Vorratsdatenspeicherung

Zu 25.1 Urteil des Bundesverfassungsgerichts zur Vorratsdatenspeicherung

Die Vorratsdatenspeicherung, die nach ihrer Zielrichtung eine Mindestdatenspeicherung meint, bedarf zwingend und möglichst kurzfristig einer bundesgesetzlichen Neuregelung. Diese ist wiederholt angemahnt worden. Schon im November 2010 haben die Generalstaatsanwälte und die Generalbundesanwältin festgestellt, dass der Wegfall der Vorratsdatenspeicherung dazu geführt habe, dass auch schwere und schwerste Straftaten nicht mehr aufgeklärt werden können. Eine schnelle gesetzliche Regelung sei dringend erforderlich. Auch der Deutsche Richterbund hielt bereits im Dezember 2010 eine gesetzliche Neuregelung für dringend notwendig. Dem Staatsanwalt dieses Instrument zu nehmen, hieße, ihm in bestimmten Fällen eine unlösbare Aufgabe aufzuerlegen. Dies schade der Justiz.

Auch von Seiten der Polizei wird eine gravierende Sicherheitslücke beklagt. So hält der Präsident des Bundeskriminalamtes Ziercke den Rückgriff auf Vorratsdaten für unverzichtbar. Ohne den Zugriff auf die bei den Diensteanbietern gespeicherte Daten wären in ca. 80% der im Jahr 2008 polizeilich registrierten Fälle im Bereich der IuK-Kriminalität keine Ermittlungsansätze vorhanden gewesen.

In Sachsen-Anhalt haben Vertreter der Strafverfolgungsbehörden ebenfalls durchgreifende Befürchtungen geäußert. Mit dem Wegfall des Zugriffs auf die bei den Providern gespeicherten Vorratsdaten sei ein wichtiges Ermittlungsinstrument weggefallen. In seiner Jahresbilanz 2010 hat der Generalstaatsanwalt hervorgehoben, dass der hohe Rückgang der Verfahren wegen pornographischer und gewaltdarstellender Schriften um 67 % vorrangig auf den Wegfall der Vorratsdatenspeicherung zurückzuführen sei, der gerade in Fällen der gewerbs- oder bandenmäßigen Verbreitung kinder- und jugendpornografischer Darstellungen im Internet einen gravierenden Erkenntnisverlust zur Folge habe.

Die Evaluation zur EU-Richtlinie über die Vorratsdatenspeicherung hat im Juni 2011 ergeben, dass die Vorratsdatenspeicherung nach wie vor „ein notwendiges Instrument für die Strafverfolgung, den Opferschutz und die Strafjustiz“ darstellt. Die KOM hat Deutschland mit Schreiben vom 16. Juni 2011 zur Umsetzung der EU-Richtlinie angehalten und zugleich

darauf hingewiesen, dass das sog. „Quick-Freeze-Verfahren“ nicht als hinreichende Umsetzung der Richtlinie angesehen werden könne.

Der von der Bundesjustizministerin im Juni 2011 vorgelegte Diskussionsentwurf genügt den Anforderungen der Strafverfolgungsbehörden nicht. Das Einfrieren von Daten ist nur möglich, solange Daten auch vorhanden sind. Dies hängt im Wesentlichen davon ab, in welchem Umfang und für welchen Zeitraum bei den Diensteanbietern zu eigenen Zwecken (etwa Rechnungslegung oder Beseitigung von externen Störungen) benötigte Verkehrsdaten nach § 96 TKG gespeichert werden. Sobald die Daten hierfür nicht mehr benötigt werden, sind sie zu löschen (§ 96 Abs. 1 Satz 3 TKG). Wegen der starken Zunahme von Flatrates und der gesetzlich geregelten Löschungspflicht werden Verkehrsdaten häufig nur noch für kurze Zeiträume gespeichert, die von Provider zu Provider unterschiedlich ausfallen und sich auch danach unterscheiden, ob es sich um Mobilfunk- oder Festnetzbetreiber handelt.

Das im Entwurf vorgesehene „Quick-Freeze“ ist zur verfassungskonformen Ausgestaltung der Vorratsdatenspeicherung nicht geboten. Das Bundesverfassungsgericht hat im Urteil vom 2. März 2010 (BVerfGE 125; 260; NJW 2010, 833) hervorgehoben, dass eine sechsmonatige, vorsorglich anlasslose Speicherung von Telekommunikationsverkehrsdaten durch private Diensteanbieter, wie sie die EU-Richtlinie vorsehe, nicht schlechthin unvereinbar mit Art. 10 GG sei. Vielmehr hat es ausdrücklich festgestellt: „Eine vorsorglich anlasslose Speicherung von Telekommunikationsverkehrsdaten zur späteren anlassbezogenen Übermittlung an die für die Strafverfolgung oder Gefahrenabwehr zuständigen Behörden (…) darf der Gesetzgeber zur Erreichung seiner Ziele als geeignet ansehen. Es werden hierdurch Aufklärungsmöglichkeiten geschaffen, die sonst nicht bestünden und angesichts der zunehmenden Bedeutung der Telekommunikation auch für die Vorbereitung und Begehung von Straftaten in vielen Fällen erfolgversprechend sind.“ Demgegenüber liege im Quick-Freeze-Verfahren – so das Bundesverfassungsgericht weiter – keine vergleichbar effektive Aufklärungsmöglichkeit.

Dies aufgreifend hatte die Justizministerkonferenz bereits im Juni 2010 in Hamburg ausdrücklich begrüßt, dass auf der Grundlage dieser Entscheidung des Bundesverfassungsgerichts nunmehr klare Maßstäbe für eine verfassungskonforme gesetzliche Regelung vorliegen.

Zu 21.2 Medienkompetenz und Datenschutzbewusstsein

Der LfD bezieht sich in seinen Ausführungen auf das Konzept zur Stärkung der Medienkompetenz in Sachsen-Anhalt, das durch das MK in Zusammenarbeit mit weiteren Ministerien und externen Sachverständigen erarbeitet und dem Landtag vorgelegt wurde.

Auf der Grundlage dieses Konzeptes ist die Arbeitsgemeinschaft „Medienbildung/-kompetenz Sachsen-Anhalt“ beim MK eingerichtet worden. Der LfD ist ständiges Mitglied dieser Arbeitsgemeinschaft. Er kann damit seine Erfordernisse direkt einbringen. Den von ihm konkret genannten Handlungsfeldern wie fächerübergreifende Unterrichtsinhalte bzw. Projekte zum Datenschutz, der Lehrerausbildung, -fortbildung und -weiterbildung wurde in den Handlungsschwerpunkten des vorgelegten Konzepts Rechnung getragen.

Die im Entwurf vorliegende Empfehlung der Kultusministerkonferenz zur Medienbildung in der Schule ist durch den Schulausschuss bestätigt und der Amtschefkonferenz zur weiteren Befassung zugeleitet worden.

Zu 21.4 Schulverwaltungssoftware

Der LfD stellt fest, dass die gesetzlichen Befugnisse ausreichen, um die für die Erfüllung von Verwaltungsaufgaben erforderliche Datenerhebung und –verarbeitung zu ermöglichen. Er verweist darauf, dass immer zuerst die Prüfung erfolgen muss, inwieweit die Aufgaben auch ohne eine umfassende zentrale Schülerdatei erledigt werden können. Die durch den LfD angeregten Verfahren zur sicheren Pseudonymisierung und der Umfang der Daten, die über die Schulverwaltungssoftware erhoben werden sollen, müssen klar definiert werden.

Dieser Position des LfD stimmt das MK zu. In einem Gespräch mit dem LfD hat der Kultusminister am 18. Oktober 2011 zugesagt, dass der LfD im Rahmen seiner Mitarbeit in der Arbeitsgruppe „Projekt Schulverwaltungssoftware“ angemessene Erörterungs- und Beteiligungsmöglichkeiten erhält.

Zu 21.5 Terminkalender für Schülerinnen und Schüler

Das Projekt wurde federführend durch das MS betrieben und mittlerweile eingestellt.

Zu 22.8 Aufruf im Wartezimmer

Genau wie im nicht-öffentlichen Bereich besteht auch bei öffentlichen Stellen mit Publikumsverkehr das Risiko, dass im Wartebereich mitanwesende Dritte Kenntnis von personenbezogenen Daten Betroffener erhalten. Der LfD zeigt auf, mit welch einfachen Mitteln dies verhindert werden kann, z. B. durch anonymisierten Aufruf, durch die Ziehung von Wartemarken oder die Schaffung von Diskretionszonen. Auch öffentliche Stellen müssen entsprechende Vorkehrungen treffen. Weder die Übermittlungsvorschriften des allgemeinen noch des bereichspezifischen Datenschutzrechts berechtigen öffentliche Stellen dazu, in Erfüllung ihrer jeweiligen Aufgabe unnötig Daten an Dritte zu übermitteln.

Zu 22.14 Kinderschutz

Die weiteren Aktivitäten des Zentrums „Frühhilfen für Familien“ und die Aktualisierung des Leitfadens „Gewalt gegen Kinder und Jugendliche“ für Lehrerinnen und Lehrer und Erzieherinnen und Erzieher werden von den beteiligten Ressorts mit dem LfD abgestimmt.

Zu 23.1 Zensus 2011

Mit Stichtag 9. Mai 2011 wurde in der Bundesrepublik Deutschland eine registergestützte Bevölkerungszählung durchgeführt. Die bundeseinheitlich neu entwickelte Zensusmethode verbindet die Auswertung vorhandener Verwaltungsregister, insbesondere der Melderegister, mit einer Stichprobenbefragung ausgewählter Haushalte und kombiniert diese Ergebnisse mit einer Gebäude- und Wohnungszählung, für die Gebäude- und Wohnungseigentümer postalisch befragt wurden. Angaben zu Bewohnern in Wohnheimen und Gemeinschaftseinrichtungen wurden direkt vor Ort erhoben. Die Durchführung des Zensus 2011 obliegt dem Statistischen Landesamt, das insbesondere für die örtliche Durchführung der Haushaltsbefragungen und der Befragungen in Sonderbereichen von örtlichen Erhebungsstellen unterstützt wird. Die statistischen Erhebungen sind im Wesentlichen abgeschlossen. Der Schwerpunkt der statistischen Arbeiten bei diesem Großprojekt liegt nunmehr in der Prüfung und Verarbeitung der erhobenen Daten. Erste Ergebnisse der Zählung werden Ende 2012 vorliegen.

Der LfD war im Gesetzgebungsprozess für ein Zensusgesetz 2011 des Bundes und für ein Zensusausführungsgesetz des Landes Sachsen-Anhalt frühzeitig beteiligt. Seine Hinweise, insbesondere zur Verbesserung der Transparenz des Verwaltungshandelns gegenüber dem betroffenen Bürger, fanden besondere Beachtung und wurden sowohl im Gesetzgebungsverfahren als auch bei der Durchführung der Zählung umgesetzt. Der seit

2009 durchgeführte regelmäßige Austausch von Informationen zwischen dem MI, dem Statistischen Landesamt und dem LfD war darauf gerichtet, die einzelnen, zum Teil statistikinternen Prozesse bei der Vorbereitung und Durchführung des Zensus 2011 darzulegen, um keine Zweifel an der Rechtmäßigkeit der Zählung und an der zu jeder Zeit gewährleisteten Sicherheit der erhobenen Daten entstehen zu lassen. Die vom LfD durchgeführten Prüfungen im Verlauf der Durchführung des Zensus 2011 haben daher, wie der Bericht aussagt, zu keinen datenschutzrechtlichen Beanstandungen geführt.

Zu 23.3 Mehrjährige Zugehörigkeit zu einer 15%-Stichprobe

Der LfD ist auf ein Urteil des Sächsischen Oberverwaltungsgerichts vom 15. Januar 2010 eingegangen, das Fragen der Stichprobenziehung für statistische Erhebungen und den Verbleib eines Unternehmens in der Auskunftspflicht für mehrere Berichtsjahre berührt. Das Gericht beanstandete das zur Durchführung des Dienstleistungsstatistikgesetzes angewandte Verfahren der Stichprobenziehung und die Heranziehung des Auskunftspflichtigen nicht.

Zum Thema Stichprobenziehung ist allgemein zu bemerken: Um Belastungen der Auskunftspflichtigen gering zu halten, werden in einer Reihe amtlicher Statistiken repräsentative Erhebungen durchgeführt. Auswahlgrundlage ist dabei das statistische Unternehmensregister. Die Stichprobenziehung erfolgt in der Regel durch das Statistische Bundesamt. Es gehört zu den üblichen statistischen Verfahren, einmal gezogene Stichproben über mehrere Jahre zu verwenden und lediglich um Neuzugangsstichproben zu ergänzen. Über Rotationen entscheiden die Bundesländer im Verbund. In Sachsen-Anhalt sind bislang keine Probleme im Zusammenhang mit der Stichprobenziehung bei der Durchführung von statistischen Erhebungen aufgetreten.

Zu 24.1 PPP-Projekt Justizvollzugsanstalt Burg – Entwicklung/Sachstand

Zu 24.2 Informations- und Kontrollbesuch der JVA Burg

Zu 24.3 Kontrolle in einer JVA – Auftragsdatenverarbeitung in der Justiz

Die Ausführungen des LfD zeigen, dass es bei diesem Projekt noch weiterer Abstimmung in Einzelfragen bedarf, bei denen das MJ die enge Abstimmung mit dem LfD suchen wird.

Zu Einzelfragen ist anzumerken:

Zum 31. Dezember 2011 ist dem LfD ein Datenschutzkonzept in Form des Entwurfs für eine Datenschutzdienstanweisung für die Justizvollzugsanstalt Burg nebst eines sie ergänzenden Entwurfs für eine Dienstanweisung zum Umgang mit der Videoanlage der JVA Burg zugeleitet worden. Im Mittelpunkt des Entwurfs für eine Datenschutzdienstanweisung stehen die Insassen der JVA Burg und der Schutz ihrer personenbezogenen Daten vor Missbrauch und unbefugtem Zugriff. Betroffen von der Videoüberwachung und einer eventuellen Übermittlung von Bildmaterial an externe Stellen ist aber nicht nur dieser Personenkreis. Betroffen sind auch die staatlichen Bediensteten, die Beschäftigten der privaten Dienstleistungsunternehmen und die Besucher der JVA Burg. Deshalb bot es sich an, nicht nur ein beschreibendes Konzept zu übermitteln, sondern gleich und ohne diesen Zwischenschritt die Entwürfe für zwei konkrete Dienstanweisungen nebst dazugehörigem Verfahrensverzeichnis zu übermitteln, die sich an den tatsächlichen Abläufen und Gegebenheiten in dem PPP-Modell JVA Burg orientieren und somit unmittelbar einer praxisorientierten Prüfung und datenschutzrechtlichen Bewertung zugänglich sind.

An der Zulässigkeit des Einsatzes privater Hilfskräfte wird festgehalten. Die Beschäftigten der privaten Dienstleistungsunternehmen handeln gegenüber den Gefangenen der Justizvollzugsanstalt Burg nicht in eigenem Namen, sondern ausschließlich im Auftrag der Justizvollzugsbehörde. Sie sind insoweit Verwaltungs- bzw. Vollzugshelfer im Sinne von § 155 Abs. 1 StVollzG, sie treffen keine Entscheidungen über den vollzuglichen Werdegang der Gefangenen. Sämtliche Arbeiten, z. B. die der Sozialarbeiter und Psychologen, sind Vorarbeiten (z. B. Mitarbeit bei der Erstellung der Vollzugspläne oder Stellungnahmen zu Vollzugslockerungen etc.), die dem Entscheidungsträger (Anstalts-, Vollzugs- oder Vollzugsabteilungsleiter) lediglich als Entscheidungshilfe dienen.

Zur Videoüberwachung ist anzumerken, dass die Kameras in Besuchsräumen für Verteidiger inzwischen mit einer festen Abdeckung in Form einer Haube versehen sind. Das hatte das MJ dem LfD bereits mitgeteilt.

Auch das Problem der Verpflegungslisten hat sich – wie der LfD einräumt - mittlerweile erledigt, seitdem Akronyme (Kurzwort, das aus den Anfangsbuchstaben der Namen zusammengesetzt wird) für die Essensausgabe verwandt werden.

Hinsichtlich der Umsetzung der übrigen Empfehlungen hat sich im Wesentlichen noch kein neuer Sachstand ergeben. Dies betrifft auch die Frage der Gefangenentelefonie. Die hierzu

erwartete Entscheidung des OLG Naumburg liegt noch nicht vor. Allerdings hat der LfD bei der Abschlussbesprechung zu seinem Informations- und Kontrollbesuch selber bekundet, insgesamt keine gravierenden Datenschutzmängel festgestellt zu haben.

Der LfD wird auch weiterhin in die datenschutzrechtliche Fortentwicklung des PPP-Modells Justizvollzugsanstalt Burg einbezogen werden.

Zu 24.4 Elektronische Fußfessel

Der Begriff „Elektronische Fußfessel“ ist eine umgangssprachliche Bezeichnung für ein elektronisches Überwachungsgerät, das am Bein des Probanden befestigt wird.

Die im Tätigkeitsbericht als offen angesprochenen Fragen des Datenschutzes betreffen zum einen die Umsetzung der Elektronischen Aufenthaltsüberwachung, die im ausstehenden Gemeinsamen Runderlass unter Einbeziehung des LfD gelöst werden. Zum anderen wird die Frage aufgeworfen, ob die Polizei die übermittelten Daten aufgrund des Polizeirechts nutzen darf oder ob hierzu eine spezialgesetzliche Rechtsgrundlage geschaffen werden muss.

Zu letzterer Frage ist anzumerken, dass dies in § 463a StPO geregelt ist. Der Gemeinsamen Überwachungsstelle der Länder wurde durch Staatsvertrag die Aufgaben der Führungsaufsichtsstellen übertragen. Die Führungsaufsichtsstelle kann nach § 463a Abs. 4 Satz 4 StPO die Polizei verpflichten, ihrem Ersuchen zu genügen. Diese Frage ist im Übrigen von anderen an der Gemeinsamen Überwachungsstelle der Länder beteiligten Länder nicht problematisiert worden.

Soweit der LfD kritisiert, dass er nicht beteiligt worden sei, ist anzumerken, dass der Berichtszeitraum im März 2011 endet und bis zu diesem Zeitpunkt der Staatsvertrag noch in der Abstimmungsphase war. Zudem wurde mit der Umsetzung des Staatsvertrages im Land erst im Juni 2011 begonnen und der LfD zwischenzeitlich beteiligt.

Zu 25.2 Neuregelung der Rundfunkfinanzierung

Die Beachtung des Datenschutzes ist ein wichtiges Anliegen des Fünfzehnten Rundfunkänderungsstaatsvertrages. Diesem Thema haben alle Beteiligten besondere Aufmerksamkeit gewidmet. Auf Fachebene fanden drei ausführliche Unterredungen mit Vertretern der Datenschutzbeauftragten der Länder statt, in denen zahlreiche

Detailveränderungen des Fünfzehnten Rundfunkänderungsstaatsvertrages und klarstellende Hinweise in der Begründung zum Staatsvertrag verabredet wurden.

Datenschutzrechtliche Regelungen treffen insbesondere die §§ 9, 11 und 14 des Rundfunkänderungsstaatsvertrages. § 9 enthält Regelungen zum Auskunftsrecht und der Satzungsermächtigung der zuständigen Landesrundfunkanstalt, § 11 regelt die Verwendung bezogener Daten. § 14 trifft Übergangsregelungen.

Im Zentrum der öffentlichen Diskussion standen insbesondere folgende datenschutzrechtliche Fragen:

Umfang des Auskunftsrechts der Landesrundfunkanstalten

§ 9 Abs. 1 des Rundfunkbeitragsstaatsvertrages sieht ein Auskunftsrecht der Landesrundfunkanstalten vor. Diese Vorschrift ist erforderlich, um eine möglichst vollständige Einziehung der gesetzlich geschuldeten Rundfunkbeiträge zu erreichen. Das Auskunftsrecht der Landesrundfunkanstalten dient nicht nur der Effektivität des Beitragseinzugs, sondern darüber hinaus auch der Beitragsgerechtigkeit sowie der Gewährleistung der verfassungsrechtlich gebotenen funktionsgerechten Finanzierung des öffentlich-rechtlichen Rundfunks.

Gemäß § 9 Abs. 1 Satz 2 des Rundfunkbeitragsstaatsvertrages ist der Eigentümer oder der vergleichbar dinglich Berechtigte der Wohnung oder des Grundstücks, auf dem sich eine Betriebsstätte befindet, verpflichtet, der Landesrundfunkanstalt Auskunft über den tatsächlichen Inhaber der Wohnung oder der Betriebsstätte zu erteilen, wenn die zuständige Landesrundfunkanstalt den Inhaber der Wohnung oder der Betriebsstätte nicht feststellen kann. Bei Wohnungseigentümergemeinschaften kann die Auskunft gemäß § 9 Abs. 1 Satz 3 des Rundfunkbeitragsstaatsvertrages auch vom Verwalter verlangt werden. Die Auskunftspflicht aus § 9 Abs. 1 Satz 2 des Rundfunkbeitragsstaatsvertrages besteht nur hinsichtlich der Identität des tatsächlichen Inhabers der Wohnung oder der Betriebsstätte. Sie erstreckt sich nicht auf sämtliche der Anzeigepflicht des Beitragsschuldners unterliegenden Angaben aus § 8 Abs. 4 des Rundfunkbeitragsstaatsvertrages, wie z.B. die Anzahl der Beschäftigten in der Betriebsstätte. Der Arbeitsaufwand für die gemäß § 9 Abs. 1 Satz 2 des Rundfunkbeitragsstaatsvertrages zu Auskunft verpflichteten Personen ist somit minimiert. Die Regelung des § 9 Abs. 1 Satz 2 des Rundfunkbeitragsstaatsvertrages wirkt sich nur aus, wenn zuvor alle anderen Möglichkeiten zur Feststellung des Inhabers einer Wohnung oder Betriebsstätte ergebnislos ausgeschöpft wurden.

Umfang von Meldedatenübermittlungen

Die Datenerhebung wird auf den für die Realisierung der Beitragsforderungen notwendigen Umfang begrenzt. Aufgrund einer Übergangsbestimmung erfolgt ein einmaliger Meldedatenabgleich. Der Normalfall ist die regelmäßige Meldedatenübermittlung nach § 11 Abs. 4 des Rundfunkbeitragsstaatsvertrages, die bezüglich des geltenden Rundfunkgebührenrechts in Sachsen-Anhalt bereits durch den Vierten Rundfunkänderungsstaatsvertrages eingeführt wurde und seit über 11 Jahren ohne Beanstandung funktioniert. Sie wird in der Übergangsbestimmung des § 14 Abs. 9 des Staatsvertrages ergänzt durch eine einmalige stichtagsbezogene Meldedatenübermittlung, damit die GEZ bei Einführung des neuen Modells eine sichere Datenbasis besitzt.

Regelungskompetenz der Landesrundfunkanstalten

§ 9 Abs. 2 des Rundfunkbeitragsstaatsvertrages ermächtigt die zuständige Landesrundfunkanstalt, Einzelheiten des Verfahrens, insbesondere für die Erfüllung von Auskunfts- und Nachweispflichten sowie zur Kontrolle der Beitragspflicht durch Satzung zu regeln. In diesen Satzungen werden die Vorgaben, die sich aus der Novellierung der Rundfunkfinanzierung ergeben, konkreter und differenzierter ausformuliert werden.

Nach Maßgabe der Ziffer 2 der Protokollerklärung zum Fünfzehnten Rundfunkänderungsstaatsvertrages werden die Länder auf der Grundlage des 19. KEF-Berichts eine zeitnahe Evaluierung des Staatsvertrages ca. 2 Jahre nach Inkrafttreten des Staatsvertrages durchführen. Die Evaluierung soll unter Mitwirkung einer unabhängigen Stelle erfolgen und unter anderem auch die den Datenschutz betreffenden Regelungen des Rundfunkbeitragsstaatsvertrages umfassen. Hierbei wird nach Maßgabe des Beschlusses des Landtages vom 10. November 2011 (LT-Drs. 65/566) die Datenschutzkonformität der Regelungen des Rundfunkbeitragsstaatsvertrages zu prüfen sein. Gleiches gilt für die praktische Anwendung der Regelungen, die Beachtung des Verhältnismäßigkeitsgrundsatzes bei der Erhebung und Verwendung personenbezogener Daten.

Der Landtag von Sachsen-Anhalt hat in seiner Sitzung vom 10. November 2011 zum Vierten Medienrechtsänderungsgesetz (LT-Drs. 6/566) unter Ziffer 4 folgenden Beschluss gefasst:

„4. Die Landesregierung ist gebeten, darauf hinzuwirken, die Datenerhebung, -verarbeitung und -speicherung im Rahmen der Beitragserhebung auf ein Mindestmaß zu beschränken. Die Löschfristen für nicht oder nicht mehr benötigte Daten müssen so kurz wie möglich gehalten werden. Um einen datenschutzrechtskonformen Umgang mit den Daten der

Bürgerinnen und Bürger zu überprüfen, wird zeitnah eine Evaluierung von unabhängiger Stelle durchgeführt.

Die Landesregierung ist gebeten, darauf hinzuwirken, dass die Landesdatenschutzbeauftragten in die Vorbereitung und Durchführung dieser Evaluierung einbezogen werden und der Evaluierungsbericht veröffentlicht wird. Ebenso ist darauf hinzuwirken, dass die Ergebnisse der Evaluierung der Datenschutzkonformität bei folgenden Novellierungen des Rundfunkstaatsvertrages berücksichtigt werden.

Wegen der im 15. Rundfunkänderungsstaatsvertrag enthaltenen Regelungen zum Adressabgleich mit nicht öffentlichen Stellen und zum Umgang der Rundfunkanstalten mit personenbezogenen Daten ist die Landesregierung gebeten, an die Rundfunkanstalten zu appellieren, bei der Erhebung und Verwendung von Daten zu Entrichtung des Rundfunkbeitrages den Grundsatz der Verhältnismäßigkeit zu wahren und den Verzicht auf den Abgleich solcher Daten zu prüfen.

Bezüglich der im 15. Rundfunkänderungsstaatsvertrag enthaltenen Regelungen zum Adressabgleich mit nicht öffentlichen Stellen und zum Umgang der Rundfunkanstalten mit personenbezogenen Daten soll die Landesregierung darauf hinwirken, dass in der an den 19. KEF-Bericht anschließenden Evaluierung des Modellwechsels in der Finanzierung des öffentlich-rechtlichen Rundfunks explizit Aspekte der Datenschutzkonformität berücksichtigt werden und dass die Erhebung und Verwendung personenbezogener Daten durch die Rundfunkanstalten auf Verhältnismäßigkeit hin untersucht werden.“

Zu 25.3 Sperrung von Internetseiten zur Bekämpfung von Kinderpornografie

Das Gesetz zur Aufhebung von Sperrregelungen bei der Bekämpfung von Kinderpornografie in Kommunikationsnetzen vom 22. Dezember 2011 (BGBl. I S. 2011, 2958) ist am 29. Dezember 2011 in Kraft getreten. In Umsetzung des Grundsatzes „Löschen statt Sperren“ werden kinderpornografische Inhalte im Netz weiterhin konsequent auf der Grundlage des geltenden Rechts gelöscht. Die verbesserten Erfolge bei den Löschbemühungen haben Sperrmaßnahmen entbehrlich gemacht. Der Gesetzgeber hat sich von der Feststellung leiten lassen, dass es besser ist, strafbare Inhalte durch konsequentes Löschen nachhaltig aus dem Netz zu verbannen. Sperren könnten umgangen werden.

Zu 26.3 GIAZ - Teil III

Soweit der LfD Bedenken in Bezug auf einen verbesserten Informationsaustausch zwischen Verfassungsschutz und Polizei äußert und dies in den inzwischen bestehenden Zugang des Mitarbeiters der Verfassungsschutzbehörde zu allen Datenbanksystemen des Verfassungsschutzes sieht, sind diese unbegründet.

Sofern Informationen durch Mitarbeiter des Verfassungsschutzes an die Polizei übermittelt werden, erfolgt dies ausschließlich auf der Grundlage der einschlägigen Vorschriften zur Datenübermittlung. Dabei ist es unerheblich, ob Mitarbeiter räumlich dem GIAZ zugeordnet sind oder ihren Dienst in der Abteilung 4 des MI versehen.

Zu 26.5 NADIS-neu

Soweit der LfD ein höheres Gefährdungspotenzial für den datenschutzgerechten Umgang mit personenbezogenen Daten sieht, wenn Dokumente in das System eingestellt werden, ist dies nachvollziehbar. Es geht um die Speicherung von personenbezogenen Daten Dritter, d. h. von solchen Personen, für die keine Speicherberechtigung nach den Vorschriften des BVerfSchG und VerfSchG LSA besteht.

Sind solche Personen in volltextsuchfähigen Dokumenten gespeichert, können die Informationen über sie jederzeit zusammengetragen werden, auch wenn sie nicht im strukturierten Datenbestand gespeichert sind. Es entspricht der Rechtsauffassung des MI, dass Daten Dritter nicht in den in NADIS-Neu gespeicherten Ursprungsdokumenten enthalten sein dürfen. Auch das BMI, das zunächst eine gegenteilige Auffassung vertrat, ist mittlerweile zu der Überzeugung gelangt, dass o. g. Dritte nicht in Dokumenten genannt sein dürfen.

Im Rahmen der Einführung von NADIS Neu wird diese Festlegung konsequent umgesetzt. Dokumente dürfen nur dann in NADIS Neu gespeichert werden, wenn dort ausschließlich Personen genannt sind, die auch in NADIS strukturiert gespeichert sind.

Zu 27.1 Online-Anbindung der Fahrerlaubnisbehörden an das KBA

Auflösung der örtlichen Fahrerlaubnisregister

Die Fristverlängerung durch Änderung des § 65 Abs. 10 Satz 2 StVG zur Auflösung der örtlichen Fahrerlaubnisregister geschah auf Initiative der Länder. Die jetzige Gesetzesformulierung beruht auf einem Vorschlag des BfDI unter Berücksichtigung eines Ergänzungsvorschlages des KBA.

Änderung des StVG

Mit Gesetz zur Änderung des StVG vom 2. Dezember 2010 (BGBl. I S. 1748) wurden durch den Bundesgesetzgeber die Rechtsnormen im StVG an die Protokollierungspraxis angepasst. Die Regelungen gehen auf ein Gespräch im KBA mit dem BfDI zurück. Die darauf folgende Stellungnahme des BfDI enthielt hingegen weitergehende Forderungen, u. a. aus dem bekannten Gutachten des AK Verkehr. Hierzu wurde seitens des KBA darauf hingewiesen, dass diese Forderungen ohne hohe finanzielle Investitionen nicht umsetzbar seien. Das wurde vom BfDI zur Kenntnis genommen.

Das MLV hatte den LfD im Vorfeld der StVG-Novelle eingebunden. Der LfD hat darauf hingewiesen, dass die Datenschutzbelange der Länder durch den BfDI in die Bundesgesetzgebung eingebracht wurden. Beschlüsse im fachlich zuständigen BLFA sind dagegen für die Länder nicht verbindlich, sondern bilden lediglich Grundlage für eine Meinungsbildung im weiteren Gesetzgebungsverfahren.

Anbindung der Fahrerlaubnisbehörden an das KBA

Bereits in der Stellungnahme zum IX. Tätigkeitsbericht (zu Nr. 26.1) wurde deutlich gemacht, dass die vom BfDI geforderte Datenanbindung und der Datenaustausch der Fahrerlaubnisbehörden mit dem KBA mittels „qualifizierter elektronischer Signatur“ mit einem erheblichen Kostenaufwand - insbesondere für die kommunalen Fahrerlaubnisbehörden - verbunden wäre und das Land keine direkte Einflussmöglichkeiten in Bezug auf die technische Ausstattung der kommunalen Fahrerlaubnisbehörden hat.

Auflösung der örtlichen Fahrerlaubnisregister

Da die Auflösung der örtlichen Register zum 31. Dezember 2012 zu Vollzugsproblemen, z. B. in Bezug auf den Nachweis von Besitzständen, die Verwaltung der Probezeit u. a., nach sich ziehen kann, wurde dieses Thema im zuständigen BLFA-FE/FL im September 2011 durch die Länder behandelt. Im Ergebnis wurde zur Erörterung von Lösungsmöglichkeiten im Sinne einer einheitlichen Handhabung eine Arbeitsgruppe unter Mitwirkung von Vertretern

der Fahrerlaubnisbehörden, des KBA, der Datenschutzbeauftragten eingerichtet, die durch die Softwarehersteller fachlich unterstützt wird. Hierüber wurde der LfD durch das MLV informiert und seine Teilnahme an der Arbeitsgruppe anheim gestellt. Die Belange der Datenschutzbeauftragten der Länder (AK Verkehr) wurden durch das Unabhängige Landeszentrum für Datenschutz des Landes Schleswig-Holstein wahrgenommen. Im Ergebnis der Arbeitsgruppensitzung am 8. November 2011 ist das BMVBS angehalten, zusammen mit dem BMJ und dem BfDI, eine Verordnungsänderung vorzubereiten. Der Sitzungsvermerk wurde dem LfD am 15. November 2011 übermittelt.

Die weiteren Forderungen der Datenschutzbeauftragten des Bundes und der Länder nach einer sicheren, integeren, authentischen, revisionsfähigen und transparenten Verarbeitung der Fahrerlaubnisdaten zwischen den Fahrerlaubnisbehörden und dem KBA bedürfen vordringlich einer Bewertung durch den Bundesgesetzgeber in Abstimmung mit dem BfDI.

Zu 27.2 Verkehrsüberwachung mittels Videoaufzeichnung

Eine verdachtsunabhängige Verkehrsüberwachung mittels Videoaufzeichnung bzw. Bildaufnahmen findet in Sachsen-Anhalt auch weiterhin nicht statt. Bei Vorliegen eines Anfangsverdachts für eine Verkehrsordnungswidrigkeit stützt sich die Videoaufzeichnung auf § 100h Abs.1 Satz 1 StPO i. V. m. § 46 Abs. 1 OWiG.

Zu 27.3 Verkehrszählung zur Ermittlung des Durchgangsverkehrs

Für normale Verkehrszählungen in der Zuständigkeit der Landesstraßenbauverwaltung (Dauerverkehrszählstellen, Verkehrsbeeinflussungsanlagen, 5-Jahreszählungen u. s. w.) werden nur anonymisierte Daten erhoben.

Abkürzungsverzeichnis

A

AEUV	Vertrag über die Arbeitsweise der Europäische Union

B

BDSG	Bundesdatenschutzgesetz
BfDI	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BLFA-FE/FL	Bund-Länder Fachausschuss Fahrerlaubnis-/Fahrlehrerrecht
BMI	Bundesministerium des Innern
BMVBS	Bundesministerium für Verkehr, Bau und Stadtentwicklung
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
BVerfGE	Bundesverfassungsgerichtsentscheidung
BVerfSchG	Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz
BZRG	Gesetz über das Zentralregister und das Erziehungsregister (Bundeszentralregistergesetz)

D

DSB-Konferenz	Konferenz der Datenschutzbeauftragten des Bundes und der Länder
DSG LSA	Gesetz zum Schutz personenbezogener Daten der Bürger (Datenschutzgesetz Sachsen-Anhalt)

E

EAG LSA	Gesetz über den einheitlichen Ansprechpartner, zur Regelung der europäischen Verwaltungszusammenarbeit sowie zur verwaltungs-kostenrechtlichen Umsetzung der europäischen Dienstleistungs-richtlinie in Sachsen-Anhalt (Einheitlicher-Ansprechpartner-Gesetz)
EuGH	Europäischer Gerichtshof
EUV	Vertrag über die Europäische Union

G

GDIG LSA	Geodateninfrastrukturgesetz für das Land Sachsen-Anhalt
GG	Grundgesetz für die Bundesrepublik Deutschland
GIAZ	Gemeinsames Informations- und Auswertungszentrum islamistischer Terrorismus
GO LSA	Gemeindeordnung für das Land Sachsen-Anhalt

I

IAM	Identitätsmanagementsystem
IKT	Informations- und Kommunikationstechnologie
IPv6	Internet Protocol Version 6
IT	Informationstechnologie
ITN XT	Zukünftiges Landesnetz
IuK	Informations- und Kommunikationstechnologie

K

KBA	Kraftfahrt-Bundesamt
KEF-Bericht	Kommission zur Ermittlung des Finanzbedarfs der Rundfunkanstalten
KOM	Europäische Kommission

L

LPSA	Landesportal Sachsen-Anhalt
LBG LSA	Beamtengesetz des Landes Sachsen-Anhalt (Landesbeamtengesetz)
LfD	Landesbeauftragter für den Datenschutz Sachsen-Anhalt
LRZ	Landesrechenzentrum Sachsen-Anhalt

N

NADIS	Nachrichtendienstliches Informationssystem

O

OFD	Oberfinanzdirektion
OLG	Oberlandesgericht
OWiG	Gesetz über Ordnungswidrigkeiten

P

PersVG LSA	Landespersonalvertretungsgesetz Sachsen-Anhalt
PolLVO LSA	Verordnung über die Laufbahnen des Polizeivollzugsdienstes des Landes Sachsen-Anhalt (Polizeilaufbahnverordnung)
PROMIS	Personal-, Ressourcen-, Organisations-, Management- und Informations-System des Landes Sachsen-Anhalt

Q

Quellen-TKÜ	Quellen-Telekommunikationsüberwachung

R

RFID	Radiofrequenz-Identifikation

S

SALSA	Secure Access Land Sachsen-Anhalt
SGB IX	Neuntes Buch Sozialgesetzbuch - Rehabilitation und Teilhabe behinderter Menschen
SGB X	Zehntes Buch Sozialgesetzbuch - Sozialverwaltungsverfahren und Sozialdatenschutz
SOG LSA	Gesetz über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt
SSL	Secure Socket Layer („sichere Sockelschicht“)
StPO	Strafprozessordnung
StVG	Straßenverkehrsgesetz
StVollzG	Gesetz über den Vollzug der Freiheitsstrafe und der freiheitsentziehenden Maßregeln der Besserung und Sicherung

T

TB	Tätigkeitsbericht
TFTP-Abkommen	Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten von Amerika für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus
TKG	Telekommunikationsgesetz

V

VerfSchG-LSA	Gesetz über den Verfassungsschutz im Land Sachsen-Anhalt