# Automatisierte Datenverarbeitung, IT-Koordinierung und E-Government in der Landesverwaltung Sachsen-Anhalt

(Zusammenfassung aus den Tätigkeitsberichten des LfD – I. bis X. von 4/1993 bis 3/2011)

## I. Tätigkeitsbericht – 1993 (01.04.1992 - 31.03.1993)

### 7. Entwicklung der automatisierten Datenverarbeitung bei den Behörden und sonstigen öffentlichen Stellen

### 7.1 Koordinierung des Einsatzes der Informationstechnik in der Landesund Kommunalverwaltung

In Sachsen-Anhalt wird die Koordinierung des Informationstechnikeinsatzes durch zwei Gremien unterstützt. Für die unmittelbare Landesverwaltung nimmt diese Aufgabe der "**Interministerielle Arbeitskreis Informationstechnik**" (**IMA-IT**) wahr. Er nahm seine Tätigkeit bereits mit der konstituierenden Sitzung am **19.12.1990** auf.
In ihm sind, neben allen Ressorts, die Landtagsverwaltung, der Landesrechnungshof, der Landesbeauftragte für den Datenschutz und Vertreter der staatlichen Hochbauverwaltung sowie der Leitstelle für IuK der kommunalen Spitzenverbände vertreten.
Der **Zentralen Stelle IT – ZIT (Referat 34 im Ministerium des Innern)** als Koordinierungsorgan für die Planung und Anwendung der IT in der Landesverwaltung (Ausarbeitung des IT-Landesplanes aus den Ressortplänen), obliegt auch die Leitung dieses Arbeitskreises.
Grundsätzliche Ziele dieser ressortübergreifenden Zusammenarbeit liegen vor allem im Informations- und Erfahrungsaustausch, in der Vorstellung und Diskussion von relevanten IT-Projekten der Ministerien, unter Einbeziehung nachgeordneter Bereiche, und der Erarbeitung von entsprechenden Stellungnahmen des IMA-IT zu diesen Projekten bzw. den Einsatz- und Entwicklungskonzeptionen der Ressorts. Weitere Schwerpunkte der Arbeit bilden die Ausarbeitung von Empfehlungen hinsichtlich von Ausstattungsnormen für die Beschaffung von Hard- und Software sowie die Festlegung von Standards und Normen beim IT-Einsatz in der Landesverwaltung.
Grundlage für diese Zusammenarbeit sind die "Grundsätze für den Einsatz der Informationstechnik in der Landesverwaltung Sachsen-Anhalt" (**IT-Grundsätze**), in denen auch die Belange der IT-Sicherheit und des Datenschutzes Berücksichtigung fanden. Veröffentlicht sind diese IT-Grundsätze vom **1.6.1992** als gemeinsamer Runderlass des Ministeriums des Innern und der übrigen Ministerien (**MBl. LSA S. 805**).

## II. Tätigkeitsbericht – 1995 (01.04.1993 - 31.03.1995)

### 8. Entwicklung der automatisierten Datenverarbeitung

### 8.1 Automatisierte Datenverarbeitung in der Landesverwaltung

Gleichzeitig war bzw. ist mit der Erhöhung des Ausstattungsgrades eine zunehmende Vernetzung der PC innerhalb der Behörden zu lokalen Netzwerken (LAN = Local Area Network) verbunden. So lag der Anteil der vernetzten PC 1992 noch unter 1% und beträgt gegenwärtig durchschnittlich ca. 37%. Ressortabhängig reicht die Spannweite bei der Vernetzung von ca. 8 bis 84%.
Zusammenfassend kann man davon ausgehen, dass durchschnittlich jeder zweite Beschäftigte in den Ressorts diese Informationstechnik nutzt und jeder dritte PC innerhalb der Landesverwaltung bereits vernetzt ist.
Dem dargestellten Strukturwandel muss auch das vom Landesgesetzgeber im § 6 DSG-LSA geforderte Datensicherheitskonzept bei jeder öffentlichen Stelle Rechnung tragen. Eine Grundlage für die weitere Inhouse-Vernetzung bildet dabei der gemeinsame Runderlass des Ministeriums der Finanzen und des Ministeriums des Innern zur landeseinheitlichen Telekommunikations- und Datenverkabelung vom 19.08.1994 (MBl. LSA S. 2237). Die Festlegung des Runderlasses zur gemeinsamen Unterbringung von Etagenverteilern bzw. Verteilerschränken der Telekommunikations- und Datenverarbeitungsnetze in nicht öffentlich zugänglichen Betriebsräumen entspricht den Forderungen des Landesbeauftragten.
In Pilotprojekten, seit Dezember 1994 im Technischen Polizeiamt und seit Februar 1995 im Ministerium des Innern, werden sog. “elektronische Postämter“ (MTA = Message Transfer Agent) eingesetzt, die Erfahrungen aus der Praxis beim elektronischen Dokumentenaustauschverfahren auf der Basis des X.400-Standards von 1988 liefern sollen. Eine zukünftige Nutzung dieser elektronischen Mitteilungssysteme erfordert aber noch grundsätzliche Regelungen durch die Landesregierung.
Die Datenschutzbeauftragten des Bundes und der Länder haben hierzu auf ihrer **49. Konferenz** am **09./10.03.1995** in einer **Entschließung** auf die Berücksichtigung von Sicherheitsaspekten bei der Nutzung hingewiesen und Empfehlungen zum Einsatz von **elektronischen Mitteilungssystemen** gegeben, die wesentliche Forderungen zur Gewährleistung eines für alle Bürger ausreichenden Datenschutzes beinhalten **(Anlage 16).**

### 8.2 Informationstechnisches Netz Sachsen-Anhalt (ITN-LSA)

Auch das im I. Tätigkeitsbericht (S. 43) bereits vorgestellte **ITN-LSA** wird immer mehr ausgedehnt. Neben dem weiteren Anschluss von Ministerien sind für das Jahr 1995 der Anschluss von Grundbuchämtern der Amtsgerichte, von Finanzämtern und einzelner kreisfreier Städte vorgesehen.
In einem gemeinsamen Runderlass des Ministeriums des Innern, der Staatskanzlei und der übrigen Ministerien vom 07.02.1994 (MBl. LSA S. 1251) sind die Grundsätze für die Nutzung dieses Landesverwaltungsnetzes durch die Ressorts festgelegt worden. Der Landesbeauftragte wurde bei der Ausarbeitung dieses Erlasses beteiligt. Wer als öffentliche Stelle einen Antrag als Netzteilnehmer stellt und personenbezogene Daten verarbeitet, muss als eine Mindestvoraussetzung ein Datenschutzkonzept gemäß § 6 DSG-LSA für den Anschluss vorlegen können.

Ein noch zu lösendes datenschutzrechtliches Problem stellt die in diesem Netz erforderliche Verschlüsselung personenbezogener Daten durch den einzelnen Netzteilnehmer dar. Die Verschlüsselung ist notwendig, damit bei eventuellen Zugriffen des Netzmanagements auf die Netzknoten die Vertraulichkeit gewahrt bleibt. Ein weiterer Grund liegt darin, dass im Netzvertrag des Ministeriums des Innern mit der Telecom AG Richtfunkverbindungen, die stark abhörgefährdet sind, zur Datenübertragung vertraglich **nicht** ausgeschlossen sind. In einigen Bereichen der Landesverwaltung erfolgt die Datenübertragung bereits verschlüsselt.
Der Landesbeauftragte wird über eingereichte Anträge öffentlicher Stellen zum Anschluss an das ITN-LSA informiert und wird bei ihnen im Rahmen seiner Kontrollen die Einhaltung datenschutzrechtlicher Bestimmungen überprüfen.
Beim Ministerium des Innern hat der Landesbeauftragte außerdem seit längerem die Erarbeitung eines Gesamtsicherheitskonzeptes für das ITN-LSA angefordert.
Es soll nun erstellt werden.

# III. Tätigkeitsbericht – 1997 (01.04.1995 - 31.03.1997)

## 8 Entwicklung der automatisierten Datenverarbeitung

### 8.1 Automatisierte Datenverarbeitung in der Landesverwaltung

Die bereits im II. Tätigkeitsbericht (S. 35 f) angesprochene dynamische Entwicklung bei der Ausstattung der Landesverwaltung mit Informations- und Kommunikationstechnik hat sich in den vergangenen zwei Jahren fortgesetzt. Grundsätzlich erhöht sich mit dieser Entwicklung auch das Gefährdungspotential für die automatisierte Verarbeitung personenbezogener Daten.
Drei Aspekte sind hier besonders zu nennen und zu beachten:

Bezogen auf die Beschäftigtenzahl hat sich insgesamt der Ausstattungsgrad in den obersten Landesbehörden mit PC von ca. 55 % im Jahr 1994 auf ca. 78 % im Jahr 1996 erhöht. In einigen Ministerien ist bereits die „100 %-Grenze“ überschritten, d.h. hier sind bereits mehr Bildschirmarbeitsplätze bzw. PC als Mitarbeiter vorhanden.

Für die nachgeordneten Bereiche der Ressorts liegen dem Landesbeauftragten solche Statistiken nicht vor. Es ist aber davon auszugehen, dass sich auch dort die gleiche Tendenz widerspiegelt.

Der zweite Aspekt betrifft die lokale Vernetzung der Informationstechnik innerhalb der Ministerien. Waren 1994 durchschnittlich ca. 37 % der Bildschirmarbeitsplätze bzw. PC lokal vernetzt, hat sich dieser Anteil im Jahr 1996 auf ca. 61 % erhöht

Von Bedeutung ist schließlich auch die Ausgestaltung der überregionalen Vernetzung (WAN) der Behörden auf der Landesebene. Die Entwicklung ist hier durch den weiteren Ausbau des ITN-LSA bzw. die weitere Anbindung von Landesbehörden an das ITN-LSA gekennzeichnet. Parallel hierzu erfolgte der Ausbau von Meldungsübermittlungssystemen (MHS) nach dem X.400-Standard, die Anfang des Jahres 1995 als Pilotprojekte begonnen wurden. Der Landesbeauftragte weist deshalb erneut auf seine Ausführungen zu den Anforderungen beim Einsatz von elektronischen Mitteilungssystemen im II. Tätigkeitsbericht (S. 36 u. Anlage 16) hin. Insbesondere sollten nur solche Produkte eingesetzt werden, die die Sicherheitsfunktionen der X.400-Empfehlung aus dem Jahr 1988 erfüllen.

Die vom Bundesverfassungsgericht herausgestellte Bedrohung der Grundrechte durch die automatisierte Datenverarbeitung kann und muss ß mit Hilfe der Technik auch wieder eingegrenzt werden.
Für das Jahr 1997 sind durch das zuständige Ministerium des Innern als Netzbetreiber des ITN-LSA die Integration der Fernmeldekommunikation und die Schaffung des „INTRANET LSA“ für die Landesbehörden innerhalb des Landesnetzes vorgesehen. Beim „INTRANET LSA“ handelt es sich um die Bereitstellung von sog. TCP/IP-basierenden „Internet-Diensten“, wie z.B.:

- WWW-Dienst (World Wide Web - als multimedialer Informationsdienst),
- FTP-Dienst (File Transfer Protocol - als interaktiver Dateitransfer) und
- E-Mail-Dienst (Electronic Mail - als elektronische Post oder sog. Internet- Mail).

Werden auf sog. FTP- bzw. WWW-Servern personenbezogene Daten eingestellt, die dann von jedem Zugangsberechtigten abgerufen werden können, handelt es sich aus datenschutzrechtlicher Sicht um die Einrichtung eines automatisierten Abrufverfahrens (§ 7 DSG-LSA). Ein solches automatisiertes Abrufverfahren darf nach § 7 Abs. 1 DSG-LSA nur eingerichtet werden, wenn ein Gesetz dies ausdrücklich zulässt.
Für die Ministerien besteht nach § 7 Abs. 2 DSG-LSA die Ermächtigung, für die Behörden und Einrichtungen ihres Geschäftsbereiches solche automatisierten Abrufverfahren durch Rechtsverordnung zuzulassen. Der Landesbeauftragte weist deshalb im Vorfeld der Planungen zum INTRANET LSA nachdrücklich auf die Beachtung dieser datenschutzrechtlichen Bestimmung hin.
Die Landesregierung hat bei der weiteren Vernetzung der Landesverwaltung und der Gestaltung des INTRANET LSA unter Berücksichtigung ihrer Rechtsverantwortung nach § 14 Abs. 1 DSG-LSA darauf zu achten, dass im Sinne eines vorgelagerten Grundrechtsschutzes die Kernaussagen des Volkszählungsurteils des Bundesverfassungsgerichts vom 15. Dezember 1983 (BVerfGE 65, 1), insbesondere die Grundsätze der Verhältnismäßigkeit und der Zweckbindung bei der Planung und Herstellung neuer Kommunikationsbeziehungen, beachtet werden.

Nicht alles, was die moderne Technik über ihre Zugangswege anbietet, muss so von jeder öffentlichen Stelle (von der kleinsten bis zur größten) und von jedem Mitarbeiter auch genutzt werden. Maßstab darf rechtlich (und finanziell) nur sein, ob die Herstellung neuer Kommunikationsbeziehungen zur Erfüllung der konkreten Verwaltungsaufgaben **erforderlich** ist. Bei mehreren technisch möglichen Wegen ist stets der für die personenbezogene Datenverarbeitung sicherste zu wählen.
Auch die Zweckbindung bei der Erhebung und Verarbeitung personenbezogener Daten und der damit verbundene Grundsatz der informationellen Gewaltenteilung sollen bei der landesweiten Vernetzung Berücksichtigung finden. Dabei müssen die Erforderlichkeit und das Risiko einer Zusammenführung von personenbezogenen Daten aus verschiedenen Stellen und Quellen durch diese Vernetzung rechtzeitig abgewogen werden.
Die gleiche Verantwortung trifft auch die Gemeinden und Landkreise für ihren jeweiligen Zuständigkeitsbereich bei der Wahrnehmung der eigenen Aufgaben.
Der Landesbeauftragte regt deshalb eine Anpassung der datenschutzrechtlichen Bestimmungen im Hinblick auf verbindliche Regelungen für die Sicherheit und Ordnungsmäßigkeit der automatisierten Verarbeitung personenbezogener Daten, unter Beachtung der sich abzeichnenden Entwicklung der weiteren lokalen und überregionalen Vernetzung innerhalb der Landesverwaltung, an. Als beispielgebend sind hier die Verordnungsermächtigung aus § 7 Abs. 4 Landesdatenschutzgesetz (LDSG) des Landes Schleswig-Holstein vom 30.10.1991 (GVOBl. Schl.-H. S. 555) und die danach erlassene Datenschutzverordnung (DSVO) vom 12.09.1994 (GVOBl. Schl.-H. S. 473) zu nennen.

## 8.2 ITN-LSA

### 8.2.1 Entwicklung des Landesverwaltungsnetzes - ITN-LSA

Das ITN-LSA ist im zurückliegenden Berichtszeitraum durch das Ministerium des Innern, als Netzbetreiber, auf 45 X.25-Netzknoten ausgebaut worden. Die Anzahl der an das Landesverwaltungsnetz angeschlossenen Behörden hat sich

weiter vergrößert. Die Übertragungskapazität zwischen den Hauptknoten des Netzes in Magdeburg, Halle und Dessau wurde auf 2 MBit/s erhöht.
Der Landesbeauftragte hält eine Aktualisierung und Präzisierung des Runderlasses vom 07.02.1994 zum ITN-LSA hinsichtlich der IT-Sicherheitsmaßnahmen (z.B. Firewall-Konzept), der Einführung neuer Kommunikationstechnologien (z.B. Intranetfunktionalität, Integration der Sprachkommunikationsdienste) sowie des Antragsverfahrens zum Anschluss von öffentlichen Stellen an das ITNLSA für erforderlich. Dabei müssen die im Rahmen des Antragsverfahrens zu einem Netzanschluss festgelegten und zu erfüllenden Mindestvoraussetzungen eine stärkere Beachtung finden. Nach Ziff. 2.1 Buchstabe g) des Runderlasses zählt dazu auch ein Datenschutzkonzept gem. § 6 DSG-LSA. Die Verantwortlichkeit hierfür liegt bei der speichernden öffentlichen Stelle selbst, nicht aber beim Netzbetreiber des ITN-LSA. Der gewährleistet mit seinen Maßnahmen nur im Transportnetz selbst eine Grundsicherheit. Als ein positives Beispiel kann der Landesbeauftragte die Umsetzung seiner Forderung nach der Verschlüsselung der Übertragung von Sozialdaten nennen. Bereits seit September 1995 erfolgt der verschlüsselte Datenaustausch zwischen den Landesämtern für Soziales und Versorgung und dem Landesrechenzentrum mittels vom BSI zertifizierter Verschlüsselungsboxen auf der Netzebene des ITN-LSA.
Eine andere Lösungsmöglichkeit besteht in der sog. Ende-zu-Ende-Verschlüsselung durch die einzelne öffentliche Stelle selbst. Dabei erfolgt durch den Benutzer die Verschlüsselung der Daten mittels des jeweils eingesetzten Programmes auf der Anwendungsebene bereits vor der Datenübertragung im ITN-LSA.

### 8.2.2 Sicherheitskonzept und Firewall-Konzept

Dem Landesbeauftragten liegt nunmehr der **1. Entwurf eines Gesamtsicherheitskonzeptes** für das ITN-LSA vor. Das Ministerium des Innern kommt damit einer langjährigen Forderung des Landesbeauftragten nach (vgl. u.a. II. Tätigkeitsbericht, S. 37).
Der Entwurf beinhaltet neben Aussagen zur Grundsicherheit im ITN-LSA auch die Darstellung eines Lösungskonzeptes für die Übergänge zu Fremdnetzen (Internet, Datex-P, ISDN). Dazu sind die Schaffung kontrollierter zentraler Übergänge und deren Absicherung durch ein entsprechendes Firewall-Konzept vorgesehen.
Die zu Beginn des Jahres 1997 getroffene Grundsatzentscheidung des Ministeriums des Innern für eine höherwertige Zertifizierung der Firewall-Lösung für das ITN-LSA wird vom Landesbeauftragten begrüßt. Bis zur endgültigen Erteilung des Zertifikates durch das BSI sollte der Anwenderkreis, der den Praxistest unterstützt, überschaubar beschränkt bleiben. Ergänzend kann auf die folgenden Ausführungen zum Anschluss von Verwaltungsnetzen an das Internet (Ziff. 13.1) verwiesen werden. Die mit der höherwertigen Zertifizierung des Firewalls verbundene zeitliche Verzögerung bis zur voraussichtlichen Inbetriebnahme im April 1998 sollte durch das Ministerium des Innern zu einer intensiven Abstimmung des Gesamtsicherheitskonzeptes des ITN-LSA mit allen Ressorts genutzt werden.

### 8.3 Intranet LSA

Die Anwendung von Internet-Prinzipien und die Nutzung von Internet-Diensten in lokalen Netzen (LAN) der Behörden und Dienststellen des Landes sowie innerhalb des Landesverwaltungsnetzes (ITN-LSA), einem sog. Fernnetz (WAN), wird als „INTRANET LSA“ bezeichnet.

Technisch verbirgt sich hinter der Bezeichnung INTRANET LSA der Einsatz von Server-Technik, die, in Verbindung mit einem Domain Name Service (DNS) für die Namen-Domain der Landesverwaltung „lsa-net.de“, diese Internet-Prinzipien und Internet-Dienste auf der Basis des TCP/IP-Protokolls umsetzt. Mit dem INTRANET LSA sollen nach Planungen des Ministerium des Innern IP-basierte Dienste (z.B. WWW, E-Mail, FTP), wie sie heute bereits zu den Standardtechnologien im INTERNET zählen, auch für die an das ITN-LSA angeschlossenen Behörden verfügbar werden.

Der Landesbeauftragte hält es bei der geplanten breiten Anwendung dieser neuen elektronischen Kommunikationstechnologien in der Landesverwaltung für erforderlich, neben den technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit, die generelle Zulässigkeit und die Anwendungsbreite der einzelnen Verfahren auch in den Geschäftsordnungen der Ministerien und der ihnen nachgeordneten Behörden zu regeln.
Den datenschutzrechtlichen Risiken, die mit der Umsetzung der behördenübergreifenden Vernetzung von Informations- und Kommunikationstechnik, **unabhängig** von einer bestimmten Verwaltungsaufgabe, allein aus dem Einsatz solcher Technologien entstehen, muss bereits in der Planungsphase begegnet werden.

## IV. Tätigkeitsbericht – 1999 (01.04.1997 - 31.03.1999)

### 8. Entwicklung der automatisierten Datenverarbeitung

### 8.1 Automatisierte Datenverarbeitung in der Landesverwaltung

Auch der zurückliegende Berichtszeitraum ist durch eine Erweiterung des Bestandes an PC-Technik und eine Verbesserung der Ausstattungsqualität in den Obersten Landesbehörden gekennzeichnet. Deutlich wird diese Entwicklung im 4. Gesamtplan der Informationstechnik - 1998 dokumentiert, den das Ministerium des Innern entsprechend dem Gem. RdErl. StK u. der übrigen Ministerien. vom 01.06. 1992, MBl. LSA, S. 805, jährlich auf der Grundlage der Ressortpläne erstellt.

Neue Dimensionen und damit verbunden Handlungsbedarf im Hinblick auf die Beachtung des Datenschutzes zeichnen sich bei der Planung, Einführung und dem Ausbau von landesweiten bzw. ressortübergreifenden Projekten und Vorhaben ab. Zu nennen sind hier z.B.

- das **H**aushalts-**A**ufstellungs-, -**M**anagement- und **I**nformations-**S**ystem **S**achsen-**A**nhalt (**HAMISSA**),
- das Projekt "**Uni**x im **F**inanz**a**mt" (**UNIFA**) und
- das länderübergreifende Projekt "**F**öderales **i**ntegriertes **s**tandardisiertes **c**omputergestütztes **S**teuersystem" (**FISCUS**) im Bereich der Finanzverwaltung,
- das Projekt "**Elektronisches Grundbuch**" im Bereich der Justiz sowie
- das **Pol**izeiliche **I**nformations**s**ystem Sachsen-Anhalt (**POLIS-neu**) im Bereich des Ministeriums des Innern.

In diesem Zusammenhang erinnert der Landesbeauftragte alle Ressorts an die gesetzliche Verpflichtung zu seiner rechtzeitigen Unterrichtung über die Planungen beim Aufbau automatisierter Informationssysteme, wenn in ihnen personenbezogene Daten verarbeitet werden sollen (§ 22 Abs. 4 Satz 2 DSG-LSA).

Neue Wege beschreitet das Land bei seiner Beteiligung am Projekt **"TESTA Deutschland"**. Kern dieses Projektes ist die Bereitstellung eines **bundesweiten** Intranet für die öffentliche Verwaltung, zu dem neben den Bundesländern auch der Bund sowie seine nachgeordneten Behörden und Einrichtungen und auch der kommunale Bereich zum Beitritt berechtigt sein sollen. Grundlage bildet ein zwischen dem Thüringer Innenministerium und der Deutschen Telekom AG im Oktober 1998 abgeschlossener Rahmenvertrag zur Erstellung der "TESTA-Plattform Deutschland". Am Pilotversuch beteiligen sich neben Thüringen die Länder Rheinland-Pfalz, Nordrhein-Westfalen, Hessen, Hamburg, Sachsen und Brandenburg.
Das Projekt "TESTA-Deutschland" ist Teil des **europäischen** Projektes **"TESTA"** (**T**rans **E**uropean **S**ervices for **T**elematics between **A**dministrations), welches die Vernetzung von Standorten der öffentlichen Verwaltung der EU-Länder zum Ziel hat. Mit dem Zugang zu "TESTA" wird neben der Kommunikation untereinander innerhalb von Deutschland auch die Nutzung länderübergreifender Dienste ermöglicht werden.
Der Rahmenvertrag, der auch dem Landesbeauftragten vorliegt, beinhaltet z.Zt. **keine** grundsätzlichen Aussagen zur Datensicherheit. Lediglich in den Leistungsbeschreibungen zum Rahmenvertrag (Anhang 2, Teil A, Beschreibung des Kommunikationssystems, Abschnitt 3: Zusätzliche Leistungen) findet sich der Hinweis, dass auf "Kundenwunsch" durch

die Deutsche Telekom AG nach vorgegebenen Anforderungen ein Firewall-Konzept erarbeitet werden kann. Ergänzend heißt es weiter, dass eine Firewall zur Zeit in diesem Rahmenvertrag nicht vorgesehen sei, aber in einer weiteren Projektphase angeboten werden könnte.
Auf seine Anfrage zu diesem Projekt wurde dem Landesbeauftragten vom Ministerium des Innern mitgeteilt, dass vorerst im Landesrechenzentrum in Halle eine Anbindung an das TESTA-Deutschland-Netz über ein zweistufiges Verfahren (Router mit IP-Filterung und ein weiterer Router mit Network-Adress-Translation (NAT)) erfolgt. Über den Einsatz von Krypto-Boxen zur Leitungsverschlüsselung ist noch keine endgültige Entscheidung getroffen worden. Die Integration weiterer Sicherheitseinrichtungen soll verfahrensbezogen und bedarfsorientiert vorgenommen werden.
Der Landesbeauftragte bekräftigt deshalb seine Hinweise und Forderungen aus dem III. Tätigkeitsbericht (S. 28 ff). Der Wahrnehmung der Rechtsverantwortung nach § 14 Abs. 1 DSG-LSA, gerade bei der Planung und Einrichtung neuer bundes- bzw. sogar europaweiter Kommunikationsbeziehungen, kommt hierbei eine Schlüsselrolle zu. Die Beachtung der datenschutzrechtlichen Grundsätze der Erforderlichkeit, der Verhältnismäßigkeit und die Realisierung angemessener Maßnahmen zur Datensicherheit auf der Basis einer entsprechenden Risikoanalyse müssen zum festen Bestandteil bei der Umsetzung von IT-Projekten für **jede** öffentliche Stelle, von der Gemeinde bis zum Ministerium, werden.
Der Landesbeauftragte steht hier im Rahmen seines Beratungsauftrages den öffentlichen Stellen zur Verfügung. Er regt weiterhin an, unter Beachtung der stürmischen Entwicklung im Bereich der Informations- und Kommunikationstechnik, die IT-Grundsätze aus dem Jahr 1992 auch hinsichtlich der Verpflichtungen der öffentlichen Verwaltung zur Sicherstellung des Datenschutzes zu überarbeiten. Auch hierfür bietet er seine Unterstützung an.

### 8.2 Neue Strukturen und Technologien im Landesnetz

Im ITN-LSA haben sich im zurückliegenden Berichtszeitraum wesentliche Veränderungen vollzogen. Hierzu zählen der Einsatz leistungsfähiger Multiplexer-Knotentechnik, die weitere Erhöhung von Bandbreiten des Leitungsnetzes, die Planung und schrittweise Realisierung von Richtfunkstrecken zur Beseitigung von Belastungsspitzen sowie die Integration der Sprachkommunikation (Einbindung der TK-Anlagen der Landesregierung). Das zuständige Ministerium des Innern als Netzbetreiber fasst seine Aktivitäten unter dem Arbeitsbegriff "**Corporate Network der Polizei und der Verwaltung des Landes Sachsen-Anhalt" (CNPV LSA)** zusammen.

#### 8.2.1 Elektronische Post

Der E-Mail-Dienst, allgemein auch als "elektronische Post" bezeichnet, ist fast flächendeckend in der Landesverwaltung eingeführt. Das Land verfügt seit Mai 1998 hierzu über zwei zentrale "Postämter" (sog. MTA-Kopfstationen), die im Ministerium für Wirtschaft und Technologie in Magdeburg und im Landesrechenzentrum (LRZ) in Halle eingerichtet wurden. Die Kopfstation im Wirtschaftsministerium deckt dabei die Nord-Region und die Kopfstation im LRZ Halle die Süd-Region des Landes ab. Gleichzeitig besteht die Möglichkeit, bei Störung einer primären Kopfstelle die andere Kopfstelle alternativ zu benutzen. Für eine gewisse Ausfallsicherheit hat die Landesregierung damit Vorsorge getroffen. Bei Maßnahmen zum Datenschutz besteht aber noch Handlungsbedarf.

Über die spezifischen **Sicherheitsrisiken** beim E-Mail-Dienst, wie die Möglichkeiten zum Mitlesen, Verändern bzw. Verfälschen von elektronischen Nachrichten oder zum Erstellen von Nutzerprofilen, hat der Landesbeauftragte in seinem III. Tätigkeitsbericht (S. 59 ff) berichtet. Die Hinweise haben nichts von ihrer Aktualität verloren. Eine weitere Gefährdung stellen **Computerviren** dar, die sich in einem Attachement der E-Mail (Anhang in einer E-Mail) befinden können.
Bisher ist es bei einem vom Ministerium des Innern vorgestellten Entwurf einer "Regelung zur elektronischen Post im Ministerium des Innern", die Grundlage für eine landesweite Regelung sein sollte, geblieben.
Der Landesbeauftragte fordert deshalb die Landesregierung auf, noch im Verlauf des Jahres 1999 zur Nutzung der "elektronischen Post" eine landeseinheitliche Regelung zu schaffen, in der auch die Belange des Schutzes personenbezogener Daten Berücksichtigung finden.

### 8.2.2 Sicherheitskonzept für das ITN-LSA

Auch das seit langem vom Landesbeauftragten **geforderte Sicherheitskonzept für das ITN-LSA** (vgl. III. Tätigkeitsbericht, S. 31 f) liegt **bisher nur als Entwurf** vor und lässt auf sich warten. Das Ministerium des Innern begründet die Verzögerung mit "personellen" Engpässen. Dieser Grund entlässt das Ministerium aber nicht aus seiner gesetzlich festgelegten Verantwortung zur Sicherstellung des Datenschutzes, die ihm besonders als Netzbetreiber obliegt. Der Landesbeauftragte fordert deshalb die Landesregierung auf, nach Abschluss der Firewall-Zertifizierung verbindliche Regelungen in einem prüffähigen Sicherheitskonzept vorzulegen.
Eine Verzögerung ist bei der Zertifizierung der Firewall zum Anschluss des ITN-LSA an das Internet eingetreten, deren Inbetriebnahme bereits für April 1998 vorgesehen war. Die Zertifizierung selbst obliegt dem BSI und ist vom Abschluss der Überprüfung durch die dafür zugelassenen Unternehmen abhängig. Die erfolgreiche Zertifizierung der Firewall bildet die Voraussetzung zur Schaffung eines zentralen und kontrollierten Übergangs vom ITN-LSA zum Internet.
Dieser Übergang stellt allerdings nur einen, wenn auch wichtigen, Baustein des Sicherheitskonzeptes für das ITN-LSA dar. Das Netz wird immer nur so stark (sicher) sein, wie die schwächste Stelle seiner Teilnehmer!
Regelungen zum Schutz besonders sensibler personenbezogener Daten bei ihrer Übertragung im Landesnetz fehlen noch in diesem Sicherheitskonzept. Hierzu gehören personenbezogene Daten, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen, wie z.B. dem Arzt-, Sozial- und Steuergeheimnis.

### 8.2.3 Datenschutz durch Technik - Datenschutzfreundliche Technologien

Auch in Sachsen-Anhalt muss zukünftig bereits bei der Planung der IuK-Systeme, die der Verarbeitung personenbezogener Daten dienen, das Prinzip der **Datensparsamkeit** wesentlich stärker durch die öffentlichen Stellen beachtet werden. Das Ziel muss darin bestehen, so wenig personenbezogene Daten wie möglich zu erheben und zu verarbeiten. Bei der Entwicklung von automatisierten Verfahren sowie bei der Auswahl von Hard- und Softwareprodukten durch öffentliche Stellen müssen diese Prinzipien zunehmend Berücksichtigung finden.

**Datenschutzfreundliche Technologien** lassen sich aber nur dann wirksam realisieren, wenn das Bemühen um Datensparsamkeit die Entwicklung und den Betrieb von IuK-Systemen ebenso stark beeinflusst wie die Forderung nach Datensicherheit. Datensparsamkeit bis hin zur **Datenvermeidung**, z.B. durch Anonymisierung und Pseudonymisierung personenbezogener Daten, spielt bisher in der Landesverwaltung und auch im kommunalen Bereich noch eine untergeordnete Rolle.
Diese Möglichkeiten der modernen Datenschutztechnologie, die mit dem Begriff **"Privacy enhancing technology - PET"** eine Philosophie der Datensparsamkeit beschreiben und ein ganzes System technischer Maßnahmen umfassen, sollten zunehmend genutzt werden. Die Datenschutzbeauftragten des Bundes und der Länder forderten im **Oktober 1997 in ihrer Entschließung (Anlage 10)** von den Gesetzgebern, dass sie die Verwendung datenschutzfreundlicher Technologien durch Schaffung rechtlicher Rahmenbedingungen unterstützen. Als positive Beispiele sind der Mediendienste-Staatsvertrag der Länder und auch das Teledienstedatenschutzgesetz des Bundes zu nennen, die bereits den Grundsatz der Datenvermeidung normieren.
Der Landesbeauftragte regt deshalb an, z.B. die Möglichkeit der Anonymisierung sensibler personenbezogener Daten bei ihrer Übertragung im ITN-LSA als eine Alternative zur Verschlüsselung zu untersuchen.

## V. Tätigkeitsbericht – 2001 (01.04.1999 - 31.03.2001)

### 6. Entwicklung der automatisierten Datenverarbeitung

### 6.1 Automatisierte Datenverarbeitung in der Landesverwaltung

Lagen in der ersten Hälfte der 90er Jahre die Problembereiche bei der Ausrüstung und Ausstattung der Landesverwaltung mit PC-Technik, dem Beginn einer lokalen Vernetzung in den Behörden und der Schaffung der Grundlagen für den Aufbau eines Landesnetzes, so haben sich die Schwerpunkte zum Übergang ins Zeitalter der „globalen Informationsgesellschaft“ und des „Internets“ für die Landesverwaltung und damit auch für den Landesbeauftragten wesentlich geändert. Ein gutes Beispiel für diese Entwicklung ist das Projekt TESTA Deutschland (vgl. IV. Tätigkeitsbericht, S. 23 f), an dem auch das Land Sachsen-Anhalt beteiligt ist. TESTA Deutschland ist ein bundesweites Intranet für die öffentliche Verwaltung in Deutschland mit der Möglichkeit eines länderübergreifenden Zugriffs im Rahmen der EU. Ziel dieses europäischen Projektes ist letztendlich die Vernetzung von Standorten der öffentlichen Verwaltung aller EU-Länder (vgl. die folgende Ziff. 6.4).
Zukünftig werden sich die Landesverwaltung, aber auch die Städte und Gemeinden, verstärkt Fragestellungen und Konzepten zum sog „**Electronic Government**“ (auch **E-Government**) zuwenden. Vorbereitungen laufen hierzu allerorten, und heute sind neben dem Land Sachsen-Anhalt und vielen Landesbehörden auch die Landkreise, viele Städte und Gemeinden mit einer Homepage im Internet vertreten. Mit dieser „Serviceorientierung“ der Verwaltung soll neben dem bereits bestehenden Informationsangebot die Nutzung der modernen Kommunikationstechnologien durch aktive Interaktionsmöglichkeiten für die Bürgerinnen und Bürgern über das Internet zur Inanspruchnahme von Verwaltungsdienstleistungen der Behörden wesentlich erweitert werden.
Aber nur Serviceangebote der Verwaltung, die dem Recht auf informationelle Selbstbestimmung gerecht werden, nützen den Bürgerinnen und Bürgern letztendlich. Deshalb hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Arbeitsgruppe im Oktober 1999 beauftragt, sich mit dieser Form der Modernisierung der Verwaltung zu befassen. Als Ergebnis dieser Arbeitsgruppe verabschiedete die **Konferenz am 12./13.10.2000 eine Entschließung**, in der grundsätzliche Empfehlungen zum Datenschutz für eine **serviceorientierte Verwaltung** gegeben wurden **(Anlage 19).** Ausführlich sind die Ergebnisse und Wertungen der Arbeitsgruppe in der **Broschüre „Vom Bürgerbüro zum Internet - Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung**“ dargestellt. Diese ist vom Landesbeauftragten in alle Bereiche der Landes- und Kommunalverwaltung verteilt worden und kann natürlich auch von den Bürgerinnen und Bürgern abgefordert werden.

Mittlerweile verfügt das Land über eine moderne Kommunikationsinfrastruktur, die sich auf der Basis des ITN-LSA entwickelt hat und die heute für die Landesverwaltung die Möglichkeit bietet, unter Nutzung der Internetdienste (wie z.B. WWW, E-Mail, NNTP (NEWS), FTP) sowohl im internen Verwaltungsnetz des Landes (Intranet), im TESTA-Deutschland-Netz als auch im Internet zu arbeiten bzw. zu kommunizieren.
Im aktuellen Berichtszeitraum hat die Landesverwaltung große Anstrengungen bei der Ausstattung der Mitarbeiterarbeitsplätze mit Informations- und Kommunikationstechnik, bei der Schaffung einer modernen Kommunikationsinfrastruktur in den Behörden und beim weiteren Um- bzw. Ausbau des ITN-LSA unternommen. Hervorzuheben ist das Konzept zur Inbe-

triebnahme weiterer neuer leistungsfähiger Netzknotentechnik (Einsatz von dynamischen Bandbreitenmultiplexern - dBBM) bei gleichzeitiger Integration der Sprachkommunikation sowie der Aufbau eines sog. Backbone-Bereiches. Die Erneuerung der Netzknotentechnik in Verbindung mit der Umstellung auf ein dynamisches Routingkonzept im Backbone-Bereich des ITN-LSA soll voraussichtlich bis Ende 2002 abgeschlossen werden.
Neben dem ITN-LSA bestehen nunmehr zwei weitere virtuelle Netze: das Telekommunikation-Sondernetz der Polizei für Telefonie (TKSoNe-Pol) und das Telekommunikation-Netz der Landesverwaltung für Telefonie (TK-Verw.). Das zuständige Ministerium des Innern als Netzbetreiber benutzt deshalb auch die Bezeichnung **"Corporate Network der Polizei und der Verwaltung des Landes Sachsen-Anhalt" (CNPV LSA)**.
Das Konzept der Trennung von Sprach- und Datenverkehr durch getrennte Bussysteme in den dBBM und die Übertragung in getrennten Basiskanälen (sog. B-Kanälen) klingt plausibel. Das für die Sicherheit im CNPV LSA verantwortliche übergeordnete Managementsystem der dBBM-Netzknoten erkennt nach Aussage des Ministeriums des Innern eventuelle Manipulationen an den dBBM und verwirft diese durch die eigene, zentrale Konfiguration. Eine Überprüfung dieser Mechanismen und deren Implementierung muss im Rahmen der **anstehenden Erstellung eines Sicherheitskonzepts für das ITN-LSA** durch das zuständige Ministerium des Innern mit in Erwägung gezogen werden.

### 6.2 Das IT-Leitbild der Landesregierung

Die Landesregierung hat im zurückliegenden Berichtszeitraum einen Schwerpunkt ihrer Arbeit auf die konzeptionelle Gestaltung zur zukünftigen Entwicklung des IT-Einsatzes in der Landesverwaltung gelegt.
Ausgangspunkt dieser Aktivitäten bildete das im Auftrag des Ministeriums des Innern erstellte **Gutachten zur „Organisations- und Wirtschaftlichkeitsuntersuchung der Informationstechnik im Land Sachsen-Anhalt“ vom 31.3.1999**. Die Untersuchung umfasste die großen Infrastruktureinrichtungen der Informationstechnik der Ressorts Inneres, Finanzen, Justiz und Landwirtschaft. Nach Auswertung dieses Gutachtens erfolgte durch die Landesregierung die Bildung einer Projektorganisation mit einer **Steuerungsgruppe auf der Ebene der Staatssekretäre** sowie die Einsetzung einer Projektgruppe KIT LSA („Konzeption für die Informations- und Kommunikationstechnik des Landes Sachsen-Anhalt“). Das durch die Projektgruppe KIT LSA erarbeitete **IT-Leitbild LSA** wurde am 20.03.2000 durch die Steuerungsgruppe verabschiedet und veröffentlicht.
Als ein Ziel soll bei der Bereitstellung von Diensten zur umfassenden Kommunikation, Kooperation und Information die Verfügbarkeit, Vertraulichkeit und die Integrität der Information gewährleistet werden. Inwieweit der Begriff „Information“ auch die personenbezogenen Informationen über die Bürgerinnen und Bürger einschließt und damit auch der im Grundgesetz geschützte und zusätzlich in der Verfassung des Landes Sachsen-Anhalt verankerte Schutz des Persönlichkeitsrechts gewährleistet wird, ist dem IT-Leitbild nicht weiter zu entnehmen.
Die Beachtung der datenschutzrechtlichen Grundsätze der Datensparsamkeit, der Erforderlichkeit, der Verhältnismäßigkeit sowie die Realisierung wirksamer Maßnahmen der Datensicherheit erachtet der Landesbeauftragte als unabdingbare Voraussetzung auf dem Weg in die Informationsgesellschaft. Die Erwähnung des Datenschutzes im IT-Leitbild hätte hier ein Zeichen setzen können.

**Wiederholt hat der Landesbeauftragte in den zurückliegenden Jahren auf Defizite beim Datenschutz und bei der Datensicherheit hingewiesen**.
Regelungsbedarf bzw. Nachholbedarf sieht er bei zentralen Themen wie:

- **dem Sicherheitskonzept für das Landesnetz (ITN-LSA),**
- **dem Projekt TESTA-Deutschland,**
- **der Neufassung der IT-Grundsätze für die Landesverwaltung,**
- **der einheitlichen Regelung zur Nutzung des E-Mail-Dienstes,**
- **dem Aufbau eines zentralen Verzeichnisdienstes einschließlich der Public Key Infrastruktur (PKI) des Landes sowie der zukünftigen Anwendungen beim E-Government.**

Der Rechtsverantwortung der Obersten Landesbehörden nach § 14 Abs. 1 DSGLSA kommt gerade bei der Planung und Einrichtung landesweiter Verfahren zur Verarbeitung personenbezogener Daten bzw. bei der umfassenden Vernetzung zur Schaffung landes- bzw. weltweiter Kommunikationsbeziehungen eine Schlüsselrolle zu.
Im Rahmen der Erfüllung eigener Aufgaben trifft diese Verantwortung nach § 14 Abs. 1 DSG-LSA auch die Gemeinden und Landkreise.

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

Bereits im März 1995 (vgl. II. Tätigkeitsbericht S. 37) hatte der Landesbeauftragte auf das fehlende, bis heute noch nicht vorliegende Sicherheitskonzept für das ITN-LSA hingewiesen. Ab September 1995 wurde vom Netzbetreiber die verschlüsselte Datenübertragung von Sozialdaten im Landesnetz in den Regelbetrieb überführt.
Im März 1997 stellte der Landesbeauftragte in seinem III. Tätigkeitsbericht (vgl. S. 31 f) fest, dass das Ministerium des Innern nicht über einen Entwurf für das Sicherheitskonzept hinausgekommen war. Allerdings wurde für den Anschluss des ITN-LSA an das Internet die Zertifizierung der eingesetzten Firewalltechnik vorbereitet, die ein wesentlicher Bestandteil des Gesamtsicherheitskonzeptes für das Land sein sollte. Die Zertifizierung sollte durch das BSI erfolgen. Dabei kam es durch das starke Engagement des Herstellers der Firewallsoftware bei der Einführung des Informationsverbundes Bonn-Berlin (IVBB) zu einer erheblichen Verzögerung. Die spätere Grundsatzentscheidung des Ministeriums des Innern, eine weitere Verzögerung bei der Ausarbeitung des Sicherheitskonzepts zugunsten einer höherwertigen Zertifizierung in Kauf zu nehmen, wurde auch vom Landesbeauftragten mitgetragen.
Im **März 1999**, beim Abschluss des IV. Tätigkeitsberichtes, begründete die Landesregierung das weitere **Fehlen eines Sicherheitskonzepts** für das ITN-LSA mit **personellen Engpässen** beim Ministerium des Innern.
Auch im März 2001 liegt dem Landesbeauftragten **kein** prüffähiges Sicherheitskonzept für das ITN-LSA vor. Dabei wäre dies - angesichts der vielfältigen Aktivitäten der Landesverwaltung im Internet bzw. auf dem von Seiten der Politik propagierten Weg in die sog. „Informationsgesellschaft“ dringender erforderlich denn je.
Für die Nutzung der von der Landesregierung so gerne als modernen Kommunikationsweg herausgestellte „Datenautobahn“ muss es Verkehrsregeln geben! Im Übrigen steht die Landesregierung unter den gesetzlichen Forderungen des § 6 DSG-LSA.

Aus den Protokollen der regelmäßig stattfindenden Netzberatungen im TPA hat der Landesbeauftragte entnehmen können, dass das **Ministerium des Innern mit der Telekom AG im Dezember 2000 die Erstellung eines Sicherheitskonzepts für das ITN-LSA vereinbart hat**. **Das ist nach langer Zeit eine gute Nachricht**. Allerdings fehlt bisher dem Landesbeauftragten die dazu gesetzlich vorgeschriebene umfassende Information durch die Landesregierung (§ 22 Abs. 4 Satz 2 DSGLSA).
Ziel muss es nun sein, dass das Ministerium des Innern schnellstmöglich dieses Sicherheitskonzept für das ITN-LSA einschließlich der Regelungen zur Nutzung der Internetdienste ausarbeitet, mit den anderen Ressorts abstimmt und bis zum Jahresende auf dem Erlasswege für die Landesverwaltung verbindlich festlegt.
Die Ressorts haben im Rahmen ihrer eigenen Rechtsverantwortung nach § 14 Abs. 1 in Verbindung mit § 6 Abs. 2 DSG-LSA für sich und ihren nachgeordneten Bereich weitere Schutzvorkehrungen bei der Verarbeitung personenbezogener Daten zu treffen, wenn dies die Sensibilität der personenbezogenen Daten, die Einsatz- und Verarbeitungsbedingungen sowie das damit verbundene Gefährdungspotential zur Sicherung schutzwürdiger Interessen der Betroffenen erfordern.
Für notwendig hält der Landesbeauftragte auch die Schaffung eines ständigen Gremiums, das sich mit der **zukünftigen** konzeptionellen Gestaltung der IT-Sicherheit und der Fortschreibung des Sicherheitskonzepts des ITN-LSA unter den sich immer schneller verändernden Bedingungen in der IT-Entwicklung auseinandersetzt.
Der Landesbeauftragte verweist im Rahmen seines gesetzlichen Beratungsauftrages auch auf die aktuelle **Broschüre** zum Thema **„Datenschutz bei der Nutzung von Internet und Intranet“** (Redaktionsschluss 15.12.2000). Sie wurde vom Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder erstellt und vom Landesbeauftragten an die Landesverwaltung und die Kommunen verteilt. Der Text ist auch auf der Homepage des Landesbeauftragten im Intranet und Internet eingestellt und so für jedermann online verfügbar.

### 6.4 Projekt TESTA Deutschland

Der Landesbeauftragte hatte erstmalig in seinem IV. Tätigkeitsbericht (vgl. S. 23 f) über dieses europäische Projekt, an dem sich auch das Land Sachsen-Anhalt unter dem Begriff „TESTA Deutschland“ seit Dezember 1999 beteiligt, berichtet.
Das Land ist dem Rahmenvertrag im Januar 2000 beigetreten. Ziel dieses ehrgeizigen Projektes ist die Realisierung einer einheitlichen Kommunikationsplattform für den Datenaustausch

- zwischen den Bundesländern, den obersten Bundesbehörden und den Bundeseinrichtungen,
- der Bundesländer mit dem Bundesrat und dem Bund,
- der Bundesländer zu ihren Landesvertretungen in Brüssel, sowie
- zukünftig zu den EU-Mitgliedstaaten und der EU und auch
- mit und zwischen kommunalen Einrichtungen.

Hierzu erfolgt für das jeweilige Landesverwaltungsnetz (hier das ITN-LSA) der Anschluss an TESTA Deutschland über **einen** Lokationszugang.

Nach den Informationen, die dem Landesbeauftragten durch Recherchen im Intranet des Landes zur Verfügung stehen, sind durch das IP-Konzept und die Leitungsverschlüsselung in TESTA-Deutschland bereits Sicherheitsmaßnahmen durch den Netzprovider, d.h. die Deutsche Telekom AG und durch die beteiligten Nutzer getroffen worden, die vom Landesbeauftragten begrüßt werden. Hierzu gehören die Umsetzung von Maßnahmen wie:

- kein Zugang zum Internet über TESTA Deutschland,
- Routing nicht öffentlicher IP-Adressen in TESTA Deutschland,
- Network-Adress-Translation (NAT) am Local Domain-Zugang beim Nutzer,
- Leitungsverschlüsselung zwischen den Lokationsstandorten durch Installation von Krypto-Boxen zwischen der Nutzer- und Providerschnittstelle am Standort des Nutzers.

Eine offizielle Information über den bisher erreichten Sicherheitsstandard des Anschlusses des Landesverwaltungsnetzes an TESTA Deutschland und weitere Vorhaben hat den Landesbeauftragten allerdings vom zuständigen Ministerium des Innern noch nicht erreicht. Die gesetzliche Verpflichtung dazu besteht auch hier nach § 22 Abs. 4 Satz 2 DSG-LSA. Viele Problembereiche sind noch ungelöst.
Mit dem Einsatz von TESTA kommen aber auf die öffentlichen Stellen des Landes auch materielle datenschutzrechtliche Probleme zu. Das vom Deutschen Bundestag am **15.02.2001** verabschiedete Gesetz über die Rahmenbedingungen für elektronische Signaturen (**Signaturgesetz - SigG**) bildet dabei nur den Anfang. Neben dem SigG wird der Bundesgesetzgeber in naher Zukunft im Privatrecht neue Formvorschriften zur Erleichterung des elektronischen Rechts- und Geschäftsverkehrs hinsichtlich der elektronischen Unterschrift als Substitut der eigenhändigen Unterschrift und die elektronische Form als Option zur Schriftform sowie hinsichtlich der Vereinfachung des Rechtsverkehrs durch die Zulassung einer Textform für unterschriftslose Erklärungen einführen. Vorgesehen sind Änderungen im BGB (z.B. Einfügung der §§ 126a u. 126b) und der ZPO (z.B. §§ 130a, 292a, 299a) sowie weiterer 31 Gesetze und Verordnungen (vgl. BT-Drs. 14/4987).

### 6.5 Verzeichnisdienste

Verzeichnisdienste nach dem X.500/X.509 Standard bieten die Möglichkeit, durch ein standardisiertes Protokoll beliebige Informationen zu Objekten und Personen zu speichern. Damit besteht die Möglichkeit, in einem einzigen zentralen Verzeichnis (Directory) alle wichtigen Daten über einen Nutzer, also auch **personenbezogene Daten**, zu speichern und diese allen angeschlossenen Systemen zugänglich zu machen. Der Zugriff auf die Daten des Directory erfolgt durch ein eigenes Zugangsprotokoll, dem Directory Access Protocol (DAP). Überwiegend wird aber heute eine vereinfachte Form dieses Protokolls, das Lightweight Directory Access Protocol (LDAP), auf den Clients eingesetzt. Es bietet die Möglichkeit, eine Authentifizierung von Benutzern gegenüber dem Directory festzulegen.

Als fortentwickeltes Modell hat sich heute der X.509 Standard in der Praxis durchgesetzt. Vor allem in der Version **X.509 Teil 3** (X.509v3; 1996) als Authentifizierungsstandard für Kommunikationsnetze (sog. X.509-Zertifikate). Dieser Teil 3 beschreibt ein Format für digitale **Zertifikate,** die von einer dritten, vertrauenswürdigen, unabhängigen Instanz (Trust Third Party) signiert werden und ein Format für Sperrlisten. Eine solche dritte, unabhängige Instanz kann z.B. ein sog. Trust Center sein. Dabei hat das digitale Zertifikat eines Trust Cen-

ters die Funktion, den Namen und den öffentliche Schlüssel eines Anwenders miteinander sicher in Verbindung zu bringen.
Nach Inkrafttreten des Signaturgesetzes (SigG vom 22.07.1997, BGBl. I S. 1870) und der Signaturverordnung (SigV vom 22.10.1997, BGBl. I S. 2498) wurde der X.509v3-Standard durch das BSI in Zusammenarbeit mit der Gesellschaft für Mathematik und Datenverarbeitung vor allem um rechtliche Inhalte erweitert. Dazu gehören folgende Zertifikatsfelder:

- Nutzungsbeschränkungen (sog. Attribut-Zertifikat des Trust Centers)
- Erstellungsdatum (des Zertifikats)
- Vertretungsvollmacht (für Dritte)
- Zulassung (Bescheinigung des Trust Centers für Zulassung z.B. als Anwalt, Notar u.ä.)
- Beschränkungen (z.B. bis zu welchem Geldbetrag der Anwender mit seinem Zertifikat bürgt).

Mit der sog. **Sperrliste** (auch schwarze Liste genannt) kann ein Trust Center ausgegebene Zertifikate, z.B. bei Verlust des geheimen Schlüssels durch den Anwender, für ungültig erklären (sperren). Das Vorhalten bzw. das zum Abruf bereithalten dieser Zertifikate der Anwender und der Sperrliste durch das Trust Center bildet eine der wesentlichen Voraussetzungen zum Aufbau einer Public Key Infrastruktur (PKI).
Dem **Vorteil** eines Verzeichnisdienstes stehen aber auch **Nachteile** gegenüber. So sind die Administratoren solcher Verzeichnisdienste in der Lage, alle zu einer Person gespeicherten Daten einzusehen. Schwache Authentifizierungsmechanismen und die oberflächliche Nutzung der Zugriffskontrollmechanismen, was anderen Nutzern möglicherweise Missbrauch erleichtert, sind weitere Risikofaktoren, die zu einer Verletzung des Datenschutzrechtes in diesem Bereich führen können.

Weitergehende Informationen finden sich in der vom Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder herausgegebenen **Orientierungshilfe „Datenschutzrechtliche Aspekte beim Einsatz von Verzeichnisdiensten“** (Stand: September 2000). Auch diese Orientierungshilfe ist auf der Homepage des Landesbeauftragten eingestellt und kann auch bei ihm abgefordert werden.

## VI. Tätigkeitsbericht – 2003 (01.04.2001-31.03.2003)

### 7. Entwicklung der automatisierten Datenverarbeitung

### 7.1 Automatisierte Datenverarbeitung in der Landesverwaltung

Über den Stand der Entwicklung des Einsatzes der Informations- und Kommunikationstechnik (IuK) in der Landesverwaltung aus datenschutzrechtlicher Sicht hat der Landesbeauftragte zuletzt in seinem V. Tätigkeitsbericht (Ziff. 6) ausführlich informiert.
Das Land verfügt über eine moderne Kommunikationsinfrastruktur, die sich auf der Basis des ITN-LSA entwickelt hat und die gegenwärtig für die Landesverwaltung Kommunikationsmöglichkeiten sowohl im internen Landesverwaltungsnetz (Intranet), im TESTA-Deutschland-Netz als auch im Internet bietet. Das Ministerium des Innern als Netzbetreiber des ITN-LSA benutzt deshalb auch die Bezeichnung "Corporate Network der Polizei und der Verwaltung des Landes Sachsen-Anhalt" (CNPV LSA). Beim Einsatz moderner IuK durch die Landesverwaltung, bei dem in vielfältiger Weise personenbezogene Daten automatisiert erhoben, verarbeitet oder genutzt werden, sind die Rechte der Bürgerinnen und Bürger wirksam zu schützen (§ 1 DSG-LSA).
Mit der Novellierung des DSG-LSA vom 21.08.2001 (GVBl. LSA S. 384) ist der Zweck des Gesetzes in § 1 Abs. 2 dahin gehend präzisiert worden, dass öffentliche Stellen Verfahren zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten an dem Ziel auszurichten haben, so wenig wie möglich personenbezogener Daten zu erheben, zu verarbeiten oder zu nutzen. Damit wird den datenschutzrechtlichen Prinzipien der Datenvermeidung bzw. Datensparsamkeit Rechnung getragen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen. Der Landesgesetzgeber hat damit rechtliche Rahmenbedingungen geschaffen, die die Anwendung datenschutzfreundlicher Technologien unterstützen. Der Landesbeauftragte hatte diese Thematik bereits in seinem IV. Tätigkeitsbericht (Ziff. 8.2.3) dargestellt und erläutert.
Der Landesbeauftragte weist in diesem Zusammenhang erneut auf die Rechtsverantwortung der Obersten Landesbehörden nach § 14 Abs. 1 DSG-LSA, gerade bei der Umsetzung komplexer Strategien zur umfassenden Vernetzung bzw. zur Schaffung landes- und weltweiter Kommunikationsbeziehungen, hin. Bei komplexen Verfahren wie u.a. dem **E-Government-Konzept Sachsen-Anhalt** oder dem **Landesportal Sachsen-Anhalt** müssen künftig Datenschutzbelange, d.h. die bereichsspezifischen Datenschutzvorschriften, wie z.B. im Telekommunikations- und Medienrecht, bereits bei der Planung bzw. Einrichtung noch stärker Beachtung finden.
Dieser Verantwortung müssen auch die anderen in § 14 DSG-LSA genannten öffentlichen Stellen, insbesondere die Kommunen und die öffentlich-rechtlichen Körperschaften, genügen.

In diesem Zusammenhang ist wegen festgestellter Defizite nachdrücklich auf die gesetzliche Verpflichtung hinzuweisen, den Landesbeauftragten **rechtzeitig** über Planungen des Landes beim Aufbau automatisierter Informationssysteme zu unterrichten (§ 22 Abs. 4 Satz 2 DSG-LSA).
Das Ministerium des Innern ist derzeit im Auftrag der Staatskanzlei mit der Ausarbeitung eines **E-Government-Konzepts** für die öffentliche Verwaltung des Landes Sachsen-Anhalt befasst. Bis zum Jahr 2005 sollen die wichtigsten Dienstleistungen des Landes online im Internet angeboten und die internen Verwaltungsprozesse op-

timiert und rationalisiert sein. Seine grundsätzliche Position zum E-Government hat der Landesbeauftragte bereits im V. Tätigkeitsbericht (Ziff. 6.1) dargelegt.
Abschließend sei auf die aktuellen Handlungsempfehlungen **"Datenschutzgerechtes E-Government"** der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 30. November 2002 hingewiesen. Diese Handlungsempfehlungen wurden als Druckauflage seitens des Landesbeauftragten an alle Ressorts verteilt. Es gibt weiter eine rege Nachfrage, auch aus dem Kommunalbereich. Die Broschüre ist auch über seine Homepage als pdf-Datei herunterzuladen.

### 7.2 Neuordnung der IT-Organisation des Landes

In seinem V. Tätigkeitsbericht (Ziff. 6.2) hatte der Landesbeauftragte über das neue IT-Leitbild der damaligen Landesregierung informiert.
Mit ihrem **Kabinettsbeschluss "Übergreifende IT-Organisationsstruktur der Landesverwaltung" vom 19.03.2002 (MBl. LSA S. 363)** wurden weitere grundlegende Entscheidungen getroffen. Zu den wesentlichen Punkten dieses Kabinettsbeschlusses gehören:

- die Einrichtung der **Landesleitstelle IT (LIT)** zum **01.07.2002** als Referat 45 im Ministerium des Innern, ehemals Zentrale Stelle IT (ZIT, Ref. 34),
- die Bildung des **IT-Koordinierungsausschusses (IT-KA)**, der der LIT zugeordnet ist und diese bei ihrer ressortübergreifenden Koordinierungsarbeit unterstützen soll und der aus den IT-Verantwortlichen der Ressorts besteht

  sowie
- die Bildung eines **Landesinformationszentrums Sachsen-Anhalt (LIZ)** durch Herauslösung des ehemaligen Landesrechenzentrums aus dem Landesamt für Landesvermessung und Datenverarbeitung als wirtschaftlich eigenständigem Landesbetrieb nach § 26 LHO – mit der Funktion eines zentralen landesinternen Dienstleisters - sowie der Schaffung eines IT-Kompetenz-Centers im LIZ, sowohl für die Landes als auch für die Kommunalverwaltung (ohne Nutzungszwang).

Gleichzeitig mit der Einrichtung des IT-Koordinierungsausschusses (IT-KA) wurde der seit 1990 existierende Interministerielle Arbeitskreis Informationstechnik (IMA-IT) aufgelöst.
Als Folge dieser Entscheidungen der Landesregierung sieht der Landesbeauftragte gute Voraussetzungen, dass seine wiederholt geübte Kritik in den Tätigkeitsberichten der zurückliegenden Jahre hinsichtlich noch bestehender Defizite bei der Datensicherheit im Rahmen der strategischen Entscheidungen der LIT und des IT-KA verstärkt Berücksichtigung finden wird. Der Landesbeauftragte regte die Befassung des IT-KA mit nachfolgenden **Themenschwerpunkten** an:

- dem Sicherheitskonzept für das Landesnetz (ITN-LSA) und seiner Fortschreibung und der Zertifizierung nach den Common Criteria (CC),
- dem Projekt TESTA-Deutschland bezüglich der Anbindung an das ITN-LSA,
- der Neufassung der IT-Grundsätze für die Landesverwaltung mit Festlegung von Sicherheitsstandards bezüglich Datensicherheit (§ 6 DSGLSA),

- der Schaffung einer einheitlichen Regelung zur Nutzung des E-Mail-Dienstes auf der Grundlage der Musterdienstanweisung zur Nutzung von Internet und E-Mail unter Beachtung sich abzeichnender Änderungen im Telekommunikationsrecht,
- der Installation der Public Key Infrastruktur (PKI) des Landes und der Lösung der Trust-Center-Problematik

  sowie
- den zukünftigen Anwendungen beim E-Government und beim Landesportal Sachsen-Anhalt.

An den Beratungen des IT-KA nimmt der Landesbeauftragte als Gastmitglied teil. Er bietet diesem Gremium seine Unterstützung an und sieht darin zugleich eine gute Voraussetzung, seinem gesetzlichen Beratungsauftrag gem. § 22 Abs. 4 Satz 1 DSG-LSA nachzukommen.

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

**Seit 1995** (III. Tätigkeitsbericht, Ziff. 8.2.2) hat sich der Landesbeauftragte wiederholt kritisch zum fehlenden Gesamtsicherheitskonzept für das bereits am **14. Oktober 1993 eingerichtete ITN-LSA** geäußert.
**Noch im März 2001** musste der Landesbeauftragte in seinem V. Tätigkeitsbericht (Ziff. 6.3) berichten, dass ihm **kein prüffähiges Gesamtsicherheitskonzept für das ITN-LSA** zur Stellungnahme vorlag, obwohl seit der Inbetriebnahme fast **8 Jahre** vergangen waren.

Das Erstaudit einer Sicherheitsuntersuchung erfolgte am 09.05.2001 und hatte eine Gültigkeit bis zum 31.07.2002. Die in Auftrag gegebene Sicherheitsuntersuchung des Landesnetzes wurde mit der Übergabe des **Erst-Zertifikates** am **29.11.2001** erfolgreich abgeschlossen.

Gegenstand der **Zertifizierung** waren **zwei** wesentliche **Sicherheitsziele**:
- Bereitstellung der *Verfügbarkeit* zentraler Kommunikationsdienste
- sehr hohe *Verfügbarkeit* der Transportfunktionalität des Netzes.

Im Januar 2003 informierte das Ministerium des Innern den Landesbeauftragten über das erfolgreich durchgeführte **Folgeaudit vom 28.11.2002**.
Dieses Zertifikat ist bis zum 31.12.2003 gültig. Der vollständige Auditbericht liegt dem Landesbeauftragten vor. Er geht davon aus, dass die im aktuellen Auditbericht noch aufgezeigten Mängel zeitnah beseitigt werden und er entsprechend unterrichtet wird.
Allerdings ist festzuhalten, dass die Erteilung des Zertifikats auf der Grundlage der Überprüfung nach der **internen** Richtlinie DOT-07 ("Zertifizierung von Organisation und Technik") der T-Systems ISS GmbH Bonn erfolgte.
Deshalb regt der Landesbeauftragte an, die Möglichkeiten der zukünftigen Zertifizierung des Landesnetzes bzw. einzelner ausgewählter Komponenten zur Abgrenzung des Evaluationsgegenstandes gemäß den international gültigen Common Criteria durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) prüfen zu lassen, auch wenn damit wesentlich höhere Kosten verbunden sein könnten.
Die Sicherheit beim Einsatz modernster Informations- und Kommunikationstechnik darf nicht aus Kostengründen vernachlässigt werden. Nur durch einen hohen Sicherheitsstandard und

dessen regelmäßiger Überprüfung durch gesetzlich dafür bestimmte Institutionen wie dem BSI wird dem Auftrag in § 1 Abs. 1 DSG-LSA langfristig Rechnung getragen, eine Beeinträchtigung des Persönlichkeitsrechts der Bürgerinnen und Bürger durch den Umgang öffentlicher Stellen mit ihren personenbezogenen Daten zu verhindern.
Die bereits vorhandenen einzelnen Dokumente zur Sicherheitspolitik des ITN-LSA sollten in ein Gesamtsicherheitskonzept einfließen, welches auch die besonderen Anforderungen der Datensicherheit für die Verarbeitung personenbezogener Daten nach § 6 Abs. 2 DSG-LSA berücksichtigt. Ein
solches Gesamtkonzept sollte ein zentrales Thema für die zukünftige Arbeit im IT-KA zur Ausarbeitung von IT-Standards sein.

Mit der Festlegung einer verbindlichen Sicherheitspolitik und den entsprechend einzuhaltenden Sicherheitsstandards für alle Teilnehmer im ITNLSA muss die längst fällige Überarbeitung der IT-Grundsätze vom 01.06.1992 (MBl. LSA S. 805) sowie des sog. Netz-Erlasses zum ITN-LSA
vom 07.02.1994 (MBl. LSA S. 1251) erfolgen.
Die Ressorts haben im Rahmen ihrer Rechtsverantwortung nach §§ 14 Abs. 1 i.V.m. 6 Abs. 2 DSG-LSA für sich und ihren nachgeordneten Bereich weitere Schutzvorkehrungen bei der Verarbeitung personenbezogener Daten zu treffen, wenn dies die besondere Qualität der personenbezogenen Daten erfordert, wie z.B. bei personenbezogenen Daten, die besonderen gesetzlichen Geheimhaltungsbestimmungen unterliegen (Sozialdaten, medizinische Daten, Steuerdaten) sowie anderen personenbezogenen Daten besonderer Art (§ 2 Abs. 1 Satz 2 DSG-LSA). Das ITN-LSA stellt insofern "nur" ein Transportsystem mit einem definierten Sicherheitsstandard dar.

### 7.4 Zentraler Verzeichnisdienst im ITN-LSA

Verzeichnisdienste sind für die reibungslose Kommunikation im Landesnetz, im TESTA-Deutschland-Netz sowie im Internet eine unabdingbare Voraussetzung. Aus diesem Grund hatte der frühere IMA-IT mit Beschluss vom 10.04.2001 die Bildung einer **Arbeitsgruppe Verzeichnisdienste** zur Erarbeitung eines Konzeptes für einen zentralen Verzeichnisdienst der Landesverwaltung unter Federführung des Landesrechenzentrums eingesetzt.
Der Landesbeauftragte wurde dabei beteiligt. Im V. Tätigkeitsbericht (Ziff. 6.5) ist bereits über den aktuellen in der Praxis verwendeten Standard (X.509v3 von 1996) für Verzeichnisdienste ausführlich informiert und dabei auf die datenschutzrechtlichen Probleme beim Einsatz solcher Verzeichnisdienste hingewiesen worden.
Problematisch sind insbesondere die Handhabung des administrativen Zugriffs auf diesen Verzeichnisdienst, seine Abschottung sowie die Veröffentlichungspraxis der Mitarbeiterdaten. Dabei ist aus datenschutzrechtlicher Sicht wichtig, in welche Netze die Einstellung dieser personenbezogenen Daten erfolgt. Bei der Einstellung ins **Landesnetz** (ITN-LSA) unter Beachtung des Grundsatzes der Erforderlichkeit - nicht jeder Mitarbeiter einer Behörde muss im Verzeichnisdienst geführt werden - ist die Zustimmung der Mitarbeiter nicht erforderlich. Eine Information durch die Behördenleitung kann aber für Transparenz und Vertrauen bei den Bediensteten sorgen.
Eine Einstellung dieser Daten für den Abruf im **TESTA-Deutschland-Netz** bedarf, da hierbei Daten außerhalb der Landesverwaltung genutzt werden können, stets der Einwilligung der betroffenen Bediensteten. Bei einer Einstellung dieser Daten im zentralen Verzeichnisdienst

für einen Abruf über das **Internet** ist vorab zu prüfen, ob dabei die gesetzlichen Voraussetzungen für die Übermittlung dieser personenbezogenen Daten ins Ausland vorliegen.

Diese grundlegenden Hinweise hat das Ministerium des Innern berücksichtigt
Das Landesinformationszentrum führt die Anbindung des zentralen Verzeichnisses des Landes über die Verwaltungs-PKI im TESTA-Deutschland-Netz durch. Über das HTTP/LDAP-Gateway im TESTA-Deutschland-Netz wird das zentrale Verzeichnis des Landes mit den Verzeichnisdiensten der anderen Bundesländer verbunden.
Mit der Differenzierung durch Ziffern beim Attribut "Veröffentlichungshinweis" in
0 – keine Veröffentlichung

1 – Veröffentlichung im Intranet (Landesnetz)

2 – Veröffentlichung im TESTA-Deutschland-Netz und

3 – Veröffentlichung im Internet,

wobei der Standard-Wert auf "1" gesetzt wurde, ist den datenschutzrechtlichen Belangen Rechnung getragen worden.
In einem Gemeinsamen Runderlass vom 01.01.2003 (MBl. LSA S. 35) hat das Ministerium des Innern im Einvernehmen mit der Staatskanzlei, den übrigen Ministerien, dem Landesrechnungshof und der Landtagsverwaltung die Richtlinie zum Verzeichnisdienst der Landesverwaltung bekannt gemacht und darin entsprechende datenschutzrechtliche Hinweise für eine über das Landesnetz hinausgehende Veröffentlichung gegeben.
Bei seinen Kontrollen wird der Landesbeauftragte ein besonderes Augenmerk auf die Erforderlichkeit der Personaleinträge in den Verzeichnissen der Ressorts und die Einhaltung der technischen und organisatorischen Maßnahmen nach § 6 Abs. 2 DSG-LSA legen, insbesondere was die Authentifizierungsmechanismen und die Nutzung der Zugriffskontrollmechanismen betrifft.

### 7.5 Neues IP- und Routingkonzept im ITN-LSA

Der Landesbeauftragte erinnert in diesem Zusammenhang an seine grundlegenden Ausführungen im III. Tätigkeitsbericht (Ziff. 8.1 f) zum Thema Vernetzung bzw. Herstellung neuer Kommunikationsbeziehungen.
In seinem V. Tätigkeitsbericht (Ziff. 6.1) hatte der Landesbeauftragte über die Erneuerung der Netzknotentechnik (Ablösung der ASCOM-Knotentechnik) in Verbindung mit dem Konzept zur Umstellung auf ein **dynamisches Routing** im Backbone-Bereich des ITN-LSA informiert. Die Erneuerung der Netzknotentechnik (Einsatz von DATUS-Knotentechnik) ist nun im Wesentlichen abgeschlossen.
Das z.Zt. noch praktizierte IP-Konzept entstand 1992 im Zusammenhang mit dem Aufbau des ursprünglichen ITN-LSA auf Basis der ASCOM-Knotentechnik.
Durch die Verwendung vorwiegend **statischer** Routen wurde die Administration im Zusammenhang mit dem Anwachsen der Verwaltung, des Internetverkehrs und der zunehmenden Routerzahl extrem
komplex und aufwendig.
Das Land Sachsen-Anhalt hatte damals im Zuge des Aufbaus des ITNLSA vom DENIC, der Deutschen Vergabestelle für IP-Adressen, die international gültige **Class B** Adresse 164.133.0.0 zugewiesen bekommen. Die Adresse wurde durch den Betreiber des ITN-LSA, das Technische Polizeiamt Magdeburg (TPA), in Subnetze (Class C) aufgeteilt und an die

Teilnehmer des Netzes auf Antrag vergeben. Zum gegenwärtigen Zeitpunkt sind fast alle Class C Netze (ca. 250 insgesamt)
im Netzwerk 164.133.0.0 vergeben. Daher mussten seitens des Netzbetreibers Maßnahmen ergriffen werden, um weiterhin IP-Adressen zur Verfügung stellen zu können.

**Neues IP-Konzept**
Zur Lösung des Problems hat sich das TPA in Abstimmung mit dem Ministerium des Innern für die Verwendung (Routing) von nicht offiziellen IP-Adressen im ITN-LSA in Verbindung mit der Umsetzung eines sog. Core-Router-Konzeptes entschieden.
Diese Lösung bietet neben der Erlangung ausreichender IP-Adressen die Möglichkeit für eine sukzessive systematische IP-mäßige Neustrukturierung des ITN-LSA. Derzeitig ist das ITN-LSA nach außen gegenüber dem Internet nur mit zwei IP-Netzen bekannt. Dies soll aus Sicherheitsgründen
so bleiben. Innerhalb des ITN-LSA ist es gleichgültig, welche IP Adressen verwendet werden. Wichtig ist dabei, dass an allen Übergängen zu anderen Fremdnetzen nur die Netzadresse 164.133.xxx.xxx des ITN-LSA sichtbar ist.

**Einsatz von sog. Core-Routern**
Mit Aufstellung der **Core-Router** und Einführung des dynamischen Routings über das dynamische Routingprotokoll **OSPF** (Open Shortest Path First – "kürzester Weg zuerst") werden neue IP Nummernkreise eingeführt. Dazu werden im Land Sachsen-Anhalt entsprechende OSPF-Sektoren eingerichtet. Jeder Sektor gehört zu einer sog. OSPF-Area. Damit wird es möglich, ein "Sammelrouting" einzuführen. Vorteile dieser Methode liegen in der Verringerung der Anzahl der zu verwaltenden Routen, in der Vereinfachung der Fehlersuche und somit der schnelleren Fehlererkennung und Beseitigung. Insgesamt entsteht für das ITN-LSA eine übersichtliche IP-Struktur. Ein Router einer Lokation braucht dann nur noch eine Defaultroute zum nächstgelegenem Core-Router zu kennen. Der Administrationsaufwand in den einzelnen Lokationen und Ressorts wird ebenfalls erheblich verringert. Veränderungen bei Netzadressen werden automatisch bekannt gemacht.

**Datenschutzrechtliches Fazit**
Die vorgenannten Veränderungen unterstützen in gewissem Umfang auch die in § 6 Abs. 2 DSG-LSA genannten Ziele der Datensicherheit (Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz).

Aus datenschutzrechtlicher Sicht bringt aber die Einführung des **dynamischen Routings** (OSPF) auch Probleme mit sich. So führt die Einführung dazu, dass **alle** Netze im gesamten ITN-LSA bekannt werden. Damit wäre theoretisch die Kommunikation "jeder mit jedem" bei automatischer Routenwahl möglich.
Unter Berücksichtigung der Rechtsverantwortung nach § 14 Abs. 1 DSGLSA sind aber im Sinne eines vorgelagerten Grundrechtsschutzes nach den Anforderungen des Bundesverfassungsgerichtes (BVerfGE 65,1) insbesondere die Grundsätze der **Verhältnismäßigkeit** und der Z**weckbindung** bei der Herstellung von Kommunikationsbeziehungen zu beachten.
Daraus folgt, die Herstellung neuer Kommunikationsbeziehungen (z.B. durch Routing) ist nur zulässig, wenn sie zur Erfüllung konkreter Verwaltungsaufgaben **erforderlich** ist. Auch sind die Zweckbindung bei der Erhebung und Verarbeitung personenbezogener Daten und der Grundsatz der informationellen Gewaltenteilung zu berücksichtigen. Deshalb müssen die Erforderlichkeit und das Risiko einer Zusammenführung personenbezogener Daten aus ver-

schiedenen Quellen, auch bei der Einführung neuer Technologien wie dem dynamisches Routing, rechtzeitig abgewogen werden.
Deshalb regt der Landesbeauftragte an, die IT-Verantwortlichen in allen Bereichen über die Folgen zu informieren und hinsichtlich der aufgezeigten datenschutzrechtlichen Problematik zu sensibilisieren. Das betrifft insbesondere die Abschottung der lokalen Netze der Ressorts und der übrigen öffentlichen Stellen als Teilnehmer am Landesnetz (ITNLSA), wenn darin die automatisierte Verarbeitung personenbezogener Daten stattfindet.

Es ist nicht nur davon auszugehen, dass "Außentäter" über das Internet versuchen, Zugang zum ITN-LSA zu erlangen, sondern es muss auch die Problematik der "Innentäter" gesehen und durch entsprechende Schutzmaßnahmen deren unbefugtes Eindringen in fremde Behördennetze verhindert werden.
In diesem Zusammenhang sind entsprechend umgesetzte Passwortrichtlinien schon ein guter Schutz. Passwörter sollten auch Ziffern und Sonderzeichen enthalten und eine entsprechende Mindestlänge von 6 bis 8 Zeichen besitzen, bei mehrmaliger Fehleingabe muss die Kennung gesperrt werden. Keine Verwendung vordefinierter Nutzerkennungen, wie z.B. "Gast" oder "Admin", keine Verwendung von Trivialpasswörtern.
Den genannten Gefährdungen soll durch den Einsatz von virtuellen privaten Netzen (**VPN - Virtual Private Network**) auf Basis von **IPSec** (IPSecurity) begegnet werden. So wird sichergestellt, dass nur die füreinander bestimmten Partner mit einander in Verbindung treten können. Daten werden über diese Verbindungen nur verschlüsselt gesendet. Die Verschlüsselung erfolgt über das sog. ESP-Protokoll (Encapsulating Security Payload).

Für die Verschlüsselung kennt IPSec zwei Betriebsmodi: Transportmodus und Tunnelmodus.

Im **Transportmodus** wird ausschließlich der Datenteil (Nutzungsdaten) des IP-Pakets verschlüsselt. Die anderen Teile der Nachricht (IP-Header) bleiben unverändert.

Im **Tunnelmodus** hingegen wird das gesamte IP-Paket **vor** der Übertragung verschlüsselt und mit einem neuen IP-Header versehen, der die Daten für den Zielknoten enthält. Diese Variante wird dann auch als **VPN** bezeichnet.

Der Landesbeauftragte hält, sichere Verschlüsselungsalgorithmen und ausreichende Schlüssellängen vorausgesetzt (symmetrisch; 128 Bit), den Einsatz von VPN für eine geeignete Maßnahme der Datensicherheit zur Übermittlung personenbezogener Daten im ITN-LSA.

## VII. Tätigkeitsbericht – 2005 (01.04.2003 - 31.03.2005)

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

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

Seit Jahren sind dabei in der Entwicklung der Informations- und Kommunikationstechnik (IuK) bestimmende Tendenzen zu beobachten. Dazu gehören:

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

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

- die stetig **zunehmende und umfassende Vernetzung** von IuK-Systemen. Das Internet ist in der sogenannten Informationsgesellschaft zwar bereits Alltag. Aber auch zukünftig werden auf diese Informationsgesellschaft neue und unter Datenschutzaspekten völlig neue Herausforderungen zukommen.
  Bereits jetzt bilden die sich ausbreitenden drahtlosen Kommunikationstechniken (Wireless LAN) die Grundlage für eine nächste Basistechnologie, die kurz mit dem Begriff **RFID** (Radio Frequency Identification) umschrieben wird.
  Mit RFID wird die Technologie bezeichnet, bei der durch Funkwellen eine kontaktlose automatische Identifikation von Gegenständen ermöglicht wird, die mit einem sogenannten RFID-tag (RFID-Etikett) versehen sind. Diese RFID-tags, die nach dem Prinzip des Transponders (Transmitter und Responder) arbeiten, bestehen aus einem Chip, je nach Bauart ein Speicher- oder ein Prozessorchip, und einer Antenne. Grundsätzlich werden diese RFID-tags noch in passive und aktive (mit eigener Energiequelle) Bauelemente unterteilt.
  Zurzeit sind Hauptanwendungsgebiete in den Bereichen Industrieautomation, Zutrittssysteme, Warenmanagement und Logistik sowie Diebstahlsicherung (z.B. an Kleidungsstücken) zu finden. Das Spektrum der Anwendungen wird sich aber schnell erwei-

tern, etwa auf Ausweisdokumente und Chipkarten, z.B. im öffentlichen Personennahverkehr. RFID-tags können der Identifizierung von Waren, Objekten, aber auch von Personen dienen. Die **Konferenz** der Datenschutzbeauftragten des Bundes und der Länder hat erste **Datenschutzhinweise** gegeben **(Anlage 19).**

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

### 7.1 E-Government-Konzept in Sachsen-Anhalt

In ihrer Stellungnahme zum VI. Tätigkeitsbericht des Landesbeauftragten hat sich die Landesregierung zur Beachtung sowohl der Anforderungen des Telekommunikations-, Tele- und Medienrechts als auch der Verbesserung der Sicherheitsbedingungen für das E-Government, insbesondere zur Umsetzung der Datensicherheit, gemäß den Schutzzielen des § 6 DSGLSA zur Wahrung der Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz, bekannt. Mit dem vorliegenden **E-Government-Konzept** hat sich die Landesregierung sehr ehrgeizige Ziele gesetzt.

Am **29. April 2003** wurde durch die Landesregierung das **Grundkonzept** E-Government in Sachsen-Anhalt. (Fassung vom 5. Februar 2003) beschlossen und das Ministerium des Innern mit der Erstellung eines **Aktionsplanes** beauftragt.
Im Grundkonzept ist die E-Government-Strategie des Landes Sachsen-Anhalt festgeschrieben. Das E-Government-Konzept des Landes besteht damit aus dem **Grundkonzept**, dem **Aktionsplan für die Jahre 2004 bis 2010** und den daraus abgeleiteten Anwendungen, die sich im **Maßnahmenplan 2005/2006** wiederfinden. Die so fixierten Projekte und Vorhaben werden von den Ressorts in Abstimmung mit der E-Government-Koordinierungsstelle, die im Juli 2004 wieder in die Landesleitstelle IT (LIT) des Ministeriums des Innern integriert wurde, ausgestaltet und umgesetzt.

Mit dem von der Landesregierung am 17. August 2004 verabschiedeten E-Government-Aktionsplan (Version 2.0 vom 3. Juni 2004), der im Zeitraum Januar bis Mai 2004 mit externer Unterstützung einer Beratungsfirma durch das Ministerium des Innern und in enger Zusammenarbeit mit den Ressorts erarbeitet wurde, konnten über 200 ressortübergreifende und ressortinterne Vorhaben im Rahmen einer Bestandsaufnahme ermittelt werden. Diese

wurden dann unter Beachtung ihres Nutzens und der entstehenden Kosten einer Bewertung und anschließenden Priorisierung unterzogen.
Im Ergebnis dieser Untersuchung und Bewertung erfolgte die Festlegung von 16 Leitprojekten. Neben diesen Leitprojekten sind bis 2010 weitere 97 sog. priorisierte Vorhaben zur stufenweisen Umsetzung geplant.

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

- Dienstleistungsportal (Landesportal) und Content Management System
- Formularserver
- Zahlungsverkehrsplattform
- Digitale Signatur/Virtuelle Poststelle
- Geodaten- und Metadatenserver
- Vorgangsbearbeitung und Dokumentenmanagementsystem.

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

Zu den **16 Leitprojekten** gehören:

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

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

Allerdings ist der Landesbeauftragte bisher **nur** im **Leitprojekt Nr. 1** Fördermittelmanagement - System "efREporter" direkt beteiligt worden. Im Rahmen dieses Projektes ist die Einführung einer elektronischen Signatur als Pilotverfahren für das Zuwendungsverfahren Fördermittel für die EU-Strukturfonds vorgesehen. Bei erfolgreicher Umsetzung bildet es zugleich den Ausgangspunkt zur landesweiten Einführung der elektronischen Signatur mit gleichzeitigem **Aufbau** der dazu notwendigen **Public Key Infrastructure (PKI) für Sachsen-Anhalt**.
Der Landesbeauftragte geht davon aus, dass er bei den übrigen E-Government-Vorhaben (Basiskomponenten und Leitprojekte) gem. § 22 Abs. 4 Satz 2 DSG-LSA **rechtzeitig** von den Ressorts unterrichtet bzw. dies für die bereits begonnenen Projekte nachgeholt wird. Zur Zeit liegt ihm nur das Feinkonzept des Leitprojektes Nr. 1 vor. Er geht weiterhin davon aus, dass sich die behördlichen Datenschutzbeauftragten der Ressorts intensiv mit der Problematik eines datenschutzkonformen E-Government befassen werden.
Nicht zuletzt lässt auch die Landesregierung, zumindest in den **Leitlinien (Thesen)** ihres Grundkonzeptes E-Government in Sachsen-Anhalt, erkennen, dass bei grundlegenden Diensten zur umfassenden Information, Kommunikation, Transaktion und Kooperation die Verfügbarkeit, Vertraulichkeit und Integrität der (sicherlich auch) personenbezogenen Informationen gewährleistet werden muss.
Denn bei der Umsetzung von E-Government sind die Sicherheitsbedürfnisse aller Partner, dazu zählen insbesondere die Bürgerinnen und Bürger des Landes, zu beachten. Nur ein datenschutzkonformes E-Government wird zur Akzeptanz und zur Nutzung der angebotenen Dienste durch die Bevölkerung führen, denn letztendlich ist E-Government kein Selbstzweck für die Landesverwaltung. Vor dem Hintergrund der rasanten technischen Entwicklungen in der Informations- und Kommunikationstechnik und insbesondere aus Gründen des Datenschutzes und der Datensicherheit hält der Landesbeauftragte einen kontinuierlichen Ausbau der grundlegenden Sicherheitsmechanismen für E-Government und deren ständige Anpassung an den Stand der Technik gem. § 6 Abs. 1 Satz 3 DSG-LSA für erforderlich.

### 7.2 Die Virtuelle Poststelle

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

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

Die Datenschutzbeauftragten des Bundes und der Länder wollten die Entwicklung unterstützen und begleiten. Eine Arbeitsgruppe unter Leitung des niedersächsischen Datenschutzbeauftragten hatte daher entsprechende Empfehlungen formuliert und als **Handreichung** „**Die**

**Virtuelle Poststelle im datenschutzgerechten Einsatz**“ veröffentlicht. In enger Kooperation
insbesondere mit den kommunalen Spitzenverbänden in Niedersachsen und dem Bundesamt für Sicherheit in der Informationstechnik beschreibt die Handreichung die datenschutzrechtlichen und technischen sowie organisatorischen Anforderungen, die zu beachtenden Sicherheitsaspekte und die Architektur der Virtuellen Poststelle. Der Landesbeauftragte
hat die Handreichung auf seiner Homepage eingestellt.

## VIII. Tätigkeitsbericht – 2007 (01.04.2005 - 31.03.2007)

### 1. Entwicklung und Situation des Datenschutzes

### 1.3 E-Government und Technik

Die technische Entwicklung im nicht-öffentlichen Bereich und auch im öffentlichen Bereich, etwa beim **E-Government**, ist bereits Thema früherer Tätigkeitsberichte gewesen (vgl. VII. Tätigkeitsbericht, Ziff. 1 und Ziff. 7.1). Naturgemäß sieht der Landesbeauftragte nicht in erster Linie die Chancen neuer Technologien, sondern deren Risiken für Datenschutz und Datensicherheit. Neue Technologien, u.a. die RFID-Technologie (beim elektronischen Pass seit November 2006 und voraussichtlich 2008 beim elektronischen Personalausweis) - siehe Ziff. 4.4 - und Voice over IP („Internet-Telefonie“ - siehe **Anlage 8**), finden bereits Anwendung im öffentlichen Bereich oder sind in Planung.

Zur Sicherung eines angemessenen Schutzniveaus für die Grundrechte ist eine Anpassung der gesetzgeberischen Maßnahmen an die Herausforderungen durch die faktischen Entwicklungen in den einzelnen Lebensbereichen erforderlich. Viele Bereiche bedürfen klarer gesetzlicher Regelungen, auch wenn das Grundanliegen von Normensparsamkeit und Deregulierung nicht aus dem Auge verloren werden darf. Der Anpassungsbedarf besteht gerade aufgrund der technischen Entwicklungen. Das Recht muss moderne Techniken einfangen, wenn sich aus diesen Risiken für den Grundrechtsschutz ergeben (vgl. Bundesverfassungsgericht, Beschluss vom 12. April 2005, 2 BvR 581/01, BVerfGE 112, 304). Insoweit gilt der Grundsatz, dass nicht alles, was technisch möglich ist, auch rechtlich zulässig ist.
Notwendig ist zudem eine datenschutzkonforme Technikgestaltung unter Beachtung der Grundsätze der Datensparsamkeit und Datenvermeidung. Datenschutz muss von vornherein und dauerhaft in die automatisierten Verarbeitungsprozesse personenbezogener Daten integriert werden.

Im Zentrum aller Aktivitäten zur Verwaltungsmodernisierung, als Basis der Kommunikationsinfrastruktur des Landes Sachsen-Anhalt, ob beim IT-Konzept der Landesverwaltung, beim E-Government-Maßnahmenplan der Landesregierung oder beim Masterplan des Landesportals Sachsen-Anhalt (LPSA) steht nach wie vor das **„Informationstechnische Netz des Landes Sachsen-Anhalt“ (ITN-LSA)**, welches die Grundlage der Kommunikation der Landesverwaltung untereinander, mit den Kommunen, mit den Bürgerinnen und Bürgern sowie mit der Wirtschaft bildet.

Obwohl die Verfügbarkeit der zentralen Kommunikationsdienste und eine sehr hohe Verfügbarkeit der Transportfunktionalität dieses Netzes dem Betreiber, dem Technischen Polizeiamt des Landes Sachsen-Anhalt (TPA), am **1. Dezember 2006 durch eine erneute Zertifizierung** durch einen externen unabhängigen Gutachter bestätigt wurde (allerdings nicht nach den national und international anerkannten Common Criteria), sind die durch den Landesbeauftragten bereits in seinem VI. Tätigkeitsbericht 2003 (Ziff. 7.3) aufgezeigten Defizite einer verbindlichen IT-Sicherheitspolitik nicht ausgeräumt.

Die im **IT-Konzept der Landesverwaltung - Fortschreibung 2005** - zur Umsetzung der IT-Strategie und zum Aufbau der Sicherheitsarchitektur festgestellte immer größere Bedeutung der Gewährleistung der IT-Sicherheit bei allen anstehenden Geschäftsprozessen (insbeson-

dere also auch Geschäftsprozessen des E-Government) und die in diesem IT-Konzept **daraus abgeleitete Notwendigkeit einer Anpassung der IT-Grundsätze (vom 1. Juni 1992) und des Netzerlasses zum ITNLSA (vom 7. Februar 1994) sind auch im April 2007 nach wie vor nicht erfolgt.**
Diese Situation wird den festgelegten Zielen des IT-Einsatzes gemäß IT-Konzept der Landesverwaltung und der Sicherstellung von Datenschutz und Datensicherheit bei der automatisierten Verarbeitung personenbezogener Daten nicht gerecht und ist auch unter Beachtung der Anforderungen für eine sichere Abwicklung von E-Government-Prozessen so nicht mehr akzeptabel (siehe Ziff. 4.1).
Das **Datenschutzgesetz des Landes wurde im November 2005 novelliert** (durch Artikel 15 des Ersten Rechts- und Verwaltungsvereinfachungsgesetzes vom 18.11.2005, GVBl. LSA S. 698, 701 - vgl. Ziff. 3.2). Die wichtigste Änderung betrifft die Neufassung und Erweiterung der **Unterrichtungspflicht der Landesbehörden über automatisierte Datenverarbeitungen,** die der Regelung zur Verantwortung und Selbstkontrolle der Verwaltung für die Einhaltung datenschutzrechtlicher Vorgaben in § 14 Abs. 1 Satz 2 (zuvor § 22 Abs. 4 Satz 2) DSG-LSA angefügt wurde:
*„Der Landesbeauftragte für den Datenschutz ist rechtzeitig über grundlegende Planungen des Landes zum Aufbau oder zur Änderung von automatisierten Verfahren zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zu unterrichten“.*
Die Regelung unterstützt die Beratungsaufgabe im Vorfeld der Einführung neuer Verfahren und ergänzt § 40 der Gemeinsamen Geschäftsordnung der Ministerien (Allgemeiner Teil), wonach der Landesbeauftragte vor der Erstellung neuer Regelungen, einschließlich Rechtsvorschriften, mit Datenschutzrelevanz zu beteiligen ist.

Der Landesbeauftragte musste feststellen, dass gerade die obersten Landesbehörden es mehrmals versäumten, rechtzeitig im Sinne einer **Bringschuld** über neue E-Government-Pläne zu informieren. Dies betrifft etwa und insbesondere das Ministerium des Innern beim E-Government-Maßnahmenplan 2007 (Ziff. 4.2), die Staatskanzlei (siehe Ziffn. 4.1 und 23.2) und das Ministerium der Justiz (siehe Ziff. 18.13).

Infolge eines grundsätzlichen kritischen Hinweises des Landesbeauftragten informierte der Chef der Staatskanzlei im Februar 2007 die Staatssekretärskonferenz über die Rechtslage.

Der Landesbeauftragte geht davon aus, dass zukünftig durch eine rechtzeitige Unterrichtung seitens der Ressorts seine Beteiligung bei Planungen des Landes erfolgt, hierzu gehören u.a. die E-Government-Leitprojekte und die E-Government-Basiskomponenten, aber auch z.B. das IT-Infrastrukturdienste-Konzept für das ITN-LSA oder die Einführung von Voice over IP in der Landesverwaltung. Nur so wird er in die Lage versetzt, seinen gesetzlichen Beratungsauftrag (§ 22 Abs. 4 DSG-LSA) zeitnah und effizient zu erfüllen (vgl. Ziff. 4.2).

## 4. Entwicklung der automatisierten Datenverarbeitung - E-Government

### 4.1 IT-Konzept der Landesverwaltung Sachsen-Anhalt

Am 15. November 2005 wurde das vom Ministerium des Innern vorgelegte IT-Konzept - Fortschreibung 2005 - vom Kabinett zustimmend zur Kenntnis genommen. Mittelfristig beruht die IT-Strategie des Landes auf einer Zusammenführung aller zentralisierbaren Rechenzentrumsdienstleistungen (einschließlich der IT-Infrastruktur), der Standardisierung der IT-

Landschaft sowie der Institutionalisierung der Kooperation mit der kommunalen Ebene zur gemeinsamen Nutzung einheitlicher IT-Standards. Durch eine interministerielle Arbeitsgruppe unter Federführung des Ministeriums des Innern, in der auch der Landesbeauftragte mitgewirkt hatte, wurde diese Kabinettvorlage vorbereitet und ausgearbeitet. Durch die Mitarbeit in der Arbeitsgruppe haben wesentliche datenschutzrechtliche Belange Berücksichtigung bei den Zielen und Leitlinien sowie bei der Umsetzung der IT-Strategie im IT-Konzept gefunden.

Hierzu gehören u.a.

- die in den Leitlinien festgelegte Beachtung des Rechts auf informationelle Selbstbestimmung als grundlegende Voraussetzung bereits bei Planungen von IT-/E-Government-Vorhaben,
- die Aufnahme eines eigenen Kapitels „Datenschutz und Datensicherheit“ mit der Darstellung der wesentlichen Änderungen der DSG-LSA-Novelle vom 21. August 2001 (GVBl. LSA S. 348) sowie den daraus resultierenden datenschutzrechtlichen Anforderungen bei Planung und Umsetzung von IT-Vorhaben,
- im Rahmen der Definition von Standards für den IT-Einsatz die Nutzung datenschutzgerechter Protokolle (z.B. OSCI-Transport) für einen sicheren Transport und die Realisierung der „Ende-zu-Ende-Verschlüsselung“,
- die Berücksichtigung datenschutzrechtlicher Belange beim Aufbau und der Umsetzung der Sicherheitsarchitektur im ITN-LSA durch die Erstellung einer IT-Sicherheitsrichtlinie unter Federführung des Ministeriums des Innern und die dementsprechende Anpassung des Netzerlasses für das ITN-LSA vom 7. Februar 1994 und der IT-Grundsätze vom 1. Juni 1992 sowie der Aufbau eines zentralen IT-Sicherheitsmanagement zum schnellen Erkennen von und Reagieren auf Gefährdungen der IT der Landesverwaltung in der Form eines CERT-LSA („Computer Emercency Response Team“).

Eine jährliche Anpassung an aktuelle Entwicklungen und die Fortschreibung dieses IT-Konzeptes 2005, wie in der Zusammenfassung des Konzeptes selbst festlegt, erfolgte allerdings nicht. Der Aufforderung zur Fortschreibung des Konzeptes und dessen erneute Vorlage durch das Ministerium des Innern im Kabinett bis spätestens November 2006, auch nochmals durch den Kabinettsbeschluss vom 15. November 2005 bekräftigt, kam das Ministerium des Innern nicht mehr nach.
Einer der Gründe für diese nicht erfolgte Fortschreibung oder deren Verzögerung liegt wahrscheinlich in den Ergebnissen eines **externen Gutachtens** „Zusammenführung aller zentralisierbaren Rechenzentrumsdienstleistungen in eine übergreifende Organisationsstruktur in der Landesverwaltung Sachsen-Anhalt“ **vom 6. Februar 2006**, dessen Erstellung bereits am 28. Februar 2005 durch den „**Ständigen Staatssekretärsausschuss Informationstechnologie**“ beschlossen worden war und für den die Staatskanzlei dann als Auftraggeber fungierte.
Anzumerken ist in diesem Zusammenhang, dass dieses Gutachten durch die Staatskanzlei den Ressorts bereits am 10. Februar 2006 zur Verfügung gestellt wurde, der Landesbeauftragte aber in dieser doch grundsätzlich auch für ihn wesentlichen Angelegenheit noch nicht einmal nachrichtlich davon in Kenntnis gesetzt wurde und erst auf Nachfrage beim nunmehr zuständigen Referat der Staatskanzlei seiner Bitte um Zusendung des besagten Gutachtens am 16. Januar 2007 entsprochen wurde.

Im Ergebnis dieses Gutachtens wird der Landesregierung eine **IT-Neuorganisation** dringend empfohlen, bei gleichzeitiger Verlagerung der Aufgabenwahrnehmung der IT-Strategie vom Ministerium des Innern (ehemals Landesleitstelle für Informationstechnik - **LIT**) in die **Staatskanzlei (Landesleitstelle für IT-Strategie -LIS)**. Mit der operationellen Steuerung und Umsetzung des gesamten Prozesses der IT-Neuorganisation soll ein gleichzeitig zu bildender **Aufbaustab** beauftragt werden. Für die Abarbeitung der ressortübergreifenden Aufgaben wird die Bildung nachfolgend genannter **neun Kompetenzteams** für dringend notwendig erachtet:

| Kompetenzteam | Team-Führung |
|---|---|
| Nutzerbetreuung | Ministerium des Innern (TPA) |
| Software-Verteilung | Ministerium des Innern (TPA) |
| Terminal-Server-Technik | Ministerium des Innern (TPA) |
| SAP | Ministerium des Innern (TPA) |
| Security / Netzinfrastruktur | Ministerium des Innern (TPA) |
| Druckstraße | Ministerium der Finanzen (FRZ) |
| Solaris | Ministerium der Finanzen (FRZ) |
| Storage / Archivierung | Ministerium der Finanzen.(FRZ) |
| E-Mail/ Intranet, Internet | Ministerium des Innern (LIZ) |

Die Konsolidierung von 307 IT-Fachbereichen auf 15 neue IT-Fachbereiche soll durch die Bildung von ressortinternen Projektteams unterstützt werden.

Als weiteres zentrales Ziel im Gutachten ist, neben dieser Konsolidierung der IT-Fachbereiche, die Schaffung eines zentralen IT-Dienstleisters für die Landesverwaltung Sachsen-Anhalt benannt. Nach zunächst ressortinterner Konsolidierung der IT-Fachbereiche sollen diese dann zu einem ressortübergreifenden Rechenzentrum zusammengeführt werden.

Folgerichtig zog die Landesregierung entsprechende Konsequenzen aus diesem Gutachten. Mit **Kabinettsbeschluss vom 14. November 2006** leitete sie die **Neuausrichtung der IT-Organisation** und eine neue Aufgabenverteilung und -abgrenzung zwischen der Staatskanzlei, dem Ministerium des Innern und dem Ministerium der Finanzen ein.

Seit dem 1. Dezember 2006 liegt nunmehr die Verantwortung für die **IT-Strategie** bei der **LIS**. Die Leitung des Landesportals sowie die Koordinierung der E-Government- Angebote für die Öffentlichkeit werden ebenfalls durch die Staatskanzlei in Abstimmung mit dem Ministerium des Innern wahrgenommen.

Dem **Ministerium des Innern** obliegt wie bisher die **Koordinierung des E-Government in der Landesverwaltung**.

Das **Ministerium der Finanzen** wird mit der Bildung eines **Aufbaustabes „Konsolidierung des IT-Betriebes“** beauftragt. Dieser soll solange bestehen bleiben, bis die neue **IT-Organisation** gesichert arbeitet. Bis spätestens zum 30. Juni 2007 hat das Ministerium der Finanzen dem Kabinett über die Einrichtung dieses Aufbaustabes, die Konzepte zur Konsolidierung des IT-Betriebes und die Zeitplanung zu berichten.

Auch im Fall dieses Kabinettsbeschlusses vom 14. November 2006 erachtete es die Staatskanzlei nicht für nötig, den Landesbeauftragten zumindest nachrichtlich durch Übersendung des gefassten Kabinettsbeschlusses in Kenntnis zu setzen. Erst auf Nachfragen des Landesbeauftragten erreichten diesen Anfang Januar 2007 die Unterlagen. Der Landesbeauftragte hofft nunmehr, dass nach Bekundungen einer zukünftig frühzeitigen Unterrichtung Taten folgen werden und damit die offene und vertrauensvolle Zusammenarbeit seitens der Staatkanzlei auch unter Beweis gestellt wird.
Es bleibt festzuhalten, dass auch durch die Staatskanzlei die Regelung zur rechtzeitigen Unterrichtung des Landesbeauftragten gem. § 14 Abs. 1 Satz 2 DSGLSA beachtet bzw. die Beteiligung des Landesbeauftragten sichergestellt werden muss. Hier kann die Staatskanzlei ein Zeichen für eine offene und vertrauensvolle Zusammenarbeit mit dem Landesbeauftragten setzen, die gleichzeitig Vorbildcharakter für andere Ressorts haben könnte.

Der Landesbeauftragte geht davon aus, dass er zu gegebener Zeit, aber rechtzeitig, im Rahmen der Aufnahme der Tätigkeit der **Kompetenzteams** entsprechend beteiligt wird, denn gerade auch bei der Neustrukturierung und Neuordnung von Verarbeitungskapazitäten, sowie Themenbereichen wie Nutzerbetreuung, Security/Netzinfrastruktur, Terminal-Server-Technik, Storage/Archivierung und der Nutzung von E-Mail, Intranet, Internet bestehen enge Bezüge auch zu Datenschutz und Datensicherheit. Dieser Datenschutzbezug wird leider von den Verantwortlichen oft nicht erkannt, obwohl der Landesgesetzgeber mit der Novellierung des DSG-LSA vom 21. August 2001 mit § 14a DSG-LSA das Institut des „behördlichen Beauftragten für den Datenschutz“ geschaffen hat, der in jedem Ressort bzw. auch in jeder anderen öffentlichen Stelle des Landes gerade bei Planungen neuer und Veränderung bestehender automatisierter Verfahren zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beteiligt werden sollte. Nach dem Kenntnisstand des Landesbeauftragten erfolgt diese Beteiligung der behördlichen Datenschutzbeauftragten, gerade wenn es um grundsätzliche bzw. Leitungsentscheidungen der Ressorts geht, zum Teil gar nicht oder nur ungenügend oder zu spät.

Der Landesbeauftragte verkennt nicht die Schwierigkeiten der nunmehr von der Staatskanzlei übernommenen Aufgaben zur Planung, Gestaltung und Umsetzung der IT-Strategie für das Land Sachsen-Anhalt. Er hofft, dass nach der Ist-Analyse, d.h. einer Sichtung und Strukturierung der vom Ministerium des Innern übernommenen Aufgaben, die Erörterung der von ihm angesprochenen Problemfelder und Informationsdefizite ab dem 2. Halbjahr 2007 intensiv auf der Arbeitsebene fortgesetzt und damit eine vertrauensvolle Zusammenarbeit erreicht werden kann.

Nach letzten Verlautbarungen aus der Staatskanzlei ist beabsichtigt, das IT-Konzept der Landesverwaltung im 4. Quartal 2007 fortzuschreiben. Der Landesbeauftragte bietet hierzu seine Mitarbeit und Unterstützung an.

### 4.2 E-Government-Maßnahmenplan 2007

Der Landesbeauftragte hatte zuletzt in seinem VII. Tätigkeitsbericht (Ziff. 7.1) über die Aktivitäten der Landesregierung zur Umsetzung ihres E-Government-Konzeptes mit dem Aktionsplan für die Jahre 2004 bis 2010 und dem daraus abgeleiteten Maßnahmenplan 2005/2006

berichtet. Für die Mehrzahl der dort vorgestellten Projekte und Verfahren in Form der 16 Leitprojekte und für alle sechs Basiskomponenten ist ein datenschutzrechtlicher Bezug gegeben, auch wenn das von mancher Seite so nicht sofort erkannt und interpretiert wird.

Die Landesregierung hatte in ihrer damaligen Stellungnahme zu Ziff. 7.1 (LT-Drs. 4/2524 vom 1. Dezember 2005, S. 7) zum VII. Tätigkeitsbericht des Landesbeauftragten (LT-Drs. 4/2189 vom 25. Mai 2005) darauf verwiesen, die alte, eher unauffällig platzierte Regelung des § 22 Abs. 4 Satz 2 DSG-LSA zur ***frühzeitigen Unterrichtung*** des Landesbeauftragten stärker in das Blickfeld der zur Unterrichtung verpflichteten Stellen gerückt zu haben. Die besagte Regelung wurde durch Artikel 15 des Ersten Rechts- und Verwaltungsvereinfachungsgesetzes vom 18. November 2005 (GVBl. S. 698) dementsprechend in ***§ 14 DSG-LSA als Satz 2*** übernommen und zugleich inhaltlich dahingehend modifiziert, dass diese Unterrichtungspflicht zukünftig neben der **Planung** auch für die **grundlegende Änderung automatisierter Verfahren** zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten Anwendung finden sollte. Der Landesbeauftragte sollte nach Aussage der Landesregierung zukünftig rechtzeitig über *grundlegende* Planungen zum Aufbau und zur Änderung von automatisierten Verfahren unterrichtet werden. In dieser Stellungnahme der Landesregierung sind auch Planungen zur Gestaltung der technischen Infrastruktur, wie z.B. das E-Government-Konzept, ausdrücklich erwähnt worden (siehe auch Ziff. 3.2 mit Hinweisen zu den geänderten Verwaltungsvorschriften). Dieser selbst auferlegten Verpflichtung ist die Landesregierung im Rückblick auf den Berichtszeitraum nicht immer nachgekommen.

Dies gilt insbesondere für die länderübergreifenden Leitprojekte des E-Government-Maßnahmenplanes 2005/2006. Mit dem Ministerium der Justiz hat der Landesbeauftragte deshalb z.B. einen jährlichen, kontinuierlichen Informationsaustausch über den Einführungsstand von IT-Projekten in dessen Geschäftsbereich vereinbart, der seitens des Ministeriums der Justiz auch eingehalten wird.
Trotzdem erfolgte z.B. die Beteiligung beim Vorhaben des Ministeriums der Justiz zu Errichtung und Betrieb eines **bundesweiten Registerportals der Länder** unter Beteiligung des Landes Sachsen-Anhalts, welches zum 1. Januar 2007 in Betrieb gehen sollte, viel zu spät. Zudem waren die erforderlichen rechtlichen Grundlagen für die hoheitliche Verarbeitung personenbezogener Daten durch eine Stelle außerhalb der rechtlichen Zuständigkeit Sachsen-Anhalts noch nicht geschaffen, da der Staatsvertrag bis Jahresende 2006 weder geschlossen noch ratifiziert werden konnte (siehe Ziff. 18.13).

Die Leitprojekte aus dem Bereich des Ministeriums des Justiz (Nr. 13: Elektronische Einsichtnahme in maschinell geführte Register, Nr. 14: Automatisiertes gerichtliches Mahnverfahren, Nr. 15: Elektronischer Rechtsverkehr in Grundbuchsachen) sowie des Ministeriums der Finanzen (Nr. 16: Elektronische Steuererklärung) sind bundesländerübergreifende Leitprojekte. In diesen Ressorts besteht eine zentralisierte Führung des nachgeordneten Bereiches und durch die Länder werden bundesrechtliche Regelungen wie z.B. der Grundbuchordnung und der Abgabenordnung umgesetzt und ausgeführt. Hier scheint deshalb teilweise die Meinung der Ressortverantwortlichen vorzuherrschen, dass damit eine rechtzeitige Beteiligung des Landesbeauftragten gem. § 14 Abs. 1 Satz 2 DSG-LSA nicht mehr erforderlich sei, weil ja schon alles, auch die datenschutzrechtlichen Fragestellungen und Themen, in den dazu eingerichteten Bund-Länder-Gremien abschließend behandelt worden seien und es damit nur noch einer Umsetzung im eigenen Bundesland bedürfe. Das ist aber, wie die Praxis zeigt, oft ein Irrtum. Der Landesbeauftragte lässt sich bei seiner datenschutzrechtli-

chen Prüfung und Beurteilung nicht von der „Wirkung“ bereits abgeschlossener Staatsverträge oder Verwaltungsvereinbarungen zwischen den Bundesländern beeinflussen. Oft stellt sich bei solchen Nachprüfungen heraus, dass entweder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit auf Bundesebene oder die Landesbeauftragten für den Datenschutz über ihre Landesressorts nicht rechtzeitig unterrichtet oder beteiligt worden sind.

Eine Beteiligung des Landesbeauftragten mit Gelegenheit zur Stellungnahme zum **E-Government-Maßnahmenplan 2007** vor Beschlussfassung der Landesregierung wäre geboten gewesen, wurde aber von den einzelnen Ressorts weder für ihre neu aufgenommenen Leitprojekte noch durch das mit der Erstellung des E-Government-Maßnahmenplanes 2007 federführend befasste Ministerium des Innern erkannt und ist offenbar vernachlässigt worden.

Gerade aber der zurückliegende Berichtszeitraum ist auf EU-, Bundes- und auch auf Landesebene von vielfältigen Aktivitäten, Programmen und Initiativen zum E-Government gekennzeichnet, die selbst dem Landesbeauftragten Mühe bereiten, die Übersicht zu behalten. „E-Government“ scheint zu einem Zauberwort der Politik geworden zu sein, welches synonym für die Verwaltungsmodernisierung durch Informations- und Kommunikationstechnologien verwendet wird.

Stellvertretend für diese Aktivitäten auf Bundesebene sei hier auf den sogenannten **„1. Nationalen IT-Gipfel“** am **18. Dezember 2006** am Hasso-Plattner-Institut in Potsdam verwiesen, zu dem die Bundeskanzlerin hochkarätige Experten aus Politik, Wissenschaft, Forschung und Wirtschaft eingeladen hatte, um über den Ausbau Deutschlands als Standort für **Informations- und Kommunikationstechnologien (IKT)** zu beraten. Nicht eingeladen waren die Datenschutzbeauftragten des Bundes und der Länder, für die Stellung und die Standortbestimmung des Datenschutzes in dieser Informationsgesellschaft geradezu ein fatales Zeichen in dieser Zeit. Der ausgegrenzte Bundesbeauftragte für den Datenschutz und die Informationsfreiheit forderte deshalb, schon bei der Konzeption von IT-Systemen verstärkt Vorkehrungen zur Gewährleistung des Rechts auf informationelle Selbstbestimmung zu treffen und veröffentlichte hierzu zeitgleich zum **1. Nationalen IT-Gipfel „Zehn Thesen für eine datenschutzfreundliche Informationstechnik“** (**Anlage 27**), denen sich der Landesbeauftragte für seinen Zuständigkeitsbereich nur anschließen kann, gelten doch diese Forderungen auch für die Landesregierung bei der konzeptionellen Gestaltung weiterer Vorhaben des E-Government in Sachsen-Anhalt.

Zu den wesentlichen Einflussfaktoren hinsichtlich der weiteren Gestaltung und Umsetzung des E-Government-Prozesses in Sachsen-Anhalt zählen aus Sicht des Landesbeauftragten nachfolgend bezeichnete EU-Richtlinien, EU-Initiativen, Initiativen des Bundes sowie die Rahmenvereinbarung der Landesregierung mit den Kommunalen Spitzenverbänden.

Europäische Union:

- **EU-Initiative** „**i2010** – Eine europäische Informationsgesellschaft für Wachstum und Beschäftigung“ vom 1. Juni 2005,
- **EU-Initiative** „**Interoperabilität** für europaweite elektronische Behördendienste (E-Government-Dienste) vom 13. Februar 2006,
- **E-Government-Aktionsplan** im Rahmen der i2010-Initiative: „Beschleunigte Einführung elektronischer Behördendienste in Europa zum Nutzen aller“ vom 25. April 2006,
- **i2010 Erster Jahresbericht** über die europäische Informationsgesellschaft vom 19. Mai 2006,
- **Richtlinie 2006/123/EG** des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über Dienstleistungen im Binnenmarkt (sog. „EU-Dienstleistungsrichtlinie“).

Bundesregierung und Bundesländer:

- **BundOnline 2005 - Abschlussbericht** - Status und Ausblick vom 24. Februar 2006
- **Aktionsplan Deutschland-Online** - Deutschland-Online Bund, Länder und Kommunen vom 22. Juni 2006 mit den fünf priorisierten Vorhaben:

  Querschnittsbereiche:
  - IT-Infrastruktur
  - Standardisierung

  Ebenenübergreifende Fachverfahren:
  - Kfz-Wesen
  - Personenstandswesen (siehe Ziff. 6.4)
  - Meldewesen (siehe Ziff. 6.1.)

  Diese **fünf priorisierten Vorhaben** werden durch eine Staatssekretärs- Lenkungsgruppe unter enger Einbindung der betroffenen Fachministerkonferenzen gesteuert und erhalten aus einem Bund-Länder-Fonds zentrale Unterstützung z. B. in Form von Beratungsleistungen.

- **E-Government 2.0** - Das Programm des Bundes - (Beschluss der Bundesregierung vom 13. September 2006: „Programm Zukunftsorientierte Verwaltung durch Innovationen“ einschließlich des Programms E-Government 2.0)
  Die Bundesregierung hat **vier Handlungsfelder** festgelegt, die in den kommenden Jahren bis 2010 gezielt ausgebaut werden, um den Modernisierungsprozess in der Verwaltung und den Standort Deutschland durch E-Government zu fördern:

  **A. Portfolio**:
  Bedarfsorientierter qualitativer und quantitativer Ausbau des E-Government- Angebots des Bundes,

  **B. Prozessketten**:
  Elektronische Zusammenarbeit zwischen Wirtschaft und Verwaltung durch gemeinsame Prozessketten,

**C. Identifizierung**:
Einführung eines **elektronischen Personalausweises** und Erarbeitung von E-Identity-Konzepten,

**D. Kommunikation**:
Sichere Kommunikationsinfrastruktur für Bürger, Unternehmen und Verwaltungen.

Land Sachsen-Anhalt:
- **Rahmenvereinbarung** zwischen dem Land Sachsen-Anhalt und den Kommunalen Spitzenverbänden vom 9. Januar 2006

Diese Aufzählung zeigt deutlich den hohen Koordinierungsaufwand, den zukünftig die Landesregierung bei der Umsetzung des E-Government-Maßnahmenplanes 2007 und der Folgejahre zu bewältigen haben wird.
Der Landesbeauftragte will diesen Prozess datenschutzrechtlich begleiten und die Landesregierung entsprechend seines gesetzlichen Beratungsauftrages (§ 22 Abs. 4 DSG-LSA) bei der anstehenden Verwaltungsmodernisierung unterstützen. Er erwartet seitens der Ressorts eine direkte Unterstützung seiner Tätigkeit durch eine rechtzeitige Unterrichtung und weitere Beteiligung beim Aufbau und der Umsetzung der **Basiskomponenten:**

**- 1 -** **Dienstleistungsportal** (Landesportal www.sachsen-anhalt.de, in Verantwortung der Staatskanzlei),
**- 2 -** **Formularserver** (Pilotlösung eines Formularmanagementsystems im LIZ Halle),
**- 3 -** **Zahlungsverkehrsplattform** (Muster eShop und Aufbau der zentralen Nutzerverwaltung im LIZ Halle),
**- 4 -** **Virtuelle Poststelle - VPS** (Beginn Testbetrieb der VPS ab Februar 2007, Echtbetrieb geplant ab 4. Quartal 2007; Public Key Infrastruktur bereits seit 11. Oktober 2006 offiziell in Betrieb),
**- 6 -** **Dokumentenmanagementsystem**/Vorgangsbearbeitungssystem (DMS/VBS) (Pilotprojekt im Ministerium des Innern).

Insbesondere bei der Basiskomponente 1, dem Landesportal Sachsen-Anhalt (LPSA) in Verantwortung der Staatskanzlei, ihrer Weiterentwicklung und ihrem Ausbau, erwartet der Landesbeauftragte zukünftig eine rechtzeitige Beteiligung und Unterrichtung gem. § 14 Abs. 1 Satz 2 DSG-LSA. Entsprechend dem Masterplan LPSA 2007-2011 (Bekanntmachung der Staatskanzlei vom 26. September 2006, MBl. LSA S. 657) soll das LPSA als Dienstleistungsportal ausgebaut werden. Damit wird die besondere Rolle des LPSA in der E-Government-Strategie des Landes deutlich. Dabei verlagert sich der Schwerpunkt im E-Government-Maßnahmenplan 2007 von reinen Informationsangeboten hin zur Transaktion, d.h. der eigentlichen Online-Erbringung von Dienstleistungen mit Bürgerinnen und Bürgern sowie der Wirtschaft. Damit ist zukünftig eine automatisierte Verarbeitung einer Vielzahl auch personenbezogener Daten von Kommunikationspartnern verbunden. Gerade hier ist die rechtzeitige Einbindung des Landesbeauftragten erforderlich, um durch die Prüfung und Abklärung der Fragen des Datenschutzes und der Datensicherheit Vertrauen in das Internetportal des Landes Sachsen-Anhalt und seine dort verfügbaren Online-Dienstleistungsangebote der Verwaltung zu erreichen (vgl. Ziff. 23.2).

Den gleichen Appell richtet der Landesbeauftragte an die Ressorts, welche die bereits begonnenen **Leitprojekte** (2, 3, 6, 9) aus 2005/2006 fortsetzen bzw. im Jahr 2007 nach Bereitstellung von Basiskomponenten weiterführen. Hierzu gehören die Leitprojekte 11, 12, 13, 14.
Beim Leitprojekt 15 (Elektronischer Rechtsverkehr in Grundbuchsachen – Federführung Ministerium der Justiz) erwartet der Landesbeauftragte eine rechtzeitige Beteiligung vor Abschluss des Feinkonzeptes.
Das Leitprojekt 1 (Fördermittelmanagement-System efREporter) ist mit Beteiligung des Landesbeauftragten erfolgreich abgeschlossen worden.
Weitere Leitprojekte (4, 5, 7, 8, 10, 16) gelten lt. E-Government-Maßnahmenplan 2007 als abgeschlossen.

Bei den in **2007** vier neu geplanten **Leitprojekten** (18, 19, 20 und 21)

- **XAusländer** (Leitprojekt 18/Ministerium des Innern, Festlegung einheitlicher Standards für Datenaustauschformate auf Basis XML im Ausländerwesen),

- **XPersonenstand** (Leitprojekt 19/Ministerium des Innern, Festlegung von Standards für das Personenstandswesen (Version 1.0) auf der Grundlage von XMeld und OSCI-Transport),

- **EUREKA-FACH** (Leitprojekt 20/Ministerium der Justiz, Erweiterung des in den Fachgerichtsbarkeiten eingesetzten Justizfachverfahrens EUREKAFACH für den Elektronischen Rechtsverkehr, einschließlich der Annahme und Archivierung von Verfahrensunterlagen in elektronischer Form sowie Workflow in der Verfahrensführung), und

- **web.sta** (Leitprojekt 21/Ministerium der Justiz, vollständige An- und Einbindung der Staatsanwaltschaften an die automatisierte Informationsbeschaffung und -verwaltung der Strafverfolgungsbehörden im Rahmen der europäischen Strafregistervernetzung; Ausbau von landesinternen Kommunikationsbeziehungen für Ermittlungsaufgaben in Wirtschaftsstrafsachen)

erinnert der Landesbeauftragte das Ministerium des Innern und das Ministerium der Justiz vorsorglich an ihre Unterrichtungspflichten.
Ein datenschutzrechtlicher Bezug wird wohl bei diesen neuen Leitprojekten nicht in Abrede gestellt werden.
Wie der Landesbeauftragte seitens des Ministeriums des Innern bei einem Gespräch in der Staatskanzlei informiert wurde, wird sich das Ministerium auch auf Grund der sog. „EU-Dienstleistungsrichtlinie“, deren IT-Umsetzung insbesondere für den Bereich der Wirtschaftsüberwachung zusätzlich in den Aktionsplan Deutschland-Online aufgenommen werden soll, verstärkt den Basiskomponenten und deren Umsetzung widmen.

### 4.3 Sicherheitsinfrastruktur in Sachsen-Anhalt

Mit der Veröffentlichung des Runderlasses des Ministeriums des Innern vom 14. März 2006 „Organisation und Aufgaben der Sicherheitsinfrastruktur des Landes Sachsen-Anhalt“ (MBl. LSA S. 233) wurden die organisatorischen Voraussetzungen für den Einsatz von fortgeschrittenen und qualifizierten Signaturen und Zertifikaten gemäß dem Signaturgesetz für den Ein-

satz bei der Signierung, Verschlüsselung und der Authentisierung in der Landesverwaltung in Sachsen-Anhalt geschaffen.
Die sog. „**Public Key Infrastruktur Land Sachsen-Anhalt - PKI LSA**“ bildet die wesentliche Grundlage für die Umsetzung der anspruchsvollen Ziele im Rahmen des E-Government-Maßnahmenplanes 2007 der Landesregierung und ist zugleich notwendige Voraussetzung für die Umsetzung des ab dem **1. Januar 2007 gesetzlich vorgeschriebenen bundesweiten, nur noch elektronisch durchzuführenden Rückmeldeverfahrens im Meldewesen**.
Das Land konnte mit der Inbetriebnahme des „Intermediär LSA“ auch die Integration des **Standards OSCI-Transport** erfolgreich abschließen. Damit wurde in Sachsen-Anhalt für die Datenübermittlung zwischen den Meldebehörden, vom Versand bis zum Empfang einer Nachricht, die Ende-zu-Ende-Verschlüsselung sichergestellt.
Mit dem **Sicherheitsstandard OSCI** (Online Services Computer Interface) werden die Vertraulichkeit, Integrität und Authentizität personenbezogener Daten bei der Übertragung über unsichere Netze, wie dem Internet, zwischen den öffentlichen Stellen in Bund, Ländern und Kommunen gewährleistet.
Insbesondere die Entwicklung von OSCI-Transport zu einem Protokollstandard für einen rechtlich anerkannten elektronisch signierten und verschlüsselten Daten austausch sowie dessen Einsatz im Rahmen des E-Government wurde in der **Entschließung** der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom **15. Dezember 2005 „Sicherheit bei E-Government durch Nutzung des Standards OSCI“** begrüßt (**Anlage 9**).

Der Landesbeauftragte hat die offizielle **Inbetriebnahme der PKI LSA am 11. Oktober 2006** durch den Staatssekretär des Ministeriums des Innern gleichzeitig zum Anlass genommen, die Ressorts auf die sachgemäße Anwendung von Authentisierungs- und Signaturverfahren hinzuweisen.

Obwohl Signatur- und Authentisierungsverfahren mit der asymmetrischen Verschlüsselung vergleichbare technische Verfahren nutzen, unterscheiden sie sich im Inhalt ihrer Aussagen und ziehen damit unterschiedliche Rechtsfolgen für die Nutzenden nach sich. Der grundlegende Unterschied dieser Verfahren muss sowohl bei der Planung als auch bei ihrem Einsatz in Verwaltungsverfahren Berücksichtigung finden.
Elektronische Signaturen liefern Aussagen über elektronische Dokumente, insbesondere über deren Authentizität und Integrität. Ausschließlich die **qualifizierte elektronische Signatur** ist durch rechtliche Regelungen der eigenhändigen Unterschrift in weiten Bereichen gleichgestellt und dient dem **Nachweis der Echtheit elektronischer Dokumente**. Zudem sind zur Zeit nur Verfahren zur Erzeugung elektronischer Signaturen rechtlich geregelt und sicherheitstechnisch genau definiert. **Authentisierungsverfahren liefern hingegen lediglich eine Aussage über die Identität einer Person oder einer Systemkomponente**. Solche Verfahren sind beispielsweise zur Authentifizierung einer Person oder eines IT-Systems gegenüber Kommunikationspartnern oder zur Anmeldung an einem IT-System geeignet. In einer **Entschließung** der Datenschutzbeauftragten des Bundes und der Länder vom **11. Oktober 2006 „Sachgemäße Nutzung von Authentisierungs- und Signaturverfahren“** werden auf die Problematik der Nutzung ungeeigneter oder weniger sicherer Verfahren hingewiesen und Forderungen für eine sachgerechten Einsatz von Signatur- und Authentisierungsverfahren erhoben (**Anlage 14**).

Darüber hinaus hat der Arbeitskreis E-Government der Datenschutzkonferenz eine **Orientierungshilfe** zu **Dokumentenmanagementsystemen** erarbeitet, die auch Aussagen zur Nut-

zung sicherer Signaturverfahren enthält; diese Orientierungshilfe ist im Serviceangebot der Homepage des Landesbeauftragten verfügbar. Die Empfehlungen sollten bei der weiteren Entwicklung der Basiskomponente Dokumentenmanagementsystem beachtet werden.

### 4.4 RFID (Radio Frequency Identification) - Chancen und Risiken

Der Landesbeauftragte hatte in seinen einleitenden Bemerkungen zum VII. Tätigkeitsbericht (Ziff. 1) zur technischen Entwicklung in Bezug auf den fortschreitenden Einsatz von RFID-Technologie aufmerksam gemacht.
In ihrer damaligen Entschließung vom März 2004 hatte die 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder sich voll inhaltlich einer Entschließung zu „Radio Frequency Identification“ der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre angeschlossen, in der erste Datenschutzhinweise gegeben wurden.
Seit dem ist eine rasante Entwicklung auf diesem Gebiet zu verzeichnen, die insbesondere diese sog. „**Funk-Chips**“ immer technologisch ausgereifter, aber auch kostengünstiger werden lässt, womit einem flächendeckenden Einsatz dieser Technologie in Wirtschaft und Verwaltung, in nicht mehr allzu ferner Zukunft, nichts mehr im Wege zu stehen scheint.

Mit der Ausstattung von Pässen ab November 2006 (ePass) und auch von Personalausweisen (ePA) ab 2008 mit einem **RFID-Chip**, der biometrische Merkmale des Ausweisinhabers speichert, hält RFID-Technologie auch Einzug in den öffentlichen Bereich (siehe Ziff. 6.3). Allerdings steht die Sicherheit, insbesondere die Schutzvorkehrungen gegen die Auslesbarkeit der Daten aus dem RFID-Chip durch unbefugte Dritte, zumindest bei den Pässen der „1. Generation“, in der Kritik. Für die Sicherheit der Daten will der Gesetzgeber bei der „2. Generation“ von Pässen, in denen dann auch Fingerabdrücke im RFID-Chip gespeichert werden, einen erweiterten Zugriffsschutz auf den RFID-Chip realisieren. Dieser erweiterte Zugriffsschutz - Extended Access Control - spezifiziert einen zusätzlichen Public-Key Authentisierungsmechanismus, mit dem sich zukünftig das Lesegerät als zum Lesen von Fingerabdrücken berechtigt gegenüber dem RFID-Chip im ePass oder später im ePA ausweisen muss. Das Lesegerät muss dazu ebenfalls mit einem eigenen Schlüsselpaar und einem vom RFID-Chip des ePass oder ePA verifizierbaren Zertifikat ausgestattet werden.

Auch u.a. aus diesem Grund hat sich der **Arbeitskreis „Technische und organisatorische Datenschutzfragen“** mit dieser als Basistechnologie für die Informationsgesellschaft bezeichneten RFID-Technologie kritisch auseinandergesetzt. Der Arbeitskreis hat hierzu eine **Orientierungshilfe „Datenschutzgerechter Einsatz von RFID“ (Stand 14. Dezember 2006)** verabschiedet; diese ist auf der Homepage des Landesbeauftragten abrufbar.

Die zuvor von der **72. Konferenz** der Datenschutzbeauftragten des Bundes und der Länder am **26./27. Oktober 2006** in Naumburg verabschiedete **Entschließung „Verbindliche Regelungen für den Einsatz von RFID-Technologien“** (**Anlage 18**) verdeutlicht nochmals die Möglichkeiten, aber auch die datenschutzrechtlichen Risiken dieser Technologie.
Zusammenfassend wird gefordert, dass bereits bei der Entwicklung, der Einführung, der Verwendung oder dem Einsatz von RFID-Technologien Datenschutzprinzipien materiellrechtlich wie technisch berücksichtigt werden müssen. Eventuell ist auch ein gesetzgeberisches Tätigwerden erforderlich (vgl. Ziff. 3.1). Zu erwähnen ist auch, dass die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, der sog. „Düsseldorfer

Kreis“, am 8./9. November 2006 in einem inhaltlich gleichlautenden **Beschluss** diese Auffassung zum datenschutzkonformen Einsatz von RFID vertreten (**Anlage 25**).

Die Entschließung der 72. Konferenz hat einen hoffentlich fruchtbaren Diskussionsprozess in Gang gesetzt, das zeigt z.B. die „Gemeinsame Stellungnahme“ von Informationsforum RFID e.V., Bundesverband Informationswirtschaft Telekommunikation und neue Medien e.V. (BITKOM), Bundesverband der Deutschen Industrie (BDI), GS1 Germany und Hauptverband des Deutschen Einzelhandel e.V. (HDE) vom Dezember 2006 als Reaktion auf diese Entschließung.

In der Antwort des Vorsitzenden der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom April 2007 an diese Interessenverbände der Wirtschaft wird das Angebot unterbreitet, die Diskussion um eine datenschutzgerechte Ausgestaltung von RFID-Anwendungen gemeinsam konstruktiv fortzuführen. Die Forderungen nach Transparenz, Kennzeichnungspflicht, dem Verbot einer Profilbildung, der Vermeidung unbefugter Kenntnisnahme und frühzeitiger Deaktivierungsmöglichkeit beim Einsatz von RFID-Technologien werden weitgehend von den Interessenverbänden der Wirtschaft akzeptiert. In der Bewertung der aus dem RFID-Einsatz resultierenden Risiken gehen die Auffassungen der Datenschutzkonferenz und der Interessenverbände noch auseinander. Dieser Umstand steht aber einer konstruktiven Diskussion nicht im Wege.
Die Datenschutzbeauftragten des Bundes und der Länder erklären sich ausdrücklich bereit, RFID-Projekte zu begleiten, und fordern dabei eine umfassende Technikfolgenabschätzung ein.

Auf europäischer Ebene hat ebenfalls, initiiert durch die EU-Kommission, eine öffentliche Konsultation zu RFID im Jahr 2006 stattgefunden. Bis Mitte des Jahres 2007 soll eine RFID-Interessengruppe eingerichtet werden, an der auch die Artikel-29-Datenschutzgruppe beteiligt ist. Die gemeinsame RFID-Strategie der EU hat das Ziel, die europäische Datenschutzrichtlinie für die elektronische Kommunikation so zu überarbeiten, dass RFID-Anwendungen unter diese Richtlinie fallen. Bis Ende des Jahres 2007 soll eine „Empfehlung über die Wahrung der Sicherheit und Privatsphäre“, die europaweit gültig sein wird, erarbeitet werden, die zugleich der IT-Branche als Rahmenrichtlinie dienen soll.

# IX. Tätigkeitsbericht – 2009 (01.04.2007 - 31.03.2009)

## 1. Entwicklung und Situation des Datenschutzes

### 1.3. E-Government und Technik

E-Government ist mittlerweile nicht nur der Weg, sondern vielmehr zum Motor der Verwaltungsmodernisierung bei Bund, Ländern und Kommunen geworden. Unterstützt und beschleunigt wird dieser Modernisierungsprozess in der öffentlichen Verwaltung durch ein weiteres Wachstum bei Speicherkapazitäten und verfügbaren Rechenleistungen vom Personalcomputer bis zum Großrechner sowie durch weiter ansteigende Nutzerzahlen im Internet sowie der fast inflationsartigen Entstehung neuer Web-Services, aber auch der Weiterentwicklung des Web 2.0, in dem die Internetnutzer selbst zu Gestaltern werden (Soziale Netzwerke, Blogs, Bewertungsportale, Chatrooms, Wikipedia, usw.).

Im zurückliegenden Berichtszeitraum ist bei den Systemen und Netzen eine Entwicklung weg vom Client-Server-System hin zum Terminal-Server-System sowie ein bis jetzt bereits seit ca. drei Jahren anhaltender Trend zur Virtualisierung von Hard- und Software zu beobachten gewesen. Virtualisierung ist heute fast schon Standard in Rechenzentren auch in Sachsen-Anhalt. Sie hält verbunden mit einer Zentralisierung und Konsolidierung der Informationstechnik von bisher dezentralen IT-Strukturen und IT-Insellösungen unvermindert an. Es findet quasi eine Rückbesinnung auf die Wurzeln der **zentralen** Datenverarbeitung statt, natürlich aber auf einem an-deren, höheren Niveau. Hierzu gehören **serviceorientierte Architekturen** (SOA) wie auch das in letzter Zeit immer häufiger als Begriff genannte „Cloud Computing“. Dabei werden Dienste im Netz bereitgestellt, ohne dass sich diese auf einem bestimmbaren Server befinden müssen. Die zugrunde liegende Plattform tritt in den Hintergrund. Der Dienst wird aus einer „Rechnerwolke“ (Cloud) erbracht. Er begegnet schon deshalb wesentlichen datenschutzrechtlichen Bedenken, hat aber gegenwärtig auf die öffentliche Verwaltung noch keine unmittelbaren Auswirkungen.
E-Government benötigt aber weit mehr als nur den Einsatz modernster Informations- und Kommunikationstechnologie. Der Berichtszeitraum zeichnet sich durch Bemühungen aus, insbesondere **elektronische Identifizierung** und **Kommunikation** im Internet **sicherer** und **rechtsverbindlicher** zu gestalten (ePass, Bürgerportale, De-Mail).

Diese neuen technischen und technologischen Entwicklungen und Möglichkeiten der Informations- und Kommunikationstechnologie bringen erhöhte Anforderungen besonders an die Sicherheit kritischer Geschäftsprozesse in der Wirtschaft und in der öffentlichen Verwaltung mit sich. Zu einem Schwerpunktthema hat sich dabei die vertrauliche Verarbeitung von Unternehmensdaten sowie Mitarbeiterdaten, aber vor allem auch die vertrauliche Verarbeitung personenbezogener Daten der Bürgerinnen und Bürger durch die öffentliche Verwaltung in Bund, Ländern und Kommunen entwickelt. E-Government benötigt vor allem Nutzer, und das wiederum setzt **Vertrauen** in die vom Staat angebotenen Online-Dienstleistungen voraus. Denn im Zeitalter der In-formationsgesellschaft nimmt die Angst der Bürgerinnen und Bürger, bei der Nutzung des Internets, bei der Nutzung von Online-Diensten der Wirtschaft und von E-Government-Diensten der öffentlichen Verwaltung zum „Gläsernen Bürger“ zu werden, immer mehr zu.

Besonderes Augenmerk legt deshalb die Bundesregierung auf den Schutz **kritischer Infrastrukturen** zur Sicherheit der IT. Mit dem hierzu im **Jahr 2005** verabschiedeten **Konzept „Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI)“** und dem insbesondere mit und für die Wirtschaft erarbeiteten **Umsetzungsplan „KRITIS“** sowie dem **2007** verabschiedeten **„Umsetzungsplan Bund“** und deren Realisierung soll dieser Bedrohungslage für IT begegnet werden. Die Bürgerinnen und Bürger können sich seit einigen Jahren über das beim Bundesamt für Sicherheit in der Informationstechnik (**BSI**) eingerichtete **„Bürger-CERT“** aktuell über die Gefährdungslage im Internet informieren und erhalten dort auch wichtige Verhaltenshinweise zum Selbstschutz.
Auch der nunmehr dritte vom BSI seit 2005 alle zwei Jahre veröffentlichte Lagebericht 2009 zur IT-Sicherheit in Deutschland schätzt die Bedrohungslage der IT-Sicherheit bei Verwaltungen, Unternehmen und den Privatanwendern auf einem anhaltend hohen Niveau ein. Das zeigt sich sowohl bei der voranschreitenden Qualität und Professionalität der Internetkriminalität (Drive-by-Downloads, Trojanische Pferde mit Backdoor- und Spyware-Funktionen, Bildung von Bot-Netzen) als auch bei der quantitativen Anzahl der Angriffe (Denial-of-Service-Angriffe, weitere Erhöhung des Spam-Anteils am E-Mail-Verkehr).

Standen am Anfang des E-Government-Prozesses in Deutschland das Bereit-stellen von Informationsangeboten der öffentlichen Verwaltung für die Bürge-rinnen und Bürger und die Erledigung von Verwaltungsangelegenheiten und -prozessen über das Internet im Mittelpunkt der Bemühungen und Aktivitäten der öffentlichen Verwaltung, ist nunmehr das sog. „**One-Stop-Government**“ das Ziel der Bemühungen auf Bundes- und Landesebene im Rahmen einer neuen E-Government-Gesamtstrategie für Deutschland. Im Idealfall sollen die Bürgerinnen und Bürger aber auch die Wirtschaft alle in einer bestimmten Situation anfallenden Verwaltungsangelegenheiten im Kontakt mit nur einer Stelle über das Internet erledigen können. Aktuelles Beispiel dieser strategischen Ausrichtung und dieses Paradigmenwechsels im Verwaltungshandeln in Deutschland stellt die Umsetzung der Europäischen Dienstleistungsrichtlinie (EU-DLR) bis zum 31. Dezember 2009 dar. Der „Einheitliche Ansprechpartner“ nach Vorgabe der EU-DLR, über oder durch den zukünftig Verwaltungsprozesse abgewickelt werden sollen, widerspiegelt diese Ausrichtung auf den neuen Dienstleistungscharakter der öffentlichen Verwaltung.

Treibende Kräfte dieses Modernisierungsprozesses sind die Initiative „**Deutschland Online**“ (DOL), d. h. die gemeinsame nationale E-Government-Strategie von Bund, Ländern und Kommunen, und der „**Nationale IT-Gipfel**“ (-Prozess) auf Initiative der Bundesregierung in enger Zusammenarbeit mit der Wissenschaft und Wirtschaft, mit dem Ziel Deutschland zu einem der führenden IKT-Standorte in Europa und der Welt zu entwickeln. Seit dem 1. Nationalen IT-Gipfel am 18. Dezember 2006 (Potsdam) wird nunmehr im Sprachgebrauch seitens der Bundesregierung und der Wissenschaft für den Begriff „**Informations- und Kommunikationstechnologie“** die Abkürzung **IKT** verwendet.

Allerdings ergeben bzw. stellen sich damit neue Fragen gerade für die öffentliche Verwaltung auf allen Ebenen:
Wie wird zukünftig die **digitale Identität** der Bürgerinnen und Bürger im Internet geschützt? Welchen Beitrag kann hier der Staat leisten?
Wer trägt die Verantwortung für die **öffentlichen IT-Infrastrukturen** (Bundes- und Landesnetze), insbesondere auch im Hinblick auf die Rechtsprechung des Bundesverfassungsge-

richts und das neue Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme?
Wie erlangt man das Vertrauen der Bürgerinnen und Bürger zu neuen E-Government-Angeboten? Wie werden effiziente Datenflüsse mit dem Recht der Bürgerinnen und Bürger auf informationelle Selbstbestimmung in Übereinstimmung gebracht?

Einige Aktivitäten zur Lösung dieser grundsätzlichen Probleme sind mittlerweile auf den Weg gebracht worden. So hat sich die **Föderalismuskommission II** in ihrer abschließenden Sitzung im **März 2009** neben den Regelungen zur Schuldenbegrenzung auch auf wichtige Maßnahmen zur Modernisierung der Verwaltung verständigt. An erster Stelle ist hier die Schaffung einer **verfassungsrechtlichen Grundlage (Art. 91c GG)** für die **Zusammenarbeit von Bund und Ländern in der Informationstechnologie (IT) der öffentlichen Verwaltungen** zu erwähnen. Die Verantwortung für die Sicherheit der länderübergreifenden IT-Netzinfrastruktur soll künftig beim Bund liegen. Der **Bund** soll eine Kompetenz für die **Errichtung** und den **Betrieb** eines **sicheren Verbindungsnetzes** erhalten, das die informationstechnischen Netze des Bundes und der Länder miteinander verbindet (BT-Drs. 16/12410). Das Nähere soll ein Bundesgesetz mit Zustimmung des Bundesrates regeln (BT-Drs. 16/12400). Der Bundesrat stimmte beiden Vorhaben am 12. Juni 2009 zu.
Auffällig und erstaunlich ist die Tatsache, dass die **Datenschutzgrundrechte** nach wie vor nicht ausdrücklich in das **Grundgesetz** aufgenommen worden sind – eine Forderung nicht nur der Datenschutzbeauftragten.

Neben dem bereits seit **Januar 2008** berufenen Beauftragten der Bundesregierung für Informationstechnik (sog. „**Bundes-CIO**“ - Chief Information Officer) soll darüber hinaus ein **neues System der IT-Steuerung** von Bund und Ländern eingerichtet werden, das insbesondere einen **IT-Planungsrat** von Bund und Ländern vorsieht, der wichtige Koordinierungsaufgaben in Fragen der Informationstechnik von Bund und Ländern, wie etwa die Festlegung von IT-Sicherheitsstandards, erhalten soll. Über die Einzelheiten besteht weitgehend Einvernehmen. Sie sollen durch Staatsvertrag und Verwaltungsabkommen verbindlich festgelegt werden.
Gleichzeitig sollen die bisherigen Gremien wie der Arbeitskreis der Staatssekretäre für E-Government in Bund und Ländern und der Kooperationsausschuss von Bund, Land und Kommunen für automatisierte Datenverarbeitung (KoopA ADV) mit allen ihren Untergremien sowie einzelne Vorhaben aus der Initiative „Deutschland Online“ damit auf- und abgelöst bzw. aufgegeben werden.

Das sind nur einige Themen, die von datenschutzrechtlicher Relevanz sind und im zurückliegenden Berichtszeitraum den Landesbeauftragten und seine Kolleginnen und Kollegen im Bund und den Ländern intensiv beschäftigt haben. Allerdings sind sie und insbesondere der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, im Gegensatz zum E-Government-Prozess in Bund und Ländern, in den „IT-Gipfel-Prozess“ der Bundesregierung nicht unmittelbar eingebunden. Der Landesbeauftragte hatte in seinem VIII. Tätigkeitsbericht (Ziff. 4.2) diesen Umstand bereits kritisch angemerkt. Nach dem 2. Nationalen IT-Gipfel in Hannover am 10. Dezember 2007 und dem 3. Nationalen IT-Gipfel am 20. Dezember 2008 in Darmstadt wird man für den **4. Nationalen IT-Gipfel Ende 2009** abwarten müssen, in wieweit angesichts der o. a. Rechtsprechung des Bundesverfassungsgerichts Antworten von Politik, Wirtschaft und Wissenschaft gegeben werden, die die Belange des Datenschutzes in dieser sich schnell fortentwickelnden Informationsgesellschaft ausreichend berücksichtigen.

Die Entwicklung in Sachsen-Anhalt und die Anstrengungen der Landesregierung in diesem **Modernisierungsprozess für die öffentliche Verwaltung** hat der Landesbeauftragte im Kapitel 4 dieses Berichts in den entsprechenden Schwerpunkten dargestellt.

## 4. Entwicklung der automatisierten Datenverarbeitung – E-Government

### 4.1. Die neue IT-Strategie des Landes Sachsen-Anhalt

Der Landesbeauftragte hatte zuletzt in seinem VIII. Tätigkeitsbericht (Ziff. 4.1) ausführlich über die Aktivitäten und Bemühungen der Landesregierung berichtet, grundlegend neue Wege bei der konzeptionellen Fortentwicklung des Einsatzes der Informationstechnologie (IT) in der Landesverwaltung zu beschreiten.

Das damals im **November 2005** vom Ministerium des Innern vorgelegte und vom Kabinett zustimmend zur Kenntnis genommene „**IT-Konzept - Fortschreibung 2005**“, an dessen Erarbeitung in einer interministeriellen Arbeitsgruppe unter Federführung des Ministeriums des Innern auch der Landesbeauftragte beteiligt war, hatte zur Berücksichtigung wesentlicher datenschutzrechtlicher Belange bei den Zielen und Leitlinien in diesem IT-Konzept geführt.
Eine vorgesehene jährliche Anpassung, spätestens im November 2006, an aktuelle Entwicklungen und die Fortschreibung dieses IT-Konzepts, wie im damaligen **Kabinettsbeschluss** vom **15. November 2005** festgelegt, erfolgte allerdings nicht mehr. Der wesentliche Grund hierfür war ein von der Staatskanzlei in Auftrag gegebenes **externes Gutachten** „Zusammenführung aller zentralisierbaren Rechenzentrumsdienstleistungen in eine übergreifende Organisationsstruktur in der Landesverwaltung Sachsen-Anhalt“ **vom 6. Februar 2006** (dessen Erstellung bereits am 28. Februar 2005 durch den Ständigen Staatssekretärsausschuss „Informationstechnologie“ beschlossen worden war).
Erst auf seine Nachfrage in der Staatskanzlei und der Bitte um Zusendung hin wurde dem Landesbeauftragten das besagte Gutachten am 16. Januar 2007 zugeleitet.

Die Landesregierung hat weitreichende Beschlüsse zur Umsetzung der im Gutachten aufgezeigten notwendigen Veränderungen und Handlungsvorschläge gefasst.
Zu nennen ist hier in erster Linie der **Kabinettsbeschluss vom 14. November 2006**, der die **Neuausrichtung der IT-Organisation und eine neue Aufgabenverteilung und -abgrenzung** zwischen der **Staatskanzlei**, dem **Ministerium des Innern** und dem **Ministerium der Finanzen** einleitete.
Die Zuständigkeit für die **IT-Strategie** liegt damit seit dem **1. Dezember 2006** bei der Staatskanzlei (**Landesleitstelle IT-Strategie - LIS**). Weiterhin ist die Staatskanzlei für das Landesportal Sachsen-Anhalt (www.sachsen-anhalt.de), in Abstimmung mit dem Ministerium des Innern, verantwortlich.

Die Koordinierung und **Umsetzung des E-Government-Aktionsplanes 2004-2010** erfolgt in der Verantwortung des **Ministeriums des Innern** durch den derzeit geltenden E-Government-Maßnahmenplan 2008-2009.
Das **Ministerium der Finanzen** ist seit diesem Zeitpunkt für die **IT-Konsolidierung** und - als wichtigste Aufgabe - für den **Aufbau eines zentralen IT-Dienstleisters** für die Landesverwaltung Sachsen-Anhalt verantwortlich.
Mittlerweile hat sich, beginnend ab dem Frühjahr 2007, die Unterrichtung und Einbeziehung des Landesbeauftragten bei grundlegenden Planungen des Landes, die eine datenschutz-

rechtliche Relevanz haben - auch wenn von manchem nicht sofort erkannt oder für nicht notwendig gehalten - doch spürbar verbessert.
Zu nennen sind hier in diesem Zusammenhang in erster Linie nachfolgende Ressorts und Themen:

- Die Landesleitstelle IT-Strategie (LIS) der Staatskanzlei zum Thema IT-Strategie des Landes,
- das Ministerium des Innern zur Umsetzung des E-Government-Maßnahmenplans 2008-2009 und insbesondere auch zur IT-Umsetzung der EU-Dienstleistungsrichtlinie,
- das Ministerium der Justiz zum IT-Ressortplan sowie zum PPP-Projekt JVA Burg,
- das Ministerium für Wirtschaft und Arbeit zur Umsetzung des Binnenmarktinformationssystems (IMI) und der Umsetzung der EU-Dienstleistungsrichtlinie,
- das Ministerium der Finanzen zur Thematik KONSENS und nach anfänglichen Verständigungsschwierigkeiten auch die Stabsstelle „Konsolidierung des IT-Betriebes“ zum Thema Aufbau eines zentralen IT-Dienstleisters (Landesrechenzentrum) in Sachsen-Anhalt.

Diese Aufzählung ist nicht abschließend, zeigt aber zugleich, dass der Landesbeauftragte im zurückliegenden Berichtszeitraum umfangreich im Rahmen seines **Beratungsauftrages** nach **§ 22 Abs. 4 DSG-LSA** in Anspruch genommen wurde. Diese auch starke personelle Belastung der Geschäftsstelle wurde durch die Bereitstellung einer IT-Referentenstelle (ab dem 1. August 2007) gemildert, so dass trotz der ausgeweiteten Beratungstätigkeit die Kontrollen im technisch-organisatorischen Bereich durchgeführt werden konnten. Es ist zu hoffen, dass diese bis Ende 2011 befristete IT-Referentenstelle in ein unbefristetes Beschäftigungsverhältnis umgewandelt werden kann, denn die Entwicklung der Informations- und Kommunikationstechnologie in Sachsen-Anhalt macht im Jahr 2012 sicher nicht Halt.
Die **Staatskanzlei** hat, federführend durch die **LIS**, nach einer Ist-Analyse der vom Ministerium des Innern übernommenen Aufgaben den Prozess der **grundlegenden Überarbeitung und Fortschreibung des IT-Konzeptes aus dem Jahre 2005 als IT-Strategie des Landes**, wie dem Landesbeauftragten Anfang des Jahres 2007 avisiert, eingeleitet.

Den Auftakt für die Erarbeitung dieser **neuen IT-Strategie** für das Land bildete ein **Workshop am 10./11. Oktober 2007**, an dem auch der Landesbeauftragte beteiligt wurde.
Im Ergebnis dieses Workshops wurden **acht Themenfelder** ermittelt, für die zur Weiterführung der Verwaltungsmodernisierung unabdingbar Handlungsbedarf besteht und für die Festlegungen von zielorientierten Maßnahmen unbedingt erforderlich sind. Zu diesen Themenfeldern gehören:

- Ziele der IT-Strategie,
- Rahmenbedingungen für die IT,
- IT-Organisation,
- IT-Standards,
- T-Architektur,
- IT-Management,
- T-Services,
- IT-Controlling.

An **drei** von insgesamt acht Arbeitsgruppen, die entsprechend den Themenfeldern gebildet wurden, **beteiligte sich der Landesbeauftragte aktiv (AG Rahmenbedingungen, AG IT-Architektur, AG IT-Management)**. Als Grundlage der Erarbeitung einer ganzheitlichen IT-Strategie für das Land in diesen Arbeitsgruppen verabschiedete der Koordinierungsausschuss Informationstechnik (**IT-KA**) mit **Beschluss 06/2007 am 4. Dezember 2007 „Thesen und Ansätze zur Erarbeitung der IT-Strategie der Landesverwaltung“**.
Durch diese intensive Arbeit, an der alle Ressorts teilnahmen, wurde es der Landesregierung letztendlich möglich, das von der Staatskanzlei vorgelegte Konzept für eine ressortübergreifende Strategie zur Modernisierung und Konsolidierung der Informations- und Kommunikationstechnologie der Landesverwaltung zu verabschieden.
Mit dem **Beschluss der Landesregierung über die IT-Strategie des Landes Sachsen-Anhalt vom 29. Juli 2008 (MBl. LSA S. 619)** liegt damit erstmals ein umfassendes strategisches Dokument vor, welches auch die Belange des Datenschutzes und der Datensicherheit berücksichtigt. Die Modernisierung der Verwaltung wird demnach unter Beachtung des **informationellen Selbstbestimmungsrechts** und des durch die aktuelle Rechtsprechung des Bundesverfassungsgerichts zum **Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme** fortgesetzt.
Diese IT-Strategie erfordert, dass das Thema IT-Sicherheit in den Führungsebenen verankert wird. Gleiches sollte auch für das Thema Datenschutz und Datensicherheit gelten.
In einer **Landesleitlinie IT-Sicherheit** sollen die wesentlichen Ziele festgelegt und damit die Grundlage für die Etablierung einer IT-Sicherheitsorganisation in den Ressorts geschaffen werden. **Der Datenschutz wird als fester Bestandteil des IT-Managements beschrieben; es ist vorgesehen, ihn in die Landesleitlinie IT-Sicherheit zu integrieren.** Der Landesbeauftragte regt in diesem Zusammenhang an, die behördlichen Datenschutzbeauftragten (§ 14a DSG-LSA) der Ressorts und auch der übrigen Landesbehörden stärker in diesen Prozess einzubeziehen, um hier einen ganzheitlichen Ansatz für IT- und Datensicherheitsmaßnahmen (§ 6 Abs. 2 DSG-LSA) zu erreichen, wenn es um die automatisierte Verarbeitung personenbezogener Daten geht.
Dieser **Erlass zur IT-Strategie** legt die Ziele sowie mittel- und längerfristige Maßnahmen für die **nächsten fünf Jahre** fest, eine Fortschreibung ist unter Beachtung der sich schnell verändernden Gegebenheiten und Entwicklungen der Informations- und Kommunikationstechnologie vorgesehen. Es bleibt zu hoffen, dass dieser Beschluss zur IT-Strategie des Landes nicht nur eine Absichtserklärung darstellt, sondern dass gerade die darin verankerten Ziele für den Datenschutz und die Datensicherheit aktiv von der Landesregierung verfolgt und umgesetzt werden.

Der Landesbeauftragte sieht in der Umsetzung der IT-Strategie, insbesondere in der Schaffung eines umfassenden Sicherheitsmanagements mit der Implementierung entsprechender Sicherheitsstandards, eine grundlegende Voraussetzung, auch das Vertrauen der Bürgerinnen und Bürger in die rechtsstaatliche, sichere und datenschutzkonforme automatisierte Verarbeitung ihrer Daten zu stärken.
Abschließend sei noch angemerkt, dass mit dem Beschluss der Landesregierung vom 29. Juli 2008 und der gleichzeitigen Aufhebung des Gemeinsamen Runderlasses des MI, der StK und der übrigen Ministerien **vom 1. Juni 1992 – IT-Grundsätze** (MBl. LSA S. 805) endlich ein vom Landesbeauftragten seit Jahren kritisierter Zustand beendet wurde (vgl. IV. Tätigkeitsbericht Ziff. 8.1, V. Tätigkeitsbericht Ziff. 6.2, VI. Tätigkeitsbericht Ziff. 7.3, zuletzt VIII. Tätigkeitsbericht, Ziff. 1.3).

### 4.2. Aufbau eines neuen zentralen IT-Dienstleisters - Landesrechenzentrum

Neben der Entscheidung der Landesregierung zur **Neuausrichtung der IT-Organisation** und der damit verbundenen Veränderung der Aufgabenverteilung und -abgrenzung zwischen der Staatskanzlei und dem Ministerium des Innern entsprechend des Kabinettsbeschlusses vom 14. November 2006 war die zweite, fast noch wesentlichere Entscheidung der Auftrag an das Ministerium der Finanzen zur **IT-Konsolidierung der Landesverwaltung** und zum gleichzeitigen Aufbau des zentralen IT-Dienstleisters, des neuen **Landesrechenzentrums (LRZ)**. Dieser Auftrag ist integraler Bestandteil der am 29. Juli 2008 vom Kabinett verabschiedeten IT-Strategie des Landes (siehe Ziff. 4.1).
Das Konzept zur IT-Konsolidierung der Landesverwaltung sah vor, innerhalb eines noch zu gründenden IT-Betriebsstättenverbundes ein LRZ als teil-rechtsfähige Anstalt des öffentlichen Rechts zu errichten. Kern des zukünftigen LRZ bildet das Finanzrechenzentrum (FRZ) der Oberfinanzdirektion Magdeburg (OFD), welches dazu mit dem Landesinformations-Zentrum (LIZ) in Halle zusammengeführt wurde. Mit **Kabinettsbeschluss vom 3. Juni 2008 (MBl. LSA S. 404) wurde das LIZ dem Geschäftsbereich des Ministeriums der Finanzen zugeordnet.**
Neben dem zukünftigen LRZ sollten das Justizrechenzentrum Barby und Teile des Rechenzentrums des Landesamtes für Vermessung und Geoinformation (LVermGeo) in einem IT-Betriebsstättenverbund zusammengefasst werden.
Zur Bewältigung dieses umfangreichen und komplexen Auftrags der Landesregierung hat das Ministerium der Finanzen hierzu eine **temporäre Stabsstelle „Konsolidierung des IT-Betriebes“ (KIT)** gebildet. Dieser sog. „**Aufbaustab**“ soll solange bestehen bleiben, bis das LRZ seine Arbeit aufgenommen hat.
Zu Beginn der Arbeitsaufnahme der Stabsstelle KIT erfuhr der Landesbeauftragte über den E-Mail-Verteiler des IT-Koordinierungsausschusses von der Ausarbeitung zweier Kabinettvorlagen durch diese Stabsstelle des Ministeriums der Finanzen. Eine **Kabinettvorlage** betraf die Einrichtung der sog. „**Kompetenzteams**“ und die **zweite Kabinettvorlage** betraf die **Errichtung des Aufbaustabes** und dessen weiteres konzeptionelles Vorgehen bei der Konsolidierung des IT-Betriebes.
Beide Kabinettvorlagen betrafen auch datenschutzrechtliche Belange. Der Landesbeauftragte hätte also gem. § 14 Abs. 1 Satz 2 DSG-LSA informiert werden müssen. Erst nach Aufforderung zur Information stellte der Aufbaustab dem Landesbeauftragten dann beide Kabinettvorlagen zur Verfügung.
Allerdings verwunderte den Landesbeauftragten die damalige Begründung des Aufbaustabes zu seiner Nichtbeteiligung wegen „Nichterwähnung“ im Kabinettsbeschluss vom 14. November 2006. Damit verkannte der Aufbaustab die Gesetzeslage und die sich daraus ergebende Verpflichtung **jeder** öffentlichen Stelle des Landes. Die rechtzeitige Beteiligung des Landesbeauftragten über grundlegende Planungen des Landes zum Aufbau oder zur Änderung von automatisierten Verfahren zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten bedarf keiner ausdrücklichen Erwähnung in einem Kabinettsbeschluss, sie gilt für **alle** Normadressaten des DSG-LSA, so auch für den Aufbaustab.
Leider kommt der Landesbeauftragte nicht umhin, auch an dieser Stelle zum wiederholten Mal (vgl. VI. Tätigkeitsbericht, Ziff. 7.1, zuletzt VIII. Tätigkeitsbericht, Ziff. 1.3) auf diese so wichtige gesetzliche Verpflichtung hinzuweisen. Bei Beachtung durch die öffentlichen Stellen des Landes ist so mit Unterstützung des Landesbeauftragten ein vorgezogener Grundrechtsschutz möglich.

Die **Unterrichtung** an den Landesbeauftragten ist an keine Form gebunden. Im einfachsten Fall reicht also zur Erfüllung dieser Pflicht eine Übersendung von Planungsunterlagen, u. a. auch Kabinettvorlagen, mit Hinweis auf eine Unterrichtung nach § 14 Abs. 1 Satz 2 DSG-LSA aus. Sie verursacht damit, im Gegensatz zu der dem Landesbeauftragten gegenüber oft geäußerten Meinung eines damit verbundenen „erheblichen zusätzlichen Aufwandes", diesen eben nicht.
Daneben müssen in einem noch viel stärkerem Maße die behördlichen Datenschutzbeauftragten (§ 14a DSG-LSA) ebenfalls bereits in der Planungsphase von IT-Projekten und -Verfahren der Ressorts beteiligt und einbezogen werden.
Diese „Meinungsverschiedenheiten" zwischen dem Aufbaustab und dem Landesbeauftragten sind aber mittlerweile ausgeräumt. Im Übrigen ist der Landesbeauftragte Mitglied des **Projektbeirates** des Aufbaustabs. Dieser hat allerdings nur eine beratende Funktion. Die Mitarbeit im Projektbeirat beeinträchtigt die Unabhängigkeit des Landesbeauftragten nicht, er ist bei seiner Aufgabenerfüllung nur dem DSG-LSA (§ 21 Abs. 1 Satz 1) unterworfen. Sie bietet ihm vielmehr eine weitere Möglichkeit zur Information und Erörterung, aber auch ansatzweise zur Beratung bei datenschutzrechtlichen Problemstellungen im Rahmen dieses anspruchsvollen und komplexen Projekts zur IT-Konsolidierung der Landesverwaltung.

Für die Abarbeitung der ressortübergreifenden Aufgaben wurden entsprechend des Kabinettsbeschlusses vom 28. August 2007 neun **Kompetenzteams** (K-Teams) in der Projektorganisation des Aufbaustabes gebildet (sie-he VIII. Tätigkeitsbericht, Ziff. 4.1). Dieser Prozess der IT-Konsolidierung auf Landesebene wird zeitgleich durch ressortinterne Projektteams unterstützt.
Die Projektorganisation des Aufbaustabs und dessen weiteres konzeptionelles Vorgehen wurden mit Kabinettsbeschluss vom 25. September 2007 bestätigt. Damit wurden die für den Aufbaustab notwendigen Regelungen zur Strukturierung und Steuerung des Projekts der IT-Konsolidierung getroffen.
Die weiteren Planungen bis Ende 2007 sahen vor, mit Unterstützung der Kompetenzteams zu den einzelnen zukünftig zentral durch das LRZ bereit-zustellenden **IT-Querschnittsdiensten** wie Datenhaltung und -archivierung, E-Mail-, Intranet- und Internet-Dienst, zentraler Verzeichnisdienst, zentrale Softwareverteilung, Benutzerbetreuung (zentraler User Help Desk) zunächst Grobkonzepte zu entwickeln und nach deren Bestätigung durch den Ständigen Staatssekretärsausschuss „Informationstechnologie" (StS-Ausschuss IT) als Lenkungsausschuss für das Gesamtprojekt IT-Konsolidierung entsprechende Fein- und Umsetzungskonzepte zu erstellen.
Die dem Landesbeauftragten im Laufe des Oktobers 2007 zugeleiteten ersten drei Entwürfe von Grobkonzepten der Kompetenzteams zu den Themen Zentralisierung und Virtualisierung von Servertechnik (K-Team „Terminal-Server-Technik"), Server-Konsolidierung (K-Team „Storage/Archivierung") und Datensicherung (K-Team „Storage/Archivierung") beinhalteten hinsichtlich der Aussagen zum Datenschutz und zur Datensicherheit nicht viel mehr als eine Kapitelüberschrift „Datenschutz". Zudem war die vom Aufbaustab gesetzte Frist von ganzen 3 Tagen für Ergänzungs- und Änderungsvorschläge mit Hinblick auf eine damals im IT-KA am 23. Oktober 2007 vorgesehenen Erörterung dieser Grobkonzepte wohl mehr als eine Zumutung anzusehen und scheinbar reine „Formsache" für den Aufbaustab. Der Landesbeauftragte hat diese Praxis gegenüber dem Aufbaustab kritisiert.
Dem Landesbeauftragten wurde nach dieser Kritik und seinem Beratungsangebot seitens des Aufbaustabs die Gelegenheit gegeben, im Rahmen seiner Besprechung mit den Teamleitern der Kompetenzteams am 15. November 2007, die Anforderungen zum Datenschutz

materiell-rechtlich, insbesondere aber aus technisch-organisatorischer Sicht mit Hinblick auf die Erfordernisse bei der automatisierten Verarbeitung personenbezogener Daten (Sicherheitsziele des § 6 Abs. 2 DSG-LSA) zu erörtern. Die genannten drei Grobkonzepte wurden am 9. Juni 2008 vom StS-Ausschuss IT bestätigt. Das vom Aufbaustab erarbeitete Grobkonzept zur zentralen Benutzerbetreuung (User Help Desk, Stand: 25.11.2008) wurde am 2. Dezember 2008 im IT-KA vor-gestellt.
Die geplante Umsetzung der technischen und organisatorischen Maßnahmen zur Datensicherheit (Sicherheitsziele) der Kompetenzteams „Software-Verteilung“, „Terminal-Server-Technik“, „SAP“, „Security- und Netzinfrastruktur“, „Solaris“, „Storage/Archivierung“ und „E-Mail/Intranet und Internet“ sind für den Landesbeauftragten von besonderem Interesse. Die hierfür besonders datenschutzrechtlich relevanten Grobkonzepte der Kompetenzteams „Security- und Netzinfrastruktur“ und „E-Mail/Intranet und Internet“ liegen dem Landesbeauftragten bisher nicht vor.

Das **Feinkonzept** zur **Server-Konsolidierung** (Vers. 2.3, Stand: 29. April 2009 des K-Teams „Storage/Archivierung“) liegt dem Landesbeauftragten vor, ebenso das Feinkonzept für **Datensicherung** (K-Team „Storage/Archivierung“). Das 125-seitige Feinkonzept zur Server-Konsolidierung lässt schon eine intensive Auseinandersetzung mit dem Thema IT-Sicherheit erkennen. Der Landesbeauftragte weist aber darauf hin, dass gerade zu den datenschutzspezifischen Sicherheitszielen **Revisionsfähigkeit** und **Transparenz**, die für eine datenschutzrechtliche Kontrolle unabdingbar ist, keine Aussagen getroffen werden. Hier besteht Nachbesserungsbedarf. Zu verweisen ist hier auf den IT-Strategie-Beschluss der Landesregierung vom 29. Juli 2008, Ziff. 3.5 Datenschutz (MBl. LSA S. 404).
Weitere datenschutzrechtliche Fragen bedürfen in diesem Zusammenhang einer Klärung, u. a. zum Thema Auftragsdatenverarbeitung (§ 8 DSG-LSA) sowie zu automatisierten Abrufverfahren (§ 7 DSG-LSA) in Verbindung mit der Vorabkontrolle bei bestimmten automatisierten Verfahren (§ 14 Abs. 2 DSG-LSA), die durch die behördlichen Datenschutzbeauftragten des jeweiligen Ressorts durchzuführen sind (§ 14a Abs. 4 Nr. 2 DSG-LSA).
Gerade zukünftige zentrale, virtuelle Server-Farmen benötigen für einen datenschutzkonformen Betrieb entsprechende Zugriffs- und Berechtigungskonzepte sowie die Sicherstellung der Revisionsfähigkeit im datenschutzrechtlichen Sinn. Umfangreiche personenbezogene Datenbestände bei einem zentralen IT-Dienstleister wie dem zukünftigen LRZ sind hinsichtlich ihrer rechtlichen Zulässigkeit und den getroffenen Maßnahmen zur Datensicherheit zu beurteilen. Zur konzeptionellen Planung dieser IT-Konsolidierungsprozesse gehört nicht zuletzt auch die Beachtung und Berücksichtigung der datenschutzrechtlichen Rahmenbedingungen.
Zu Beginn des Jahres 2008 erfolgte seitens des Aufbaustabs ein Strategie-wechsel, was die Übernahme der IT-Querschnittsdienste durch das zukünftige LRZ betraf. Die bisherige Planung, über die drei Phasen Test-, Probe- und Pilotbetrieb diese Dienste beim LRZ aufzubauen und danach landesweit einzuführen, wurde aufgegeben und statt dessen durch ein Migrationskonzept je Behörde ersetzt, welches eine Ist-Analyse und Konzepterstellung zur Ablösung der IT-Querschnittsdienste und danach die Übernahme dieser IT-Querschnittsdienste von der jeweiligen Behörde durch das LRZ vorsieht. Wesentlicher Vorteil dieser Vorgehensweise ist die jeweils nur einmal not-wendige Befassung mit einer Behörde.
Das vom Aufbaustab erarbeitete Konzept zum übergreifenden **IuK-Betriebsmodell** des Landes Sachsen-Anhalt wurde **vom Kabinett am 1. Juli 2008 bestätigt**. Das IuK-Betriebsmodell bestimmt die vom LRZ und dem Betriebsstättenverbund zukünftig zu erbrin-

genden IT-Dienstleistungen und die allein von diesen zu betreibenden IT-Querschnittsaufgaben. Es trifft Festlegung zum sog. Leistungsschnitt, d. h. der Abgrenzung der Verantwortung zwischen zukünftigen LRZ und den Ressorts und sieht Servicevereinbarungen der Ressorts und der jeweiligen Dienststellen mit dem LRZ vor. Für den operativen Betrieb werden ebenfalls Regelungen für die Zusammenarbeit zwischen den Ressorts und dem LRZ getroffen.

Noch am **18./19. November 2008** wurde den Ressorts und dem Landesbeauftragten in einem **Workshop** vom Aufbaustab das **Geschäftsmodell** für den zukünftigen zentralen IT-Dienstleister in Form einer teilrechtsfähigen **Anstalt des öffentlichen Rechts** (sog. Anstalts-Modell) als Zusammenschluss von FRZ und LIZ vorgestellt. Die Anstalt sollte Bestandteil eines IT-Betriebsstättenverbundes werden, der im Errichtungszeitraum mit dieser Anstalt und dem Rechenzentrum im Technischen Polizeiamt (TPA), dem Justizrechenzentrum Barby und dem Rechenzentrum des LVermGeo gebildet werden sollte. Der künftige zentrale IT-Dienstleister sollte über zwei Standorte in Magdeburg und Halle (Saale) verfügen, mit Hauptsitz in Halle (Saale). Die Bildung der Anstalt sollte durch ein entsprechendes Errichtungsgesetz erfolgen.

Nach einer **Grundsatzentscheidung** durch das Ministerium der Finanzen im **Januar 2009** wurde das bisherige Geschäftsmodell überraschend geändert. Nunmehr sollen in Form einer **Verwaltungslösung**, d. h. innerhalb der Oberfinanzdirektion Magdeburg (OFD), das FRZ und das LIZ den Kern des zentralen IT-Dienstleisters bilden. Das LRZ soll nunmehr als **Abteilung 4 der OFD** angegliedert werden.

Dieses neue Geschäftsmodell wurde am **12. Mai 2009** in einem **Workshop** den Ressorts durch den Präsidenten der Oberfinanzdirektion persönlich erläutert. Ein wesentlicher Vorteil dieser Verwaltungslösung (sog. Behörden-Modell) soll darin bestehen, dass die Fusion von FRZ und LIZ zum LRZ zu-nächst in den bewährten Strukturen erfolgen kann. Das LRZ soll in den kommenden Jahren sukzessive alle IT-Querschnittsaufgaben für über 300 Behörden des Landes übernehmen.

Eine Entscheidung zum Betreiber für das **zukünftige Landesnetz (ITN XT)** anstelle des bisherigen Betreibers des Landesnetzes (ITN-LSA), des TPA, steht aber bisher noch aus.

Der Landesbeauftragte hat an dem genannten Workshop ebenfalls teilgenommen. Er hat insbesondere in Bezug auf die vorgesehene Übernahme von über 90 Leistungsvereinbarungen des LIZ in das LRZ an die Beachtung datenschutzrechtlicher Bestimmungen erinnert und gleichzeitig seine Unterstützung für die Begleitung dieses Überführungsprozesses angeboten.

**Der Betriebsbeginn des LRZ ist für den 1. Juli 2009 geplant**. Zeitgleich soll die Pilotierung im Geschäftsbereich des Ministeriums der Finanzen, als erstem Ressort, zur Migration der IT-Querschnittsdienste beginnen.

Der Landesbeauftragte wird sich im kommenden Berichtszeitraum verstärkt mit dem Aufbau des LRZ beschäftigen und insbesondere sein Augenmerk auf die datenschutzkonforme Einrichtung und Übernahme von IT-Querschnittsdiensten durch das LRZ und die Überführung der Leistungsvereinbarungen des LIZ in das LRZ legen.

Er geht davon aus, dass er weiterhin zeitnah und ausreichend über die weite-er Umsetzung des IT-Konsolidierungsprozesses informiert wird und ihm da-durch die Gelegenheit und Möglichkeit gegeben wird, auf eine datenschutzgerechte Realisierung dieses komplexen und ehrgeizigen Vorhabens der Landesregierung zur IT-Konsolidierung der Landesverwaltung Sachsen-Anhalt hinzuwirken und allen dabei Beteiligten beratend zur Verfügung zu stehen.

### 4.3. Grundkonzept IT-Architektur der Landesverwaltung

Bereits im **Dezember 2006** hatte die Staatskanzlei dem Landesbeauftragten den **Entwurf „Konzept für IT-Infrastruktur Land Sachsen Anhalt“** mit der Bitte um Stellungnahme zugeleitet. Dieser Konzeptentwurf resultierte aus einem davor bereits Anfang 2006 erteilten Auftrag des damals noch für die IT-Strategie zuständigen Ministeriums des Innern für ein solches Grundkonzept für IT-Infrastrukturdienste an das Landesinformations-Zentrum (LIZ).
Grundsätzlich begegnete dieses Konzept keinen datenschutzrechtlichen Bedenken, schuf es doch die grundlegende Voraussetzung für eine längst überfällige landesweite einheitliche IT-Infrastruktur, die den optimalen Einsatz standardisierter E-Government-Verfahren der öffentlichen Stellen des Landes erst ermöglicht. Bei einer datenschutzgerechten Umsetzung wird damit der Grundstein für die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität personenbezogener Daten in IT-Infrastrukturdiensten (u. a. Mitarbeitereinträge im zentralen Namens- und Verzeichnisdienst) entsprechend den Sicherheitszielen des § 6 Abs. 2 DSG-LSA gelegt.
Mit Beschluss 02/2007 des Koordinierungsausschusses Informationstechnik (IT-KA) vom 23. Januar 2007 wurden dieses Konzept bestätigt und grundlegende Entscheidungen zur Überarbeitung und Fortentwicklung zu einem Grundkonzept „IT-Architektur der Landesverwaltung Sachsen-Anhalt“ getroffen. Gleichzeitig wurde das LIZ mit der Erarbeitung eines Konzepts für das Identitäts- und Zugriffsmanagement (engl.: Identity and Access Management-System - IAM-System) beauftragt.
Zur Zentralisierung des Namens- und Verzeichnisdienstes wurde die im Konzept vorgeschlagene Architekturvariante III „Zentral - integriert“ auf homogener Microsoft Plattform vom IT-KA mit Beschluss 05/2007 vom 1. Oktober 2007 bestätigt.
Wesentliches Merkmal dieser Architekturvariante ist die Trennung der Administration von **Diensten** und **Daten**. Das bedeutet, dass zukünftig mehr **IT-Querschnittsdienste** zentral bereitgestellt werden (siehe Ziff. 4.2), zu denen u. a. der Namens- und Verzeichnisdienst zählt, ohne damit die Selbständigkeit der Ressorts und deren Verantwortlichkeit für die eigene Datenverwaltung zu beeinträchtigen. Ein solcher Infrastrukturdienst wird landesweit zur Verfügung stehen und ist von jeder öffentlichen Stelle der Landesverwaltung nutzbar. Dieser Prozess geht einher mit der Vereinheitlichung und Standardisierung von Datenformaten und Schnittstellen. Die Bereitstellung und die Administration erfolgt durch den zentralen IT-Dienstleister. Die Ressorts werden Nutzer dieses Infrastrukturdienstes sein, betreiben diesen aber nicht.
Zur Begleitung der Weiterentwicklung des IT-Architektur-Konzepts LSA wurde eine ressortübergreifende Arbeitsgruppe **IT-Architektur** unter Federführung der Staatskanzlei (LIS) gebildet.
Mit **IT-KA-Beschluss 07/2007** vom **4. Dezember 2007** wurde das in der AG IT-Architektur erarbeitete **Namenskonzept** für diesen einheitlichen Namens- und Verzeichnisdienst des Landes für verbindlich erklärt und durch den Ständigen Staatssekretärsausschuss „Informationstechnologie“ bestätigt. Dieses umfassende **Namenskonzept** ist als **Anlage 2** Bestandteil des Beschlusses der Landesregierung über die IT-Strategie des Landes Sachsen-Anhalt vom 29. Juli 2008 (MBl. LSA S. 619). Es ist damit verbindlich für die gesamte Landesverwaltung die Migration zu einem zentralen Namens- und Verzeichnisdienst festgeschrieben.
Der Landesbeauftragte ist Mitglied dieser Arbeitsgruppe, die ihre Tätigkeit über den jetzigen Berichtszeitraum hinaus auch in den nächsten Jahren noch fortsetzen wird.
Die erste Bewährungsprobe für diesen integrierten IT-Infrastrukturdienst und dessen zentrale Verwaltung stellt die zum 1. Juli 2009 geplante Betriebsaufnahme des zentralen IT-

Dienstleisters in Sachsen-Anhalt dar. Eine funktions-fähige einheitliche IT-Infrastruktur mit zentralem Management und der Auf-bau eines IAM-Systems bilden die Grundlage für eine optimale standardisierte E-Government-Infrastruktur und die weitere Umsetzung der im E-Government-Maßnahmenplan 2008-2009 vorgesehenen Leitprojekte und Basiskomponenten (siehe Ziff. 4.5).
Die Konzepte zum Namens- und Verzeichnisdienst und zum Aufbau eines IAM-Systems, die von der AG IT-Architektur mit externer Unterstützung eines Beratungsunternehmens erarbeitet und durch den IT-KA bestätigt wurden, sowie der Beschluss der Landesregierung zur IT-Strategie bilden zugleich die Grundlage für die konzeptionelle Arbeit des Kompetenzteams „E-Mail/Intranet und Internet“ (siehe Ziff. 4.2).
Die dem Landesbeauftragten seit dem **22. Mai 2009** vorliegende **Endfassung des Grobkonzepts „Verzeichnisdienste/Identity und Access Management“ (Stand: 19. Mai 2009)** dieses Kompetenzteams berücksichtigt seine Empfehlungen zur Absicherung und Veröffentlichung personenbezogener Daten. Hierzu gehören geplante Regelungen zu abgestuften Zugriffsrechten und zur Revisionsfähigkeit der Administration sowie für die Absicherung der Systeme des Namens- und Verzeichnisdienstes durch den Einsatz geeigneter IT-Sicherheitstechnologien wie Firewall und Proxy-Server.
Zum Schutz der Accounts des zentralen Namens- und Verzeichnisdienstes folgt das Kompetenzteam in seinem Grobkonzept ebenfalls der Empfehlung des Landesbeauftragten zum Einsatz eines chipkartenbasierten Anmeldeverfahrens. Die Sicherheitsinfrastruktur hat das Land bereits im Jahr 2006 geschaffen (siehe VIII. Tätigkeitsbericht, Ziff. 4.3). Der Landesbeauftragte begrüßt ausdrücklich den Einsatz der Signaturkarte Sachsen-Anhalt mit Zertifikaten der Public Key Infrastruktur Land Sachsen-Anhalt (PKI LSA) für eine vertrauliche und sichere Anmeldung an den zentralen Namens- und Verzeichnisdienst.
Für die Veröffentlichung der Daten, insbesondere der personenbezogenen Mitarbeiterdaten, ist im Grobkonzept vorgesehen, die bereits mit dem Landesbeauftragten für das Zentrale Adressverzeichnis abgestimmte abgestufte Veröffentlichungsregelung anzuwenden (siehe VI. Tätigkeitsbericht, Ziff. 7.4).
Der Landesbeauftragte geht davon aus, dass mit der Erstellung des Feinkonzepts „Verzeichnisdienste/Identity und Access Management“ diese vorgesehenen Regelungen zum Datenschutz und der Datensicherheit mit konkreten Maßnahmen untersetzt werden und er hiervon rechtzeitig unterrichtet wird. Besonderes Augenmerk wird er auf die Erarbeitung des IT-Sicherheitskonzepts für diesen zentralen Namens- und Verzeichnisdienst richten, welches die datenschutzrechtlichen Anforderungen berücksichtigen muss.
Ziel eines Identitäts- und Zugriffsmanagement-Systems ist es, personenbezogene Daten konsistent, sicher und ständig verfügbar für das IT-Management bereitzuhalten. Die Vielzahl von Services, deren Daten unter-einander abzugleichen sind, stellt an die Administration hohe Anforderungen. Veränderungen der Daten der Mitarbeiter und Mitarbeiterinnen, bei Neueinstellungen oder Dienstbeendigung sowie aufgrund von Funktions- oder Behördenwechsel, müssen in allen beteiligten Systemen dann sicher und automatisch erfolgen können.
Die datenschutzrechtlichen Anforderungen hinsichtlich der Einrichtung von Accounts (Benutzerkonten), deren Benutzerrechte und Vergabe für eine natürliche Person in einem Identitäts- und Zugriffsmanagement-System sind aus den Arbeitsaufgaben (Dienstposten / Arbeitsplatzbeschreibung) der Mitarbeiter und Mitarbeiterinnen abzuleiten.
In diesem Zusammenhang kommt der durch die Landesregierung beabsichtigten Schaffung eines IT-gestützten **Personalmanagementsystems (PMS)** für die gesamte Landesverwal-

tung (siehe Ziff. 17.2) eine besondere Bedeutung zu. Für eine **natürliche Person** muss zukünftig eine **digitale Identität** durch das PMS erzeugt werden können.
Historisch bedingt existiert für die Landesverwaltung kein zentrales Identitäts- und Zugriffsmanagement-System. Dadurch sind in den Ressorts unterschiedliche Identitätsspeicher im Einsatz. Die Informationen über diese digitalen Identitäten werden in einem zentralen Verzeichnis aus Identitätsspeichern der Ressorts über Schnittstellen zusammengeführt werden. Zukünftig wird der überwiegende Teil der Behörden der Landesverwaltung einen **Active Directory (AD)** als primären einheitlichen Identitätsspeicher nutzen. Das AD dient als standardisierter und zentraler Verzeichnisdienst und primärer (führender) Identitätsspeicher. Es bildet die Voraussetzung für eine effektive und sichere Identitäts- und Zugriffsverwaltung.
Nach der Einführung eines PMS kann die Zuordnung einer Person zu einer bestimmten Stelle (Verwaltungsrolle) und zu ihrer Rolle im IT-System (IT-Rolle) durch die Personalabteilung vorgenommen werden. Deshalb besteht auch aus datenschutzrechtlicher Sicht das Erfordernis, zukünftig das PMS hinsichtlich der Zuordnung einer Person zur Verwaltungsrolle als führendes System einzuführen. Über eine Datenschnittstelle des PMS können dann die Daten für das IAM-System bereitgestellt werden. Digitale Identitäten (Benutzer, Gruppen, Geräte, Dienste) werden zentral mit Hilfe des IAM-Systems verwaltet. Diesen Identitäten werden die im IAM-System abgebildeten IT-Rollen und Rechte für Applikationsrollen (z. B. für Anwendungen im Landesportal, E-Mail, HAMISSA, SALSA usw.) zugeordnet: Dieses Konzept zur Verbindung von PMS mit einem IAM-System setzt aber für seine optimale Umsetzung die Umstellung auf **ein** PMS für alle Landesbehörden voraus.
Der Landesbeauftragte ist bereit, das Kompetenzteam „E-Mail/Intranet und Internet“ bei dieser schwierigen Aufgabe beratend zu unterstützen. Als Mitglied in der AG IT-Architektur wird er die Konzepterarbeitung und Einführung eines auf dem zentralen integrierten Namens- und Verzeichnisdienstaufbau-enden IAM-Systems für das Land weiter begleiten.

### 4.4. Landesleitlinie IT-Sicherheit

In den zurückliegenden Jahren wurde seitens der Landesregierung mehrfach versucht, durch entsprechende Beschlüsse den Prozess zur Etablierung einer IT-Sicherheitsplattform für die Landesverwaltung voran zu bringen.
Im damaligen Kabinettsbeschluss vom 15. Juli 2003 wurde das der Kabinettvorlage des Ministeriums des Innern beigefügte „Landeseinheitliches Konzept Informationstechnologie, IT-Investitionen 2003“ vom 10. Juli 2003 als verbindliche Grundlage der informationstechnischen Basisversorgung der Landesverwaltung bestätigt.
In diesem Konzept wurde hinsichtlich der IT-Infrastruktur und deren Sicherheit Handlungsbedarf festgestellt.
Eine entsprechende Konzeption zu einem IT-Sicherheitsmanagement auf Landesebene sollte durch das Technische Polizeiamt (TPA) und das Landesinformations-Zentrum (LIZ) erarbeitet werden. Darin sollten auch die Grundlagen und Bedingungen zum kurzfristigen Einrichten eines sog. **CERT-LSA** (Computer Emergency Response Team) definiert werden. Nach einem Beschluss des IT-KA am 28. Oktober 2003 wurde das TPA durch das Ministerium des Innern mit der Leitung der hierzu gebildeten Projektgruppe beauftragt. Dabei sollen die Erfahrungen des CERT-Bund und der in den Ländern vorhandener CERTs einfließen.
**Die von der Projektgruppe erarbeiteten Vorschläge wurden aber nicht aufgegriffen und weiterverfolgt.**

Ein Jahr später, im November 2004, leitete die damalige Landesleitstelle IT/E-Government (LIT) des Ministeriums des Innern in Vorbereitung einer Kabinettsbefassung zum Thema IT-Sicherheit in der Landesverwaltung dem Landesbeauftragten den Entwurf eines geplanten Gem. RdErl. „Kommunikations- und Infrastrukturerlass Sachsen-Anhalt (KommIn-LSA)“ zu. Die LIT er-arbeitete gleichzeitig unter Mitwirkung des TPA und des Landesbeauftragten den Entwurf einer Sicherheitsrichtlinie für das Informationstechnische Netz des Landes Sachsen-Anhalt (ITN-LSA), welche als Anlage Bestandteil des KommIn-LSA werden sollte. Dazu kam es jedoch nicht.

Im November 2005 wurde dem Landesbeauftragten per E-Mail durch das Ministerium der Innern (LIT) die „IT-Sicherheitsrichtlinie des ITN-Betreibers für das Informationstechnische Netz des Landes Sachsen-Anhalt (ITN-LSA)“ als ab sofort anzuwendende Richtlinie bekannt gegeben.

Eine Fortschreibung dieser **IT-Sicherheitsrichtlinie des ITN-Betreibers (dem TPA)** soll gemäß Ziff. 6 nach regelmäßiger Prüfung erfolgen und dem neuesten Stand der Technik angepasst sowie der LIT/E-Government des Ministeriums des Innern (die es aber seit dem 1. Dezember 2006 nicht mehr gibt!) zur Genehmigung vorgelegt werden. Die Bekanntgabe der jeweils aktuellen Fassung soll in geeigneter Weise erfolgen.

Die im Informationsportal der Staatskanzlei veröffentlichte Fassung trägt das Datum 18. Juli 2007. Das sich innerhalb von fast zwei Jahren kein Anpassungsbedarf dieser IT-Sicherheitsrichtlinie ergeben hat, darf bezweifelt werden.

Nach der Übernahme der Zuständigkeit für die IT-Strategie durch die Staatskanzlei hatte deshalb die Leitstelle für IT-Strategie (LIS) die Initiative ergriffen und zu einem 1. Erfahrungsaustausch zum Thema IT-Sicherheit im November 2007 eingeladen. Auch der Landesbeauftragte ist dieser Einladung gefolgt. Das Ministerium der Finanzen hatte sich nicht an diesem Erfahrungsaustausch beteiligt. Das Ergebnis der Bestandsaufnahme war für alle am Er-fahrungsaustausch Beteiligten ernüchternd. Bis auf den Bereich der Landespolizei (IT-Sicherheitsleitlinie; RdErl. des Ministeriums des Innern vom 29. Januar 2004), dem LIZ, und dem Ministerium für Landwirtschaft und Umwelt für den INVEKOS-Verbund **war kein IT-Sicherheitsmanagement in den übrigen Ressorts etabliert.**

Das Thema „**IT-Sicherheitsmanagement**“ rückt aber mit dem Beschluss der Landesregierung über die IT-Strategie des Landes Sachsen-Anhalt vom 29. Juli 2008 (MBl. LSA S. 619) wieder mehr in den Fokus der Aufmerksamkeit der Ressorts. Als mittelfristige Maßnahme im Rahmen der IT-Strategie des Landes soll nunmehr die IT-Sicherheit institutionalisiert werden. In einer neuen **Landesleitlinie IT-Sicherheit** werden zukünftig wesentliche Ziele so-wie deren Umsetzung für die Landesverwaltung verbindlich festgelegt. Diese soll dann die Grundlage für die Etablierung einer IT-Sicherheitsorganisation in der Verantwortung der Ressorts bilden.

Und auch das etwas in Vergessenheit geratene CERT-LSA soll wieder zum Leben erweckt werden und zur Lösung akuter Sicherheitsvorfälle im Land beitragen.

Im Rahmen der IT-Konsolidierung der Landesverwaltung befasst sich auch das Kompetenzteam „Security/Netzinfrastruktur“ unter Federführung des TPA mit dieser Thematik. Dem Landesbeauftragten liegt aber bisher kein Grobkonzept des Kompetenzteams hierzu vor.

In diesem Zusammenhang erinnert der Landesbeauftragte auch an seine Kritik aus zurückliegenden Berichtszeiträumen zum Thema IT-Sicherheitskonzept für das ITN-LSA und dem damit in Zusammenhang stehenden sog. „Netz-Erlass“, dem Gem. RdErl. des Ministeriums des Innern, der Staatskanzlei und der übrigen Ministerien vom 7. Februar 1994 (MBl. LSA S. 1251) (siehe IV. Tätigkeitsbericht, Ziff. 8.2.2, V. Tätigkeitsbericht, Ziff.6.3, VI. Tätigkeitsbericht, Ziff. 7.3, zuletzt VIII. Tätigkeitsbericht, Ziff. 1.3). Dieser sollte im Zuge der Erarbeitung

einer Landesleitlinie IT-Sicherheit entweder aufgehoben oder grundsätzlich überarbeitet und den aktuellen Gegebenheiten des ITN-LSA angepasst werden.
Abschließend sei noch auf das zentrale IT-Sicherheitsmanagement des Landes Mecklenburg-Vorpommern durch Nutzung des „GSTOOL“ (einem kostenfreien BSI Software-Tool zum IT-Grundschutz) durch den dortigen zentralen IT-Dienstleister hingewiesen. Damit wurde eine effiziente und praktikable Verfahrensweise gefunden, die Ressorts bei Erstellung, Verwaltung und Fortschreibung von IT-Sicherheitskonzepten entsprechend dem IT-Grundschutz zu unterstützen. Zugleich ist damit die Möglichkeit verbunden, diesen IT-Sicherheitsprozess zu planen, Maßnahmen umzusetzen und auch den Umsetzungsstand bei der IT-Sicherheit im Land darzustellen und abzurechnen.

### 4.5. E-Government-Maßnahmenplan 2008-2009

Über die Umsetzung des von der Landesregierung am **29. April 2003 beschlossenen „Grundkonzept E-Government in Sachsen-Anhalt“**, dem daraus durch das Ministerium des Innern erarbeiteten und vom **Kabinett am 17. August 2004 verabschiedeten Aktionsplan** für den **Zeitraum 2004 bis 2010** und zu dessen Umsetzung unter Federführung des Ministeriums des Innern in daraus abgeleiteten E-Government-Maßnahmenplänen für die Jahre 2005/2006, 2007 berichtet der Landesbeauftragte in seinen Tätigkeitsberichten regelmäßig (siehe VII. Tätigkeitsbericht, Ziff. 7.1, VIII. Tätigkeitsbericht, Ziff. 4.2). Die Informationen und Beurteilungen des Landesbeauftragten erfolgen dabei aus datenschutzrechtlicher Sicht und stellen damit keine grundsätzliche Kritik an dieser Form der Verwaltungsmodernisierung dar. Gleichwohl sind bei allen diesen Leitprojekten die bereichsspezifischen und die allgemeinen Regelungen zum Datenschutz und der Datensicherheit zu berücksichtigen und einzuhalten. Anfragen zu Beratung bzw. Unterrichtung der Ressorts zeugen zumindest von einer stärkeren Beachtung datenschutzrechtlicher Belange.
Das Ministerium des Innern hat gegenüber dem Landesbeauftragten, wie in der Stellungnahme der Landesregierung zum VIII. Tätigkeitsbericht des Landesbeauftragten vom 23. Januar 2008 (LT-Drs. 5/1097) angekündigt, seine Informationspolitik verbessert. Dem Landesbeauftragten wurde der aktuelle **E-Government-Maßnahmenplan 2008-2009**, wenn auch sehr kurzfristig, doch noch vor der Beschlussfassung des Kabinetts am 4. März 2008 zugeleitet.
Auch beide Sachstandsberichte zum Umsetzungsstand des derzeitigen E-Government-Maßnahmenplans zur Information des Kabinetts (vom 16. Oktober 2008 und 20. Februar 2009) hat das Ministerium des Innern dem Landesbeauftragten zeitnah zur Verfügung gestellt.
Der aktuelle **E-Government-Maßnahmenplan 2008-2009** umfasst mittlerweile **23 Leitprojekte** und **6 Basiskomponenten**. Sowohl bei der Bereitstellung von Basiskomponenten als auch bei der Umsetzung von Leitprojekten sind Fortschritte zu verzeichnen. So hat sich das **Landesportal** (www.sachsen-anhalt.de) zu einem Dienstleistungsportal entwickelt. Besondere Anstrengungen sind bei der weiteren IT-Umsetzung der **EU-Dienstleistungsrichtlinie** und des **Binnenmarktinformationssystem IMI** (Internal Market Information System) erforderlich. Auch die Umsetzung der Vorhaben zur Deutschland Online Initiative (DOL), als der nationalen E-Government-Strategie von Bund, Ländern und Kommunen in Sachsen-Anhalt, erfordert erhebliche Anstrengungen. Das Land beteiligt sich hier aktiv an solchen DOL-Projekten. Beispielhaft sind hier das DOL-Projekt „IT-Umsetzung der EU-DLR“, die Mitarbeit

im Verbund der Länder zum „Zuständigkeitsfinder“ und den Arbeitsgruppen der „D115-Initiative“, der einheitlichen Behördenrufnummer für Deutschland, zu nennen.
Mit dem Ministerium des Innern wurde im o. a. Sinne eine grundsätzliche Verfahrensweise in Bezug auf Unterrichtungen des Landesbeauftragten zu eingesetzten automatisierten Verfahren im Geschäftsbereich des Ministeriums des Innern im beiderseitigen Einvernehmen erörtert und abgestimmt.
Positiv ist auch die Berichterstattung des Ministeriums der Justiz hinsichtlich der Unterrichtung des Landesbeauftragten zur Planung und Umsetzung seines IT-Ressortplans zu erwähnen. Der Landesbeauftragte informierte sich in diesem Zusammenhang bei Besuchen im September 2008 über das beim Amtsgericht Stendal geführte EDV-Handels-, Genossenschafts-, Partnerschafts- und Vereinsregister (Regis STAR) sowie im Dezember 2008 beim Amtsgericht Aschersleben über das in der Zweigstelle Staßfurt geführte Elektronischen Mahnverfahren Sachsen-Anhalt (EMSA), welches gemeinsam mit den Freistaaten Sachsen und Thüringen betrieben wird.
Hinsichtlich der zukünftigen Aufstellung der IT-Ressortpläne wurde der Landesbeauftragte im Februar 2009 von der Landesleitstelle IT-Strategie (LIS) der Staatskanzlei darüber informiert, dass ein sog. **„IT-Kataster“** geplant wird. Im Rahmen einer Ausschreibung und externen Vergabe dieser Dienstleistung soll mit diesem IT-Kataster eine Datenbanklösung zur Erfassung, Darstellung und anwenderübergreifenden Nutzung von Informationen über alle relevanten IT-Verfahren der Landesverwaltung entwickelt werden. Diese Datenbanklösung soll mandantenfähig gestaltet werden.
Auf Anregung des Landesbeauftragten sind in dem an die LIS einzureichen-den IT-Ressortplan bzw. -konzept auch die jeweiligen Maßnahmen zum Datenschutz und Datensicherheit darzustellen. Diese Informationen wären für den Landesbeauftragten natürlich von besonderem Interesse und ständen ihm zeitnah und aktuell zur Verfügung, ohne den Ressorts zusätzlichen Aufwand zu bereiten. Voraussetzung bildet natürlich die Umsetzung der geplanten anwenderübergreifenden Nutzung.
Der Landesbeauftragte bittet deshalb die Staatskanzlei, bei der Entwicklung dieses IT-Katasters eine solche Nutzungsmöglichkeit für ihn zu berücksichtigen.
Natürlich entbindet dies die Ressorts nicht von ihrer gesetzlichen Unterrichtungspflicht gemäß § 14 Abs. 1 Satz 2 DSG-LSA. Es würde aber unnötige Nachfragen vermeiden helfen und zusätzliche Berichterstattungen an den Landesbeauftragten auf ein Minimum beschränken, wenn ihm mittels des Zugangs zum IT-Kataster diese Informationen aktuell zur Verfügung stehen würden.

### 4.6. Masterplan Landesportal Sachsen-Anhalt 2007-2011

Aufbauend auf dem „Grundkonzept E-Government in Sachsen-Anhalt“ wurde ein E-Government-Aktionsplan für die Landesverwaltung für die Jahre 2004-2010 erarbeitet. Nach der Systematik dieses Aktionsplans wurde das **Landesportal Sachsen-Anhalt (LPSA)** als **Basiskomponente (Nr. 1)** eingestuft, da es den Anforderungen eines Dienstleistungsportals bereits in beachtlichen Ansätzen gerecht wurde. Im Leitprojekt Internetportal wurden zahlreiche Online-Dienstleistungen zusammengefasst, die unter Federführung der Staatskanzlei umgesetzt und in das Landesportal eingebunden werden sollen (vgl. Beschluss der Landesregierung vom 26. September 2006 zum Masterplan Landesportal Sachsen-Anhalt). Der Landesbeauftragte hatte bereits in seinem VIII. Tätigkeitsbericht unter Ziff. 4.2 ausführlich dazu berichtet.

Die Landesregierung beabsichtigt, das Landesportal zum zentralen Einstiegspunkt zu allen Dienstleistungen des Landes auszubauen. Es wird weit über eine reine Informationsplattform hinaus verstärkt transaktionsorientierte Dienstleistungen gebündelt anbieten. Mit diesem Ziel kommuniziert eng die Bereitstellung der Basiskomponenten

- Geodatenserver
- Zahlungsverkehrsplattform
- Formularserver
- elektronische Signatur/virtuelle Poststelle.

Dass diese Basiskomponenten erhebliche datenschutzrechtliche Relevanz besitzen und bei ihrer weiteren Gestaltung der Landesbeauftragte gem. § 14 Abs. 1 Satz 2 DSG-LSA zur Wahrnehmung seines gesetzlichen Beratungs- und auch Kontrollauftrages rechtzeitig zu beteiligen ist, versteht sich von selbst. Der Landesbeauftragte hatte in diesem Zusammenhang mehrfach, auch im VIII. Tätigkeitsbericht in Ziff. 4.2, entsprechende Appelle an die Landesregierung und an die für die einzelnen Basiskomponenten verantwortlichen Fachministerien gesandt.
Gleiches gilt im Übrigen auch für die zahlreichen im Rahmen der E-Government-Initiative umzusetzenden Leitprojekte, die für den Masterplan Landesportal von Relevanz sind.
Das sind, neben dem o. g. Internetportal www.sachsen-anhalt.de, die **Leitprojekte**

- elektronische Steuererklärung/ELSTER
- Geoinformationsdienste
- elektronisches Grundbuch
- elektronisches Mahnverfahren
- elektronische Vergabe- und Beschaffung
- Internetgestützte Einsicht in die Handels-, Genossenschaft- und Partnerschaftsregister
- zentrale Stellenbörse
- Bürgerinformationssystem der Landesverwaltung
- IBA-Stadt-Monitor sowie
- das nachträglich als Leitprojekt qualifizierte Sperrinformationssystem

mit sehr unterschiedlichem Realisierungsstand, die je nach Entwicklungsfort-schritt in das Landesportal eingebunden werden. Der Landesbeauftragte hat bei vielen Projekten im Rahmen seiner Zuständigkeit mitgearbeitet und wert-volle Hinweise zu datenschutzrechtlichen Verbesserungen geben können.

### 4.7. Umsetzung der EU-Dienstleistungsrichtlinie in Sachsen-Anhalt

In Sachsen-Anhalt koordiniert das Ministerium für Wirtschaft und Arbeit die inhaltliche Umsetzung der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über die Dienstleistungen im Binnenmarkt (ABl. EU Nr. L 76 S. 36) (**EU-Dienstleistungsrichtlinie** - EU-DLR). Für die IT-Umsetzung der EU-DLR ist das Ministerium des Innern verantwortlich. Nach einer Abstimmung des Ministeriums für Wirtschaft mit dem Ministerium des Innern wurde auf der Grundlage einer vom Ministerium für Wirtschaft und Arbeit abgegebenen Empfehlung durch Kabinettsbeschluss am 23. September 2008 als

**Einheitlicher Ansprechpartner (EA)** nach Art. 6 der EU-DLR das Landesverwaltungsamt bestimmt.

Der Landesbeauftragte hatte zuvor das Ministerium für Wirtschaft und Arbeit bereits im April 2008 über den Beschluss der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Umsetzung des Binnenmarktinformationssystems IMI (Internal Market Information System) vom 3. und 4. April 2008 **(Anlage 14)** in Kenntnis gesetzt und sich gleichzeitig für die seit August 2007 erfolgten, regelmäßigen Informationen zum IMI bedankt.
Der Wirtschaftsminister hatte im Mai 2008 positiv auf das Angebot des Landesbeauftragten zur Mitarbeit in der Projektgruppe zur Umsetzung der EU-DLR reagiert und den Landesbeauftragten über die weitere Vorgehensweise zur Umsetzung der EU-DLR und zugleich über den Sachstand bei der Umsetzung des IMI informiert.
Sowohl die Umsetzung der EU-DLR als auch des IMI waren Gegenstand intensiver Beratungen des Arbeitskreises „Grundsatzfragen der Verwaltungsmodernisierung“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder. Datenschutzrechtliche Grundanforderungen bei der Umsetzung der EU-DLR und insbesondere für den EA wurden von diesem Arbeitskreis erarbeitet und von der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 zustimmend zur Kenntnis genommen. Diese Ausarbeitung zu datenschutzrechtlichen Anforderungen hat der Landesbeauftragte ebenfalls dem Ministerium für Wirtschaft und Arbeit zur Verfügung gestellt.
Eine erste Beratung der Unterarbeitsgruppe „Einheitlicher Ansprechpartner“ (UAG EA) unter Beteiligung des Landesbeauftragten hat am 12. März 2009 stattgefunden. Schwerpunkt der Beratung des Ministeriums für Wirtschaft über diese Sitzung hinaus bildet zum gegenwärtigen Zeitpunkt der vom Ministerium erarbeitete Entwurf des Gesetzes über den einheitlichen Ansprechpartner in Sachsen-Anhalt (EAG LSA).
Die Überprüfung der datenschutzrechtlichen Ausgangssituation unter Berücksichtigung der Verortung des EA beim Landesverwaltungsamt in Halle lässt eine spezifische normative Regelung zum Datenschutz im Entwurf des EAG LSA als nicht unbedingt notwendig erscheinen. Die Aufgaben des EA sind bereits im Verwaltungsverfahrensrecht geregelt. Zu beachten ist insofern der § 3 Abs. 4 DSG-LSA. Danach gehen die Bestimmungen des DSG-LSA denen des Verwaltungsverfahrensgesetzes des Landes vor, wenn bei der Ermittlung des Sachverhaltes personenbezogene Daten erhoben, verarbeitet oder genutzt werden. Der EA unterliegt als öffentliche Stelle des Landes (§ 2 Abs. 8 DSG-LSA) ohnehin den Bestimmungen des DSG-LSA. Inwieweit darüber hinaus spezielle Regelungen zur Ausgestaltung der Rolle des EA in seiner Vermittler- bzw. Koordinierungsfunktion erforderlich sind, kann durch den Landesbeauftragten zum gegenwärtigen Zeitpunkt nicht beurteilt werden.
Das dem Landesbeauftragten zur Stellungnahme im Januar 2009 vorgelegte „Konzept zur Einführung des elektronischen Binnenmarktinformationssystems (Internal Market Information System - IMI) nach der Europäischen Dienstleistungsrichtlinie“ mit der Vorzugsvariante „Kombinationsmodell“ wurde in Version 1.3 (Stand: 9. April 2009) um eine weitere Variante, dem „**Koordinierungsmodell**“ als neue Vorzugsvariante, erweitert. Mit **Kabinettsbeschluss** vom **12. Mai 2009** wurde die Umsetzung dieses Konzepts mit der Vorzugsvariante „**Koordinierungsmodell**“ verbindlich für das IMI-Basismodul EU-DLR festgelegt. Als IMI-Behörden werden nach diesem Modellvariante die Landkreise und kreisfreien Städte registriert, soweit sie fachlich oder fachaufsichtlich zuständig sind. Andere Zuständigkeiten werden ebenfalls berücksichtigt, so dass ergänzend auch Kammern und Gerichte registriert wer-den. Gegenüber dem vorher favorisierten Kombinationsmodell entfällt hier beim Koordinierungsmodell der zentrale Eingang von Anfragen bei einer registrierten zentralen Behörde.

Auch das Ministerium des Innern hat den Landesbeauftragten bei der IT-Umsetzung der EU-DLR rechtzeitig durch die Übergabe eines **Grobkonzepts** (Stand: 27. Oktober 2008) informiert. Am 23./24. Februar 2009 hat hierzu ein Workshop zum Kommunikationskonzept der IT-Umsetzung der EU-DLR unter Beteiligung des Landesbeauftragten stattgefunden. Der **Ständige Staatssekretärsausschuss „Informationstechnologie“** hat dem nunmehr vorgelegten I**T-Umsetzungskonzept zur EU-DLR** des Ministeriums des Innern (Stand: 8. April 2009) zugestimmt.
Für diese Lösung werden sowohl Basiskomponenten gemäß Rahmenvereinbarung zwischen dem Land Sachsen-Anhalt und den Kommunen genutzt, aber auch in anderen Ländern bereits bestehende Lösungen wie z. B. das Elektronische Gerichts- und Verwaltungspostfach (EGVP). Neu beschafft werden müssen für das Service-Portal das Registrierungs- und das Authentifizierungsmodul sowie das Fallmanagement für den EA und die zuständige Stelle (jeweilige entscheidungsbefugte Fachbehörde).
Damit ist die IT-Umsetzung der EU-DLR bis zur Umsetzungsfrist (31. Dezember 2009) möglich.
Der Landesbeauftragte ist gerne bereit, zu gegebener Zeit weiterhin das Ministerium für Wirtschaft und Arbeit und den interministeriellen Arbeitskreis Umsetzung der EU-DLR und dessen UAG EA sowie und das Ministerium des Innern bei der IT-Umsetzung der EU-DLR beratend zu unterstützen, insbesondere im Hinblick auf die technische Umsetzung (Datensicherheitsziele gemäß § 6 Abs. 2 DSG-LSA).

### 4.8. Umsetzung des Binnenmarktinformationssystems IMI

Das Binnenmarktinformationssystem IMI (Internal Market Information System) stellt ein mehrsprachiges System (Datenbank) zum Austausch von Informationen zwischen den EU-Mitgliedsstaaten untereinander sowie mit der Europäischen Kommission dar. Die Europäische Kommission betreibt dieses System und stellt es den EU-Mitgliedsstaaten kostenlos zur Verfügung. Zur Umsetzung der Richtlinie 2005/36/EG des Europäischen Parlaments und des Rates vom 7. September 2005 über die Anerkennung von Berufsqualifikationen (ABl. EU Nr. L 255 S. 22) - Berufsanerkennungsrichtlinie - wurde dieses System auch in Sachsen-Anhalt mit vier Pilotberufen getestet. Im Zeitraum März bis August 2008 wurden insgesamt 150 Anfragen über das IMI-System verschickt. Nach einer erfolgreichen Testphase sollen sämtliche Berufe, die unter die Berufsanerkennungsrichtlinie fallen, in das IMI integriert werden, so das Ministerium für Wirtschaft und Arbeit in seiner Information.
Die Landesregierung traf am 18. September 2007 in einem Kabinettsbeschluss Regelungen zur Einführung des IMI im Rahmen der Umsetzung der Berufsanerkennungsrichtlinie. Dem Landesinformations-Zentrum (LIZ) wurde die Aufgabe des IMI-Koordinators für technische Fragen übertragen. IMI-Koordinatoren für fachliche Fragen sind die Ministerien im Rahmen ihrer Zuständigkeit für die von der Berufsanerkennungsrichtlinie erfassten Berufsgruppen.
Bereits im Februar 2008 informierte das Ministerium für Wirtschaft und Arbeit den Landesbeauftragten über das IMI.
Der Landesbeauftragte seinerseits unterrichtete das Ministerium für Wirtschaft und Arbeit im April 2008 über den Beschluss der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3. und 4. April 2009 in Berlin zur Umsetzung des Binnenmarktinformationssystems IMI **(Anlage 14).** Die Forderung, das IMI-System auf eine tragfähige Rechtsgrundlage zu stellen, besteht auf europäischer Ebene nach wie vor. Der Landesbeauftragte verweist hierzu nochmals auf die Stellungnahme des Europäischen Datenschutzbeauftragten

zur Entscheidung der Kommission vom 12. Dezember 2007 über den Schutz personenbezogener Daten bei der Umsetzung des Binnenmarkinformationssystems (IMI) (2008/49/EG) (ABl. EU Nr. C 270/1 vom 25. Oktober 2008).
Nach der Stellungnahme des Europäischen Datenschutzbeauftragten und Gesprächen mit Datenschutzbeauftragten und der Art. 29 Arbeitsgruppe hat man sich jetzt auf einen Kompromiss geeinigt.
Mit Hilfe des Europäischen Datenschutzbeauftragten hat die Europäische Kommission Datenschutzleitlinien für das Binnenmarktinformationssystem IMI entwickelt. Diese Datenschutzleitlinien sind von der Europäischen Kommission am 26. März 2009 angenommen worden. Spätestens nach neun Monaten (bis zum 26. Dezember 2009) sollen alle EU-Mitgliedsstaaten aufgrund der im Rahmen der Pilotphase gesammelten Erfahrungen Rückmeldungen zu den Datenschutzleitlinien und zu deren praktischer Anwendbarkeit geben. Die Europäische Kommission wird danach in einem zweiten Schritt einen Bericht zu den bisherigen Erfahrungen erstatten, welcher im 1. Quartal 2010 angenommen werden soll. Der Inhalt des Berichts wird eine datenschutzrechtliche Bewertung beinhalten, nach der dann entschieden werden soll, ob noch verbindliche EU-Rechtsvorschriften zum IMI-System erlassen werden müssen.
Der Landesbeauftragte hat daraufhin die Situation mit dem Ministerium für Wirtschaft und Arbeit im April 2009 erörtert und als datenschutzrechtliche Grundlage für die Erhebung und Verarbeitung personenbezogener Daten im IMI-System eine modifizierte informierte Einwilligung gemäß § 4 Abs. 2 DSG-LSA empfohlen. Dieser Empfehlung ist das Ministerium für Wirtschaft und Arbeit gefolgt und hat alle beteiligten IMI-Behörden des Landes entsprechend informiert.

### 4.9. Geodateninfrastrukturgesetzgebung in Sachsen-Anhalt

Bereits Ende April 2003 hatte die Landesregierung das „Grundkonzept E-Government in Sachsen-Anhalt“ beschlossen. Ziel des vorgesehenen 7-Jahre-Aktionplans, der bis zum Jahr 2010 gilt, ist das Bereitstellen verschiedener Basiskomponenten, zu denen auch ein Geo- und Metadatenserver gehört.

Die Basiskomponenten dienen der Umsetzung der 23 E-Government-Leitprojekte. Eines dieser Leitprojekte, das **Leitprojekt Nr. 9**, ist die Bereitstellung von Geoinformationsdiensten, zu denen u. a. die Bereitstellung von Geobasisinformationen zählt (vgl. VII. Tätigkeitsbericht, Ziff. 7.1). Verantwortlich für die Bereitstellung von Geobasisinformationen ist das Landesamt für Vermessung und Geoinformation als Vermessungs- und Geoinformationsbehörde des Landes nach dem Vermessungs- und Geoinformationsgesetz Sachsen-Anhalt.
Mit der Richtlinie 2007/2/EG des Europäischen Parlamentes und des Rates vom 14. März 2007 (ABl. L 108/1 vom 25.4.2007) zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (**INSPIRE** – Infrastructure for Spatial Information in the European Community) war den Mitgliedsstaaten aufgegeben worden, bis zum 14. Mai 2009 Vorschriften in Kraft zu setzen, die die Schaffung und den Betrieb eines Netzes für Geodatensätze und -dienste rechtlich regeln.
Zunächst begann der Bund, dem durch Erarbeitung des Entwurfes eines Geodatenzugangsgesetzes (GeoZG) nachzukommen. Unbeeindruckt von jeglicher Kritik schränkt das im Februar 2009 in Kraft getretene GeoZG zur Umsetzung der INSPIRE-Richtlinie den Schutz personenbezogener Daten stärker ein, als dies durch die INSPIRE-Richtlinie gefordert war.

Während die INSPIRE-Richtlinie die Vertraulichkeit personenbezogener Daten bereits vor jeder **nachteiligen Auswirkung** durch den Zugang der Öffentlichkeit zu Geodatensätzen und -diensten schützt (Art. 13 Abs. 1 INSPIRE-Richtlinie), greift der Schutz des Einzelnen nach § 12 Abs. 2 GeoZG (BGBl. I S. 278) i. V. m. §§ 8, 9 Umweltinformationsgesetz erst bei einer **erheblichen Beeinträchtigung** seiner personenbezogenen Daten. Dies ist vor allem vor folgendem Hintergrund kritisch zu sehen: Geodaten sind Daten mit direktem oder indirektem Bezug zu einem bestimmten Standort oder geografischen Gebiet. Entsprechend georeferenzierte Angaben beliebiger Art können aufgrund der Erschließungsmöglichkeit über Wohnanschriften oder Eigentümer- bzw. Standortdaten schnell zu sensiblen personenbezogenen Daten werden. Dies kann entsprechende Schutz- und Abwehransprüche Betroffener auslösen.

Leider wurde der Aufforderung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in der **Entschließung „Datenschutzgerechter Zugang zu Geoinformationen" vom 6./7. November 2008 (Anlage 19)** im Zuge des Gesetzgebungsverfahrens einen angemessenen Ausgleich zwischen den Informations- und den Schutzinteressen zu schaffen und wenigstens die „mageren" Mindestvorgaben der INSPIRE-Richtlinie zu beachten, nicht Rechnung getragen.

Wesentlich datenschutzfreundlicher war dagegen der dem Landesbeauftragten im Berichtszeitraum vorgelegte **Entwurf eines Geodateninfrastrukturgesetzes für das Land Sachsen-Anhalt** (GDIG LSA). Dieser Gesetzentwurf beruht auf den unter Beteiligung von Sachsen-Anhalt erarbeiteten Musterempfehlungen für die Geodateninfrastrukturgesetzgebungen in den Ländern. Das Gesetz soll den Zugang der Öffentlichkeit zu Geodaten und Geodatendiensten grundsätzlich zwar erlauben. Es beschränkt ihn aber, datenschutzrechtlich viel wirkungsvoller als das GeoZG, u. a. genau dann, wenn durch den Zugang zu Geodaten personenbezogene Daten offenbart und damit schutzwürdige Interessen der Betroffenen beeinträchtigt würden. Der Landesbeauftragte wurde bei der Erarbeitung des Gesetzentwurfs frühzeitig durch das federführende Innenministerium beteiligt und konnte Änderungsempfehlungen abgeben (LT-Drs. 5/1786).

So hatte sich der Landesbeauftragte gegenüber dem Ministerium des Innern beispielsweise dafür eingesetzt, den Geltungsbereich des § 10 GDIG LSA auszudehnen. § 10 GDIG LSA regelt den Schutz öffentlicher und sonstiger Belange, darunter auch die Belange des Datenschutzes. Im ersten Entwurf des GDIG LSA sollten diese Vorschriften zum Schutz öffentlicher und sonstiger Belange in Anlehnung an die INSPIRE-Richtlinie nach § 4 Abs. 2 GDIG LSA ausschließlich auf die sog. Referenzversionen von Geodaten beschränkt werden, also auf die Ursprungsversion eines Datenbestandes. Da aber auch von bei anderen Behörden gespeicherten Kopien dieser Daten Beeinträchtigungen öffentlicher und sonstiger Belange ausgehen könnten, hatte der Landesbeauftragte dringend dazu geraten, den Geltungsbereich des § 10 GDIG LSA auch auf diese Daten auszudehnen.

Leider zunächst nicht durchsetzen konnte er sich in Bezug auf die Ausdehnung des Geltungsbereichs des GDIG LSA auf Geodaten der Kommunen, deren elektronische Erfassung und Bereitstellung gesetzlich nicht explizit vorgeschrieben ist, sondern auf freiwilliger Basis erfolgt. Er teilte dem Innenausschuss des Landtags im Rahmen der Anhörung zum GDIG LSA mit, dass er es begrüßen würde, wenn eine Formulierung des § 4 Abs. 4 GDIG LSA gewählt würde, die einerseits der Intention des Ministeriums des Innern entspräche, eine neue Kostenerstattungspflicht des Landes gegenüber den Kommunen zu verhindern, andererseits aber den Geltungsbereich des GDIG LSA - insbesondere des § 10 GDIG LSA - auch auf die genannten Daten er-streckte. Dadurch wäre der Schutz öffentlicher und sonstiger Belange, für al-le Fälle geregelt in § 10 GDIG LSA, aus einem Guss. Der Datenschutz ist,

darauf wies der Landesbeauftragte das Innenministerium und später den Innenausschuss hin, z. B. neben dem Schutz von Betriebs- und Geschäftsgeheimnissen nur eine der denkbaren Beeinträchtigungen öffentlicher und sonstiger Belange durch den Zugang der Öffentlichkeit zu Geodaten und Geodatendiensten.
Das Ministerium des Innern unterstützt jedoch in diesem Zusammenhang den Vorschlag des Landesbeauftragten, Art und Umfang der von Kommunen außerhalb des Anwendungsbereiches des GDIG LSA gespeicherten Geodaten feststellen zu lassen. So könnte ermittelt werden, wie dringlich eine ei-genständige Regelung für diesen Datenbestand wäre.
Auch im nicht-öffentlichen Bereich entsteht weitergehender Schutzbedarf bei der Veröffentlichung georeferenzierter Dienste im Internet durch digitale Bildaufnahmen von Straßenpanoramen. Zunächst haben hierzu die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich im November 2008 den Beschluss „Datenschutzrechtliche Bewertung von digitalisierten Straßenansichten, insbesondere im Internet“ gefasst **(Anlage 38).** Auch im Rahmen solcher **Street-View-Projekte** ist die Wahrung der Persönlichkeitsrechte der Betroffenen sicherzustellen (Information, Widerspruchs-recht, Datenlöschung auch der Rohdaten). Gegenüber Google wurden durch den zuständigen Hamburgischen Datenschutzbeauftragten entsprechende Maßnahmen erwirkt.

### 4.10. Mehr Befugnisse für das BSI

Durch den am 14. Januar 2009 vom Bundeskabinett beschlossenen Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes (BT-Drs. 16/11967) wird das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** in die Lage versetzt, Angriffe auf Bundesbehörden ab-wehren zu können. Dem BSI wird damit ermöglicht, die Datenströme der Bundesbehörden zu scannen, aufzuzeichnen und gesammelte Daten an Verfassungsschutz sowie die Polizei weiterzureichen. Parallel dazu werden Änderungen des Telemediengesetzes und des Telekommunikationsgesetzes vorgenommen (vgl. Ziff. 24.4).

Der Entwurf des BSI-Gesetzes enthielt keine datenschutzgerechten Regelungen. Wenn es z. B. erlaubt werden soll, ein- und ausgehende Daten des Bundes auf Viren zu untersuchen, dann hätte dies auch im Gesetz formuliert werden müssen. Die Regelung, dass das BSI im Rahmen der Schadsoftwarebekämpfung *„die an den Schnittstellen der Kommunikationstechnik des Bundes anfallenden Daten automatisiert auswerten“ darf,* ist zu allgemein formuliert, und so ist es nicht verwunderlich, dass dieses Gesetz weiterhin aus den Reihen der Internetgemeinschaft, von Datenschutzbeauftragten und auch Berufsverbänden kritisiert wird.
Auch die im Gesetzgebungsverfahren durch Berücksichtigung der Empfehlungen des Innenausschusses des Bundestages (BT-Drs. 16/13259 vom 29. Mai 2009) eingeflossenen leichten Verbesserungen u. a. wie:

- Möglichkeit der Pseudonymisierung erfasster Daten (§ 5 Abs. 2),
- Regelungen zur Benachrichtigung der von einer Datenübermittlung Betroffenen sowie Dokumentation bei Nichtbenachrichtigung (§ 5 Abs. 4),
- Einschränkung der Übermittlungsbefugnisse des BSI auf die Katalogstraftaten (§§ 202a, 202b, 303a, 303b StGB),

- Richtervorbehalt bei der Übermittlung von Daten zu sonstigen Zwecken (§ 5 Abs. 6) bei der Strafverfolgung und der Gefahrenabwehr,
- Beweisverwertungsverbot für zeugnisverweigerungsberechtigte Berufsgruppen sowie verbesserter Schutz des Kernbereichs privater Lebensgestaltung (§ 5 Abs. 7),
- Kalenderjährliche Benachrichtigungspflichten des BSI an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und den Innenausschuss des Bundestages (§ 5 Abs. 9) und
- Rechtzeitige Information zu Sicherheitslücken an Hersteller (§ 7 Abs. 1)

ändern nichts an der grundsätzlichen Kritik an diesem Gesetz.

Mögliche Eingriffe in die Grundrechte von Bürgerinnen und Bürgern durch zu umfangreiche Befugnisse für eine Behörde stellen eine Gefahr für Demokratie und Rechtsstaat dar. Die Datenschutzbeauftragten des Bundes und der Länder forderten deshalb in der **Entschließung** vom **18. Februar 2009 „Stärkung der IT-Sicherheit - Aber nicht zu Lasten des Datenschutzes!“ (Anlage 26)** konkrete Nachbesserungen für den damaligen Entwurf des BSI-Gesetzes.

Im Gesetz wurden leider nicht alle Forderungen dieser Entschließung umgesetzt, um bei Maßnahmen zur Stärkung der IT-Sicherheit auch die Privatsphäre und den Datenschutz der Nutzerinnen und Nutzer umfassend zu gewährleisten.
Der Bundesrat hat mit seinem Beschluss vom 10. Juli 2009 (BR-Drs. 578/09) den Gesetzentwurf gebilligt. Er will das Gesetzgebungsvorhaben nicht verzögern, gleichzeitig die Interessen der Länder wahren und erwartet eine Beteiligung in wichtigen Bereichen.

### 4.11. Bürgerportale und De-Mail

Die Bundesregierung plant, durch die Errichtung von Bürgerportalen eine zur herkömmlichen E-Mail-Kommunikation alternative Methode der Kommunikation zu schaffen. Vorteil soll die sichere Zustellung nach dem Vorbild der herkömmlichen Papierpost sein. Es sollen also bspw. Einschreiben und Ein-schreiben mit Rückschein auf elektronischem Wege möglich werden. Nutzer eines Bürgerportals sollen eine De-Mail-Adresse erhalten, über welche mit anderen De-Mail-Nutzern kommuniziert werden kann. Übertragungen sollen verschlüsselt erfolgen, so dass das Manko der normalen E-Mail-Übertragungen - die grundsätzliche Unsicherheit, sofern alle beteiligten Nutzer nicht durch Verschlüsselungsmaßnahmen gemeinsam Vorkehrung treffen - behoben wird. Schnittstellen zum Internet, sogenannte Gateways, soll es nach aktueller Planung nicht geben, so dass auch kein SPAM von außen ins De-Mail-Netz gelangen können soll. Sinn der De-Mails ist die Schaffung eines medienbruchfreien und kostengünstigen Kommunikationsweges zwischen Verwaltung und Bürger (BT-Drs. 16/12598).

Die Intention, die Schaffung einer sicheren Kommunikationsmöglichkeit per E-Mail, ist sinnvoll und wird begrüßt. Über Stellungnahmen zu Gesetzentwürfen, z. B. dem des Bundesmeldegesetzes, wurde versucht, an Verbesserun-gen mitzuarbeiten. Dabei traten immer mehr Kritikpunkte zu Tage. Die Realisierung als Webportal ist zwar einfach möglich, erlaubt jedoch nur mit unverhältnismäßig hohem Aufwand oder unter Komforteinbußen eine Ende-zu-Ende-

Verschlüsselung. Es ist unverständlich, warum nicht herkömmliche Standards weiterentwickelt werden. Solche existieren bereits und deren Nutzung würde sogar eine Ende-zu-Ende-Verschlüsselung erlauben. Stattdessen soll eine neue E-Mail-Form geschaffen werden. Eine De-Mail-Adresse muss genauso wie normale E-Mails mit einem E-Mail-Client abrufbar sein. Dies ist derzeit nicht vorgesehen. Der Zwang, sich täglich in Erwartung neuer Post zusätzlich an einem Web-Mail-Portal anzumelden, könnte dafür sorgen, dass De-Mails nicht akzeptiert werden.

Für die sichere und authentische elektronische Kommunikation mit Einwilligung des Betroffenen wird die elektronische Bürgeradresse, die De-Mail, er-fasst. Mit Hilfe des elektronischen Personalausweises soll eine sichere Kommunikation in Bürgerportalen ermöglichen werden. Das bedeutet jedoch nicht, dass der Bürger dadurch erreichbar ist und die De-Mails auch aktiv liest. Viele Nutzer werden De-Mails nur für gelegentliche Behördenkommunikation verwenden, jedoch nicht regelmäßig die Nachrichten abfragen, da da-zu keine automatisierbaren Abfrageprotokolle geplant sind und nur Bürgerportale den Zugang gewähren werden.
Die Konferenz der Datenschutzschutzbeauftragten des Bundes und der Länder wies in einer **Entschließung** vom **16. April 2009 „Datenschutz beim vor- gesehenen Bürgerportal unzureichend“ (Anlage 31)** darauf hin, dass der Gesetzentwurf noch Mängel aufwies, welche zu korrigieren sind. **Forderungen** wie eine **verschlüsselte Ende-zu-Ende-Kommunikation** nach dem Stand der Technik sind darin ebenso enthalten wie die nach optionaler Pseudonymnutzung oder grundsätzlich sicherer Anmeldung am Portal, ohne ausschließlich auf Passwörter zu setzen. Die Umsetzung dieser Forderungen hat direkte Auswirkungen auf die Sicherheit und Akzeptanz von Bürgerportalen und darf deshalb nicht ignoriert werden.

Der Bundestag vertagte die Initiative; im Rahmen einer Gesamtstrategie zu Datenschutz und Sicherheit in E-Government und eBusiness soll auch das Projekt De-Mail fortgesetzt werden.

Ob Web-Portale wirklich eine Alternative zu normalen E-Mails werden können, ist noch völlig offen, da hier eine Technologie genutzt wird, welche nicht nur Vor-, sondern auch Nachteile bei der Nutzung bietet. Nutzer müssen ein Web-Portal nutzen, um auf De-Mails zugreifen zu können. Ein Nutzen des Zugangs mit einem E-Mail-Programm unter Verwendung von Standard-Protokollen ist somit nicht möglich. Warum werden nicht herkömmliche Methoden für sichere Mail-Kommunikation wie PKI-basierte Zertifikate in Verbindung mit standardisierten E-Mail-Übertragungsprotokollen eingesetzt? Das würde die Akzeptanz deutlich verbessern und die Verbreitung von Zertifikat-basierten Sicherheitsfunktionen erhöhen.

## X. Tätigkeitsbericht – 2011 (01.04.2009 - 31.03.2011)

### 1 Entwicklung und Situation des Datenschutzes

*„Die anlasslose Speicherung von Telekommunikationsverkehrsdaten ist geeignet, ein diffus bedrohliches Gefühl des Beobachtetseins und des ständigen Überwachtwerdens hervorzurufen, das eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen kann. Die verfassungs-rechtliche Unbedenklichkeit einer vorsorglich anlasslosen Speicherung der Telekommunikationsverkehrsdaten setzt voraus, dass diese eine Ausnahme bleibt. Sie darf auch nicht im Zusammenhang mit anderen vorhandenen Dateien zur Rekonstruierbarkeit praktisch aller Aktivitäten der Bürger führen. Die Einführung einer Telekommunikationsverkehrsdatenspeicherung kann nicht als Vorbild für die Schaffung weiterer vorsorglich anlassloser Datensammlungen dienen, sondern zwingt den Gesetzgeber bei der Erwägung neuer Speicherungspflichten oder -berechtigungen in Blick auf die Gesamtheit der schon vorhandenen Datensammlungen zu größerer Zurückhaltung.* ***Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss.*** *Durch eine vorsorgliche Speicherung der Telekommunikationsverkehrsdaten wird der Spielraum für weitere anlasslose Datensammlungen auch über den Weg der Europäischen Union erheblich geringer.“* (**aus dem Urteil des Bundesverfassungsgerichts vom 2. März 2010, 1 BvR 256/08 u. a.)**.

Die **Freiheitsmaßstäbe** des Bundesverfassungsgerichts, abgeleitet aus den Grundrechten des Grundgesetzes, bleiben Richtschnur für den Datenschutz, die datenschutzrechtlich verantwortlichen Stellen und die Datenschützer. Der Europäische Gerichtshof hat die unabhängigen Datenschutzbeauftragten als „Hüter von Grundrechten und Grundfreiheiten“ bezeichnet (Urteil vom 9. März 2010, C-518/07, NJW 2010, 1265). Die Aufgabe ist unverändert anspruchsvoll und erfordert ein entsprechendes Verantwortungsbewusstsein. Der Landesbeauftragte bezieht in sein Verständnis der Aufgabenwahrnehmung auch die Leitaussage des Bundesverfassungsgerichts seit dem **Volkszählungsurteil von 1983** ein, wonach Datenschutz bzw. informationelle Selbstbestimmung nicht nur subjektives Recht ist, sondern dass sich im objektiven Wertgehalt des Grundrechts auch eine Funktionsbedingung des demokratischen Gemeinwesens widerspiegelt (s. IX. Tätigkeitsbericht, Nr. 1).

**Datenschutz ist Freiheitsmaßstab und Vertrauensfaktor**. Das Vertrauen der Dateninhaber kann leiden, wenn der Staat beim Kampf gegen Kriminalität übermäßige Eingriffe in Persönlichkeitsrechte vornimmt und Betroffene sich infolgedessen in ihrer Verhaltensfreiheit auch bei anderen Grundrechtswahrnehmungen eingeschüchtert fühlen oder wenn der Staat der übermäßigen Datenverarbeitungspraxis der Wirtschaft nicht Einhalt gebietet und somit sei-ne grundrechtliche Schutzaufgabe vernachlässigt. Nur wenn der Bürger und Konsument Vertrauen in das Datenschutzgebaren von Staat und Wirtschaft hat, wird er Angebote des E-Government oder E-Commerce in Anspruch nehmen.

Die eingangs zitierten Passagen aus dem Urteil des Bundesverfassungsgerichts zur Nichtigkeit der Vorratsspeicherung von Telekommunikationsverkehrsdaten beschreiben einen Kern der Freiheitsgrundrechte und zugleich den Nerv einer aktuellen Debatte, bei der es auch um das Verhältnis von europäischem und nationalem Recht geht (ausführlicher Nr. 25.1). Ohne-

hin wird der Datenschutz in Deutschland zunehmend durch europäische Entwicklungen geprägt werden; dabei handelt es sich nicht nur um die Ausweitung von Datensammlungen, sondern auch um ein der Grundrechtecharta der Europäischen Union entsprechendes Regelungswerk für den Datenschutz (vgl. Nr. 3.1).
Konzeptionen und Maßnahmen des Datenschutzes betreffen im Wesentlichen **vier Bereiche**: **1. Recht, 2. Technik, 3. Kontrolle und 4. Bildung oder Medienkompetenz** (vgl. auch **Grundsatzentschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. Oktober 2009**, **Anlage 1**; s. Nr. 1.4). In diesem Tätigkeitsbericht werden diese Bereiche übergreifend und anhand von Einzelvorhaben und Aktivitäten näher beschrieben.

Im Hintergrund steht dabei auch das merkwürdige Phänomen, dass private Daten einerseits für den Menschen, ob als Bürger oder als Verbraucher oder Internetnutzer, trotz eines insgesamt veränderten Verständnisses von Privatsphäre durchaus einen Wert haben im Sinne einer persönlichkeitsbezogenen Wertschätzung, ausgeprägt besonders etwa bei Konto- oder Gesundheitsdaten, und dass der Datenschutz im Verhältnis Bürger – Staat rechtspolitische Akzeptanz erfahren hat und weiter erfährt, andererseits aber Empfehlungen zu mehr Datensparsamkeit und Selbstdatenschutz insbesondere bei der Internetnutzung auf weniger Widerhall stoßen. Dies ist auch eine Anfrage an Konzepte und Methoden der Medienbildung (vgl. Nr. 21.2). Das Internet wird jedenfalls weit verbreitet als Privatsache empfunden, vermeintlich unbeobachtet und anonym wird die Technik, an die ohnehin eine Gewöhnung stattgefunden hat, gern genutzt. Doch das Internet vergisst nichts. Deshalb ist der Ansatz eines „Vergessens im Internet“ so wichtig, doch zugleich so schwierig (vgl. Nr. 1.3).

Der X. Tätigkeitsbericht des Landesbeauftragten umfasst den Zeitraum vom 1. April 2009 bis zum 31. März 2011. Darüber hinaus reichende Entwicklungen wurden soweit möglich mitberücksichtigt.

Der Datenschutzbericht dient der

- **Unterrichtung des Landtages**, zusammen mit der zum Bericht ab-zugebenden Stellungnahme der Landesregierung (§ 22 Abs. 4a Satz 1 und 2 DSG-LSA),

- der **Öffentlichkeitsarbeit** (§ 22 Abs. 4a Satz 3 DSG-LSA),

- der **Information der Behörden** und behördlichen Datenschutzbeauftragten und interessierter **Bürgerinnen** und **Bürger**.

Der X. Bericht beinhaltet wiederum datenschutzpolitische Feststellungen und greift Grundsatzthemen auf. Er enthält Informationen, Kritik und Lob zu rechtlichen und technischen Entwicklungen. Dabei werden auch Kommentare der Landesregierung aus ihrer Stellungnahme zum IX. Tätigkeitsbericht (**LT-Drs. 5/2385**) einbezogen. Der aktuelle Bericht stellt Materialien und praxisbezogene Hinweise aus anschaulichen Einzelfällen, Beratungen und Kontrollen zur Verfügung.

Seit dem VII. Tätigkeitsbericht werden die Berichte nicht nur in den Ausschüssen des Landtages für Inneres und Recht und Verfassung, sondern auch im Plenum im Rahmen einer Debatte beraten und zur Kenntnis genommen. Diese gegenüber Vorgängerberichten abwei-

chende Verfahrens-weise geht auf einen Vorschlag des Landesbeauftragten zurück. Sie entspricht Wortlaut und Sinn der o. a. Gesetzesregelung und dem Gegenstand. Eine öffentliche Debatte zum Datenschutzbericht empfiehlt sich auf Dauer (vgl. auch Nr. 2.3).

### 1.3 IuK-Technik und Organisation – Grundsatzthemen

Zu einer der ständigen Aufgaben des Landesbeauftragten zählt die Beobachtung der Entwicklung der **Informations- und Kommunikationstechnologien (IuK, synonym auch IKT)** und deren Bewertung aus der Sicht des Datenschutzes und der Datensicherheit. Dabei sind die rasant steigenden Teil-nehmerzahlen im Internet und eine starkes Anwachsen internetbasierter Angebote und Services für Bürgerinnen und Bürger auffällig. Gefördert wird die-se Entwicklung durch die erhöhte Verfügbarkeit von Breitbandanschlüssen für den Zugang zum Internet. Das Internet selbst durchdringt immer mehr Lebensbereiche der Bürgerinnen und Bürger und ist mittlerweile als fester Bestandteil von Geschäftsprozessen der Wirtschaft, aber auch von
E-Government-Angeboten der öffentlichen Verwaltung, aus dem Alltag nicht mehr wegzudenken.

Für die Informationsgesellschaft selbst sind damit die sichere und verlässliche Funktion von IuK, die Informationssicherheit sowie die generelle Verfügbarkeit des Internets zu existenziellen Faktoren geworden. Das betrifft insbesondere die „Kritischen Infrastrukturen“ (KRITIS, s. IX. Tätigkeitsbericht, Nr. 1.3) von Wirtschaft und Verwaltung, aber auch Fragen der informationellen Selbstbestimmung bei der Nutzung des Internets selbst. Das Thema „Cybersicherheit“ hat damit für die Informationsgesellschaft des 21. Jahrhunderts neben „Cloud Computing“ eine herausragende Bedeutung erlangt.

Der Datenschutz und die Datensicherheit waren im zurückliegenden Berichtszeitraum so häufig Gegenstand öffentlicher Diskussionen und Debatten, besonders in den Medien. Als Stichworte seien hier beispielhaft Google Street View (s. Nr. 3.1.3), die Vorratsdatenspeicherung (s. Nr. 25.1), Cloud Computing (s. Nr. 1.3.2), Mobile Computing (s. Nr. 1.3.3) und Open Government (s. Nr. 1.3.4) genannt.

Exemplarisch für neue Bedrohungsszenarien bei kritischen Infrastrukturen ist hier an den im Juli 2010 bekanntgewordenen Angriff einer Schadsoftware namens „**Stuxnet**“, die für Störungen in Anlagen des iranischen Atomprogramms entwickelt wurde, zu erinnern. Dabei handelte es sich beim sogenannten „Stuxnet-Wurm“ nach Ansicht der Fachwelt um das bis dato komplexeste Schadprogramm, das nahezu alle bisher bekannten Angriffsformen vereint.

In Fortsetzung ihrer Strategie zum Schutz kritischer Infrastrukturen in Wirtschaft und Verwaltung hat die Bundesregierung im Februar 2011 eine Cyber-Sicherheitsstrategie beschlossen. Kern dieser Strategie ist das neue „Nationale Cyber-Abwehrzentrum“, welches beim Bundesamt für die Sicherheit in der Informationstechnik (BSI) eingerichtet wurde. Damit soll die Information und operative Zusammenarbeit aller staatlichen Stellen optimiert und die Koordinierung von Schutz- und Abwehrmaßnahmen bei entsprechenden Vor-fällen verbessert werden.

**Das Internet vergisst nichts**. Diese Erfahrung müssen immer mehr Internetnutzer machen, die Suchmaschinen wie „Google“, soziale Netzwerke wie „**Facebook**“, **Webforen** und **Blogs** oder auch Mikroblogging wie „**Twitter**“ nutzen. In der öffentlichen Debatte zur Möglichkeit der Löschung von Daten im Internet bzw. zur Sicherstellung der Herrschaft über die eigenen Daten im Internet wurde der Ruf nach einem „Digitalen Radiergummi“ laut, der in Anlehnung an den guten alten Radiergummi der „offline-Welt“ solche Probleme lösen sollte. Der unter dem Slogan „Digitaler Radiergummi“ mit Unterstützung der Politik vorgestellte durchaus lobenswerte Ansatz, bekannt geworden als Browser-Plugin „X-pire!“, hielt aber einer kritischen Auseinandersetzung mit seiner Wirksamkeit nicht stand. Mittels X-pire! sollen Bilder vor dem Hochladen ins Internet mit einem Verfallsdatum versehen und damit zeitlich begrenzt zugänglich gemacht werden. Allerdings ist dies allein nur mit einer Softwarelösung nicht möglich. Diese Meinung wird auch vom Landesbeauftragten geteilt. Der gewissenhafte und sparsame Umgang mit den eigenen Daten im Internet ist gegenwärtig immer noch die wichtigste Voraussetzung für den Schutz der eigenen Privatsphäre.

Mit dem neuen Artikel **91c Grundgesetz (GG)** hat der Gesetzgeber eine verfassungsrechtliche Grundlage für die **Zusammenarbeit von Bund und Ländern bei Planung, Errichtung und Betrieb ihrer informationstechnischen Systeme geschaffen** sowie dem **Bund** die Zuständigkeit für ein **Verbindungsnetz** übertragen. Mit der Bildung des IT-Planungsrats wurde auf organisatorischer Ebene in Zusammenarbeit zwischen Bund, Ländern und Kommunen ein völlig neuer Weg beschritten. Inwieweit dieses Gremium auch die Belange des Datenschutzes und der Datensicherheit, insbesondere die Belange der Länder, ausreichend berücksichtigt, muss nach der bisherigen Erfahrung des Landesbeauftragten mit einer gewissen Skepsis betrachtet werden (s. Nr. 1.3.1). 9 X. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Sachsen-Anhalt (04/2009 bis 03/2011)

### 1.3.1 IT-Planungsrat – eine Zwischenbilanz

Der Landesbeauftragte hat in seinem IX. Tätigkeitsbericht (Nr. 1.3) über die Beschlüsse der Föderalismuskommission II (5. März 2009) und die damit verbundene Einführung des neuen **Artikel 91c GG** berichtet, der am **1. August 2009** in Kraft trat. Unter dem bekannten Begriff „IT ins Grundgesetz“ wurde damit erstmals ein verfassungsrechtlicher Rahmen für diese Kooperation von Bund und Ländern geschaffen. Er ermöglicht Bund und Ländern, bei der Planung, der Errichtung und dem Betrieb der für ihre Aufgaben notwendigen informationstechnischen Systeme zusammenzuarbeiten. Hierzu können Bund und Länder die dafür notwendigen Standards und Sicherheitsanforderungen festlegen. Darüber hinaus können die Länder den gemeinschaftlichen Betrieb informationstechnischer Systeme sowie die Errichtung von da-zu bestimmten Einrichtungen vereinbaren. Abschließend erhält der Bund die ausschließliche Kompetenz zur Errichtung und zum Betrieb eines **Verbindungsnetzes** zwischen den informationstechnischen Netzen des Bundes und der Länder auf der Grundlage eines Bundesgesetzes mit Zustimmung des Bundesrates.

Mit dem am **18. August 2009** in Kraft getretenen Gesetz über die Verbindung der informationstechnischen Netze des Bundes und der Länder – Gesetz zur Ausführung von Artikel 91c Absatz 4 des GG – **IT-NetzG** (Artikel 4 des Begleitgesetzes zur zweiten Föderalismusreform vom 10. August 2009, BGBl. I S. 2072) wurde diese Zuständigkeit des Bundes gesetzlich

verankert. Allerdings tritt **§ 3 des IT-NetzG**, der den Datenaustausch zwischen Bund und den Ländern über das **Verbindungsnetz** regelt, erst mit dem **1. Januar 2015 in Kraft**.

Die bisher vom Deutschland-Online Infrastruktur e.V. (DOI-Netz e.V.) wahrgenommenen Aufgaben wurden zum 31. Dezember 2010 dem Bund über-tragen. Die Verantwortung für den operativen Betrieb des Verbindungsnetzes trägt seit dem 1. Januar 2011 die Bundesstelle für Informationstechnologien im Bundesverwaltungsamt. Die strategischen Aufgaben werden durch das Bundesministerium des Innern wahrgenommen.

Am **1. April 2010** trat der sogenannte **IT-Staatsvertrag** (Gesetz zum Vertrag über die Errichtung des IT-Planungsrates und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in der Verwaltung von Bund und Ländern vom 27. Mai 2010) nach vorausgegangener Ratifizierung durch alle Bundesländer in Kraft (BGBl. I S. 662). Sachsen-Anhalt stimmte diesem Staatsvertrag mit Gesetz vom 23. März 2010 (GVBl. LSA S. 142) zu. **Der IT-Staatsvertrag bildet die Grundlage für die Arbeitsweise des IT-Planungsrates (IT-PLR)**.

Demnach hat der IT-PLR folgende wesentliche Aufgaben:

- Koordination der Zusammenarbeit von Bund und Ländern in Fragen der Informationstechnik,
- Beschlussfassung über fachunabhängige und fachübergreifende IT-Interoperabilitäts- und IT-Sicherheitsstandards,
- Projektsteuerung zu Fragen des informations- und kommunikations-technisch unterstützten Regierens und Verwaltens (E-Government-Projekte), die dem IT-PLR zugewiesen werden,
- Koordinationsgremium nach Maßgabe des Gesetzes zur Ausführung von Artikel 91c Abs. 4 GG – (IT-NetzG).

Die konstituierende Sitzung des IT-PLR erfolgte am 22. April 2010 in Berlin. Die 4. Sitzung des IT-PLR fand am 3. März 2011 anlässlich der CeBIT in Hannover erstmals unter Ländervorsitz (Baden-Württemberg) statt. Dem IT-PLR gehören als Mitglieder die Beauftragte der Bundesregierung für Informationstechnik sowie je ein für Informationstechnik zuständiger Vertreter jedes Landes an. Beratende Teilnehmer an den Sitzungen sind drei Vertreter der Kommunalen Spitzenverbände auf Bundesebene sowie der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit.

Die Nichtberücksichtigung eines Vertreters der Datenschutzbeauftragten der Länder zur beratenden Teilnahme war angesichts der Themen des IT-PLR (Sicherheitsstandards, Verbindungsnetz, E-Government-Projekte), welche auch gerade Datenschutzfragen der Länder unmittelbar berühren, unverständlich.

Gerade diese ständige Einbeziehung in die Sitzungen des IT-PLR war u. a. eine der Forderungen einer **Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. Oktober 2009 zu diesem IT-Staatsvertrag** (**Anlage 2**).

Mit Unterstützung verschiedener Landesparlamente, in Sachsen-Anhalt durch einen Beschluss des Landtages vom 18. März 2010 (LT-Drs. 5/73/2508 B), wurden die Landesregie-

rungen aufgefordert, für eine entsprechende Änderung der Geschäftsordnung des IT-PLR einzutreten und damit die ständige beratende Teilnahme eines Vertreters der Datenschutzbeauftragten der Länder zu ermöglichen.

Nach diesen Interventionen wurde die vom IT-PLR verabschiedete **Geschäftsordnung** in § 6 Abs. 3 dahingehend ergänzt, dass zusätzlich ein Vertreter der Datenschutzbeauftragten der Länder an den Sitzungen teilnehmen darf, sofern die Länder betreffende datenschutzrelevante Belange erörtert werden. Diese Regelung entspricht nicht ganz der Forderung nach einer regelmäßigen Einbindung der Datenschutzbeauftragten der Länder, sollte aber, da die Mehrzahl der zu beratenden Themen einen Datenschutzbezug für die Länder besitzt, in der Praxis nicht weiter hinderlich sein.

Die Aufgabe des **Länder-Vertreters** nimmt der **Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern** wahr, der gleich-zeitig auch Vorsitzender des Arbeitskreises technische und organisatorische Datenschutzfragen ist.

In **Sachsen-Anhalt** hat die Staatskanzlei allerdings für eine regelmäßige Beteiligung des Landesbeauftragten Sorge getragen. Dazu wurde die **Geschäftsordnung** des Ständigen Staatssekretärsausschusses „Informationstechnologie“ entsprechend ergänzt. Der Landesbeauftragte sowie auch die Vertreter der Kommunalen Spitzenverbände nahmen danach an den vorbereitenden Sitzungen des Staatssekretärsausschusses für den IT-PLR beratend teil. Zukünftig ist der IT-Beauftragte der Landesregierung im Finanzministerium der zuständige Ansprechpartner (vgl. Nr. 4.3).

So weit, so gut könnte man nun denken, kritisch angemerkt an dieser Stelle seien aber die bis zur 4. Sitzung sehr formalistische Vorbereitung der Tagesordnungspunkte durch die Geschäftsstelle des IT-PLR in sogenannten „Steckbriefen zur Themenanmeldung“ sowie der sehr enge Zeitrahmen für die Vorbereitung der bisherigen Sitzungen des IT-PLR. Nicht selten wurde die datenschutzrechtliche Relevanz von Tagesordnungspunkten nicht erkannt.

Aus diesem Grund erscheint es dem Landesbeauftragten notwendig, in einem weiteren Beitrag (Nr. 4.2) auf einige datenschutzrelevante Vorhaben des IT-PLR hinzuweisen, welche auch eine Bedeutung für Sachsen-Anhalt haben. In den vorbereitenden Sitzungen des Staatssekretärsausschusses bestand zudem für den Landesbeauftragten, natürlich auch aus praktischen und zeitlichen Gründen, kaum die Möglichkeit einer vertieften Diskussion bzw. Erörterung von datenschutzrelevanten Einzelthemen der Tagesordnung.

Gleichzeitig ist damit die Aufforderung an die betroffenen Ressorts verbunden, unabhängig von der Geschäftsordnung der Landesregierung, ihrer rechtzeitigen Unterrichtungspflicht gem. § 14 Abs. 1 Satz 2 DSG-LSA nach-zukommen. Diese verpflichtet bei grundlegenden Planungen des Landes zum Aufbau bzw. zur Änderung von Vorhaben zur automatisierten Verarbeitung personenbezogener Daten zur rechtzeitigen Unterrichtung des Landesbeauftragten bereits im **Planungsstadium**. Dieser Umstand trifft sicherlich für den überwiegenden Teil der Vorhaben, insbesondere die zukünftige E-Government-Strategie des Landes Sachsen-Anhalt zu, die sich an der **Nationalen E-Government-Strategie** (**NEGS**) ausrichten und wie diese einen Zeithorizont bis zum Jahr 2015 umfassen soll.

### 1.3.2 Cloud Computing – virtuelle „Rechnerwolke“

Der Landesbeauftragte hatte in seinem IX. Tätigkeitsbericht (Nr. 1.3) auf den sich abzeichnenden Paradigmenwechsel beim Einsatz der Informations- und Kommunikationstechnologie(IKT) bzw. der Informationsverarbeitung durch Nutzung internetbasierter Dienste unter dem damals neuen Schlagwort „Cloud Computing“ hingewiesen. Große Internet-Unternehmen wie Amazon, Google oder Microsoft stellen mittlerweile potentiellen Nutzern IT-Ressourcen (ganze Entwicklungs-Plattformen, Infrastrukturen und Software) als IT-Dienstleistungen auf Mietbasis über das Internet zur Verfügung. Damit soll den Kunden die Konzentration auf ihr sogenanntes Kerngeschäft erleichtert werden, weil damit ein Großteil der sonst durch sie selbst zu betreibenden und zu unter-haltenden IT-Ressourcen überflüssig werden. Aus wirtschaftlicher Sicht versprechen die Anbieter und Befürworter des Cloud Computing den Nutzern bzw. Kunden neben einem möglichen weltweit verfügbarem Zugriff auf diese IT-Ressourcen insbesondere eine enorme Kosteneinsparung, eine hohe Flexibilität bei der Bereitstellung sowie eine schnelle und dynamische Anpassung der benötigten IT-Ressourcen, ob es nun um Bandbreite, Speicherkapazität (Daten- und Arbeitsspeicher) oder Rechenleistung geht.

So wie heutzutage von jedermann Strom aus der Steckdose bezogen wer-den kann und nur das bezahlt werden muss, was man verbraucht, soll jedermann IT-Dienstleistungen aus der „Rechnerwolke“ über das Internet beziehen können. Datenbanken, Fach-Anwendungen, Server oder Webservices – es gibt gegenwärtig beim Thema Informationsverarbeitung fast nichts, was nicht auch in einer Cloud genutzt werden könnte.

Natürlich ist damit die Anwendung von Cloud Computing auch für die öffentliche Verwaltung gerade unter dem Aspekt der Verwaltungsmodernisierung (Kosteneinsparung und Effizienzsteigerung beim Einsatz von IuK) ein aktuelles Thema geworden, ob nun als öffentliche Stelle in der Rolle des Nutzers von Cloud-Diensten oder der eines zentralen IT-Dienstleisters in einem Land als Anbieter von Cloud-Diensten. Aus datenschutzrechtlicher Sicht bleibt aber ein zentrales Problem des Cloud Computing das Thema der Datensicherheit und hier insbesondere die Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit sowie die Revisionssicherheit bei der Verarbeitung personenbezogener Daten. Weitere Erläuterungen zum Thema Cloud Computing und Datenschutz werden in Nr. 14.1 dieses Tätigkeitsberichts gegeben.

### 1.3.3 Mobile Computing

Seit einigen Jahren bereits entwickeln sich Mobiltelefone immer mehr zu Mini-PCs, sogenannten „**Smartphones**“, welche eine allumfassende Vernetzung mit dem Internet aufweisen und so ein wesentliches Werkzeug zur Nutzung von Netzdiensten und Angeboten sowohl der Privatwirtschaft als auch des E-Government und Angeboten öffentlicher Stellen darstellen. Erkennbar sind hierbei eine rasante Steigerung der Verbreitung solcher Geräte, aber auch der Datenvolumina, und eine stetige Vernetzung von öffentlichen und nicht-öffentlichen Diensten.

Zuletzt durch die Aufdeckung und das Bekanntwerden der heimlichen Aufzeichnung geografischer Ortungsdaten von WLAN- und Mobilfunkzellen in Verbindung mit Zeitstempeln in ei-

ner entsprechenden Datenbank beim beliebten „iPhone“ und dem „iPad“ der Firma Apple im April 2011 wurde die Öffentlichkeit wieder einmal mit Defiziten beim Datenschutz konfrontiert, die den privaten Nutzern nicht bekannt bzw. bewusst waren. Diese sogenannte Ortungsfunktion dient Apple bei seinem Betriebssystem „iOS“ eventuell schon länger zur unverschlüsselten Aufzeichnung von Ortungsdaten und damit der Pflege dieser bisher scheinbar unbekannten Datenbank in den Smartphones selbst. Ähnliche Anwendungsszenarien sind auch bei den Mitbewerbern wie Google mit dem Betriebssystem „Android“ und Microsoft mit dem Betriebssystem „Windows Phone 7“ im heiß umkämpften Markt dieser mobilen „Alleskönner“ zu vermuten.

Ob es sich hier bei Apple um einen schlichten Programmierfehler handelte oder die Speicherung in der Datenbank u. a. zur Vorbereitung der Nutzung zukünftiger Dienste dienen könnte (z. B. Aufbau einer Verkehrsdatenbank für Staumeldungen), wurde in Fachkreisen kontrovers diskutiert. Auf ihrer Internetseite nahm die Firma Apple zu den Vorwürfen, dass das iPhone und das iPad vermeintlich Bewegungsprofile von Nutzern aufzeichnen würde, Stellung. Defizite bei Datenschutz und Transparenz für den Nutzer wurden dabei eingeräumt. Apple sprach bezüglich der Fortschreibung dieser Datenbank – fast wie immer in solchen Fällen üblich – von einem Softwarefehler. Auch wenn sich mittels dieser Datenbank kein komplettes Bewegungsprofil eines Nutzers erstellen lässt, beabsichtigt die Firma Apple mit einem Update des Betriebssystems diesen Softwarefehler zu beheben und das Backup dieser Ortungsdatenbank auf dem PC des Nutzers nicht mehr zu ermöglichen. Zu-künftig soll die Datenbank auf die Ortungseinträge der letzten sieben Tage beschränkt und beim Ausschalten des Ortungsdienstes komplett gelöscht werden. Zudem soll mit einem nachfolgenden größeren Update des Betriebssystems „iOS“ diese Datenbank auf dem iPhone zusätzlich verschlüsselt werden.

Eventuell geplanten Einsatzszenarien für Smartphones durch öffentliche Stellen sollte deshalb auch eine Gefährdungs- und Risikoanalyse vorausgehen, um eine datenschutzgerechte Nutzung zu gewährleisten.
Mobile Geräte werden zusätzlich zu den beschriebenen auch von weiteren Risiken und Angriffsszenarien bedroht, sodass in diesem Tätigkeitsbericht das Thema aufgegriffen wird (s. Nr. 14.3).

### 1.3.4 Open Government / Open Data

Der Begriff „**Open Government**“ umschreibt allgemein Initiativen und Maßnahmen mit dem Ziel der Öffnung von Staat und Verwaltung gegenüber allen gesellschaftlichen Gruppen (Wirtschaft, Bürgerinnen und Bürgern). **Open Government** gliedert sich dabei in **drei wesentliche Themenbereiche**:

- **Transparenz** (Offenlegung der Entscheidungen und Prozesse von Staat und Verwaltung sowie öffentliche Verfügbarkeit dieser Daten),
- **Partizipation** (Mitwirkungsmöglichkeiten der Allgemeinheit an staatlichen Entscheidungsprozessen),
- **Kooperation** bzw**.** Kollaboration (Zusammenarbeit zwischen staatlichen und gesellschaftlichen Gruppen).

Der Begriff „**Open Data**“ umfasst allgemein die vorhandenen Datenbestände des öffentlichen Sektors (insbesondere der öffentlichen Verwaltung), die durch ihre elektronische Bereitstellung der Allgemeinheit mit gewissen Einschränkungen (insbesondere unter Beachtung des Datenschutzes sowie von Betriebs- und Geschäftsgeheimnissen) zur Nutzung und Weiterverwendung zur Verfügung gestellt werden.

Die Umsetzung der Open Government-Strategie soll dabei den gesellschaftlichen Zusammenhalt fördern, die Glaubwürdigkeit des poltischen Handelns stärken, neue Geschäftsmodelle für die Wirtschaft erschließen und nicht zuletzt auch die Qualität und die Effizienz der öffentlichen Verwaltung erhöhen.

Nach den Zielvorstellungen im Regierungsprogramm „Vernetzte und transparente Verwaltung“, beschlossen vom Bundeskabinett am 18. August 2010, ist für das Projekt Open Government die Abstimmung einer gemeinsamen Strategie mit den Ländern bis 2012 und für 2013 die Umsetzung dieser gemeinsamen Strategie geplant.
Die vom IT-Planungsrat am 13. September 2010 verabschiedete Nationale E-Government-Strategie hat hierzu den Themengebieten Transparenz, Datenschutz und Datensicherheit (Zielbereich C) sowie gesellschaftliche Teil-habe (Zielbereich D) zwei wesentliche Zielbereiche gewidmet.

In der „Dresdner Vereinbarung“ wird diese Zielstellung des Regierungsprogramms aufgenommen. Die Bundesregierung vereinbarte gemeinsam mit Verwaltung, Wirtschaft und Wissenschaft auf dem 5. IT-Gipfel am 7. Dezember 2010 in Dresden das ehrgeizige Ziel, im Rahmen des Open Government bis zum Jahr 2013 eine zentrale Open Data-Plattform aufzubauen. Sie soll die Plattformen von Bund, Ländern und Kommunen vernetzen und einen Bei-trag zum Zugang zu Daten und Informationen der öffentlichen Verwaltung sowie zum weiteren Ausbau des prozessorientierten und ebenenübergreifenden E-Governments leisten.

Die Senatorin für Finanzen der Freien Hansestadt Bremen, das Institut für Informationsmanagement Bremen und die Landesbeauftragte für Datenschutz und Informationsfreiheit haben aufgrund ihrer Erfahrungen mit dem Informationsregister Bremen in der Bremer Empfehlung zu Open Government bereits konkrete Vorschläge unterbreitet, welche Maßnahmen bei der Entwicklung einer solchen Open Data-Plattform berücksichtigt werden sollten.

Da bei der Umsetzung dieser Open Government-Strategie auf der Basis einer Open Data-Plattform Datenschutz und Informationsfreiheit Hand in Hand gehen, ist die aktive Einbeziehung des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz und die Informationsfreiheit wünschenswert. Insbesondere wird es im Wesentlichen darauf ankommen, den Belangen der Informationsfreiheit unter Beachtung des Datenschutzes Rechnung zu tragen. Unter diesem Aspekt wird der Landesbeauftragte die weitere Entwicklung auf Bundes- wie Landesebene beobachten und die Ressorts beratend unterstützen. Das Thema wird auch Gegenstand des II. Tätigkeitsberichts zur Informationsfreiheit sein.

## 4 Entwicklung der automatisierten Datenverarbeitung

### 4.1 IT-Strategie – Landesleitlinie Informationssicherheit

Der Landesbeauftragte hat in seinem IX. Tätigkeitsbericht (Nr. 4.4) über die seit Jahren andauernden Bemühungen zur Erarbeitung einer IT-Sicherheitsstrategie für das Land berichtet. Mit dem Beschluss der Landesregierung über die IT-Strategie des Landes Sachsen-Anhalt vom 29. Juli 2008 (MBl. LSA S. 619) wurden Festlegungen getroffen, welche die Belange des Datenschutzes und der Datensicherheit berücksichtigen.
Eine **Landesleitlinie Informationssicherheit (LL IS)** soll demnach die Grundlage für die Etablierung einer IT-Sicherheitsorganisation in den Ressorts bilden. Im damaligen Beschluss zur IT-Strategie wurde noch von „IT-Sicherheit“ gesprochen, für die Landesleitlinie soll aber die **Informationssicherheit** bei allen Verwaltungsprozessen und Fachaufgaben berücksichtigt werden. Vorgesehen war als mittelfristige Maßnahme der IT-Strategie, den Datenschutz – als Bestandteil des IT-Managements – in die LL IS zu integrieren, um damit bei der Modernisierung der Verwaltung die Beachtung des informationellen Selbstbestimmungsrechts und des Grund-rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sicherzustellen.

Der Datenschutz muss dabei als integraler Bestandteil dieses IT-Managementprozesses verstanden werden. Durch eine rechtzeitige Einbeziehung des Landesbeauftragten bei grundlegenden Planungen des Landes zum Aufbau oder zur Änderung automatisierter Verfahren bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten, die Unterrichtung bei automatisierten Abrufverfahren und bei Auftragsdatenverarbeitung durch Dritte, die Durchführung einer Vorabkontrolle für bestimmte automatisierte Verfahren durch die behördlichen Beauftragten für den Datenschutz, sowie die Führung von Verfahrensverzeichnissen, so die Festlegungen im Beschluss zur IT-Strategie, soll den Belangen des Datenschutzes und der Datensicherheit im Rahmen der IT-Managementprozesse entsprochen werden.

Der Landesbeauftragte hatte Gelegenheit, zu einem 1. Entwurf der LL IS der Staatskanzlei im März 2010 Stellung zu nehmen. Seine Empfehlungen, insbesondere zur Aufnahme datenschutzspezifischer Schutzziele wie Authentizität, Revisionssicherheit und Transparenz in die LL IS, wurden berücksichtigt. Er hat sich aktiv an der weiteren Ausarbeitung, in der vom IT-Koordinierungsausschuss mit Beschluss vom 25. Oktober 2010 eingesetzten Arbeitsgruppe „Informationssicherheit“ unter Leitung der Staatskanzlei, beteiligt. Mit Fertigstellung der LL IS sollte die Beschlussfassung der Landesregierung zum Aufbau eines Informationssicherheitsmanagements im Land vorbereitet werden.

Kritisch ist anzumerken, dass es beim Entwurfsstand dieser Landesleitlinie Informationssicherheit vom Februar 2011 vorerst geblieben ist, denn eine abschließende Sitzung der Arbeitsgruppe wurde im April 2011 kurzfristig abgesagt.

Der Landesbeauftragte hofft, dass nach dem Wechsel der Zuständigkeit für die IT-Strategie von der Staatskanzlei zum Ministerium für Finanzen zu Beginn der 6. Wahlperiode, auf Grund der Regierungsneubildung, die Erarbeitung der LL IS schnell zum Abschluss gebracht werden wird.
Inwieweit die nunmehr bereits drei Jahre alte IT-Strategie des Landes Sachsen-Anhalt unter den neuen Bedingungen der Zusammenarbeit vom Bund und Ländern im Rahmen des IT-

Staatsvertrages und dem Aufbau eines Verbindungsnetzes durch den Bund (s. Nr. 1.3.1) einer Überarbeitung bzw. Fortschreibung bedarf, sollte ebenfalls vom jetzt zuständigen Finanzministerium überprüft werden. Der Landesbeauftragte geht davon aus, dass er rechtzeitig unterrichtet und beteiligt wird, wenn es dabei um die Lösung datenschutzrechtlicher Probleme geht.

### 4.2 IT-Planungsrat – spezifische Datenschutzthemen

In Vorbereitung der aus dem IT-Staatsvertrag zur Ausführung von Artikel 91c GG resultierenden Aufgaben wurde bereits mit einem Beschluss des Arbeitskreises der E-Government-Staatssekretäre vom 7. Mai 2009 die Arbeitsgruppe „IT-Planungsrat“ (IT-PLR) damit beauftragt, Vorschläge für das zukünftige Aufgabenspektrum und den Wirkungskreis sowie die Gremienstrukturen des IT-PLR zu erarbeiten. Dabei waren vor allem die bestehenden Gremien und deren Untergremien und Einrichtungen sowie die bisher bestehenden Initiativen, Vorhaben und Projekte zu berücksichtigen. Dies betraf insbesondere die Vorgängergremien des IT-PLR:

- den Arbeitskreis der E-Government-Staatssekretäre in Bund und Ländern (Aktionsplan Deutschland-Online – **DOL**) und

- den Kooperationsausschuss Automatisierte Datenverarbeitung Bund/Länder/Kommunaler Bereich – **KoopA ADV**.

Im Ergebnis wurden vom IT-PLR entsprechende Beschlüsse zu seinem Aufgabenspektrum, der Gremienstruktur und zur Aufgabenüberführung aus den Vorgängergremien DOL und KoopA ADV gefasst.

Mehr oder minder Datenschutzrelevanz für die Länder, so auch für Sachsen-Anhalt, haben danach fast alle Themen des IT-PLR, welche im **Projekt- und Anwendungsplan 2011** des IT-PLR auf seiner 3. Sitzung am 24. September 2010 beschlossen wurden. Mit einem Großteil der nachfolgend genannten Projekte sind bzw. waren die verschiedenen ständigen Arbeitskreise der Datenschutzkonferenz befasst oder daran beteiligt.

Nach diesem Projekt- und Anwendungsplan werden die bestehenden Projekte und Themenfelder in **drei Kategorien** unterteilt:

Kategorie 1 – **Steuerungsprojekte** des neuen Aktionsplans Deutschland-Online. (Dieser ersetzt den bisherigen Aktionsplan der Bundeskanzlerin und der Regierungschefs der Länder in der Fassung vom 21. November 2009).

**Steuerungsprojekte** werden nach Zuweisung durch die Bundeskanzlerin im Ergebnis der Ministerpräsidentenkonferenz durch den IT-PLR in einem Aktionsplan festgelegt. Hierzu zählen:

- **Infrastruktur** (Auf-und Ausbau einer abgestimmten Netzinfrastruktur der deutschen Verwaltung: Bund/Länder/Kommunen),

- **Kfz-Wesen** (Ziel des Vorhabens ist es, den Registrierungsprozess von Fahrzeugen unter konsequenter Nutzung der Möglichkeiten von E-Government möglichst ohne Medienbrüche online zu ermöglichen),

- **Personenstandswesen** (Einführung eines elektronischen Personenstandsregisters),

- **Meldewesen** (Aufbau eines Bundesmelderegisters; zur Zeit ruhendes Projekt),

- **Nationales Waffenregister** (Einführung eines einheitlichen elektronischen Systems).

Kategorie 2 – **Koordinierungsprojekte**

**Koordinierungsprojekte** des IT-PLR sind die bestehenden E-Government- und IT-Projekte, die eine wesentliche Komponente zur Weiternutzung im so-genannten „föderativen E-Government" darstellen. Die Steuerung und Finanzierung bleibt hier, im Unterschied zu den Steuerungsprojekten des IT-PLR, vollständig bei den Projektverantwortlichen des Bundes, der Länder bzw. der jeweiligen Fachministerkonferenz. Hierzu zählen:

- **Geodaten** (Ziel: Harmonisierung der heterogenen Geoinformationsstrukturen in Deutschland zur Nutzung durch Verwaltungen, die Wirtschaft, Bürgerinnen und Bürger),

- **S.A.F.E.** („Secure Access to Federated E-Justice/E-Government" - Einheitliche Kommunikationsinfrastruktur für den elektronischen Rechtsverkehr),

- **D 115** (Telefonischer Bürgerservice mit der einheitlichen Behördenrufnummer 115; seit dem 14. April 2011 im Regelbetrieb).

Kategorie 3 – **Anwendungen**

**Anwendungen** des IT-PLR sind E-Government- bzw. IT-Lösungen, die nach einer entsprechenden Entwicklungs- und Testphase dauerhaft zur Unterstützung von automatisierten Prozessen der öffentlichen Verwaltung in Bund und Ländern regelmäßig zum Einsatz kommen. Hierzu zählen:

- **DVDV** (Das Deutsche Verwaltungsdiensteverzeichnis bildet die zentrale Registrierungsstelle für Online-Dienste der öffentlichen Verwaltung und ermöglicht eine rechtsverbindliche Kommunikation zwischen Behörden über vorhandene Fachverfahren.),

- **LeiKa-plus** (Der sogenannte Leistungskatalog bietet Bürgerinnen und Bürgern sowie Unternehmen in Deutschland ein einheitliches, voll-ständiges und umfassendes Verzeichnis der Verwaltungsleistungen über alle Verwaltungsebenen hinweg. Ziel von LeiKa-plus ist es, bis Ende 2011 möglichst viele Objekte des Leistungskatalogs mit Stamm-texten zu verknüpfen.),

- **Behördenfinder** (Mit dem Behördenfinder Deutschland wird das Informationsangebot der öffentlichen Einrichtungen standardisiert und im Zusammenwirken mit dem Portal

http://www.behoerdenfinder.de um-gesetzt. Die zuständigen Geschäfts- und Koordinierungsstellen für die Anwendung Leistungskatalog und Behördenfinder sind beim Ministerium des Innern des Landes Sachsen-Anhalt eingerichtet.),

- **Governikus** (Governikus ermöglicht den sicheren und verbindlichen elektronischen Nachrichten- und Dokumentenaustausch via OSCI und kommt beim Bund, den Ländern und Kommunen als Basiskomponente der Virtuellen Poststelle zum Einsatz).

Neben der Geschäftsstelle des IT-PLR als ständiges Gremium wurde auf der 4. Sitzung des IT-PLR am 3. März 2011 der Start der **Koordinierungsstelle für IT-Standards (KoSIT)** beschlossen. Die KoSIT, ebenfalls eine ständige Einrichtung, hat ihre Arbeit zum 1. April 2011 in der Freien Hansestadt Bremen aufgenommen. Sie ist aus der bisherigen OSCI-Leitstelle des Landes Bremen hervorgegangen, welche bisher im Auftrag des KoopA ADV die Entwicklung fachlicher Standards für durchgehende elektronische Prozesse im Meldewesen, in der Justiz, im Ausländerwesen sowie im Personenstandswesen koordinierte und leitete. Damit wurde eine wesentliche Aufgabe des IT-PLR nach § 1 des IT-Staatsvertrages, die Beschlussfassung über fachunabhängige und fachübergreifende IT-Interoperabilitäts- und IT-Sicherheitsstandards, dauerhaft an einer Stelle gebündelt. Zukünftig wird die KoSIT zuständig sein für:

- die Koordination der Entwicklung fachlicher Standards (XÖV),
- die Pflege und Weiterentwicklung von OSCI Transport,
- die Erarbeitung fachlicher Standards im Auftrag einiger Fachministerkonferenzen.

An dieser Stelle sei nochmals auf die **Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. Oktober 2009 zum IT-Staatsvertrag** (**Anlage 2**) hingewiesen. Neben der Forderung der Beteiligung der Landesbeauftragten für den Datenschutz zur Vertretung der Interessen der Länder im Bereich Datenschutz wurde vom Landtag in seinem Beschluss vom 18. März 2010 (Drucksache 5/73/2508 B) die Landesregierung aufgefordert sich dafür einzusetzen, dass die im Staatsvertrag vorgesehene vorrangige Verwendung bestehender **Marktstandards** nicht dazu führt, dass der Einsatz von Verfahren ohne angemessenen Datenschutz beschlossen wird. In diesem Zusammenhang sei daran erinnert, dass das Bundesverfassungsgericht gerade die besondere Bedeutung der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme für den Schutz des Persönlichkeitsrechts hervorgehoben hat (1 BvR 370/07, 1 BvR 595/07, Urteil vom 27. Februar 2008). Der Arbeitskreis technische und organisatorische Datenschutzfragen hat deshalb bereits Kontakt zur KoSIT aufgenommen und seine Bereitschaft zur Mitarbeit und Unterstützung in diesem Gremium erklärt.

Ein weiterer Schwerpunkt der 4. Sitzung war das Thema IT-Sicherheit in Deutschland. Der IT-PLR hat sich am 3. März 2011 darauf verständigt, gemeinsam Rahmenbedingungen für die IT-Sicherheit von Bund, Ländern und Kommunen in einer **Leitlinie für Informationssicherheit** zu erarbeiten.

Eine Evaluierung der Gremienstrukturen und Abläufe ist seitens des IT-PLR vorgesehen. Eine Vorkonferenz zur vertieften inhaltlichen Vorbereitung des IT-PLR ist in der Diskussion.

Es bleibt daher abzuwarten, ob eine solche Vorkonferenz auch die inhaltliche Auseinandersetzung mit datenschutzrelevanten Themen verbessern wird.

### 4.3 Zentraler IT-Dienstleister – Sachstand zum Landesrechenzentrum

In seinem IX. Tätigkeitsbericht (Nr. 4.2) hatte der Landesbeauftragte ausführlich von der Umsetzung des grundlegenden Kabinettbeschlusses der damaligen Landesregierung vom 14. November 2006 zur Bildung eines zentralen IT-Dienstleisters, dem **Landesrechenzentrum** (LRZ), berichtet und sich kritisch damit auseinandergesetzt sowie entsprechende Empfehlungen gegeben.

Wichtiger als die Entscheidung des Kabinetts zur Neuausrichtung der IT-Organisation und der Aufgabenverteilung und -abgrenzung zwischen der Staatskanzlei (IT-Strategie) und dem Ministerium des Innern (E-Government, Betrieb des Landesnetzes – ITN-LSA) war die zweite Entscheidung, nämlich der Auftrag an das Ministerium der Finanzen zur IT-Konsolidierung der Landesverwaltung und zum gleichzeitigen Aufbau des LRZ, unter datenschutzrechtlichen Gesichtspunkten, insbesondere in ihrer zukünftigen Auswirkung auf alle Ressorts des Landes Sachsen-Anhalt.

Der Landesbeauftragte hatte bereits im Mai 2009 im Rahmen des Workshops der Oberfinanzdirektion Magdeburg (OFD) bei der Vorstellung des Entwurfs einer Kabinettvorlage zum Geschäftsmodell „Landesrechenzentrum“, als den zukünftigen zentralen IT-Dienstleister des Landes, zum Thema Migration der IT-Querschnittsdienste/Übernahme von Fachverfahren auf die bestehenden restriktiven datenschutzrechtlichen Bestimmungen hingewiesen und eine diesbezügliche Berücksichtigung im Entwurf der Kabinettvorlage gefordert. Er hatte zugleich seine Unterstützung für die Begleitung dieses Migrationsprozesses angeboten. Eine weitere Information oder Beteiligung des Landesbeauftragten erfolgte allerdings nicht. Erst Ende August 2009 erreichte den Landesbeauftragten per E-Mail der Entwurf der Kabinettvorlage zum Geschäftsmodell für das LRZ.

Im Hinblick auf eine rechtzeitige Unterrichtungspflicht des Landesbeauftragten nach § 14 Abs. 1 Satz 2 DSG-LSA war das nicht akzeptabel. Nach Intervention des Landesbeauftragten beim Ministerium der Finanzen wurde ihm die Kabinettvorlage im November 2009 zur Verfügung gestellt. Den dazugehörigen Kabinettbeschluss erhielt der Landesbeauftragte aber nur „auszugsweise“.

In Zeiten des propagierten „Open Government/Open Data“ (vgl. Nr.1.3.4) hält der Landesbeauftragte diese Verfahrensweise der Landesregierung mittlerweile für anachronistisch, zumal er hier nicht aus reiner Neugier, sondern im Rahmen seines gesetzlichen Beratungsauftrages als Kontrollbehörde tätig wurde und damit seine unabhängige Amtsführung beeinträchtigt wird. Zeugt sie doch von einer gewissen Ignoranz in Bezug auf die Verpflichtung aller öffentlichen Stellen zur Unterstützung ihm gegenüber (§ 23 Abs. 1 DSG-LSA).

Unter diesem Gesichtspunkt wäre, im Hinblick auf die Unterrichtungspflicht aus § 14 Abs. 1 Satz 2 DSG-LSA, eine Anpassung der bisherigen Regelung im Abschnitt VI der Gemeinsamen Geschäftsordnung der Ministerien – Allgemeiner Teil (Zusammenarbeit der Ministerien, Beteiligung, §§ 37, 38, 40 GGO LSA I) zur besseren Beteiligung des Landesbeauftragten mit Beginn der 6. Wahlperiode durch die neue Landesregierung wünschenswert. So wie in einer

Kabinettvorlage ein „Gleichstellungspolitischer Bericht“ enthalten sein muss (§ 38 GGO LSA I), könnten zukünftig in einem „**Datenschutz-Bericht**“ etwaige Belange des Datenschutzes dargestellt werden.

Die **Unterrichtung** des Landesbeauftragten ist an keine Form gebunden. Im einfachsten Fall reicht also zur Erfüllung dieser Pflicht eine rechtzeitige Übersendung von Planungsunterlagen, u. a. auch von Entwürfen von Kabinettvorlagen, unter Hinweis auf eine Unterrichtung nach § 14 Abs. 1 Satz 2 DSG-LSA aus. Sie verursacht damit, im Gegensatz zu der dem Landesbeauftragten gegenüber oft geäußerten Meinung eines damit verbundenen „erheblichen zusätzlichen Aufwandes“, diesen eben nicht, sondern unterstützt seine gesetzliche Aufgabe, bereits im Planungsstadium bei Vorhaben der Landesregierung einen vorgezogenen Grundrechtsschutz zu gewährleisten. Zu diesen Vorhaben gehören zweifellos die IT-Konsolidierung der Landesverwaltung und der Aufbau des LRZ.

Mit der gegenwärtigen formalen Festlegung in § 40 GGO LSA I, den Landesbeauftragten nur zu beteiligen, soweit personenbezogene Daten verarbeitet werden, steht die Landesregierung selbst im Widerspruch zu Grundsätzen und Zielen in ihrer eigenen IT-Strategie, in der den Belangen des Datenschutzes und der Datensicherheit im Rahmen des IT-Managementprozesses durch rechtzeitige Einbeziehung des Landesbeauftragten bei grundlegenden Planungen des Landes zum Aufbau oder zur Änderung automatisierter Verfahren bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten entsprochen werden soll. Einem solchen IT-Managementprozess gehen bekanntermaßen Grundsatzentscheidungen in Form von Kabinettbeschlüssen voraus.
Der **Kabinettbeschluss vom 1. September 2009** bestätigte die Vorlage des Ministeriums der Finanzen zum Geschäftsmodell des LRZ. Die darin u. a. aufgeführten mittelfristig nur noch durch das LRZ bereitzustellenden **IT-Querschnittschnittdienste** für über 300 Behörden innerhalb der Landesverwaltung

- zentraler User Help Desk (UHD), Benutzerbetreuung,
- zentrale Softwareverteilung,
- Terminal-Server-Technik,
- Virtualisierung (Server und Anwendungen),
- SAP-Kompetenz-Center,
- zentrale Datenspeicherung und -archivierung,
- Betrieb E-Mail-Infrastruktur/zentraler Verzeichnisdienst und Druck

lassen erkennen, dass die damit im Zusammenhang stehenden datenschutzrechtlichen Fragen nach wie vor der Erörterung und Beachtung bedürfen. Das ist u. a. bei den Themen Auftragsdatenverarbeitung (§ 8 DSG-LSA), Wartung von Datenverarbeitungsanlagen oder -verfahren durch externe Dritte (§ 8 Abs. 7 DSG-LSA) sowie automatisierte Abrufverfahren (§ 7 DSG-LSA) in Verbindung mit der Vorabkontrolle bei automatisierten Verfahren (§ 14 Abs. 2 DSG-LSA) der Fall.

Dem **Datenschutz** wurde in der **Kabinettvorlage** selbst kein und in der 37-seitigen **Anlage A** (Geschäftsmodell des LRZ) ein ganzer Satz gewidmet: *„Die bei den einzelnen Querschnitts- und Fachverfahren bestehenden datenschutzrechtlichen Bestimmungen und Regelungen werden bei der Übernahme der einzelnen Verfahren berücksichtigt bzw. eingehalten."*

Das LRZ wurde aus dem Finanzrechenzentrum (FRZ) der OFD und dem ehemaligen Landesinformationszentrum (LIZ) in Halle als Abteilung 4 der OFD gebildet. Mit dem 1. September 2009 erfolgte gleichzeitig die Gründung des LRZ in dieser neuen Struktur. Die Zusammenführung des LIZ als LHO-Betrieb mit dem FRZ zum LRZ mit Hauptsitz in Halle (Saale) und einer Nebenstelle in Magdeburg erfolgte am 1. Januar 2010.

Der Projektbeirat, der vom Aufbaustab der sogenannten Stabsstelle „Konsolidierung des IT-Betriebes" eingerichtet wurde, begleitete den IT-Konsolidierungsprozess beratend. Der Landesbeauftragte war Mitglied dieses Projektbeirates. In der 6. und letzten Sitzung des Projektbeirates im Mai 2010 wurde seiner Auflösung zugestimmt. Die Grundsatzentscheidung bezüglich der strukturellen Anbindung des LRZ in Form einer Verwaltungslösung an die OFD (Behördenmodell anstelle einer Anstalt des öffentlichen Rechts) machte diesen Projektbeirat quasi überflüssig.

Die Landesregierung hatte in ihrer Stellungnahme zum IX. Tätigkeitsbericht des Landesbeauftragten (**LT-Drs. 5/2385**) sehr knapp darauf verwiesen, dass der Aufbau des zentralen IT-Dienstleisters entsprechend dem Kabinettsbeschluss vom 14. November 2006 durch das Ministerium der Finanzen erfolgt. Inhaltlich wurde auf die Empfehlungen des Landesbeauftragten nicht eingegangen. *„Bei der technischen und organisatorischen Umsetzung durch das MF bzw. das LRZ wird auf die datenschutzkonforme Einrichtung und Übernahme der IT-Querschnittsdienste geachtet."*, so die damalige Antwort der Landesregierung.
Die praktische Umsetzung der Migration der zentralisierbaren IT-Querschnittsdienste zum LRZ als ein wesentlicher Schritt zur IT-Konsolidierung innerhalb der Landesverwaltung hat das Ministerium der Finanzen für seinen Geschäftsbereich selbst als Pilotprojekt am 6. April 2010 abgeschlossen. Gleichzeitig nahm der zentrale User Help Desk im LRZ seinen Betrieb zur Nutzerbetreuung der migrierten Dienststellen auf.

Die dem Landesbeauftragten im Mai 2010 vom Ministerium der Finanzen an-gekündigte Kabinettvorlage zur Migration weiterer Ressorts liegt bisher nicht vor. Er soll aber bei der nächsten Ressort-Migration zur Bestandsaufnahme eingeladen und beteiligt werden. Der Vorteil des derzeitigen Migrationskonzepts je Behörde, welches eine Ist-Analyse, eine Konzepterstellung zur Ablösung der IT-Querschnittsdienste und danach die Übernahme dieser IT-Querschnittsdienste von der jeweiligen Behörde durch das LRZ vorsieht, liegt in der damit nur einmal notwendigen Befassung mit einer Behörde.

Eine grundsätzliche Entscheidung zum **Betrieb des zukünftigen Landesnetzes** (**ITN XT** – „eXTended"), anstelle des bisherigen Betriebes des Landesnetzes (ITN-LSA) durch das Technische Polizeiamt, steht immer noch aus und wurde auch in der damaligen Kabinettvorlage zum Geschäftsmodell des LRZ bislang von einer Übernahme durch das LRZ ausgenommen.

Mit dem "Gesetz über die Verbindung der informationstechnischen Netze des Bundes und der Länder – Gesetz zur Ausführung von Artikel 91c Absatz 4 des Grundgesetzes – vom 10.

August 2009 (BGBl. I S. 2706) – **IT-NetzG**“ errichtet der Bund (gemäß § 1 IT-NetzG) zur Verbindung der informations-technischen Netze des Bundes und der Länder ein **Verbindungsnetz**. Das IT-NetzG wurde als Art. 4 des Gesetzes vom 10. August 2009 (BGBl. I S. 2702) vom Bundestag mit Zustimmung des Bundesrates beschlossen. Gemäß § 3 IT-NetzG erfolgt der Datenaustausch zwischen dem Bund und den Ländern über dieses Verbindungsnetz. § 3 des IT-NetzG tritt gem. Art. 13 Abs. 3 des Artikelgesetzes allerdings erst am 1. Januar 2015 in Kraft.

Hier bleibt abzuwarten, welche Entscheidungen das Ministerium der Finanzen als nunmehr zuständiges Ressort für die IT-Strategie und als Vertreter des Landes Sachsen-Anhalt im IT-PLR treffen wird. Nach fünf Jahren erfolgt nach der Aufteilung der Verantwortlichkeiten für die IT-Strategie, das E-Government und den zentralen IT-Dienstleister auf verschiedene Ressorts (s. VIII. Tätigkeitsbericht, Nr. 4.1) nunmehr mit Beginn der 6. Wahlperiode die **Bündelung** dieser Verantwortlichkeiten in einem Ressort, dem Ministerium der Finanzen. Damit verfügt das Land Sachsen-Anhalt nun erstmalig auch über einen „**IT-Beauftragten der Landesregierung**“, dessen Aufgaben ein Staatssekretär im Ministerium der Finanzen zukünftig im Sinne eines **CIO** wahrnehmen wird.
Die Staatskanzlei hat sich beim Landesbeauftragten im Mai 2011 für die vertrauensvolle Zusammenarbeit im Ständigen Staatssekretärsausschuss „Informationstechnologie“ zur Vorbereitung der bisherigen vier Sitzungen des IT-PLR bedankt. Der Landesbeauftragte setzt nach der Konzentration der Zuständigkeiten im Ministerium der Finanzen für die IT-Strategie, das E-Government und das LRZ auf eine ebenso vertrauensvolle wie effektive Zusammenarbeit. Seine frühzeitige Einbeziehung etwa im Rahmen der Entwicklung eines zentralen Personalmanagementsystems (**PROMIS**) lässt trotz noch zu lösender datenschutzrechtlicher und -technischer Fragestellungen (s. Nr. 18.2) auf eine gute Zusammenarbeit hoffen.

Zu einem der zukünftig zu behandelnden Themen gehört z. B. die Aufgabenstellung für das LRZ auf Basis des **Beschlusses des IT-Koordinierungsausschusses vom 5. April 2011** zur zentralen Identitäts- und Zugriffsverwaltung der Landesverwaltung (**IAM – Identity and Access Management**). Das Ministerium der Finanzen wird durch diesen Beschluss aufgefordert, das LRZ mit der Ausschreibung auf der Basis der Arbeitsgruppe IT-Architektur der Landesleitstelle IT-Strategie der Staatskanzlei zu beauftragen. An den Ergebnissen der Arbeitsgruppe war auch der Landesbeauftragte als Mitglied beteiligt. Datenschutzrechtliche Belange sollten bereits bei der Ausschreibung durch das LRZ berücksichtigt werden (s. IX. Tätigkeitsbericht, Nr. 4.3).

### 4.4 E-Government-Maßnahmenplan 2010 – Fehlanzeige

Noch im Frühjahr 2010 wurde dem Landesbeauftragten seitens des Ministeriums des Innern eine Vorabbeteiligung zum E-Government-Maßnahmenplan 2010 des Landes avisiert. Auch die Staatskanzlei informierte den Landes-beauftragten auf seine Nachfrage zum Sachstand, dass im Mai 2010 seitens des Ministeriums des Innern eine Vorlage zur Mitzeichnung geplant sei. Allerdings war hier von der Fortschreibung einer „E-Government-Strategie des Landes“ und nicht mehr von einem E-Government-Maßnahmenplan 2010 die Rede. Denn nach dem am 29. April 2003 von der Landesregierung beschlossenen Grundkonzept E-Government in Sachsen-Anhalt (E-Government-Grundkonzept mit dem E-Government-Aktionsplan für die Landesverwaltung 2004-2010 und den sich daraus ergebenden Maß-

nahmenplänen 2005-2006, 2007 und 2008-2009) – der Landesbeauftragte berichtete hierzu regelmäßig in seinen vorangegangenen Tätigkeitsberichten (VII. Tätigkeitsbericht, Nr. 7.1; VIII. Tätigkeitsbericht, Nr. 4.2; IX. Tätigkeitsbericht, Nr. 4.5) – wäre eigentlich ein solcher E-Government-Maßnahmenplan auch für das Jahr 2010 zu erwarten gewesen.

Dafür erreichte den Landesbeauftragten auf seine Nachfrage hin im Juni 2010 ein erster **Entwurf** der „E-Government-Strategie des Landes Sachsen-Anhalt – Verwaltung 2020 – koordiniert, prozessorientiert und eigenverantwortlich handelnd“ (Stand: 22.06.2010). Unter Bezugnahme auf diesen Strategieentwurf sollte dem Landesbeauftragten danach ein E-Government-Maßnahmenplan 2010-2011 zur Vorabstimmung zugeleitet werden. Bei diesem Entwurfsstadium, für einen Zeitraum von 2010 bis 2020, ist es nach Kenntnis des Landesbeauftragten dann auch geblieben, der damals avisierte E-Government-Maßnahmenplan 2010-2011 liegt nicht vor und die für Juli 2010 vorgesehene Kabinettsbefassung fand nicht statt.

Im Resümee dieses Strategieentwurfs ging das Ministerium des Innern davon aus, dass von den bekannten 23 **E-Government-Leitprojekten** bereits 19 abgeschlossen sind und die restlichen vier sich in Umsetzung befinden bzw. zu Daueraufgaben geworden sind.

Eine wesentliche Ursache für die Nichteinbringung dieses Entwurfs dürfte in der am **24. September 2010** vom **IT-Planungsrat** in seiner **3. Sitzung** verabschiedeten **Nationalen E-Government-Strategie (NEGS)** liegen. Zur Ausarbeitung der NEGS wurde eine bis zum 31. Oktober 2010 befristete länderoffene Kooperationsgruppe „Strategie“ gebildet, in der auch das Ministerium des Innern vertreten ist. Deren Wirken wurde bis zum 30. Juni 2011 verlängert. Zukünftig geht es um die Umsetzung mit konkreten Maßnahmen zum Aufbau einer föderalen IT-Infrastruktur.

Positiv ist anzumerken, dass der erste Strategieentwurf des Ministeriums des Innern nach dem Vorbild der NEGS auch den Belangen des Datenschutzes zumindest in der Beschreibung des Zielsystems der E-Government-Strategie 2010-2020 eine entsprechende Bedeutung beimisst: *„Durch die fortschreitende Weiterentwicklung des E-Government können zielgruppenabhängig spezifische Risiken für die informationelle Selbstbestimmung entstehen. Um dieses Recht zu wahren, ist dem **Datenschutz** im Land Sachsen-Anhalt **besondere Beachtung zu schenken**.“*

An diesem Bekenntnis zur besonderen Beachtung des Datenschutzes wird auch die zukünftige E-Government-Strategie der neuen Landesregierung zu messen sein. Der Landesbeauftragte ist in diesem Zusammenhang bereit, wie bisher mit der Staatskanzlei und dem Ministerium des Innern, auch nach den strukturellen Veränderungen innerhalb der Landesregierung, d. h. der Verlagerung der Zuständigkeit und Verantwortlichkeit für die IT-Strategie und das
E-Government im Land Sachsen-Anhalt zum Ministerium der Finanzen, die Zusammenarbeit fortzusetzen, um den **Prozess** der **Verwaltungsmodernisierung** weiterhin beratend zu begleiten.

## 4.5 Landesportal Sachsen-Anhalt

Das Landesportal (http://www.sachsen-anhalt.de) hat sich im Berichtszeitraum deutlich weiterentwickelt. Die Zugriffszahlen haben sich im Vergleich zu 2007 mehr als verdoppelt. 2010 gab es ca. 44,5 Millionen Zugriffe. Die Staatskanzlei hat eine Redaktionsrunde eingerichtet, in welcher sich der Landesbeauftragte nicht nur als Behörde beteiligt, sondern sich auch inhaltlichen datenschutzrechtlichen Aspekten widmet. Hierzu gehören beispielsweise Themen wie: SSL-Verschlüsselung von Webportalen mittels Zertifikaten, datenschutzgerechte Auslieferung von Videos im Landesportal und datenschutzgerechte Auswertung der Zugriffe auf das Landesportal.

SSL-Verschlüsselung von Web-Portalen

Der Landesbeauftragte wurde im Jahr 2010 durch Dritte mehrfach darauf hingewiesen, dass das Landesportal keine Absicherung durch SSL-Verschlüsselung und Zertifikate nutzt. Sowohl Behörden wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) als auch Nutzern, welche Wert auf einen abgesicherten Zugriff legen, fiel das fehlende Zertifikat auf. Aus Kostengründen will die Staatskanzlei hier leider so schnell nichts ändern. Es gab jedoch eine Zusage, den Web-Mailer und auch den Zugang für Redakteure am Landesportal durch Zertifikate der Landes-PKI abzusichern. Damit werden personenbezogene Daten und schreibende Zugriffe auf die Datenbank über die Redaktionsschnittstelle besser geschützt. Dennoch ist ein Hinweis, dass die Verbindung fälschungs- und abhörsicher und mit dem richtigen Gegenüber aufgebaut wurde, sinnvoll. Auch gibt es nicht-personenbezogene Daten, die nur von einem Anbieter mit gesicherter Identität bezogenen werden sollten. Beispielsweise der PGP-Schlüssel des Landes-beauftragten. Die Webseiten des Landesportals sind auf Wunsch des Nutzers auch verschlüsselt auszuliefern. Dazu ist ein X.509-Zertifikat auf dem Webserver zu installieren, welches eine Auslieferung HTTPS-verschlüsselter Webseiten erlaubt. Im Browser wird das z. B. mit einem farbig hinterlegten Domainnamen oder einer solchen URL gekennzeichnet. Unsichere Adressen fallen dem Nutzer zunehmend auch auf. Leider ist ohne größere finanzielle Investition in ein Zertifikat einer bereits dem Webbrowser bekannten **Zertifizierungsstelle** (**CA – Certificate-Authority)** nur ein Minimalschutz möglich, in-dem preiswerte Zertifikate der Landes-PKI oder die von kostenfreien Anbietern genutzt werden. Bei allen preiswerten Lösungen ist die Absicherung der Zertifikate beim Importieren in den Webbrowser mangelhaft, da die sichere manuelle Beschaffung, Prüfung und Installation den Normalbenutzer häufig überfordert. Auch das ist ein Grund, warum die Wurzelzertifikate der Verwaltungs-PKI in den gängigen Webbrowsern von Haus aus hinterlegt werden sollten. Die SSL-Schnittstellen sind mittlerweile freigeschaltet, jedoch verliefen Tests zur Nutzung der Verschlüsselung auf Rechnern in der Geschäftsstelle des Landesbeauftragten sowohl beim Web-Mailer als auch beim Redaktionssystem nicht erfolgreich. Aus diesem Grund versucht der Landesbeauftragte, durch kontinuierliches Aufgreifen des Themas u. a. in der AG Verwaltungs-PKI und damit auch beim BSI, die Wichtigkeit der Hinterlegung der Wurzelzertifikate der V-PKI in den Webbrowsern zu verdeutlichen und so über diesen Umweg dem Land die Nutzung der eigenen Landes-PKI für Webseiten zu ermöglichen. Viele Webseiten, angefangen von Google bis hin zur Wikipedia, ermöglichen es, ihre Dienste verschlüsselt zu nutzen. Das klappt noch nicht bei jedem Anbieter perfekt, aber die Entwicklung ist abzusehen, da Webserver-Zertifikate und verschlüsselte Datenübertragungen Stand der Technik sind. Spätestens mit der Einbindung von Open Data und Web 2.0-Funktionen direkt

in das Portal werden Benutzerzugänge notwendig, und dann wird es nicht mehr ohne Verschlüsselung gehen.

Dass bei der Nutzung von HTTPS/SSL weltweit Defizite herrschen, ist auch Projekt-Thema der Internet Engineering Task Force. Diese will mittels HTTP Strict Transport Security (HSTS) die Verschlüsselung standardisieren. Konkret nutzen viele Webseiten nur auf wenigen Seiten – etwa zum Anmelden – Verschlüsselung und schalten im Anschluss wohl wegen Performance-Bedenken auf unverschlüsselten Betrieb zurück. HSTS-fähige Server erlauben es, Nutzer aktueller Browser (z. B. Firefox, Chrome) zur durchgehenden Verschlüsselung zu zwingen. Der Server sendet hierzu eine Kennung („ich kann HSTS“) zusammen mit der Sitzungslaufzeit, für welche verschlüsselt werden soll. Der Browser wird nun eine durchgehende Verschlüsselung sicherstellen und auch Verweise auf servereigene Seiten mittels HTTP-Protokoll automatisch nach https korrigieren.

Aber auch die Browser-Hersteller müssen dazu angeregt werden, Zertifikate kontrollierbarer zu hinterlegen. In den Browsern selbst sind unzählige CAs hinterlegt und es ist unmöglich, einen Überblick über die Vertrauenswürdigkeit aller CAs zu erlangen. Was weiß ein Nutzer schon über eine CA irgend-wo am anderen Ende der Welt? Wird diese überhaupt benötigt? Hier könnte die Verteilung der Wurzelzertifikate z. B. mittels Profilen geregelt werden. Wer der Verwaltung vertraut, kann diese aktivieren, wer nur großen Unter-nehmen vertraut, kann sich diese gebündelt installieren. Lokale Anbieter könnten dynamisch bei Bedarf oder sogar webseitenbezogen freigeschaltet werden, sodass die Menge der CAs die immer aktiv ist, überschaubar bleiben würde.

Neue Inhaltselemente im TYPO3

Im Landesportal selbst wurden im Rahmen einer Aktualisierung des TYPO3 neue Inhaltselemente freigeschaltet. Hier wurde bereits in den frühen Phasen in der Redaktionsrunde darauf hingewiesen, dass Google bzw. YouTube ggf. durch das Videoelement unbemerkt Daten der Besucher weitergeleitet bekommen, obwohl diese gar nicht das Video abspielen. Dieses Problem ist z. B. auch bei der Einbindung von Twitter und Facebook in eigene Webseiten vorhanden. Möglich ist, das Startbild des Videos als Grafik auf dem eigenen Webserver zu hinterlegen und ggf. einen Hinweis einzublenden, ob wirklich Daten vom externen Anbieter nachgeladen werden sollen. Letztlich hat sich das Land – vorbildlich – dafür entschieden, die Videos komplett im Landesportal zu hinterlegen und über ein ebenfalls hinterlegtes Abspielprogramm zu präsentieren. Videos können via Plugin im Landesportal genutzt werden – entweder als YouTube-Video mit der entsprechenden Film-Nummer oder als Flash-Video (FLV) auf dem Landesportal. Die Auslieferung des Videos vom eigenen Webserver ist die datenschutzgerechte Lösung. Ein YouTube-Video zum Test war jedoch nicht auffindbar.

Nutzung aktueller Web-Standards

Der Versuch, die Webseiten nach aktuellen Web-Standards ausliefern zu lassen, scheiterte. Der aktuelle „XHTML 1.0 Transitional“-Standard der Website (und der wird noch nicht einmal erfüllt) aus dem Jahr 2000 ist eine Neuformulierung des HTML4-Standards in XML. Jede Weiterentwicklung des Landesportals hin zu XHTML 1.1 (Empfehlung des W3C zur Nutzung erfolgte bereits im Jahr 2001) blieb aus. Es ist bis heute keine syntaktische Überprüfbarkeit

der Website möglich, da zu viele Fehler enthalten sind. Laut Aussage des Portal-Betreibers soll es so bleiben, da der Internet Explorer 6 (laut Wikipedia „Webbrowser“ derzeit mit 1,6% Marktanteil, Stand 05/2011) unbedingt unterstützt werden muss. Das sieht der Landesbeauftragte nicht so. Für aus-zuliefernde Webseiten ist mindestens XHTML 1.1 als Format zu nutzen. Vereinzelt anzutreffende Uralt-Browser können daraus abgeleitete, angepasste HTML-Dokumente erhalten. Auch eine ausschließliche Formatierung per CSS ist sinnvoll. Das Layout sollte schnellstmöglich komplett auf Nutzung von CSS umgestellt werden, da erst dadurch sauberer HTML-Code und die Nutzung aktueller Standards möglich werden. Das kommt der Benutzbarkeit der Website im Allgemeinen zugute. Derzeit erzeugt der automatische Editor sehr viele Formatanweisungen selbst. Damit ist leider keine einfache Wiederverwendbarkeit von Daten des Landesportals realisierbar. Da diese nicht personenbezogener Art sind, wurde die Standardisierung an dieser Stelle je-doch nicht weiter verfolgt.

Datenschutzgerechte Auswertung der Zugriffe auf das Portal

Die Informationen der bisherigen Loganalyse-Software Sawmill reichten nicht aus, da diese nur TYPO3-Logs auswerten konnte. Google Analytics sollte nicht genutzt werden (vgl. Nr. 14.6). Die Wahl fiel auf Piwik. Fast alle Landkreise wurden mittlerweile auf Piwik umgestellt und haben bereits erste Erfahrungen gesammelt. Sawmill und Piwik laufen derzeit parallel, um Vergleichswerte zu erhalten.

### 4.6 EU-Dienstleistungsrichtlinie – eine Bestandsaufnahme

Die Umsetzung der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über die Dienstleistungen im Binnenmarkt – EU-Dienstleistungsrichtlinie (EU-DLR) – (ABl. EU Nr. L 376 S. 36) in Sachsen-Anhalt erfolgte federführend durch das Ministerium für Wirtschaft und Arbeit, deren IT-Umsetzung durch das Ministerium des Innern. Zum Einheitlichen Ansprechpartner (EA) nach Art. 6 der EU-DLR in Sachsen-Anhalt wurde mit Kabinettbeschluss vom 23. September 2008 das Landesverwaltungsamt bestimmt.
Der Landesbeauftragte wurde in diesen Umsetzungsprozess von beiden Ministerien rechtzeitig informiert und beteiligt. Durch seine Mitarbeit in den dazu gebildeten Arbeitsgruppen fanden rechtliche wie technische Anforderungen des Datenschutzes eine entsprechende Berücksichtigung (IX. Tätigkeitsbericht, Nr. 4.7).

Die Kommunikation des EA und der zuständigen Behörden mit den Behörden der europäischen Mitgliedstaaten erfolgt mittels IMI-Basismodul EU-DLR (Internal Market Information System – IMI) im sogenannten Koordinierungsmodell. Als IMI-Behörden wurden nach dem Koordinierungsmodell die Landkreise und kreisfreien Städte und ergänzend die Kammern registriert, soweit sie fachlich oder fachaufsichtlich zuständig sind. Der Vorteil des Koordinierungsmodells, auch aus datenschutzrechtlicher Sicht, liegt im Wegfall des zentralen Eingangs von Anfragen beim EA. Damit gehen Anfragen direkt an die zuständigen Behörden.
Für diese IT-Lösung wurden sowohl Basiskomponenten gemäß Rahmenvereinbarung zwischen dem Land Sachsen-Anhalt und den Kommunen genutzt, u. a. auch das Elektronische Gerichts- und Verwaltungspostfach (EGVP) zur Kommunikation. Neubeschaffungen wurden nur für das Service-Portal, das Registrierungs- und das Authentifizierungsmodul sowie das Fallmanagement für den EA und die zuständigen Behörden durchgeführt. Das Betriebskon-

zept für die technische Umsetzung im Landesrechenzentrum (LRZ) basiert auf dem IT-Umsetzungskonzept zur EU-DLR des MI (Stand: 8. April 2009).

Mit der noch rechtzeitigen Verabschiedung des Gesetzes zur Umsetzung der europäischen Dienstleistungsrichtlinie in Sachsen-Anhalt vom 16. Dezember 2009 (GVBl. LSA S. 700) konnte die vorgegebene Umsetzungsfrist der EU-DLR bis zum 31. Dezember 2009 eingehalten werden.
Artikel 1 dieses Gesetzes ist das **Einheitlicher-Ansprechpartner-Gesetz** (EAG LSA). In ihm werden Regelungen zum EA, der europäischen Verwaltungszusammenarbeit und zur verwaltungskostenrechtlichen Umsetzung der EU-DRL getroffen. Nach § 6 Abs. 1 EAG LSA sind der EA und die zuständigen Behörden zur Zusammenarbeit verpflichtet, die in der Regel auf elektronischem Weg, mit Ausnahme der „Verbundenen Verfahren“ erfolgt. Die Zusammenarbeit des EA mit den zuständigen Behörden hat die Landesregierung gemäß § 6 Abs. 2 EAG LSA durch Verordnung zu regeln. In dieser Verordnung wären u. a. Vorgaben zur Sicherstellung der elektronischen Verfahrensabwicklung und der elektronischen Kommunikation sowie die Befugnisse zum Datenzugriff und dem Datenaustausch zu regeln. Die Landesregierung hat diese Verordnung bisher nicht erlassen.

Im darauffolgenden Jahr hat der Landesbeauftragte bewusst bei den dafür zuständigen Behörden auf formelle Kontrollen verzichtet. Erst im Frühjahr 2011 führten ihn Informationsbesuche bezüglich des praktischen Umsetzungsstandes zum EA in das Landesverwaltungsamt sowie das für die IT-Umsetzung zuständige LRZ nach Halle.

Als Ergebnis der Informationsbesuche ist festzustellen, dass das System sehr zurückhaltend genutzt wird. Nur zwei Dienstleistungserbringer haben im Jahr 2010 den Versuch unternommen, über den EA ihre Anträge elektronisch abzuwickeln.

18 Dienstleistungserbringer haben sich seither am EA-Portal registriert. Die Mehrheit der Anfragen erreicht den EA als E-Mail und wird entsprechend beantwortet oder zur Beantwortung an die zuständige Behörde weitergeleitet. Im Jahr 2010 erfolgten vermehrt Informationszugriffe auf das EA-Portal. Die Zugriffsstatistik (Pageviews: 2009: 2649; 2010: 26392; 2011(I. Q.): 7987) ist dafür ein Beleg.

Der EA ist zugleich IMI-Koordinator. Als sogenannte Verbindungsstelle nach Art. 28 Abs. 2, Art. 29 Abs. 3 und Art. 32 Abs. 1 der EU-DLR wurde noch keine Vorwarnung veranlasst. Der sogenannte „Vorwarnungsmechanismus“ (bei ernster Gefahr für die Gesundheit oder die Sicherheit von Personen oder die Umwelt durch einen Dienstleistungserbringer) wurde von deutschen Behörden bisher nicht genutzt. Auch aus den EU-Mitgliedstaaten trafen bisher keine Vorwarnungen ein. Durch die zuständigen Behörden (Landkreise und kreisfreie Städte, Kammern) wurden 14 Anfragen an die EU-Mitgliedstaaten über das Modul IMI-EU-DLR gestellt.

Bei der IT-Umsetzung im LRZ besteht allerdings nach Einschätzung des Landesbeauftragten hinsichtlich des Betriebskonzepts EU-DLR und der Aufgabenbeschreibung (Vers. 0.8, 2. Dezember 2009) Handlungsbedarf. Das betrifft vor allem das noch fehlende Sicherheitskonzept, welches die Grundlage für die Umsetzung von Datenschutz und Datensicherheit bilden soll, im Betriebskonzept aber nur auf dem Papier existiert. Hier sieht der Landesbeauftragte auch das zuständige Ministerium des Innern als Auftraggeber in der Pflicht. Als eigentlicher

Betreiber des EA-Portals des Landes hat es die Betreuung des Portals durch das LRZ zusammen mit Fremdfirmen konzipiert. Beim Betrieb und der Wartung des modular aufgebauten Gesamtsystems tragen auch diese externen Dritten für einzelne der von ihnen betreuten Komponenten die Verantwortung für die Systemsicherheit. Inwieweit bei der Vertragsgestaltung mit diesen externen Anbietern datenschutzrechtliche Belange ausreichend (auch vertraglich) berücksichtigt wurden, ist dem Landes-beauftragten nicht bekannt. Zu verweisen ist hier in erster Linie auf die Regelungen zur Auftragsdatenverarbeitung und deren Beachtung (§ 8 DSG-LSA).

Auch wenn aus nachvollziehbaren zeitlichen Gründen und Zwängen bei der technischen Umsetzung der EU-DLR die Ausarbeitung eines umfassenden Sicherheitskonzepts zum damaligen Zeitpunkt zurückgestellt wurde, ist das nunmehr nachzuholen. Der Landesbeauftragte ist bereit, das Ministerium des Innern und das LRZ bei Bedarf dabei zu unterstützen. Gleiches gilt für die Ausarbeitung der Verordnung nach § 6 Abs. 2 EAG LSA durch das Wirtschaftsministerium.

### 4.7 Binnenmarktinformationssystem IMI – Sachstand

Neben der Umsetzung der **Richtlinie 2005/36/EG** des Europäischen Parlaments und des Rates vom 7. September 2005 über die Anerkennung von Berufsqualifikationen (ABl. EU Nr. L 255 S. 22) (**Berufsanerkennungsrichtlinie**) wird dieses System (IMI-Modul EU-DLR) mit Beginn des Jahres 2010 ebenfalls zum Informationsaustausch bei der Umsetzung der **Richtlinie 2006/123/EG** des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über die Dienstleistungen im Binnenmarkt (ABl. EU Nr. L 376 S. 36) (**EU-Dienstleistungsrichtlinie – EU-DLR**) in Sachsen-Anhalt durch die zuständigen Behörden genutzt.

Der Landesbeauftragte hatte in seinem IX. Tätigkeitsbericht (Nr. 4.8) die Probleme bei der Umsetzung des Binnenmarktinformationssystems IMI (Internal Market Information System) dargestellt. Die Europäische Kommission (KOM) betreibt dieses System selbst und stellt es den EU-Mitgliedsstaaten kostenlos zur Verfügung. Grundsätzlich soll es die Verwaltungszusammenarbeit in der Europäischen Union (EU) wesentlich vereinfachen und verbessern und zukünftig für weitere Rechtsbereiche genutzt wer-den. Unterschiedliche Auffassungen zur Notwendigkeit einer spezifischen Rechtgrundlage für das IMI bestehen aber zwischen der KOM und den Datenschutzbeauftragten. Die Forderung, dieses komplexe Informationssystem zur europäischen Verwaltungszusammenarbeit auf eine tragfähige Rechtsgrundlage zu stellen, besteht nach wie vor (IX. Tätigkeitsbericht, Anlage 14, Beschluss der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 4. April 2009 zur Umsetzung des Binnenmarktinformationssystems IMI).

Nach der Stellungnahme des Europäischen Datenschutzbeauftragten und in Abstimmung mit den Datenschutzbeauftragten und der Art. 29 Arbeitsgruppe hatte sich die KOM auf einen Kompromiss verständigt, der mit Hinblick auf die fehlende Rechtsgrundlage für das IMI ein schrittweises Vorgehen zur Lösung dieses Problems vorsah. Der Landesbeauftragte hatte die damalige Situation mit dem Ministerium für Wirtschaft und Arbeit im April 2009 erörtert und als datenschutzrechtliche Grundlage für die Erhebung und Verarbeitung personenbezogener Daten im IMI-System eine modifizierte informierte Einwilligung gemäß § 4 Abs. 2

DSG-LSA empfohlen. Dieser Empfehlung war das Ministerium für Wirtschaft und Arbeit gefolgt und hatte alle beteiligten IMI-Behörden des Landes entsprechend informiert.

Bis zum Ende 2009 erfolgten danach durch die EU-Mitgliedsstaaten aufgrund der im IMI gesammelten Erfahrungen Rückmeldungen zu den Datenschutzleitlinien der KOM vom 23. März 2009 und zu deren praktischer Anwendbarkeit. Die Landesdatenschutzbeauftragten hatten in einer gemeinsamen Stellungnahme nachdrücklich ihre grundsätzliche Forderung bekräftigt, dass der Betrieb des IMI auf eine ausreichende Rechtsgrundlage zu stellen ist. Vorsorglich wurde in diesen Zusammenhang nochmals in Bezug auf die neuen Vorschriften des Verwaltungsverfahrensgesetzes (VwVfG) zur europäischen Verwaltungszusammenarbeit festgestellt, dass die Amtshilfebestimmungen der §§ 8a ff. VwVfG keine datenschutzrechtliche Befugnisnorm darstellen. Die damaligen Datenschutzleitlinien der KOM verwiesen selbst mit Hinweis auf Artikel 7 c) und e) der Richtline 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 24. Oktober 1995 (EU-DSRL) auf notwendige Rechtsgrundlagen für eine Datenverarbeitung.

Hatte sich die KOM in ihrem Bericht über den Stand des Datenschutzes im IMI vom 22. April 2010 noch zufrieden bezüglich der dazu getroffenen Regelungen gezeigt, ist nunmehr Bewegung in die Diskussion um eine tragfähige Rechtsgrundlage gekommen. Auslöser könnte u. a. die Anfrage des Bundesratsbeauftragten eines Landes in der beratenden Arbeitsgruppe der KOM zum IMI-Modul der EU-DLR an den Vorsitzenden des Arbeitskreises Grundsatzfragen der Verwaltungsmodernisierung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Juni 2010 gewesen sein, mit der gleichzeitigen Bitte um Unterstützung bei der Beantwortung der datenschutzrelevanten Fragen.

Der Arbeitskreis Grundsatzfragen der Verwaltungsmodernisierung hat diesen Fragenkomplex auf seiner Sitzung im September 2010 behandelt und dem Bundesratsbeauftragten im Oktober 2010 geantwortet.

Für eine Vorabkontrolle (gem. Art. 20 EU-DSRL) bestehen in den Länder unterschiedliche Regelungen. Bei einer beabsichtigten gesetzlich verbindlichen Einführung des IMI-Systems wäre aber nach Meinung des Landesbeauftragten diese Vorabkontrolle grundsätzlich entbehrlich.

Grundsätzlich bestehen beim IMI keine Zweifel an der Datenschutzkonformität in technischer Hinsicht. Mit Hinweis auf die bisher nicht erfolgte Bereitstellung eines Sicherheitskonzepts für IMI, seiner technischen Verfahrensbeschreibung sowie von Testergebnissen der KOM an die Mitgliedsländer bzw. die Datenschutzbeauftragten hat sich der Arbeitskreisvorsitzende an den Europäischen Datenschutzbeauftragten (EDSB) gewandt und um Unterstützung bzw. Vermittlung gebeten. Die KOM verweist im Bezug auf das IMI-System darauf, nur der datenschutzrechtlichen Kontrolle des EDSB zu unterliegen.

Weiter wurde in der Antwort klargestellt, dass die §§ 8a ff. VwVfG allgemeine Verfahrensbestimmungen und eben keine Befugnisnorm für eine Datenverarbeitung darstellen. Das Verfahren IMI würde bei einer innerstaatlichen Anwendung, für die es in anderen Bundesländern scheinbar Überlegungen gibt – in Sachsen-Anhalt nach Auskunft des Ministeriums für Wirt-

schaft und Arbeit aber nicht – den durch die Datenschutzgesetze in den Ländern und beim Bund vorgegebenen Prüfbestimmungen unterliegen.

In der nunmehr dem Landesbeauftragten vorliegenden Mitteilung der Europäischen Kommission vom 21. Februar 2011 bezüglich einer Strategie für den Ausbau und die Weiterentwicklung des Binnenmarktinformationssystems IMI ist erkennbar, dass die KOM damit ihre Auffassung zur Notwendigkeit einer eigenen Rechtsgrundlage für das IMI geändert hat und beabsichtigt, noch im Jahr 2011 ein Rechtsinstrument vorzuschlagen.

Der Landesbeauftragte wird die Entwicklung weiter verfolgen und dabei den bewährten Kontakt zum Wirtschaftsministerium zur gegenseitigen Information und zur Erörterung datenschutzrechtlicher Fragen halten.

### 4.8 De-Mail

Mit dem De-Mail-Gesetz vom 28. April 2011 (BGBl. I S. 666) soll der Aufbau einer Infrastruktur für eine sichere und vertrauensvolle elektronische Kommunikation im Rechts- und Geschäftsverkehr vorangetrieben werden. Diese dient der Verbesserung des Sicherheitsniveaus gegenüber herkömmlichen E-Mails, von denen derzeit mehr als 95% unverschlüsselt und abfangbar transportiert werden. Bereits im IX. Tätigkeitsbericht (Nr. 4.11) wurden erste Entwicklungen der De-Mail aufgegriffen. Im Februar 2009 wurde mit dem Bürgerportalgesetz die Einrichtung einer sicheren, vom Bundesamt für Sicherheit in der Informationstechnik (BSI) überwachten, Kommunikationsplattform und deren Nutzung durch den Bürger unter Zuhilfenahme des neuen Personalausweises (nPA) beschlossen. Die Bundesregierung legte im Oktober 2010 einen Entwurf für ein "Gesetz zur Regelung von De-Mail-Diensten" vor, welches den Rechtsrahmen für private De-Mail-Anbieter regeln sollte. Der Bundesrat nahm zum Jahresende Stellung und forderte umfangreiche Verbesserungen, welche hauptsächlich den Datenschutz betrafen. Die Forderungen werden vom Landesbeauftragten unterstützt.

Das wichtigste Merkmal einer De-Mail ist die Verbindlichkeit. Bei der Beantragung eines De-Mail-Kontos wird die Identität des Antragstellers überprüft. Da Absender und auch Empfänger eindeutig identifizierbar sind, ist der systematische Missbrauch wie etwa das Versenden von Spam oder Nachrichten mit gefälschtem Absender unmöglich. Dennoch gibt es verschiedene Kritikpunkte. Nicht alle sind in jedem Fall relevant. So wird häufig kritisiert, dass De-Mail keine anonyme Nutzung zulässt. Man muss dabei bedenken, dass das System der Kommunikation mit Behörden dient, welche ihre Antragsteller in der Regel kennen müssen, um auf Anfragen sinnvoll eingehen zu können. Anonyme Anfragen sind insbesondere für einfache Auskünfte vorstell-bar, jedoch ist eine vollständig anonyme Einlieferung von De-Mails wie im E-Mail-System schon aus Gründen des Spamschutzes nicht möglich. Insofern muss der Nutzer sich darüber im Klaren sein, dass De-Mail eben kein absolut anonymes Netzwerk ist. Der Landesbeauftragte hält die Möglichkeit des Versendens von anonymen Mitteilungen von einem De-Mail-Postfach aus den-noch für sinnvoll. Hauptkritikpunkt des De-Mail-Systems ist, dass De-Mails zwar verschlüsselt transportiert und ebenso auf den Servern der Anbieter gelagert werden, zur Viren- und Spamprüfung aber kurzzeitig entschlüsselt werden sollen. Das ist weder notwendig noch datenschutzgerecht, da ein missbräuchlicher Zugriff auf die De-Mails so nicht ausgeschlossen werden kann.

Leider konnte sich nicht auf ein einheitliches Kennzeichen von De-Mail-Adressen geeinigt werden. Der Dienst soll anhand der verwendeten De-Mail-Adresse sowohl auf den Anbieter als auch auf die De-Mail-Konformität hin-weisen. Die Aufnahme des Anbieternamens in die Adresse wird den Transfer von De-Mail-Konten zu anderen Anbietern verhindern bzw. einen Umzug von einem Anbieter zu einem anderen Anbieter erheblich erschweren. Eine sinn-volle Regelung wäre es, De-Mail-Adressen zentral in anbieterneutraler Form zuzuteilen. Dies würde auch eine dauerhafte Identifikation des Anwenders mit „seiner“ Adresse gewährleisten können. Die vom Bundesrat geforderte Abstimmung des Verfahrens mit dem Signaturgesetz ist obligatorisch. Hier muss eine derartige Umsetzung realisiert werden, welche die bestehenden Kryptografieverfahren nicht verwässert, gleichzeitig aber die Rechtsfolgen für die De-Mail-Nutzung klar definiert. Eine Portierbarkeit von Dokumenten zwischen den einzelnen Diensteanbietern ist wünschenswert. Auch die vom Bundesrat geforderte Verpflichtung akkreditierter Diensteanbieter, den Zugriff des De-Mail-Nutzers auf sein Konto durch eine Anmeldung mit mindestens zwei voneinander unabhängigen Sicherungsmitteln sicher zu gestalten, statt nur auf die gängige Verwendung von Benutzername und Passwort zu setzen, ist als Stand der Technik unumgänglich. Das wäre mit Nutzung des neuen Personalausweises sogar einfach realisierbar.

Offen ist derzeit insbesondere die Frage der zwingenden Erforderlichkeit einer **Ende-zu-Ende-Verschlüsselung**. Der jeweilige Schutzbedarf personenbezogener Daten ist immer wirksam mittels technisch-organisatorischer Maßnahmen zu gewährleisten. Im Einzelfall sind damit auch De-Mails durch geeignete Maßnahmen sicherheitstechnisch aufzuwerten, sofern das bereits höhere De-Mail-Sicherheitsniveau nicht dem den Daten angemessenen Schutzbedarf entspricht. Damit kann für die Übermittlung von Daten mit höherem Schutzbedarf auch eine Ende-zu-Ende-Verschlüsselung erforderlich werden.

Bleibt hierzu noch die Betrachtung der Realisierbarkeit. Die Begründung, dass der Verzicht auf eine durchgehende Ende-zu-Ende-Verschlüsselung aus Gründen des Virenschutzes und der dazu notwendigen Entschlüsselung notwendig sei, ist nicht haltbar. Auch das BSI weist darauf hin, dass eine Ende-zu-Ende-Verschlüsselung bei De-Mail einfach realisierbar ist und die Schlüssel sogar einfach im öffentlichen Verzeichnisdienst hinterlegt werden können. Ebenso könnte eine Virenprüfung auf dem Rechner des De-Mail-Anbieters zum Zeitpunkt des Abrufs der De-Mail bei Eingabe eines Passworts zum geheimen Benutzerschlüssel erfolgen und die De-Mail anschließend nur per Secure Sockets Layer (SSL) bzw. Transport Layer Security (TLS) transportverschlüsselt übertragen werden. Das wäre strenggenommen keine richtige Ende-zu-Ende-Verschlüsselung, weil der Schlüssel auch hinterlegt werden würde, aber das würde den Zugriff auf die E-Mails nicht völlig offen lassen, da er jeweils gezielt mit einer Anmeldung des Nutzers am System verbunden und so freigeschaltet werden müsste. Vorteil wäre, dass die Virenprüfung jeweils mit aktuellen Signaturen erfolgen würde. Die Sicherheit der De-Mail wäre immer noch direkt abhängig vom Vertrauensstatus des Providers, also ob Passwörter im Profil hinterlegt werden oder sofort nach Ablauf der Sitzung wieder vergessen werden oder der Provider gar anderen Behörden Zugriff gewährt. Aber ist ein Mehr an Sicherheit gegenüber dem Provider im WebMail-Kontext überhaupt realisierbar? Diese Variante böte zusätzlich die Möglichkeit einer echten Ende-zu-Ende-Verschlüsselung, wenn sich der kryptografische Schlüssel im Hoheitsbereich des Nutzers befindet. Dann wäre kein Virenschutz und ggf. kein Zugriff per Web-Schnittstelle möglich, aber das wäre in diesem Zusammenhang auch gar nicht erforderlich, da der Nutzer entweder weiß, was er tut (wenn er manuell verschlüsselt) oder die entsprechenden Daten in seinem E-Mail-Programm

hinterlegt hat und auch in diesem Fall das System des Nutzers für Schutz-maßnahmen verantwortlich ist. Technisch denkbar wäre auch, dass der De-Mail-Ersteller oder ein von diesem beauftragter Dritter kryptografisch beglaubigt, dass die De-Mail nur bestimmte Inhalte aufweist; also beispielsweise nur Textzeichen enthält, oder dass eine Grafik oder eine PDF-Datei mit einem bestimmten Generator in einem bestimmten Format gespeichert wurde. Damit könnte ein Finanzamt z. B. Bescheide herausgeben, die nicht entschlüsselt werden müssten, da eine separate Signatur existiert, die die Unbedenklichkeit des verschlüsselten Inhalts bescheinigt.

Aus Spamschutzgründen auf Sicherheit zu verzichten, ist ebenso wenig vernünftig. Da sowohl die Identität des Nutzers als auch des Dienstleisters, der De-Mail ins System eingespeist hat, bekannt sind, sollte es ohne Mehraufwand möglich sein, möglichen Spam von Dritten bspw. durch Filterung auch ohne Entschlüsselung Einhalt zu gebieten. Auch Behörden-Spam darf es nicht geben. Dieser wäre bei Auftreten sofort – ggf. auch administrativ – zu unterbinden.

Eine Nutzung von Ende-zu-Ende-Verschlüsselung ist ohne Komforteinbußen auch für Nutzer, denen die Möglichkeit zu vorbereitenden Aktivitäten auf den eigenen Rechnern fehlt, durch die De-Mail-Dienstleister ohne Mehraufwand anbietbar. Selbst einer echten Ende-zu-Ende-Verschlüsselung steht prinzipiell nichts im Wege, sofern der Nutzer mit der ggf. nicht möglichen und bei entsprechenden Zusatzmaßnahmen auf Absender- und Providerseite auch nicht erforderlichen Spam- und Virenprüfung einverstanden ist. Die Schlüssel könnten einfach im Verzeichnisdienst hinterlegt werden. Damit gibt es aus technischer Sicht gar keinen Bedarf, ein niedrigeres Sicherheitsniveau als Ende-zu-Ende-Verschlüsselung überhaupt in Erwägung zu ziehen. Hier sind die De-Mail-Anbieter in der Pflicht, entsprechende Angebote bereitzustellen, der Gesetzgeber sollte Ende-zu-Ende-Verschlüsselung wie beschrieben als Mindeststandard vorschreiben.

Anbieter von De-Mail sind derzeit 1&1, GMX.de, Web.de, die Deutsche Post AG und die Deutsche Telekom. Die Deutsche Post AG stieg aus dem De-Mail-Projekt aus, baut jedoch mit dem E-Post-Brief ein ebensolches System auf, welches später auch eine Zulassung als De-Mail-Dienstleister erhalten soll.
Das **De-Mail-Gesetz** wurde im **März 2011** trotz heftiger Kritik mit nur wenigen Änderungen beschlossen. Die geforderte Ende-zu-Ende-Verschlüsselung wurde nicht aufgegriffen. Jedoch soll darüber informiert werden. Auch die Entscheidung zur Datenbereitstellung in einem Verzeichnisdienst liegt nun beim Nutzer. Der Bürger hat des Weiteren ein Wahlrecht, ob er die De-Mail-Adresse zur Nutzung freigeben will oder nicht. Die Präsenz der Adresse im Verzeichnisdienst ist keine Zustimmung zur Nutzung durch öffentliche Stellen.

Stellen, die einen De-Mail-Zugang anbieten, sollten auch einen Ende-zu-Ende verschlüsselten Zugang vorsehen. Schließlich entscheidet allein der Nutzer durch Kontaktaufnahme, welches Sicherheitsniveau angemessen ist. Ohne Wahlmöglichkeit würde dieser ggf. zu einer zu niedrigen Stufe gezwungen werden. Das darf aber nicht sein. Aus datenschutzrechtlicher Sicht ist eine Ende-zu-Ende-Verschlüsselung bei der Kommunikation die beste Lösung.

Als Fazit lässt sich sagen, dass De-Mail eine sinnvolle Ergänzung zu herkömmlichen E-Mails und Briefen darstellt. Sie ist jedoch keine 1:1-Nachbildung des Briefes und somit auch kein in jedem Fall nutzbarer Ersatz für diesen. Die neu gewonnenen Vorteile der De-Mail, wie eine

eindeutige Identifizierbarkeit aller Beteiligten, sind gleichzeitig auch die Nachteile und es ist sinnvoll, nicht alle Möglichkeiten moderner Datenverarbeitung zu erlauben und umzusetzen. De-Mail kann zu Datenschutzverletzungen führen. Ein normaler Brief in der Wohnung ist besser vor dem Zugriff Dritter geschützt als eine De-Mail. Eine solche Zugriffsmöglichkeit auf De-Mails beim Anbieter bedeutet auch den Verzicht auf Rechte des Betroffenen, die bisher nicht zur Diskussion standen.