Landtag von Sachsen-Anhalt **Drucksache 5/2385**
Fünfte Wahlperiode **22.01.2010**

Unterrichtung

Chef der Staatskanzlei Magdeburg, 14. Januar 2010

Stellungnahme der Landesregierung zum IX. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz für die Zeit vom 1. April 2007 bis 31. März 2009

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 IX. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz für die Zeit vom 1. April 2007 bis 31. März 2009

mit der Bitte um Kenntnisnahme.

Mit freundlichen Grüßen

Rainer Robra

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) sowie für Recht und Verfassung.

Hinweis: *Die Drucksache steht vollständig digital im Internet/Intranet zur Verfügung. Die Stellungnahme ist in Word als Objekt beigefügt und öffnet durch Doppelklick den Acrobat Reader.*
Die Anlage wird aufgrund des Umfangs zur Einsichtnahme in der Bibliothek des Landtages von Sachsen-Anhalt bereitgestellt und kann in gedruckter Form abgefordert werden.

(Ausgegeben am 22.01.2010)

Stellungnahme der Landesregierung zum IX. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz (Drs. 5/2091)

Gliederung:

Vorbemerkung

Die Landesregierung nimmt zum IX. Tätigkeitsbericht des LfD (zu Abkürzungen vgl. das Abkürzungsverzeichnis, S. 40 ff) gemäß § 22 Abs. 4a Satz 2 DSG-LSA Stellung. Dabei verzichtet sie wie in der Vergangenheit darauf, auf zutreffende Sachverhaltsdarstellungen einzugehen; gleiches gilt für rechtliche Bewertungen, die von der Landesregierung geteilt werden. Weiter äußert sich die Landesregierung grundsätzlich nicht zu Themen, die nicht zum Aufgabenbereich des LfD nach § 22 DSG-LSA gehören. Aus Achtung vor dem Parlament unterbleibt schließlich auch eine Auseinandersetzung mit kritischen Aussagen des LfD zu verabschiedeten Bundes- oder Landesgesetzen. Abgesehen wird auch von vertieften Ausführungen zu Themen, die Gegenstand besonderer Beratungen im Landtag und seinen Gremien waren.

Zu 1. Entwicklung und Situation des Datenschutzes,
Zu 1.1 Freiheit und Sicherheit,
Zu 1.2 Nicht-öffentlicher Bereich und
Zu 1.4 Zusammenfassung und Ausblick

Der LfD gibt zu Beginn seines Tätigkeitsberichts einen Überblick über Gefährdungen, denen der Datenschutz im Berichtszeitraum vom 1. April 2007 bis 31. März 2009 ausgesetzt war. Dabei geht er im Interesse der Gesamtschau auch auf Themen ein, die außerhalb seiner eigentlichen Zuständigkeit liegen, wie den Datenschutz im nicht-öffentlichen Bereich.

Fälle des unzulässigen Umgangs mit Kunden- bzw. Kontoverbindungsdaten sowie ausufernder Überwachung von Mitarbeiter durch bundesweit tätige Unternehmen haben zu einer breiten Reaktion in den Medien und in der Politik geführt. Hierdurch und durch bedeutsame – vom LfD unter 1.4 aufgeführte – Entscheidungen des Bundesverfassungsgerichts ist in der Öffentlichkeit das Interesse für Belange des Datenschutzes neu belebt worden. Es geht vor allem um den Schutz des Rechts auf informationelle Selbstbestimmung und des Rechts auf Vertraulichkeit und Integrität informationstechnischer Systeme. Vor dem Hintergrund dieser Ereignisse ist es noch in der 16. Legislaturperiode des Deutschen Bundestages zu den unter 3.1 dargestellten Änderungen im Datenschutzrecht des Bundes gekommen. Das erstarkte Datenschutzbewusstsein der Allgemeinheit wird ein Ansporn sein, die Novellierung des Datenschutzrechts in Bund und Ländern in den nächsten Jahren konsequent und zukunftsweisend fortzuführen. Dieses Datenschutzrecht muss den veränderten Bedingungen der modernen Informations- und Kommunikationstechnik gerecht werden. Zugleich müssen diese Bedingungen genutzt werden, um auch neue – durch

Einsatz der Technik unterstützte – Wege zur Gewährleistung des Persönlichkeitsschutzes zu gehen. Dies entspricht auch den Vorstellungen der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung vom 8./9. Oktober 2009 zum aktuellen Handlungsbedarf beim Datenschutz.

Angesichts der zunehmenden Globalisierung der Informationsverarbeitung, auch durch die Nutzung des Internets und den weltweiten Einsatz von Techniken wie der RFID-Technologie, wird sich die Landesregierung weiterhin dafür einsetzen, dass auch bei grenzüberschreitender Datenverarbeitung den Belangen des Persönlichkeitsschutzes ausreichend Rechnung getragen wird. Vorrangig aufgefordert sind hierzu aber die Bundesregierung und auf europäischer Ebene die zuständigen Gremien und Organe der Europäischen Gemeinschaft. So befasst sich beispielsweise die Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen mit dem „Internet der Dinge – ein Aktionsplan für Europa“ (BR-Drs. 619/09). Der Aktionsplan zeigt die Risiken für die Wahrung der Privatsphäre und den Schutz personenbezogener Daten auf, wenn Gegenstände über das Internet, insbesondere über die Nutzung von RFID-Technik, vernetzt werden. Die im Rahmen des Aktionsplans vorgesehenen Maßnahmen und Überlegungen dürften geeignet sein, Anregungen für den Prozess der Modernisierung des Datenschutzrechts auf europäischer und nationaler Ebene zu liefern, wenn entgegen der bisherigen Einschätzung auch durch die Europäische Kommission und die Bundesregierung Selbstverpflichtungen der Wirtschaft nicht ausreichen sollten, den Einsatz dieser Technik für die Betroffenen transparent zu gestalten und am Grundsatz der Datensparsamkeit auszurichten.

Die Landesregierung wird – wie schon in der Vergangenheit – beim Entwurf landesrechtlicher Vorschriften sowie bei ihrer Mitwirkung an Rechtsvorschriften des Bundes und auf europäischer Ebene konsequent das Ziel verfolgen, den Belangen des Persönlichkeitsschutzes in besonderem Maße Rechnung zu tragen. Unter Berücksichtigung der ständigen Rechtsprechung des BVerfG zum Schutz der Persönlichkeitssphäre dürfen staatliche Eingriffe nur zugelassen sein, wenn sie zur Wahrung überwiegender öffentlicher Interessen unerlässlich sind. Zudem müssen geeignete verfahrensmäßige Sicherungen bestehen; dazu gehört grundsätzlich auch die Möglichkeit des Betroffenen, zumindest nachträglich von Beschränkungen des Rechts auf informationelle Selbstbestimmung Kenntnis zu erlangen.

Beim praktischen Vollzug bestehender Gesetze wird die Landesregierung auch künftig darauf hinwirken, dass staatliche Stellen den Umgang mit personenbezogenen Daten auf das zur Aufgabenerfüllung erforderliche Maß beschränken und angemessene Vorkehrungen

technischer und organisatorischer Art zur Gewährleistung des Persönlichkeitsschutzes getroffen werden. Die Landesregierung vertraut sowohl bei der Konzeption als auch beim Vollzug von Normen mit datenschutzrechtlichem Inhalt auf die bewährte Beratung und Unterstützung durch den LfD.

Das grundrechtlich geschützte Recht auf Datenschutz in seinen verschiedenen Ausprägungen, insbesondere in der Gewährleistung des Rechts auf informationelle Selbstbestimmung und der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, ist nicht nur ein Abwehrrecht gegen den Staat, sondern legt den staatlichen Organen auch eine Schutzpflicht auf. Diese bezieht sich auf die Gewährleistung der für die Persönlichkeitsentfaltung konstitutionellen Bedingungen (vgl. BVerfGE 54, 148, 153: 79, 256, 258; 96, 56, 64). Die aus den Grundrechten folgenden subjektiven Abwehrrechte gegen staatliche Eingriffe einerseits und die sich aus der objektiven Bedeutung der Grundrechte ergebenden Schutzpflichten andererseits unterscheiden sich aber grundlegend voneinander. Das Abwehrrecht fordert in Zielsetzung und Inhalt ein bestimmtes staatliches Verhalten, während die Schutzpflicht grundsätzlich unbestimmt ist und ihr auf verschiedene Weise genügt werden kann. Die Landesregierung wird weiterhin ihre Möglichkeiten nutzen, den grundrechtlich geforderten Schutz personenbezogener Daten auch im nicht-öffentlichen Bereich zu verbessern. In diesem Sinne hat die Landesregierung maßgeblich an dem Zustandekommen der im Jahre 2009 erfolgten Änderungen des BDSG mitgewirkt.

Zu 1.3 eGovernment und Technik

Der LfD gibt an dieser Stelle einen Überblick über die Bundes- und Landesaktivitäten im eGovernment-Bereich. In die Entwicklungen auf Landesebene, die sich zum Großteil an Bundes- und europäischen Aktivitäten ausrichten, ist der LfD durch seine Mitarbeit an Projekten und in Gremien sowie durch seine Beteiligung an der Maßnahmenplanung eingebunden.

Zu 2.5 Internet-Homepage des Landesbeauftragten und Internetkontakt

Wie vom LfD dargestellt, kann von fast jeder Seite des Landesportals unter „www.sachsen-anhalt.de“ nach Anklicken eines Briefumschlagsymbols eine E-Mail an die Portalredaktion der Staatskanzlei gesendet werden. Um den Absender von der ungewollten Preisgabe

sensibler Daten gegenüber der Portalredaktion abzuhalten, wurde zunächst ein Hinweis in das Kontaktformular aufgenommen, dass für andere Stellen bestimmte E-Mails an diese weitergeleitet werden, also ihnen nicht unmittelbar zugehen.

Inzwischen hat die StK die Möglichkeit eröffnet, auch ressorteigene Kontaktformulare einzustellen. Diese Gelegenheit besteht auch für den LfD. Jedes Fachressort kann zudem seit Dezember 2008 auf den in seiner Verantwortung liegenden Seiten ein eigenes Kontaktformular einrichten.

Zu 3.1 Novellierung des Datenschutzrechts

Im Jahr 2009 ist das BDSG durch zwei Änderungsgesetze in wesentlichen Punkten, die fast ausschließlich den Datenschutz im nicht-öffentlichen Bereich betreffen, verändert worden.

Das Gesetz zur Änderung des Bundesdatenschutzgesetzes vom 29. Juli 2009 (BGBl. I S. 2254) tritt am 1. April 2010 in Kraft. Es regelt den Datenschutz beim Scoring, das heißt bei der Berechung und Verwendung mathematisch-statistischer Wahrscheinlichkeitswerte zur Erstellung von Verhaltensprognosen, insbesondere zur Beurteilung der Kreditwürdigkeit Betroffener. Damit gehen Vorschriften einher, die die Auskunft an den Betroffenen über die Berechnung und Verwendung von Scorewerten ausdrücklich regeln. Darüber hinaus werden Normdefizite im Datenschutz bei Auskunfteien beseitigt. So dürfen Stellen, die Daten für eigene Geschäftszwecke verarbeiten und nutzen, nur bestimmte Daten und auch nur bei Vorliegen bestimmter, abschließend aufgeführter Voraussetzungen an Auskunfteien übermitteln.

Das in weiten Teilen am 1. September 2009 in Kraft getretene Gesetz zur Änderung datenschutzrechtlicher Vorschriften vom 14. August 2009 (BGBl. I S. 2814) ist vor allem eine Reaktion auf in den Jahren 2008 und 2009 bekannt gewordene Verstöße im Umgang mit Adress- und Kontoverbindungsdaten sowie mit Arbeitnehmerdaten. Das MI als für Grundsatzangelegenheiten zuständiges Ressort wird in enger Abstimmung mit dem LfD ermitteln, in welchen Punkten die durch Artikel 1 des Gesetzes erfolgte Änderung des BDSG auch Veranlassung zur Änderung des für öffentliche Stellen im Lande geltenden DSG-LSA geben könnte. Denkbar erscheint es, den Grundsatz der Datensparsamkeit und Datenvermeidung unabhängig vom Vorliegen automatisierter Verfahren festzuschreiben, die Rechtsstellung der (behördlichen) Beauftragten für den Datenschutz nach § 14a DSG-LSA

zu verbessern, die Regelungen zur Auftragsdatenverarbeitung zu verschärfen und den Beschäftigtendatenschutz zu überprüfen.

Auch die Landesregierung sieht die im Jahr 2009 erreichten Verbesserungen im Datenschutzrecht des Bundes nur als einen Zwischenschritt an in Richtung einer umfassenden Novellierung des allgemeinen und bereichsspezifischen Datenschutzrechts. Hierzu heißt es in der von Sachsen-Anhalt mitgetragenen Stellungnahme des Bundesrates [BR-Drs. 4/08 (Beschluss)] zu vorstehendem Gesetz:

> „Der Bundesrat bittet die Bundesregierung, einen Diskussionsentwurf für ein grundsätzlich überarbeitetes Datenschutzrecht vorzulegen, der die allgemeinen Regelungen im Bundesdatenschutzgesetz mit den bereichsspezifischen Vorschriften zusammenführt und systematisiert sowie das Datenschutzrecht angesichts neuer Formen und Techniken der Verarbeitung personenbezogener Daten risikoadäquat fortentwickelt."

Die Forderung des Bundesrates nach Rechtsvereinfachung und -vereinheitlichung steht in Einklang mit dem Beschluss der Landesregierung zu Leitlinien für Vorschriften- und Bürokratieabbau vom 21. Oktober 2008 (MBl. LSA S. 732). Hierzu heißt es in Abschn. II Nr. 4 des Beschlusses:

> „Die Bedeutung von Querschnittsgesetzen (wie zum Beispiel der Verwaltungsverfahrensgesetze des Bundes und des Landes Sachsen-Anhalt, des Gesetzes zum Schutz personenbezogener Daten der Bürger ...) ist weiter zu stärken. Diese wirken der Zersplitterung der Rechtsordnung in viele einzelne Sachgebiete entgegen. Das Anliegen, ein bestimmtes Sachgebiet in einem einzigen Gesetz möglichst umfassend zu regeln, hat zurückzutreten hinter das höherrangige Ziel, das betreffende Gesetz möglichst präzise in die bestehende Rechtsordnung einzufügen. Deshalb sind fachrechtliche Sonderregelungen zu streichen, soweit sie die Regelung eines schon vorhandenen Querschnittsgesetzes wiederholen. Ebenso sind Sonderregelungen, die von der Regelung eines solchen Querschnittsgesetzes inhaltlich abweichen, zu streichen, wenn kein sachlicher Grund für diese Abweichung besteht. ..."

Der Stellungnahme des Bundesrates liegt zudem die Erwägung zu Grunde, dass das geltende Datenschutzrecht noch zu sehr auf das Konzept der räumlich abgegrenzten Datenverarbeitung fixiert ist und nur unzureichend auf die Gefahren, aber auch Chancen neuer Techniken der Datenverarbeitung eingeht. Ein modernes Datenschutzrecht kann sich nicht mehr auf rein normative Vorgaben verlassen. Bestimmungen, die das Recht auf informationelle Selbstbestimmung einschränken, müssen Vorgaben für die Entwicklung und verbindliche Nutzung technischer Vorkehrungen enthalten, die einen datenschutzgerechten Ablauf des Verarbeitungsprozesses sichern. Dies entspricht den Vorstellungen des LfD.

Das Datenschutzrecht in Bund und Ländern muss internettauglich gemacht werden. Selbst wenn nur allgemein zugängliche Daten zusammengeführt werden, müssen im Interesse der Betroffenen rechtliche Vorgaben und technische Sicherungen der Bildung unerwünschter Persönlichkeitsprofile entgegenwirken. Auch sollte das Datenschutzrecht stärker als bisher dem Umstand Rechnung tragen, dass herkömmliche Papierakten mehr und mehr durch elektronische Aktenführung abgelöst werden. Zu beiden Komplexen bisher vereinzelt ergangene fachgesetzliche Regelungen in Bund und Ländern sollten im Interesse der Rechtsvereinheitlichung und -vereinfachung einander angeglichen bzw. im Rahmen des Möglichen durch Querschnittsregelungen im allgemeinen Datenschutzrecht abgelöst werden.

Mit dem neuen § 32 enthält das BDSG erstmals eine bereichsspezifische Regelung zum Arbeitnehmerdatenschutz, die nach § 12 Abs. 4 BDSG auch für Bundesbedienstete gilt. Diese Vorschrift findet nach § 1 Abs. 2 Nr. 2, § 12 Abs. 2 und § 27 Abs. 1 Satz 1 Nr. 2 Buchst. b BDSG auf Landesbedienstete keine Anwendung. Für unmittelbare und mittelbare Landesbedienstete ist der Umgang mit Personaldaten umfassender und detaillierter in den §§ 84 ff. des Landesbeamtengesetzes und in § 28 DSG-LSA geregelt. In Abstimmung mit dem LfD wird aber geprüft, inwieweit § 32 Abs. 1 Satz 2 BDSG, der die Verarbeitung und Nutzung von Personaldaten zu Zwecken der Aufdeckung von im Beschäftigungsverhältnis begangenen Straftaten regelt, bei der Auslegung bestehender landesrechtlicher Vorschriften zum Personaldatenschutz heranzuziehen ist oder ausdrücklich in Landesrecht umgesetzt werden soll. Grundlegende Änderungen im Landesrecht zum Umgang mit Personaldaten dürften erst dann erforderlich werden, wenn es im Bund zu der für die 17. Legislaturperiode des Deutschen Bundestages vorgesehenen Schaffung eines Arbeitnehmerdatenschutzgesetzes gekommen ist.

In Erfüllung des Gesetzgebungsauftrages des § 9a BDSG sollte in der 16. Legislaturperiode des Bundestages auch ein Datenschutzauditgesetz erlassen werden. Wenn öffentliche oder nicht-öffentliche Stelle auditierte – d. h. extern auf die Einhaltung datenschutzrechtlicher

Vorgaben überprüfte – Hard- und Software einsetzen, kann dies das Vertrauen der Bürger bzw. Kunden in den datenschutzgerechten Umgang mit ihren Daten erhöhen. Ein Gesetzentwurf der Bundesregierung aus dem Jahr 2008 sah vor, dass datenverarbeitende Stellen ihr Datenschutzkonzept und Anbieter von Datenverarbeitungsanlagen und -programmen diese von unabhängigen Stellen auf die Einhaltung datenschutzrechtlicher Vorgaben überprüfen lassen sollten und dafür ein Gütesiegel hätten verwenden dürfen. Die geplanten Regelungen erschienen allerdings vollzugsuntauglich und hätten unverhältnismäßigen Verwaltungsaufwand ausgelöst. Auf Grund dieser auch vom Bundesrat geübten Kritik wurde das Gesetz vom Deutschen Bundestag nicht verabschiedet. Vor einer gesetzlichen Regelung soll nun zunächst ein dreijähriges Pilotprojekt für eine Branche erfolgen (siehe BT-Drs. 16/13657, S. 27).

Zu 4.1 Die neue IT-Strategie des Landes Sachsen-Anhalt

Die StK hat ihre seit dem 1. Dezember 2006 bestehende Zuständigkeit zum Anlass genommen, die IT-Strategie unter Einbindung des LfD grundlegend zu überarbeiten. Datenschutz und Datensicherheit sind fester Bestandteil des IT-Managements, nicht zuletzt aufgrund der guten Zusammenarbeit mit dem LfD im IT-KA.

Die Anregung des LfD zur Einbindung der behördlichen Datenschutzbeauftragten bei der Umsetzung der IT-Strategie wird aufgegriffen.

Zu 4.2 Aufbau eines neuen zentralen IT-Dienstleisters – Landesrechenzentrum

Der Aufbau des zentralen IT-Dienstleisters erfolgt entsprechend dem Kabinettsbeschluss vom 14. November 2006 über die Änderung des Beschlusses der Landesregierung über den Aufbau der Landesregierung und die Abgrenzung der Geschäftsbereiche (MBl. LSA S. 723) durch das MF. Die LIS erarbeitet – mit dem IT-KA als integralem Bestandteil – die strategischen Vorgaben. Bei der technischen und organisatorischen Umsetzung durch das MF bzw. das LRZ wird auf die datenschutzkonforme Einrichtung und Übernahme der IT-Querschnittsdienste geachtet.

Zu 4.3 Grundkonzept IT-Architektur der Landesverwaltung

Das Konzept für IT-Infrastrukturdienste des Landes Sachsen-Anhalt zeigt unterschiedliche Architekturvarianten für den Aufbau eines gemeinsamen Namens- und Verzeichnisdienstes für die Landesverwaltung auf. Dieser Dienst bildet die Voraussetzung für die zukünftige Bereitstellung von Querschnittsdiensten durch das LRZ. Der LfD wurde frühzeitig in die Abstimmung des Konzeptes eingebunden. Die Fortschreibung der landesweiten IT-Architektur erfolgt in einer ressortübergreifenden Arbeitgruppe, in der auch der LfD vertreten ist.

Aufbauend auf der vom IT-KA beschlossenen zentral-integrierten Architekturvariante wurde vom Kompetenzteam „E-Mail/Intranet, Internet" das Grobkonzept „Verzeichnisdienst/Identity und Access Management" vorgelegt. Es skizziert die Anforderungen an einen zentralen Namens- und Verzeichnisdienst und die Identitäts- und Zugriffsverwaltung. Die Empfehlungen des LfD zum Umgang mit personenbezogenen Daten wurden berücksichtigt, u. a. durch die Möglichkeit eines chipkartenbasierten Anmeldeverfahrens und abgestufte Veröffentlichungsregeln für das zentrale Adressverzeichnis. Der LfD hat Recht, dass ein IT-Sicherheitskonzept für den zentralen Namens- und Verzeichnisdienst außerordentlich wichtig ist; deshalb wird der LfD frühzeitig in die Erstellung dieses Konzeptes eingebunden.

Die digitalen Identitäten der mit IT arbeitenden Landesbediensteten werden durch das geplante landesweite Personalmanagementsystem erzeugt und über die Identitäts- und Zugriffsverwaltung im zentralen Namens- und Verzeichnisdienst abgelegt. Durch ein Rollenmodell können auf diesem Wege den Mitarbeitern der Landesverwaltung einfach und sicher die Rechte zum Zugriff auf die notwendigen IT-Systeme zugewiesen werden. Dieses Vorgehen erhöht die Transparenz, reduziert System- und Prozessbrüche und ermöglicht die zuverlässige Umsetzung von gesetzlichen Vorgaben zum Datenschutz und zur Datensicherheit. Wegen der besonderen Anforderungen des Projektes ist eine Begleitung und Unterstützung durch den LfD unumgänglich.

Zu 4.4 Landesleitlinie IT-Sicherheit

Die Regelungen zum IT-Sicherheitsmanagement in der Landesverwaltung wurden letztmalig 2002 aktualisiert. Dabei wurde auf die Regelungen auf Bundesebene Bezug genommen. IT-

Sicherheitskonzepte sind danach an den Vorgaben des BSI auszurichten. Planungen zum Aufbau einer IT-Sicherheitsorganisation wurden in die IT-Strategie aufgenommen.

In einer Landesleitlinie „IT-Sicherheit“ werden die wesentlichen Ziele der IT-Sicherheit sowie die Strategie zu deren Umsetzung für die Landesverwaltung verbindlich festgelegt. Gemäß den Empfehlungen des BSI soll in jedem Ressort eine IT-Sicherheitsorganisation eingerichtet und für jedes Ressort ein IT-Sicherheitsbeauftragter benannt werden (orientiert an den Vorgaben des BSI nach Standard 100-1). Die Einrichtung von IT-Sicherheitsorganisationen liegt in der Verantwortung der Ressorts. Unter Berücksichtigung des Risikopotentials kann es je Ressort eine oder mehrere IT-Sicherheitsleitlinien und auch IT-Sicherheitsbeauftragte geben.

In der IT-Strategie wird anstelle von Leitlinien noch von IT-Sicherheitsrichtlinien gesprochen. Jetzt steht dieser Begriff für konkrete Sicherheitsregelungen für den Einsatz von IT-Verfahren – meist als Ergebnis der Erstellung eines Sicherheitskonzeptes. Bei der Einrichtung neuer IT-Verfahren auf Behördenebene und für ressortübergreifende Fachverfahren werden die dafür Verantwortlichen IT-Sicherheitskonzepte erstellen. Im IT-KA sind bereits Vereinbarungen getroffen worden, wonach das LIZ bei der Erstellung von Sicherheitskonzepten Unterstützung gewährt. Auch kann auf Erfahrungen des zentralen IT-Dienstleisters in Mecklenburg-Vorpommern mit dem GSTOOL für den IT-Grundschutz zurückgegriffen werden. Des Weiteren ist vorgesehen, den Zentralen IT-Dienstleister nach ISO 27001 zertifizieren zu lassen.

Zu 4.5 eGovernment Maßnahmenplan 2008-2009

Die Fortschreibung des eGovernment-Grundkonzeptes und des eGovernment-Aktionsplanes wird im ersten Quartal des Jahres 2010 erfolgen. Daneben wird der Government-Maßnahmenplan 2010-2011 erstellt. Das MI wird den LfD entsprechend den Vorgaben des § 14 Abs. 1 Satz 2 DSG-LSA und den dazu getroffenen Absprachen frühzeitig bei der Erarbeitung dieser Papiere einbinden.

Die Erfahrungen, unter anderem mit dem eGovernment-Maßnahmenplan 2008-2009, haben gezeigt, dass Belange des Datenschutzes und der Datensicherheit nicht erst bei der tatsächlichen Umsetzung der einzelnen eGovernment-Projekte berücksichtigt, sondern bereits bei strategischen Überlegungen und Zielsetzungen für solche Projekte bedacht werden müssen. Die Zusammenarbeit mit dem LfD liefert hierfür wichtige Impulse. Bei besonders bedeutenden und ebenenübergreifenden eGovernment-Vorhaben, z. B. der IT-Umsetzung

der EG-Dienstleistungsrichtlinie und der behördeneinheitlichen Rufnummer D115, ist deshalb eine ständige intensive Begleitung durch den LfD unerlässlich.

Zu 4.9 Geodateninfrastrukturgesetzgebung in Sachsen-Anhalt

Der LfD hat vorgeschlagen, Art und Umfang der von Kommunen außerhalb des Anwendungsbereiches des Geodateninfrastrukturgesetzes für das Land Sachsen-Anhalt gespeicherten Geodaten festzustellen. So könne ermittelt werden, wie dringlich eine eigenständige Regelung für diesen Datenbestand ist.

In Sachsen-Anhalt werden gegenwärtig die bei öffentlichen Stellen vorhandenen Geodatenbestände nach Art und Umfang gesichtet und bewertet, um über deren Einbeziehung in die Geodateninfrastruktur des Landes zu entscheiden. Dies gilt auch für vorhandene Geodaten auf kommunaler Ebene. Daher wird das MI mit ausgewählten Kommunen auf der Basis freiwilliger Beteiligung Pilotprojekte durchführen, um so bis spätestens Ende 2010 Art und Umfang der bei Kommunen gespeicherten Geodaten zu ermitteln. In die Bewertung der in den Pilotprojekten gewonnenen Erkenntnisse soll der LfD eingebunden werden.

Zu 7.1 Elektronischer Reisepass

Das MI hat den Passbehörden mit Runderlass vom 11. November 2008 die vom BSI erarbeitete Handreichung zur „Informationssicherheit für deutsche Passbehörden“ zur Beachtung übersandt. Die Handreichung gibt einen Überblick über organisatorische und technische Standard-Sicherheitsmaßnahmen (z. B. zur Gebäudesicherheit, zur Anbindung der eingesetzten IT-Systeme und zu lokalen Netzwerken innerhalb der Passbehörde), mit denen den Zielvorgaben des § 6 Abs. 2 DSG-LSA an technische und organisatorische Maßnahmen zur Gewährleistung der Datensicherheit genügt werden kann.

Die bei einer Passbehörde festgestellten Defizite im Verwaltungsvollzug wird das MI zum Anlass nehmen, die Passbehörden auf ihre Pflicht hinzuweisen, Passinhabern auf Antrag umfassend Einsicht in die im Chip ihres Passes gespeicherten Daten zu gewähren. Außerdem werden die Passbehörden angehalten, eventuell parallel zum Passregister vorgehaltene Unterlagen mit Lichtbildern oder der Wiedergabe von Unterschriften der Passinhaber zu vernichten.

Zu 7.3 Zentrales Bundesmelderegister

Nachdem dem Bund die ausschließliche Gesetzgebungskompetenz für das Meldewesen zugewiesen wurde, soll das Melderechtsrahmengesetz durch ein Bundesmeldegesetz abgelöst werden. Ein entsprechender Gesetzentwurf wurde im August 2008 vorgelegt. Die Stellungnahme des LfD hierzu hat das MI dem Bundesministerium des Innern zugeleitet. Ein überarbeiteter Gesetzentwurf liegt bislang nicht vor.

Nach bisherigem Kenntnisstand ist die Errichtung eines Bundesmelderegisters vorgesehen, in dem bestimmte – von den Meldebehörden täglich zu aktualisierende – Grunddaten aller Einwohner gespeichert werden sollen. Dieses Register soll Behörden und sonstigen öffentlichen Stellen des Bundes und gegebenenfalls auch der Länder zugänglich sein. Dann würden regelmäßige Datenübermittlungen der Meldebehörden an öffentliche Stellen des Bundes (z. B. an die Kreiswehrersatzämter, das Bundeszentralregister oder an das Bundeszentralamt für Steuern) entbehrlich werden, die bislang in der Zweiten Bundesmeldedatenübermittlungsverordnung geregelt sind.

Zu 9.1 Auskunftsrecht für Betroffene im Steuerverfahren

Das MF teilt nicht die Ansicht des LfD. Dies gilt zum einen für die Ausführungen des LfD zur Reichweite des Beschlusses des BVerfG vom 10. März 2009, zum anderen für die Annahme des LfD, das BDSG bzw. das DSG-LSA begründe Auskunftsrechte des Betroffenen im Besteuerungsverfahren gegenüber den Finanzämtern.

Das BVerfG hat nicht entschieden, dass ein umfassender Auskunftsanspruch für das gesamte Besteuerungsverfahren zu normieren ist. Der Beschluss betrifft nur Datensammlungen, die bei einer Bundesbehörde geführt werden. Gegenstand des Beschlusses sind Datensammlungen, bei denen die Daten entweder ohne Mitwirkung des Betroffenen erhoben werden oder deren Speicherung von dem ursprünglichen Erhebungszweck gelöst wird. Das ist aber bei Daten, die von den Finanzämtern im Besteuerungsverfahren erhoben, verarbeitet und genutzt werden, grundsätzlich nicht der Fall. Diese Daten beruhen in der Regel auf den Erklärungen der Steuerpflichtigen. Die Daten werden – für den Steuerpflichtigen vorhersehbar – ausschließlich für den Zweck „Besteuerungsverfahren“ verwendet.

Für die Landesfinanzbehörden gilt das BDSG grundsätzlich nicht. Auch kann der Landesgesetzgeber im Anwendungsbereich der AO 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 und im Anwendungsbereich der Abgabenordnung in den Ländern sind unterschiedliche steuerliche Verfahrensrechte unzulässig. Daher ist § 15 DSG-LSA im Besteuerungsverfahren nicht anwendbar.

Mit Schreiben vom 17. Dezember 2008 hat das BMF im Vorgriff auf eine gesetzliche Regelung in der AO im Verwaltungsweg einvernehmlich mit den Ländern einen generellen Auskunftsanspruch der Betroffenen im Besteuerungsverfahren anerkannt. Ein entsprechender Hinweis wird in die Verwaltungsvorschriften zum DSG-LSA aufgenommen. Durch die vorläufige Regelung im Verwaltungsweg ist zunächst eine gleichmäßige Rechtsanwendung gewährleistet. Die Anforderung der Darlegung eines berechtigten Interesses ist vor dem Hintergrund des Umfangs der im Besteuerungsverfahren gespeicherten Daten unumgänglich und verhältnismäßig. Darüber hinaus haben die Länder auf Nachfrage des BMF ermittelt, dass die übergangsweise Verwaltungsregelung bisher problemlos angewendet wurde.

Zu 9.6 Koordinierte neue Softwareentwicklung der Steuerverwaltung

Mit dem Vorhaben KONSENS, das auf der Basis eines ab 1. Januar 2007 in Kraft getretenen Verwaltungsabkommens realisiert wird, haben alle Länder den Weg zur länderübergreifenden, arbeitsteiligen und damit ressourcenschonenden Entwicklung von Software für das Besteuerungsverfahren eingeschlagen. Das Projekt FISCUS, an dem Bayern nicht beteiligt war, wurde mit dem Inkrafttreten des KONSENS-Abkommens beendet.

Zu 9.7 Unsichere Authentifizierung bei der ElsterOnline-Anmeldung

Das ElsterOnlinePortal (EOP) ist nur ein Teil des Verfahrens ELSTER und eröffnet für festgelegte Anwendungen eine Kommunikationsschnittstelle der Finanzverwaltung. Das Verfahren ELSTER insgesamt ist dabei nicht auf die Nutzung dieses Portals festgelegt, sondern bietet je nach Aufgabenstellung verschiedene Schnittstellen an. Das EOP wird als Schnittstelle im Verfahren ELSTER seit 2006 ergänzend zu kryptografischen Signatur- und

anderen Verfahren erfolgreich eingesetzt. Gesetzliche Grundlage des Verfahrens ist die Verordnungsermächtigung gemäß § 87a Abs. 6 AO. Diese ist zur Verfahrensevaluation zeitlich bis zum 31. Dezember 2011 begrenzt.

§ 150 Abs. 7 AO ist im Hinblick auf ab 2011 geltende Pflichten, Steuererklärungen obligatorisch elektronisch zu übermitteln, erlassen worden. Auch nach dieser Vorschrift kann neben kryptografischen Signaturverfahren ein anderes sicheres Verfahren, das die Authentizität und die Integrität des übermittelten Dokuments sicherstellt, zugelassen werden. Dies ermöglicht die Öffnung von Zugängen über das EOP.

Ein kryptografisches Verfahren bietet allein keinen angemessenen zusätzlichen Sicherheitsgewinn. Die Behauptung, die qualifizierte elektronische Signatur sei alternativlos, ist nicht zutreffend. Innerhalb und außerhalb der Verwaltungen des Bundes und der Länder sowie im Ausland sind auch andere Verfahren als sicher anerkannt und im Einsatz. Innerhalb weniger Jahre hat sich das EOP als effiziente, wirtschaftliche und sichere Kommunikationsplattform der Steuerverwaltung bewährt. Als zentrale Schnittstelle für Bürger, Behörden und Institutionen zur Steuerverwaltung wird sie stetig erweitert. Überdies lassen sich große Teile des Portal-Angebots-Portfolios nicht durch Signaturverfahren ersetzen. In diesem Zusammenhang von einer Fehlleitung investiver Mittel zu sprechen, ist unberechtigt.

Eine Gleichmäßigkeit der Besteuerung ist allein mit sicheren Verfahren möglich. Effektive Verschlüsselungsmechanismen bei der Datenübertragung sowie die sichere Verarbeitung und Speicherung der Daten sind obligatorische technische Anforderungen. Authentisierungsverfahren einschließlich aller Signaturverfahren ergänzen diesen Schutz um die Prüfung der Identität des Signierenden und der Unverfälschtheit des übersendeten Datenmaterials. Die durch die Steuerverwaltung eingesetzten elektronischen Kommunikationsverfahren sind auf die unterschiedlichen Sicherheitsstufen zugeschnittene risikoadäquate und gemeintaugliche Kommunikationsangebote, in deren Weiterentwicklung die Datenschutzbeauftragten des Bundes und der Länder im Interesse eines noch wirkungsvolleren Schutzes permanent eingebunden sind.

Zu 9.8 Einführung der Kraftfahrzeugsteuer-Rückständeprüfung in Sachsen-Anhalt

Seit dem 1. Juli 2009 ist die Ertrags- und Verwaltungskompetenz für die Kraftfahrzeugsteuer auf den Bund übergegangen. Der Bund bedient sich bei der Verwaltung der Kraftfahrzeugsteuer für einen Übergangszeitraum von längstens fünf Jahren im Wege der Organleihe der Finanzämter und der Zulassungsbehörden, soweit diese für Zwecke der Rückstandsprüfung als Finanzbehörde tätig werden. Dies ist in Sachsen-Anhalt der Fall, weil der Landesgesetzgeber mit § 3 Abs. 2 Satz 1 MZulKraftStG die Rückstandsprüfung auf die Zulassungsbehörden übertragen hat.

Die Landesfinanzbehörden gelten – soweit sie die Kraftfahrzeugsteuer verwalten – als Bundesbehörden und unterstehen insoweit gemäß § 18a Abs. 1 S. 1 und 2 FVG der Fachaufsicht des BMF. Die Kontrolle der Einhaltung datenschutzrechtlicher Belange bei der Verwaltung der Kraftfahrzeugsteuer obliegt damit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI). Daher wird von einer detaillierten Stellungnahme zu den Ausführungen des LfD zur Übermittlung der Rückstandsdatei an die Zulassungsstellen abgesehen. Das MF hat sich nicht nur aus Kostengründen für die dezentrale Lösung entschieden, sondern weil es das Verfahren nach § 30 Abs. 4 Nr. 1 AO für zulässig erachtet.

Zu 12.6 Einschulungsuntersuchungen/schulärztliche Untersuchungen

Die Ausführungen des LfD werden bei der Abfassung eines Erlasses, der eine landeseinheitliche Datenerhebung und -verarbeitung im Rahmen von Einschulungsuntersuchungen vorsieht, berücksichtigt.

Zu 14.1 Sozialdaten auf Laptops

Landesstandards für den Einsatz von Laptops werden durch die AG „Standards" des IT-KA entwickelt.

Eine Verschlüsselung von Daten auf Laptops ist bisher nicht durchgängig geregelt. Schon jetzt empfiehlt auch der IT-KA, Verschlüsselungssoftware zu verwenden und BSI-Empfehlungen für Sicherheitssoftware zu beachten. Die Bediensteten werden entsprechend belehrt. Außerdem ist beim Einsatz von Laptops der Grundsatz der Datensparsamkeit strikt zu beachten.

Zu 14.2 Fernwartung einer Firewall

Die IT-Sicherheitsrichtlinie des ITN-Betreibers enthält konkrete Vorgaben für Fernwartungsverbindungen. Die Übergänge vom ITN-LSA in Fremdnetze, hierzu zählen ausdrücklich auch analoge Modem-, ISDN- und xDSL-Zugänge mit direkter oder indirekter Verbindung zum ITN-LSA, werden grundsätzlich zentral durch den ITN-Betreiber eingerichtet und administriert. Wenn ein ITN-Nutzer eigene Übergänge in Fremdnetze benötigt, dürfen diese nur im Einvernehmen mit dem ITN-Betreiber und nach Genehmigung durch die LIS errichtet und betrieben werden.

Bei der Einführung neuer Fachanwendungen, die die Transportwege des ITN-LSA nutzen, hat der ITN-Nutzer den ITN-Betreiber schon in der Planungsphase zu beteiligen. Dies gilt insbesondere bei „remote-Zugriffen“ (Zugriffen aus der Ferne) für Wartungs- und Installationsarbeiten durch Dritte. Solche Zugriffe sind auf das unumgängliche Maß zu beschränken und stets von der aktiven Mitwirkung des Auftraggebers abhängig zu machen. Der ITN-Nutzer hat alle notwendigen Maßnahmen umzusetzen und zu dokumentieren, um Gefahren für das ITN-LSA und die anderen ITN-Nutzer durch die in seiner Verantwortung betriebene IT zu vermeiden. Hierzu wird nach Bedarf im IT-KA berichtet, um alle Teilnehmer, auch die kommunalen Spitzenverbände, zu sensibilisieren.

Zu 14.5 Die elektronische Signatur in der Verwaltung

Mit Runderlass des MI vom 14. März 2006 „Organisation und Aufgaben der Sicherheitsinfrastruktur des Landes Sachsen-Anhalt" erfolgte die Einführung der elektronischen Signatur in der Landesverwaltung. Im November 2008 trat eine Organisationsänderung ein, weil die dezentralen Registrierungsstellen durch das POST-IDENT-Verfahren abgelöst wurden.

Die Public Key Infrastruktur (PKI) des Landes arbeitet mit qualifizierten Zertifikaten der TeleSec Public Key Service (PKS), um elektronische Unterschriften (Signaturen) und fortgeschrittene Zertifikate der TESTA-PKI zur Verschlüsselung zu erstellen. Danach werden getrennte Schlüsselpaare für die Signatur (laut Signaturgesetz) und die Verschlüsselung verwendet.

Die Ausführungen des LfD zur Signaturprüfung werden zum Anlass genommen, hierfür in Zusammenarbeit mit dem LfD sachgerechte Lösungen zu finden.

Zu 14.7 Sicherheit des Windows Encrypted File Systems (EFS)

MS Windows Betriebsysteme ab Version 2000 bieten die Möglichkeit, das Dateisystem per EFS zu verschlüsseln. Allerdings hat EFS einige Nachteile. So bleiben trotz Datei- und Verzeichnisverschlüsselung die Dateinamen und die Verzeichnisstruktur sichtbar. Dies gibt einem potentiellen Angreifer nicht nur Hinweise auf die Art der Daten, sondern ermöglicht sogar, die Dateien zu kopieren und sie ungestört mit einer „Brute-Force-Attacke“ (Durchprobieren aller potentiellen Lösungen) zu entschlüsseln. Schwierigkeiten kann es auch mit Antivirenprogrammen geben, da diese keinen Zugriff auf die verschlüsselten Dateien haben. Wird für diesen Zweck ein Konto für einen Wiederherstellungsagenten angelegt und der Virenschutz unter diesem Konto gestartet, bekommt dieser zwar Zugriff auf die Dateien, aber das System weist eine zusätzliche Schwachstelle auf. Der Administrationsaufwand, der betrieben werden muss, um Daten vor Verlust zu schützen, wenn z. B. das Passwort des Nutzers vom Administrator zurückgesetzt wird oder das Nutzerkonto gelöscht wurde, ist sehr hoch. Zur Verschlüsselung lokaler Daten wird aus diesem Grund auch Lösungen von Drittanbietern der Vorzug gegeben. Im Rahmen der Standardisierung ist die Erarbeitung von Sicherheitsstandardanwendungen zur Verschlüsselung geplant.

Zu 14.8 Datenschutzgerechte Webserver-Logs

Für die Speicherung von IP-Adressen beim LIZ wurde zusammen mit dem LfD eine Lösung gefunden. Für die kurzfristige Speicherung von IP-Adressen wird durch den zentralen IT-Dienstleister die Anregung des LfD geprüft, das Erweiterungsmodul zur IP-Anonymisierung an Web-Servern zu nutzen.

Zu 14.10 BlackBerry-Einsatz sicher gestaltbar

Zum BlackBerry-Einsatz in der Landesverwaltung hat das TPA Empfehlungen herausgegeben, die auch organisatorische Regelungen zur IT-Sicherheit vorsehen. Mit der Übernahme der IT-Querschnittsdienste durch den zentralen IT-Dienstleister soll es eine zentrale einheitliche Administration des BlackBerry-Einsatzes geben. Wenn die Konfigurationsempfehlungen des LfD vorliegen, sollen diese beachtet werden. Allerdings löst auch eine sichere Konfiguration nicht alle Sicherheitsbedenken, die sich aus der BlackBerry-Architektur ergeben.

Die Polizei verzichtet auf den Einsatz der Blackberry-Technik; sie nutzt die IR-Infrastrukturkomponente „SALSA“.

Zu 14.11 Offene Verteilerlisten in Rundschreiben per E-Mail

Wenn beim Versenden von E-Mails die CC-Funktion verwendet wird, erkennt jeder Adressat, wer die E-Mail noch erhalten hat. Er erfährt auch die dazugehörigen E-Mail-Adressen. Dies ist bei der Abstimmung zwischen öffentlichen Stellen in der Regel erforderlich: Grundsätzlich müssen die jeweiligen Adressaten schon aus Gründen der Transparenz der Verwaltungsverfahren wissen, welche anderen öffentlichen Stellen in ihren jeweiligen Belangen berührt sind und deshalb in das Abstimmungsverfahren einbezogen wurden. Anders kann es sich bei privaten Adressaten verhalten. Mit der BCC-Funktion kann auf einfache Weise verhindert werden, dass ungewollt und unbefugt komplette E-Mail-Verteilerlisten an alle Adressaten einer E-Mail versendet werden. Hierauf werden die Mitarbeiter der Landesverwaltung in geeigneter Weise hingewiesen.

Eine technische Unterstützung durch Listenmanagement-Funktionen wird erwogen.

Zu 14.12 Hinweise zur Absicherung von Wireless-LAN

Kabellose Netzwerkverbindungen, z. B. Wireless-LAN-Verbindungen, dürfen in der Landesverwaltung wegen der damit verbundenen Risiken nur ausnahmsweise genutzt werden. Daher ist nach der IT-Sicherheitsrichtlinie des ITN-Betreibers die Einrichtung solcher Verbindungen dem ITN-Betreiber mit der Darstellung der vorgesehenen Sicherheitsmaßnahmen vorab anzuzeigen und durch diesen zu genehmigen. Wireless-LAN dürfen nur nach dem neuesten Stand der Technik betrieben werden. Der ITN-Betreiber ist berechtigt, für derartige Verbindungen Auflagen zu erteilen und deren Einhaltung zu überprüfen. Einen unkontrollierten Einsatz von Funknetzen in lokalen Netzen der Landesverwaltung wird es nicht geben.

Zu 14.14 Telearbeit

Um neue Perspektiven für die Integration von Beruf, Freizeit und Familie zu eröffnen, wird auch öffentlichen Bediensteten auf deren Wunsch in geeigneten Fällen die Möglichkeit von Telearbeit eröffnet. Die Regel ist alternierende Telearbeit. Dabei wird ein Großteil der Arbeitszeit am häuslichen Arbeitsplatz verbracht; der Telearbeiter ist aber zu vereinbarten Zeiten an seinem Arbeitsplatz in der Dienststelle.

Noch gibt es keine landeseinheitlichen Standards für die Bewilligung und die Ausgestaltung von Telearbeit, wohl aber Dienstvereinbarungen, Hausverfügungen usw.. Regelmäßig bestehen generelle oder einzelvertragliche Regelungen, die darauf gerichtet sind, den besonderen Anforderungen an Datenschutz und Datensicherheit, wie sie im Bericht des LfD beschrieben sind, zu genügen. Innerhalb der unmittelbaren Landesverwaltung können bei alternierender Telearbeit dienstlich zur Verfügung gestellte Laptops sowohl in der Dienststelle als auch am häuslichen Arbeitsplatz über das Verfahren „SALSA“ zur gesicherten Netzeinwahl in das landeseigene Netz und in das jeweilige Hausnetz genutzt werden. So können Daten grundsätzlich auf dem zentralen Server der Dienststelle gespeichert werden, ohne redundant auf dem Laptop vorgehalten zu werden. Hierdurch und durch weitere technisch-organisatorische Maßnahmen können die Schutzziele des § 6 Abs. 2 DSG-LSA erreicht werden.

Der vorstehend beschriebene Einsatz dienstlich zur Verfügung gestellter Laptops ist nicht mit nennenswerten Mehrkosten für die Verwaltung verbunden. Gleichwohl muss der Einsatz privater Hard- und Software bei Telearbeit nicht generell ausgeschlossen sein. Dies gilt dann, wenn Arbeitsergebnisse nicht in dienstliche Anwendungen übernommen werden und bei der Verarbeitung personenbezogener Daten sichergestellt ist, dass den Anforderungen des § 6 DSG-LSA genügt wird. So ist z. B. Lehrkräften des Landes nach einem RdErl. des MK vom 15. März 1995 (MBl. LSA S. 472) unter gewissen Voraussetzungen gestattet, Daten von Schülern auf privaten Rechnern zu verarbeiten. Der LfD war an dieser Regelung beteiligt.

Das MI erwägt, den Entwurf seiner Dienstvereinbarung nebst dazugehörigen Mustern für Individualvereinbarungen, Merkblätter usw. den übrigen Ressorts vorzustellen, um abzuklären, ob unter Einbindung der zuständigen Personalvertretungen und des LfD eine Musterdienstvereinbarung „Telearbeit“ erarbeitet werden soll. Solche Musterdienstvereinbarungen existieren bereits in mehreren Ländern.

Zu 16.3 Bezüge einzelner Geschäftsführer im Beteiligungsbericht

Nach § 118 GO LSA sind die Kommunen, die sich im Rahmen der §§ 116 ff. GO LSA wirtschaftlich betätigen, verpflichtet, einen Bericht über ihre unmittelbaren und mittelbaren Unternehmensbeteiligungen zu erstellen. Der Beteiligungsbericht ist ein Informationsinstrument sowohl für die Mitglieder des Gemeinderates als auch für die Öffentlichkeit. Er ist nach § 118 Abs. 2 GO LSA dem Entwurf der Haushaltssatzung als Anlage beizufügen und im Gemeinderat (bzw. im Kreistag) in öffentlicher Sitzung zu erörtern. Nach § 118 Abs. 3 GO LSA sind die Einwohner über den Beteiligungsbericht in geeigneter Weise zu unterrichten.

Der Beteiligungsbericht soll Angaben über die Gesamtbezüge der Mitglieder der Organe des Unternehmens nach § 285 Nr. 9 Buchst. a HGB enthalten, mithin nicht Angaben über die Bezüge Einzelner. Nach § 286 Abs. 4 HGB kann von einer Angabe der Gesamtbezüge abgesehen werden, wenn sich anhand der Angaben die Bezüge eines einzelnen Organmitgliedes feststellen lassen. Regelmäßig wird das private Interesse der betroffenen Person an einer Nichtveröffentlichung entsprechender Angaben überwiegen. Nach § 118 Abs. 2 Satz 2 Nr. 4 GO LSA in der Fassung, die diese Vorschrift durch das Zweite Gesetz zur Fortentwicklung des Kommunalverfassungsrechts vom 26. Mai 2009 (GVBl. LSA S. 238) erhalten hat, findet § 286 Abs. 4 HGB sinngemäß Anwendung.

Um sicherzustellen, dass die Mitglieder des Gemeinderates (Kreistages) gleichwohl Kenntnis über die Höhe der Vergütung einzelner Geschäftsführer erhalten, wird den Kommunen geraten, die entsprechende Information im Rahmen einer nichtöffentlichen Sitzung des Gemeinderates (Kreistages) zu geben.

Zu 17.5 Daten bei der Personalvertretung

Sofern Personalvertretungen im Rahmen ihrer Aufgabenstellung nach dem PersVG LSA personenbezogene Daten speichern, besteht regelmäßig die Möglichkeit der Speicherung auf zentralen Servern oder dienstlich zur Verfügung gestellten Laptops. Die Speicherung erfolgt passwortgeschützt, so dass nur derjenige einen Zugriff auf gespeicherte Daten erhält, der eine entsprechende Berechtigung nachweist. Der Zugriff durch einen Systemadministrator ist nur mit Einverständnis des Berechtigten zulässig. Darüber hinaus können die Personalvertretungen bei Bedarf dienstlich bereitgestellte Verschlüsselungssoftware

einsetzen, die auch zur Verschlüsselung mobiler Datenträger oder von E-Mail-Anhängen geeignet ist.

Zu 17.8 Polizeiliche Auskunftssysteme und Zentralregisterauskunft

Zum geplanten Umgang mit unbeschränkten Auskünften aus dem Bundeszentralregister im Auswahlverfahren für Bewerber an der Fachhochschule der Polizei in Aschersleben hat das MI dem LfD mit Schreiben vom 6. März 2009 mitgeteilt:

> „Hinsichtlich der beabsichtigten Einholung einer unbeschränkten Auskunft nach § 41 Abs. 1 Nr. 2 BZRG durch das MI teile ich Ihre Bedenken nicht.
>
> Für oberste Bundes- und Landesbehörden sieht § 41 Abs. 1 Nr. 2 BZRG – im Gegensatz zu Nrn. 1 und 3-10 – ausdrücklich keine Zweckbegrenzung vor, d. h., sie erhalten diese Auskünfte für jeden Zweck. Der Zweck ist nach § 41 Abs. 4 anzugeben und die Auskunft darf nur für diesen Zweck verwendet werden (siehe auch Hase, Bundeszentralregistergesetz, Kommentar, München 2003, § 41 Rz. 3). Eine Umgehung der Vorschriften des BZRG vermag ich insoweit nicht zu erkennen.
>
> Dies gilt ebenso hinsichtlich der beabsichtigten Weiterleitung der unbeschränkten Auskünfte über abgelehnte Bewerber an die FH Pol für eventuelle gerichtliche Verfahren, wenn der Bewerber sein Einverständnis erklärt hat. Denn die Erklärung ist lediglich für die Frage entscheidend, ob in einem später eventuell geführten Rechtsstreit das MI oder die FH Pol Verfahrensgegner des abgelehnten Bewerbers wird.
>
> Bei der Auswertung der unbeschränkten Auskünfte durch das MI spielt sie keine Rolle, da dem MI lediglich die Namen der Bewerber, die die Auswahlgespräche positiv durchlaufen haben, mitgeteilt werden, nicht jedoch, ob diese Bewerber in die Übermittlung der Inhalte einer unbeschränkten Auskunft eingewilligt haben. Nach erfolgter Auswertung der unbeschränkten Auskünfte durch das MI erhält die FH Pol lediglich eine Liste der für eine Ernennung in Frage kommenden Bewerber, nicht jedoch die Auskünfte aus dem BZRG selbst. Diese würden erst dann zum Bestandteil des Bewerbungsverfahrens und vom MI an die FH Pol übermittelt, wenn ein Bewerber gegen seine Ablehnung gerichtlich vorgehen will und in die Übermittlung zuvor eingewilligt hat.
>
> Um jedoch gänzlich den Eindruck zu vermeiden, dem Bewerber könnten durch die Nichteinwilligung in die Weiterleitung der Inhalte der unbeschränkten Auskunft aus dem BZRG Nachteile im Bewerbungsverfahren entstehen, werde ich die FH Pol bitten, die „Erklärung über die Übermittlung von Erkenntnissen aus dem Bundeszentralregister-

gesetz an die FH Polizei“ sowie den Hinweis b) zur Belehrung (siehe Anlage 2 des Bezugsschreibens) zu streichen und gesondert lediglich jenen abgelehnten Bewerbern vorzulegen, die gegen ihre Ablehnung Widerspruch eingelegt haben.“

Die Reaktion des LfD steht noch aus.

Zu 17.9 PersonalServiceCenter

Das PersonalServiceCenter (PSC) arbeitet ressortübergreifend mit dem Ziel, die Ressorts bei der Umsetzung des von der Landesregierung beschlossenen Stellen- und Personalabbaukonzeptes zu unterstützen. Hierfür übersenden die Ressorts nach dem Gem. RdErl. vom 15. März 2007 (MBl. LSA S. 333) dem PSC Angaben über auf Planstellen bzw. Stellen der Titelgruppe 96 geführte Personen sowie – auf Anforderung des PSC – auch Angaben über vergleichbare Landesbeschäftigte mittels des bereitgestellten elektronischen Vordrucks "Personalprofil". Daneben können sich Landesbeschäftigte, die eine andere Verwendung anstreben, mit dem Vordruck „Kurzbewerbung" beim PSC mit der Bitte um Vermittlung oder um Teilnahme an einer Qualifizierungsmaßnahme bewerben. Bestandteil der Vordrucke sind von den betroffenen Landesbeschäftigten abzugebende Einwilligungserklärungen.

Nach einem Hinweis, dass die Muster der Einwilligungserklärungen nicht den Anforderungen des § 4 Abs. 2 DSG-LSA entsprachen, wurden diese in Abstimmung mit dem LfD überarbeitet. Die neuen Muster der Einwilligungserklärungen sind zwischenzeitlich als Anlage zu den Vordrucken „Personalprofil" und „Kurzbewerbung" im Intranet bereitgestellt. Die Personaldienststellen der Ressorts sind gebeten worden, die alten Vordrucke nicht mehr zu verwenden.

Auch dem Hinweis des LfD, dass bei der Erhebung von Personalaktendaten ohne Einwilligung der Betroffenen die begrenzten Übermittlungsregelungen des § 88 des landesbeamtengesetzes i. V. m. § 28 DSG-LSA zu beachten sind, wird Rechnung getragen. Personalaktendaten werden seitens des PSC ohne Einwilligung der Betroffenen nicht erhoben.

Zu 18.2 Datenschutz bei der Polizei

Wie vom LfD ausgeführt, haben die Polizeibehörden und –dienststellen nach einem RdErl. des MI vom 27. August 2008 (MBl. LSA S. 676) weiterhin den Dienstweg einzuhalten, wenn Stellungnahmen gegenüber dem LfD im Zusammenhang mit Kontrollen stehen oder solche

Auskunftsersuchen des LfD beantwortet werden, die Angelegenheiten von grundsätzlicher landesweiter Bedeutung betreffen. Antworten auf sonstige Auskunftsersuchen erhält das MI nachrichtlich.

Diese Verfahrensweise ist festgelegt worden, damit das MI seiner Verantwortung nach § 14 Abs. 1 DSG-LSA nachkommen kann. Der LfD wird dadurch in seiner Arbeit nicht behindert. Für eine zügige Weiterleitung von Stellungnahmen und Antworten aus dem nachgeordneten Bereich an den LfD ist gesorgt. Das Verfahren hat den Vorteil, dass bei erkannten Defiziten im Datenschutz oder der Datensicherheit unverzüglich fach- bzw. dienstaufsichtlich reagiert werden kann. Auch erhält der LfD sofort Kenntnis, wenn das MI die Stellungnahme einer nachgeordneten Polizeidienststelle nicht in allen Punkten teilt.

Zu 18.5 Videoüberwachung öffentlicher Plätze

Gemäß § 16 Abs. 2 Satz 2 SOG LSA kann die Polizei an „verrufenen Orten“ Bildaufnahmen oder -aufzeichnungen anfertigen. Die Polizeibehörden prüfen bei jeder einzelnen Maßnahme im Abstand von zwei bis sechs Monaten, ob die rechtlichen Voraussetzungen noch vorliegen, und entscheiden sodann über die Fortsetzung bzw. Einstellung der Maßnahme.

Zu 18.8 Beschwerdestelle Polizei

Die Zentrale Beschwerdestelle Polizei ist am 1. September 2009 als Stabsstelle des MI, die unmittelbar dem Staatssekretär zugeordnet ist, eingerichtet worden. Die Zentrale Beschwerdestelle hat ihren Sitz im Technischen Polizeiamt, Halberstädter Straße 69, 39112 Magdeburg. Ihr obliegt die abschließende Bearbeitung aller die Polizei des Landes Sachsen-Anhalt betreffenden Beschwerden, die direkt an sie bzw. das MI gerichtet sind.

Zu 18.13 Protokollierung von Datenabfragen beim Technischen Polizeiamt

Bei dem fehlenden Protokolldatensatz über die Abfrage eines Kfz-Kennzeichens handelte es sich um einen Einzelfehler, dessen Ursache im Nachhinein nicht feststellbar war. Technische Überprüfungen haben ergeben, dass eine Wiederholung mit hoher Wahrscheinlichkeit ausgeschlossen werden kann. Dennoch werden seitdem die Protokolldaten in unregelmäßigen Abständen durch die fachliche Leitstelle des TPA auf Auffälligkeiten überprüft.

Zu 18.16 Speicherung im polizeilichen Informationssystem INPOL

Das BMI prüft unter Berücksichtigung der vom LfD angeführten Entscheidung des Niedersächsischen Oberverwaltungsgerichtes, ob zu INPOL eine Rechtsverordnung zu erlassen ist.

Zu 19. Rechtspflege

Zu 19.1 Allgemeines

Das MJ wird in den bereits angelaufenen Fortbildungsveranstaltungen zum Datenschutz die vom LfD angesprochenen Themen „Erstellung von Verfahrensverzeichnissen“ und „Datenverarbeitung im Auftrag“ ansprechen, um evtl. vorhandene Unsicherheiten im Umgang hiermit zu beseitigen. Diese Themen gehören auch zum Katalog der durch einen externen Sachverständigen zu erarbeitenden Handlungsanweisungen zum Umgang mit dem Datenschutz in der Justiz. Darüber hinaus bietet das MJ seinem Geschäftsbereich Hilfestellungen bei der mitunter nicht einfachen Erstellung der Verfahrensverzeichnisse.

Die ADV-Stelle Justiz erstellt für die in ihrer Zuständigkeit liegenden Fachverfahren die Verfahrensverzeichnisse in eigener Zuständigkeit und stellt sie den betroffenen Dienststellen zur Verfügung. Ebenso führen die Generalstaatsanwaltschaft und der Justizvollzug die Verfahrensverzeichnisse in eigener Zuständigkeit.

Zu 19.2 Telekommunikationsüberwachung überarbeitet – Vorratsdatenspeicherung eingeführt

Die Ausführungen des LfD betreffen im Schwerpunkt den Regelungsinhalt des zum 1. Januar 2008 in Kraft getretenen Gesetzes zur Neuregelung der Telekommunikation und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 9. November 2007 (BGBl. I S. 3198). Hierzu äußert sich die Landesregierung unter Hinweis auf die Vorbemerkung nicht.

Soweit die Landesregierung konkret angesprochen wird, sei darauf hingewiesen, dass sie entsprechend dem Beschluss des Landtages vom 27. Juni 2008 – Drs. 5/42/1333 B – in den Ausschüssen für Recht und Verfassung sowie für Inneres über die Anwendung der in

§ 100g StPO geregelten sogenannten Vorratsdatenspeicherung in Sachsen-Anhalt berichtet und sich hinsichtlich der Auskunftserteilung über Telekommunikationsverbindungsdaten positioniert.

Zu 19.3 Verfolgung der Absicht der Vorbereitung von Terrordelikten

Das „Gesetz zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten“ ist am 4. August.2009 in Kraft getreten.

Zu 19.4 Videotechnik in der Justiz

Der LfD befasst sich ausführlich mit den Auswirkungen der Installation von optisch-elektronischen Einrichtungen am Justizzentrum Magdeburg. Eine Wiederholung des geschilderten Sachverhalts ist entbehrlich, weil er sowohl Gegenstand umfangreicher Erörterungen im Ausschuss für Recht und Verfassung des Landtages von Sachsen-Anhalt als auch ausführlicher Presseberichterstattung war. Der LfD hat, wie im Tätigkeitsbericht ausgeführt, den Sachverhalt abschließend gewürdigt; eine förmliche Beanstandung wurde nicht erhoben.

Festzuhalten bleibt:
Zum Schutz der dort Beschäftigten und zur Wahrung der Integrität des Gebäudes des Justizzentrums Magdeburg bestand und besteht die dringende Notwendigkeit einer optisch-elektronischen Beobachtung.

Die Landesregierung legt Wert auf die Feststellung, dass hierbei die Vorgaben des DSG-LSA, namentlich des § 30, im Interesse der Wahrung des verfassungsrechtlich verbürgten Rechts auf informationelle Selbstbestimmung der Bürger peinlich genau zu beachten sind. Das bedeutet, dass die Voraussetzungen, unter denen eine Videoüberwachung eines solchen öffentlichen Gebäudes installiert werden darf, einer genauen Prüfung zu unterziehen sind. Deshalb hat das MJ unmittelbar nach Bekanntwerden der datenschutzrechtlichen Mängel alle notwendigen Maßnahmen getroffen, um nicht nur diese Mängel unverzüglich abzustellen, sondern auch auf eine Sensibilisierung aller öffentlichen Stellen seines Geschäftsbereichs hingewirkt, um auszuschließen, dass sich Mängel vergleichbaren Ausmaßes andernorts wiederholen.

Neben der sofort angeordneten dauerhaften Zerstörung der in den Videokameras herstellerseitig eingebauten Audiofunktionen, welche von den Nutzern nicht bestellt worden waren, ist ein Datenschutz-Paket geschnürt worden, das weit über den Anlass hinausgeht. Die sieben zentralen Punkte des Pakets werden zu Recht vom LfD zitiert.

Der konkrete Vorfall im Justizzentrum Magdeburg sollte allerdings nicht zu der Fehleinschätzung verleiten, dass die Mängel symptomatisch für einen gedankenlosen Umgang mit personenbezogenen Daten in der Justiz wären. Aus dem Dienstverkehr des MJ ist bekannt, dass allenthalben die Notwendigkeit anerkannt ist, die berechtigten Interessen der Bürgerinnen und Bürger an der Wahrung des verfassungsrechtlich geschützten Rechts auf informationelle Selbstbestimmung zu schützen, wenn es darum geht, die Funktionstüchtigkeit der Justiz zu wahren und Angriffe auf sensible Bereiche der Justiz und der Verwaltung abzuwehren. Deshalb sind die im Sommer 2009 in Halle und Magdeburg durchgeführten Auftaktveranstaltungen einer Fortbildungsreihe zum Datenschutz, an denen der LfD dankenswerterweise beteiligt ist, mit einer Gesamtteilnehmerzahl von ca. 100 Personen auf große Resonanz gestoßen. Die Reihe wird mit speziellen Themenschwerpunkten fortgesetzt.

Das MJ ist zudem davon überzeugt, dass die Vielzahl rechtlicher und tatsächlicher Fragestellungen, die sich aus dem Umgang mit dem Datenschutz in der Justiz ergeben, die Herausgabe von Handlungsanweisungen angezeigt erscheinen lassen. Diese sollen die Arbeit der Praktiker in den Bereichen der Gerichtsbarkeit, Staatsanwaltschaft und Verwaltung erleichtern. Das MJ hat hierfür einen ausgewiesenen Fachmann gewinnen können, nämlich Herrn Prof. Dr. Ralf B. Abel, Schleswig/Schmalkalden. Er ist Herausgeber der Monographie „Datenschutz in Anwaltschaft, Notariat und Justiz“ und bietet nach Auffassung des MJ Gewähr, dass Vorschläge entwickelt werden, die jedem Anwender eine echte Hilfe und praktischen Mehrwert bieten werden. Die Bereitschaft des LfD, in diesem Prozess mitzuwirken, wird ausdrücklich dankend begrüßt.

Zu 19.5 Namen von Verfahrensbeteiligten auf Monitoren im Eingangsbereich eines Justizzentrums

Der LfD bemängelt, dass auf Monitoren im öffentlichen Eingangsbereich eines Justizzentrums neben dem Namen der Verfahrensbeteiligten gerichtlicher Verfahren auch der Vorname eingeblendet wird. Die Angabe des Vornamens sei für die Wahrung des Öffentlichkeitsgrundsatzes und die Bezeichnung der Verhandlung nicht erforderlich. Unabhängig

davon, dass darauf zu achten sein wird, den der Kontrollbefugnis des LfD nicht unterliegenden Bereich der Rechtsprechung nicht zu tangieren, dürfte die Angabe des Vornamens der vollständigen Information der Öffentlichkeit über die Verfahren dienen. Grundsätzlich gehört der Vorname zur sicheren Kennzeichnung einer Person.

Zu 19.6 Schülergremien

Die noch im VIII. Tätigkeitsbericht des Landesbeauftragten unter 18.7 aufgezeigten Problemkreise hat der Landesbeauftragte zwischenzeitlich ausweislich seiner neuerlichen Stellungnahme zum Punkt „Schülergremien“ als beseitigt oder offensichtlich relativiert angesehen. So werden die Bedenken an der Verhältnismäßigkeit eines Schülergerichtsverfahrens nicht mehr aufgegriffen. Auch § 45 Abs. 2 des Jugendgerichtsgesetzes als Ermächtigungsgrundlage für die Einschaltung eines Schülergremiums wurde nicht beanstandet. Allerdings sieht der LfD diese Vorschrift nicht als ausreichende Befugnisnorm für eine Datenübermittlung an private Dritte an. Daraus zieht er aber nicht den Schluss einer Unzulässigkeit, sondern sieht die hierbei erfolgende Datenübermittlung als von den §§ 10 und 12 DSG-LSA hinreichend gedeckt an. Die Landesregierung teilt diese Einschätzung.

Der weiterhin angesprochene Punkt der Verschwiegenheitsverpflichtung von Schülerrichtern nach dem Verpflichtungsgesetz und die hiergegen nach wie vor erhobenen Zweifel relativiert der LfD in seinen Ausführungen sogleich selbst. Er führt aus, dass jedenfalls der wesentliche Sinn des Verpflichtungsvorgangs, nämlich seine besondere Warnfunktion und damit auch seine Schutzfunktion hinsichtlich der im Schülergremium bekannt werdenden persönlichen Daten, in der Regel erreicht werden könne. Diese Einschätzung ist zutreffend. Bis zum heutigen Tage sind keine Fälle bekannt geworden, in denen ein irgendwie gearteter Verstoß datenschutzrechtlicher Belange festgestellt worden wäre. Zur Wirksamkeit der Verpflichtungserklärung ist anzumerken, dass auf Grund der Minderjährigkeit der Betroffenen bei Abgabe der Verpflichtungserklärung regelmäßig darauf geachtet wird, dass hierzu die Genehmigung der gesetzlichen Vertreter vorliegt. Entsprechend ist auch das Formular ausgestaltet.

Zu 19.8 Justizaktenaufbewahrung

Das Gesetz zur Aufbewahrung von Schriftgut der Justiz im Land Sachsen-Anhalt (JSchrG LSA) vom 19. Juni 2008 (GVBl. LSA S. 236) ist am 1. Juli 2008 in Kraft getreten. In

Ausführung des Gesetzes wurde mit Verordnung vom 16. Juni 2009 (GVBl. LSA S. 264) das Nähere über die bei der Aufbewahrung von Schriftgut zu beachtenden Aufbewahrungsfristen für die Gerichte der ordentlichen Gerichtsbarkeit, die Staatsanwaltschaften, die Justizvollzugsbehörden und den Sozialen Dienst der Justiz des Landes Sachsen-Anhalt bestimmt. Entsprechende Bestimmungen für die Fachgerichtsbarkeiten liegen den Gerichten derzeit zur abschließenden Prüfung vor und werden voraussichtlich noch im Jahr 2009 erlassen.

Zu 19.9 Abfrage von Kreditkartendaten in einem Ermittlungsverfahren

Unter Hinweis auf die Entscheidung des BVerfG vom 17. Februar 2009 (NJW 2009, 1405) erörtert der LfD noch einmal die Rechtmäßigkeit der sog. „Kreditkarten-Rasterfahndung“ im Ermittlungsverfahren wegen des Besitzes und der Verbreitung von Kinderpornographie (§ 184b StGB). Dieses Verfahren war bundesweit unter dem Begriff „Operation Mikado“ bekannt geworden und hatte zu einer streitigen öffentlichen Diskussion geführt.

Im Ergebnis tritt der LfD der vom BVerfG bestätigten Rechtsauffassung der Staatsanwaltschaft Halle bei und stellt unter Hinweis auf seine früheren Ausführungen nochmals die Rechtmäßigkeit dieser Ermittlungsmaßnahme fest.

Zu 19.10 Zwangsversteigerung und Internet

Am 10. Dezember 2008 ging im MJ das Schreiben des LfD ein, in dem er um Mitteilung bat, ob es sich bei der zum Anlass genommenen Internetveröffentlichung des Wertgutachtens in der Zwangsversteigerung um ein landesweit vergleichbar gehandhabtes Verfahren handelt und wie diese Verfahrensweise vom MJ rechtlich beurteilt werde. Zur Aufklärung des Sachverhalts wurde daraufhin am 15. Dezember 2008 der Direktor des betroffenen Amtsgerichts um Bericht gebeten. Sein Bericht ging am 20. Januar 2009 ein. Hieraus ergaben sich weitere Fragen zur landes- und bundesweiten Praxis, so dass mit Verfügung vom 10. Februar 2009 ein ergänzender Bericht des Präsidenten des Oberlandesgerichts Naumburg eingeholt wurde. Gleichzeitig hat das MJ die übrigen Landesjustizverwaltungen um Auskunft zur dortigen Veröffentlichungspraxis und zu den dafür herangezogenen Rechtsgrundlagen gebeten. Der LfD erhielt eine Zwischennachricht, die auf die weiteren Ermittlungen verwies und eine hierauf beruhende Verzögerung bei der Beantwortung der aufgeworfenen Fragen ankündigte. Eine Sachstandsanfrage des LfD wurde mit Schreiben vom 16. März 2009 in gleicher Weise beantwortet.

Nach Auswertung des Berichts des Präsidenten des OLG Naumburg und der Stellungnahmen mehrerer Landesjustizverwaltungen beantwortete das MJ mit Schreiben vom 12. Mai 2009 ausführlich die Anfrage des LfD. Es wurde dargestellt, dass die Internetveröffentlichung von Gutachten – auch unter Einbeziehung privater Anbieter – in Zwangsversteigerungsverfahren bundesweit die Regel sei und hierfür auf § 38 Abs. 2, § 39 Abs. 1 und § 40 Abs. 2 ZVG zurückgegriffen werde. Zur Veröffentlichung gelangen überarbeitete und anonymisierte Exemplare, um schutzwürdigen Interessen der Betroffenen Rechnung zu tragen. Mit der Veröffentlichung nähmen die Vollstreckungsgerichte eine Aufgabe der Rechtspflege wahr. Die zuständigen Rechtspfleger handelten dabei in sachlicher Unabhängigkeit.

Durch AV vom 24. August 2009 (JMBl. LSA S. 221) hat das MJ ab 1. Oktober 2009 die Internetadresse www.zvg-portal.de für die Veröffentlichung von Wertgutachten und Abschätzungen im Sinne von § 38 Abs. 2 ZVG bestimmt. Hierbei handelt es sich um das von den Landesjustizverwaltungen geschaffene Portal zur Information über Zwangsversteigerungsverfahren.

Zu 20.2 Umstellung der Schulstatistik auf Individualdaten (Kerndatensatz)

Sachsen-Anhalt wird – wie die meisten Länder auch – erst dann einer nationalen Schülerdatenbank zustimmen und Daten dafür bereitstellen, wenn es dafür ein schlüssiges, mit den LfD abgestimmtes Konzept gibt. Derzeit ist eine Arbeitsgruppe, bestehend aus Mitgliedern der Kommission Statistik und Mitarbeitern des KMK-Sekretariates sowie des Statistischen Bundesamtes, mit der Erstellung eines solchen Konzepts beauftragt.

Zu 20.3 Schulverwaltungssoftware

Die geplante einheitliche Schulverwaltungssoftware soll zur Verwaltungsvereinfachung in den Schulen führen. Zugleich soll der Beschluss der KMK aus dem Jahre 2003 über die Einführung eines bundesweit einheitlichen Kerndatensatzes umgesetzt werden, indem die Schulen mit der Schulverwaltungssoftware die geforderten schulstatistischen Daten mit vertretbarem Aufwand zur Verfügung stellen können.

Der LfD wird in die Entwicklung der Software einbezogen; seine Hinweise und Anregungen werden berücksichtigt. Besonderes Gewicht wird darauf gelegt, das Trennungsgebot von Verwaltung und Statistik zu beachten.

Zu 20.4 Medienkompetenz und Datenschutzbewusstsein von Schülern

Die fortschreitende Entwicklung hin zu einer Informationsgesellschaft bringt auch für den Einzelnen erhebliche Vorteile. So haben vor allem junge Menschen die Chancen, die das Internet z. B. bei der Informationsbeschaffung und beim Austausch von Meinungen bietet, schnell erkannt und genutzt. Dagegen sind bei Kindern und Jugendlichen die Kenntnis und die richtige Einschätzung der Risiken der modernen Informations- und Kommunikationstechnik nicht immer hinreichend ausgeprägt. Es besteht die Gefahr der unbewussten Weitergabe persönlicher Daten, des ungewollten Eingehens erheblicher finanzieller Verpflichtungen und von Belästigungen aus dem Netz (sog. Cyber-Mobbing). Um ein Gespür für die Risiken zu entwickeln, soll das Thema „Datenschutz“ verstärkt in den Schulen behandelt werden. Fortbildungsveranstaltungen bieten die Gelegenheit, Lehrkräfte zu Multiplikatoren im Datenschutz auszubilden. Sowohl der LfD als auch das Landesverwaltungsamt als Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich nutzen aber auch die Gelegenheit zur direkten Ansprache von Schülern. Solche Veranstaltungen wurden in der Vergangenheit positiv aufgenommen; weitere Projekte sind in Planung.

Zu 20.9 Ersatzschulverordnung

Der LfD hatte vorgeschlagen, in der Ersatzschulverordnung vorzusehen, keine Angaben zur Staatsangehörigkeit über die Personen zu erheben, die eine Ersatzschule errichten, betreiben oder leiten wollen. Der Vorschlag bliebe jedoch im Ergebnis wirkungslos. Denn nach § 16 Abs. 4 SchulG LSA müssen die genannten Personen die verfassungsmäßige Ordnung wahren; dies wird anhand von Führungszeugnissen geprüft. Führungszeugnisse weisen aber stets die Staatsangehörigkeit aus.

Der LfD hatte angeregt, in Genehmigungsverfahren anstelle vollständiger Gesellschaftsverträge nur Auszüge hieraus einreichen zu dürfen. Der Anregung wurde nicht gefolgt. Abgesehen davon, dass der Schutz von Daten juristischer Personen kein Datenschutzbelang ist, enthalten die Gesellschaftsverträge in der Regel keine Betriebs- und Geschäftsgeheimnisse. Ohnehin ist der Gesellschaftsvertrag der Anmeldung zur Eintragung

in das Handelsregister beizufügen (§ 8 Abs. 1 Nr. 1 GmbHG). Die Einsichtnahme in das Handelsregister sowie in die zum Handelsregister eingereichten Dokumente ist jedem zu Informationszwecken gestattet (§ 9 Abs. 1 Satz 1 HGB).

Nach § 16 Abs. 3 Nr. 3 SchulG LSA muss die wirtschaftliche und rechtliche Stellung der Lehrkräfte genügend gesichert sein. Liegen diese Voraussetzungen nicht mehr vor, ist der Betrieb einer Ersatzschule zu widerrufen. Um den gesetzlichen Prüfauftrag erfüllen zu können, ist insbesondere zum Zeitpunkt der Anerkennung die Überprüfung der Arbeitverträge erforderlich. Die Anerkennung wird nur erteilt, wenn die Ersatzschule Gewähr dafür bietet, dass sie dauernd die Genehmigungsvoraussetzungen erfüllt.

Unbedenklich ist es auch, schon bei der Festsetzung der Finanzhilfe für Schulen in freier Trägerschaft die Vorlage von Klassenlisten zu fordern. Dies beugt Überzahlungen vor, zu denen es in der Vergangenheit gekommen ist. Unter Hinweis auf die Regelungen zur Zweckidentität in § 10 Abs. 4 DSG-LSA können im Zeitpunkt der Festsetzung der Finanzhilfe bereits vorhandene Unterlagen, die schwerpunktmäßig zur nachträglichen Kontrolle (Verwendungsnachweisführung und Rechnungsprüfung) vorzuhalten sind, beigezogen werden. Die Finanzhilfe wird für die Zeit der Verweildauer eines Schülers bzw. einer Schülerin an einer Schule gewährt. Die Klassenlisten enthalten für den Vergleich mit den Schulverträgen lediglich Angaben zu Vor- und Familiennamen der Schüler. Nach Überprüfung werden die Klassenlisten an den Schulträger zurückgegeben, der diese fünf Jahre aufzubewahren hat. Eine dauerhafte Speicherung der Schülerdaten durch das Landesverwaltungsamt unterbleibt.

Zu 21.16 Kinderschutzgesetz des Landes

Zur Abrundung weist die Landesregierung darauf hin, dass es mittlerweile in 10 Ländern Verfahren gibt, mit denen eine Erhöhung der Teilnahmequote an Früherkennungsuntersuchungen erreicht werden soll.

Derjenige Teil des Gesetzentwurfs (Drs. 5/1331), der zur Verbesserung des Schutzes von Kindern ein verbindliches Einladungswesen für Früherkennungsuntersuchungen vorsah, ist wegen verfassungsrechtlicher Bedenken, die vor allem vom LfD und vom Gesetzgebungs- und Beratungsdienst des Landtages vorgetragen wurden, vom Landtag nicht verabschiedet worden. Inzwischen hat der Verfassungsgerichtshof Rheinland-Pfalz mit Urteil vom 28. Mai 2009 – VGH B 45/08 – zu weitgehend parallelen Regelungen in Rheinland-Pfalz

entschieden, dass der Landesgesetzgeber befugt war, im Landeskinderschutzgesetz durch ein behördliches Einladungs- und Erinnerungsverfahren Eltern zur Inanspruchnahme von Früherkennungsuntersuchungen anzuhalten und so Gefährdungen der Kindesgesundheit sowie möglicher Vernachlässigung oder Misshandlung von Kindern entgegenzuwirken. Die dazu im Gesetz vorgesehenen Einschränkungen des Grundrechts der Eltern auf Selbstbestimmung über personenbezogene Daten sowie das Recht der Eltern zur Erziehung ihrer Kinder seien bei Beachtung vorgegebener verfahrensmäßiger Sicherungen und vorbehaltlich des Ergebnisses der erstmals im Jahr 2010 vorgesehenen Evaluation gerechtfertigt.

Der LfD übt ungewöhnlich scharfe Kritik an diesem Urteil. Er wirft dem Verfassungsgericht eines anderen Landes vor, den Grundsatz der Verhältnismäßigkeit und Rechtsprechung des Bundesverfassungsgerichts zum Recht auf informationelle Selbstbestimmung nicht ausreichend berücksichtigt zu haben.

Zu 23.1 PPP-Projekt Justizvollzugsanstalt Burg

Geradezu beispielhaft wird am PPP-Modell JVA Burg das Spannungsverhältnis zwischen dem Schutz der personenbezogenen Daten der Bürger und der Erfüllung der Aufgabe des Strafvollzugs, Gefangene sicher zu verwahren, deutlich. Die Ausführungen des LfD zu Datenschutzfragen bei Public Private Partnerships (PPP) im Justizvollzug zeigen, dass es noch weiterer Abstimmung in Einzelfragen bedarf, bei denen das MJ die Beratung durch den LfD dankend entgegennimmt. Unabhängig davon, in welcher Rechtsform und von wem Aufgaben des Strafvollzugs wahrgenommen werden, bedarf PPP im Justizvollzug einer öffentlich-rechtlichen Umhegung.

Zu Einzelfragen ist anzumerken:
Hinsichtlich der Verwendung der vom LfD angesprochenen RFID-Chips zur Kennzeichnung von Wäschestücken der Gefangenen ist darauf hinzuweisen, dass diese Technik – obgleich sie nur der im Interesse der Gefangenen liegenden verwechslungsfreien Zuordnung der Wäsche zu den jeweiligen Gefangenen gedient hätte – nicht zum Einsatz kommt. Die Wäsche wird durch den Gefangenen in einen oder mehrere dem Haftraum zugeordnete Wäschesäcke verpackt und abgegeben. Nach erfolgter Reinigung kommt die Wäsche auf dem gleichen Weg zurück zum Gefangenen. Eine Öffnung der Wäschesäcke erfolgt nicht. Aufgrund der Angabe der Haftraumnummer und des hierzu gebundenen Wäschesackes ist eine ausreichende Anonymisierung erfolgt.

An der Notwendigkeit einer den Sicherheitsbedürfnissen der JVA Burg entsprechenden Zugangskontrolle durch Handvenenscannung wird weiterhin festgehalten. Allerdings würde nur ein solches System eingeführt, das den baulichen Gegebenheiten der JVA Burg und allen datenschutzrechtlichen Anforderungen gerecht wird. Das ist bisher nicht geschehen. Der LfD wird weiterhin beteiligt bleiben.

Zu 23.4 Mobilfunkblocker im Justizvollzug

Die Feststellungen des Berichts betreffen ein seinerzeit laufendes Gesetzgebungsverfahren. Das MJ hat die Anregungen des LfD aufgenommen und achtet darauf, dass die rechtlichen – auch datenschutzrechtlichen – Vorgaben für Mobilfunkblocker im Justizvollzug eingehalten werden. Diesem Zweck dienen nicht zuletzt auch die Richtlinien der Bundesnetzagentur (BNA), der im Rahmen der Neukonzeption von Mobilfunkblockern die Unterlagen zur Verfügung zu stellen sind, ohne deren Vorlage weder eine Genehmigung zum Testbetrieb noch eine endgültige Betriebsgenehmigung erteilt werden kann.

Zu 24.6 Musterdienstanweisung zur Nutzung von E-Mail und Internet am Arbeitsplatz

Zu der Darstellung des LfD hinsichtlich eines Eingriffs in das Fernmeldegeheimnis wird angemerkt, dass nach dem Urteil des BVerfG vom 27. Februar 2008 zur Online-Durchsuchung (BVerfGE 120, 274, 340 ff.) der Schutzbereich des Telekommunikationsgeheimnisses aus Art. 10 Abs. 1 GG nur das Vertrauen des Einzelnen darin umfasst, dass eine Fernkommunikation nicht von Dritten zur Kenntnis genommen wird, nicht jedoch das Vertrauen der Kommunikationspartner zueinander. Das Grundrecht findet also Anwendung, wenn der Staat Telekommunikationsbeziehungen von außen überwacht, ohne selbst Kommunikationsadressat zu sein. Es schützt allerdings nicht davor, dass eine staatliche Stelle selbst die Kommunikation zu einem Grundrechtsträger aufnimmt. Demnach erfasst eine staatliche Stelle bereits dann Kommunikationsinhalte in zulässiger Weise, wenn nur einer von mehreren Beteiligten ihr diesen Zugriff freiwillig ermöglicht. Bei dem bislang praktizierten Verfahren fehlt es bereits am Merkmal einer gezielten staatlichen Ermittlungsmaßnahme, auch im Verhältnis zu dem an der Kommunikation beteiligten Außenstehenden. Die ausnahmsweise unvermeidliche Kenntnisnahme vom Inhalt der Kommunikation durch andere und die Protokollierung von Verkehrsdaten ist technisch die unvermeidliche Konsequenz, wenn ein Landesbediensteter anstelle eines sog. Webmailers

als Serviceleistung seines Arbeitgebers/Dienstherrn ausnahmsweise den dienstlichen E-Mail-Account für private Zwecke in Anspruch nimmt. Hierin kann der Landesbedienstete einseitig einwilligen; dies ist dem LfD mitgeteilt worden.

Einvernehmen besteht mit dem LfD, dass für die Landesbediensteten der dienstherren-/arbeitgeberseitige Umgang mit Protokolldaten bei ausnahmsweise erfolgender privater E-Mail-Kommunikation transparent erfolgen muss. Daher wird die Musterdienstanweisung in diesem Sinne - wie angekündigt - überarbeitet.

Zu 24. 7 SPAM-Filterung von E-Mails

Die bisher durch den IT-Dienstleister LIZ realisierte Antispam-Strategie des Landes Sachsen-Anhalt ist vor dem Hintergrund aktueller technischer und rechtlicher Rahmenbedingungen mit dem Ziel überprüft worden, eine für alle Behörden des Landes Sachsen-Anhalt verbindliche Strategie festzulegen, wie am zentralen E-Mail-Gateway mit Spams zu verfahren ist.

Die Grundlage der Betrachtung war die Studie „Antispam-Strategien, Unerwünschte E-Mails erkennen und abwehren" des BSI. Die Studie bündelt Informationen zu technischen, rechtlichen und organisatorischen Aspekten des Themas Spam und ist daher für eine Bewertung vorhandener und eine Planung zukünftiger Strategien besonders geeignet.

Es wird eine dezentrale Lösung angestrebt, die noch mit dem LfD abgestimmt werden soll. Der IT-Dienstleister für netznahe Dienste (LRZ) betreibt das zentrale E-Mail-Gateway des Landes nach zentralen Vorgaben. Dort soll ein „Greylisting“ erfolgen. Anschließend soll die Gültigkeit der Empfänger anhand des zentralen Verzeichnisdienstes geprüft werden („Recipient Check“). Danach sollen die E-Mails einer Filterung und einem Virenscanning unterzogen und – ggf. mit Markierung – per DNS-Routing an die Postfachserver weitergeleitet werden. Für die Pflege der Adresseinträge und den Umgang mit den markierten E-Mails wird das jeweilige Ressort zuständig sein. Entsprechend der IT-Sicherheitsrichtlinie des ITN-Betreibers werden diesem auf Anforderung die Dokumentationen zu IT-Sicherheitsmaßnahmen, insbesondere für den Schutz vor Schadsoftware (Viren, Würmer u. ä.), vorzulegen sein.

Zu 25.1 Änderung des Verfassungsschutzgesetzes und
Zu 25.2 Dokumentenmanagement beim Verfassungsschutz

Im Rahmen der 49. Sitzung des Ausschusses für Inneres am 5. März 2009 hat der Minister des Innern um Zurückstellung des Entwurfs eines Zweiten Gesetzes zur Änderung des Gesetzes über den Verfassungsschutz im Land Sachsen-Anhalt gebeten. In der Sitzungsniederschrift ist hierzu Folgendes ausgeführt:

> "Nach Auswertung der Tatbestände, die im Rahmen der Sitzung des Ausschusses für Recht und Verfassung[1] bekannt geworden seien, habe er den Datenschutzbeauftragten des Ministeriums des Innern gebeten, erläutert Herr Minister Hövelmann, gemeinsam mit Herrn Dr. von Bose zu prüfen, ob zur Klarstellung ggf. Ergänzungen oder Änderungen gegenüber dem vorliegenden Gesetzentwurf erforderlich seien. Diese gemeinsamen Gespräche hätten noch nicht zu einem Ergebnis geführt. Von daher rate er dazu, die Behandlung des Gesetzentwurfs zurückzustellen, um die Anregungen, die in den genannten Gesprächen erarbeitet würden, mit aufnehmen zu können."

Die angekündigten Vorschläge befinden sich in der Abstimmung.

Zu 26.1 Online-Anbindung der Fahrerlaubnisbehörden an das Kraftfahrt-Bundesamt

Die Problematik der Online-Anbindung der örtlichen Fahrerlaubnisbehörden (FEB) an das Kraftfahrt-Bundesamt (KBA) und deren Zugriff auf das Zentrale Fahrerlaubnisregister (ZFER) wurde zunächst zwischen dem BfDI, dem Bundesministerium für Verkehr, Bau und Stadtentwicklung (BMVBS) und dem MLV Sachsen-Anhalt (in der damaligen Eigenschaft als Vorsitzland der Verkehrministerkonferenz) schriftlich erörtert. Im Anschluss daran hat das BMVBS die Thematik in einer Sitzung des Bund-Länder-Fachausschusses Fahrerlaubnis-/Fahrlehrerrecht (BLFA-FE/FL) zur Diskussion gestellt, bei der auch je ein Vertreter des BfDI und des Landeszentrums für Datenschutz des Landes Schleswig-Holstein zugegen waren.

Da es sowohl für den direkten Zugriff der FEB auf den Datenbestand des ZFER als auch für die vom KBA durchgeführten Protokollierungen an Rechtsgrundlagen im StVG bzw. in der FeV fehlt, hat der BfDI den BMVBS aufgefordert, die erforderlichen Gesetzesänderungen zu veranlassen. Das KBA hat dem BMVBS bereits Formulierungsvorschläge zugeleitet.

---

[1] 36. Sitzung am 18. Februar 2009

In der Diskussion über die sichere Gestaltung der elektronischen Kommunikation zwischen KBA und FEB lag allen Ländern das im Tätigkeitsbericht des LfD angeführte Gutachten vom 19. Oktober 2007, das von einem Arbeitskreis der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeitet wurde, erstmals am 18. November 2008 vor. Das KBA und die Vertreter der Länder haben im BLFA-FE/FL darauf hingewiesen, dass die geforderte Datenanbindung und der Datenaustausch mittels qualifizierter elektronischer Signatur mit einem erheblichen Kostenaufwand – insbesondere für die kommunalen FEB – verbunden wäre. Auch hätten die Länder keine direkte Einflussmöglichkeit auf die technische Ausstattung der kommunalen FEB. Daher müssten die kommunalen Spitzenverbände in die Diskussion eingebunden werden. Die Beratungen im BLFA-FE/FL sind noch nicht abgeschlossen. Das MLV wird den LfD zeitnah über den Beratungsstand unterrichten und bei der Meinungsbildung des Landes einbeziehen.

Abkürzungsverzeichnis

A

ADV	Automatisierte Datenverarbeitung
AG	Arbeitsgruppe
AO	Abgabenordnung
AV	Justizverwaltungsvorschrift

B

BCC	Blind-Carbon Copy (andere E-Mail-Empfänger nicht sichtbar)
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BGBl.	Bundesgesetzblatt des Landes Sachsen-Anhalt
BLFA–FE/FL	Bund-Länder-Fachausschuss Fahrerlaubnisrecht/ Fahrlehrerrecht
BMF	Bundesministerium der Finanzen
BMVBS	Bundesministerium für Verkehr, Bau und Stadtentwicklung
BNA	Bundesnetzagentur
BR-Drs.	Bundesratsdrucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungssammlung des Bundesverfassungsgerichts
BZRG	Bundeszentralregistergesetz

C

CC	Carbon Copie (andere E-Mail-Empfänger sichtbar)

D

DNS	Domain Name System (Namensauflösung)
Drs.	Landtagsdrucksache
DSG-LSA	Gesetz zum Schutz personenbezogener Daten der Bürger

E

EFS	Encrypted File System (verschlüsseltes Dateisystem)
ELSTER	Elektronische Steuererklärung
EOP	ElsterOnlinePortal
ESch-VO	Ersatzschulverordnung

F

FEB	Fahrerlaubnisbehörde
FeV	Fahrerlaubnis-Verordnung
FHPol	Fachhochschule der Polizei
FISCUS	Föderales Integriertes Standardisiertes Computer-Unterstütztes Steuersystem
FVG	Finanzverwaltungsgesetz

G

Gem. RdErl.	Gemeinsamer Runderlass
GG	Grundgesetz
GGO LSA I	Gemeinsame Geschäftsordnung der Ministerien – Allgemeiner Teil –
GmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung
GO LSA	Gemeindeordnung des Landes Sachsen-Anhalt
GSTOOL	Datenbankanwendung zur Erstellung von Sicherheitskonzepten
GVBl. LSA	Gesetz und Verordnungsblatt für das Land Sachsen-Anhalt

H

HGB	Handelsgesetzbuch

I

INPOL	polizeiliches Informationssystem
IP	Internetprotokoll
ISO	International Organization for Standardization
IT	Informationstechnik
IT-KA	IT-Koordinierungsausschuss
ITN	Informationstechnisches Netz
ITN-LSA	Informationstechnisches Netz des Landes Sachsen-Anhalt
JMBl. LSA	Justizministerialblatt für das Land Sachsen-Anhalt

J

JVA	Justizvollzugsanstalt

K

KBA	Kraftfahrtbundesamt
KMK	Kultusministerkonferenz
KONSENS	bundeseinheitliche Software für das Besteuerungsverfahren

L

LfD	Landesbeauftragter für den Datenschutz
LIS	Landesleitstelle IT-Strategie (in der Staatskanzlei)
LIZ	Landesinformationszentrum
LRZ	Landesrechenzentrum

M

MBl. LSA	Ministerialblatt für das Land Sachsen-Anhalt
MF	Ministerium der Finanzen
MI	Ministerium des Innern
MJ	Ministerium der Justiz
MLV	Ministerium für Landesentwicklung und Verkehr
MZulKraftStG	Gesetz über die Mitwirkung der Zulassungsbehörden bei der Verwaltung der Kraftfahrzeugsteuer

O

OLG	Oberlandesgericht

P

PKI	Public Key Infrastruktur (Infrastruktur für öffentliche Schlüssel)
PKS	Public Key Service (System zur Ausstellung digitaler Zertifikate)
PPP	Public Private Partnership (Zusammenarbeit von öffentlicher Hand und Privatwirtschaft bei der Erledigung öffentlicher Aufgaben)
PSC	PersonalServiceCenter

R

RFID	Radio Frequency Identification

S

SchulG LSA	Schulgesetz des Landes Sachsen-Anhalt
SOG LSA	Gesetz über öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt
StK	Staatskanzlei
StVG	Straßenverkehrsgesetz

T

TESTA	Trans-European Services for Telematics between Administrations (Internes Netzwerk von europäischen Verwaltungen
TPA	Technisches Polizeiamt

W

WLAN	drahtloses lokales Netzwerk

Z

ZFER	Zentrales Fahrerlaubnisregister
ZVG	Gesetz über die Zwangsversteigerung und die Zwangsverwaltung