



Datum
17.08.2010

**Stellungnahme der Landesregierung zum 8. Tätigkeitsbericht des
Thüringer Landesbeauftragten für den Datenschutz
für den Berichtszeitraum:
1. Januar 2008 bis 31. Dezember 2009**

Gemäß § 40 Abs. 1 des Thüringer Datenschutzgesetzes (ThürDSG) hat der Thüringer Landesbeauftragte für den Datenschutz (TLfD) seinen Tätigkeitsbericht für den Zeitraum 2008/2009 abgegeben. Die Thüringer Landesregierung hat hierzu nach § 40 Abs. 2 ThürDSG Stellung zu nehmen, wobei sich diese Stellungnahme im Wesentlichen auf einzelne Ergänzungen bzw. die Erläuterung von Problemen, zu denen bislang kein Konsens gefunden werden konnte, beschränkt.

Die vorliegende Stellungnahme orientiert sich an der Systematik des Tätigkeitsberichts und verwendet die vom TLfD gebrauchten Abkürzungen.

I. Allgemeines

Seit dem letzten Tätigkeitsbericht des TLfD haben die Belange des Datenschutzes im öffentlichen Bewusstsein noch mehr an Bedeutung gewonnen. Dies zeigt sich insbesondere an großen Themen wie der Vorratsdatenspeicherung, SWIFT, ELENA oder Google Street View, die regelmäßig präsent sind und schon auf Grund ihrer Tragweite in der aktuellen Debatte einen bedeutsamen Platz einnehmen. Die Landesregierung begrüßt diese Entwicklung und setzt sich auch über die Grenzen Thüringens hinaus für die Belange des Datenschutzes ein.

Der Freistaat Thüringen hat unter anderem im Bundesrat durch einen gemeinsamen Antrag mit einer Vielzahl anderer Länder auf die Aufnahme gesetzlicher Regelungen für Internet-Dienste wie Google Street View in das Bundesdatenschutzgesetz (BDSG)

hingewirkt und so klar Position zum Schutz des Grundrechts der Bürger auf informationelle Selbstbestimmung, wie es in Art. 6 Abs. 2 der Thüringer Verfassung (ThürVerf) ausdrücklich aufgeführt und dem Schutz durch den Thüringer Landesbeauftragten für den Datenschutz nach Art. 69 ThürVerf unterstellt ist, bezogen.

Auch für den Bereich der Datenverarbeitung durch öffentliche Stellen im Bereich der Sicherheitspolitik und des „eGovernment“ haben die Belange des Datenschutzes weit reichende Bedeutung. Sie geben wesentliche Maßstäbe vor, die bei staatlichem Handeln zu beachten und mit den Erfordernissen des Sicherheitsrechts sowie der Effektivität staatlichen Handelns in Einklang zu bringen sind.

Das Bundesverfassungsgericht spricht z. B. in seiner Entscheidung zur Vorratsdatenspeicherung vom 2. März 2010 (1 BvR 256/08) von einer „diffusen Bedrohlichkeit“ durch die staatliche Datenverarbeitung, der durch hohe Anforderungen an Transparenz und Überprüfbarkeit Rechnung getragen werden muss.

Gleiches gilt mit Blick auf die Übermittlung und Auswertung von Banktransaktionsdaten zur Bekämpfung des internationalen Terrorismus (SWIFT-Abkommen). Die Landesregierung hat hier über einen gemeinsamen Bundesratsantrag mit dem Freistaat Bayern darauf hingearbeitet, dass das neue Abkommen höhere Datenschutzstandards wahrt, transparenter ist und somit eine deutlich europäischere Handschrift trägt als sein Vorgänger-Abkommen.

Neben den Sicherheitsinteressen, die mit dem Recht auf informationelle Selbstbestimmung in Einklang gebracht werden müssen, begegnet auch die Datenverarbeitung durch öffentliche Stellen mit dem Fortschreiten technischer Entwicklungen kontinuierlich neuen Herausforderungen. Diese gilt es zu erkennen und anzunehmen, um auch hier dem Datenschutz den Stellenwert zu sichern, den er benötigt.

Die wohl wichtigsten Themen, die mit fortschreitenden technischen Möglichkeiten zu Tage treten, stellen hier die Datenverarbeitungsmöglichkeiten des Internet und Fragen der Videoüberwachung dar. Gerade Fragen der Videoüberwachung bilden wie bereits im letzten Bericht des TLfD einen Schwerpunkt der Kontrolltätigkeit, wobei der TLfD das Hauptaugenmerk seiner Prüfung im Berichtszeitraum 2008 und 2009 auf den kommunalen Bereich gelegt hat.

Die öffentliche Beachtung der angesprochenen „großen Themen“ darf aber nicht vergessen machen, dass auch sonst die Belange des Datenschutzes von Bedeutung sind. Die Landesregierung hat sich deshalb eingehend mit dem 8. Tätigkeitsbericht des TLfD befasst. Die Beanstandungen und Hinweise wurden ausgewertet und finden bei der weiteren Arbeit Beachtung.

II. Zum Tätigkeitsbericht im Einzelnen

zu 3.3 Polizeilicher Datenaustausch in der EU nicht immer auf höchstem Datenschutzniveau

Das Bundesministerium der Justiz (BMJ) hat zwischenzeitlich einen Arbeitsentwurf (Stand: 8. April 2010) für ein Gesetz zur Vereinfachung des Austausches von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedsstaaten der Europäischen Union zur Umsetzung des Rahmenbeschlusses 2006/960/JI vorgelegt.

zu 5.1 Kommunalkontrollen: Datenschutz – auch das noch!

Die Verpflichtung der Gemeinden und Gemeindeverbände zur Sicherstellung des Datenschutzes nach § 34 ThürDSG ist eine Aufgabe des eigenen Wirkungskreises und damit eine Pflichtaufgabe, die diese in eigener Verantwortung zu erfüllen haben. Sie haben u. a. einen Beauftragten für den Datenschutz nach § 10 a ThürDSG zu bestellen.

Auf Grund der gem. Art. 28 Abs. 2 Grundgesetz (GG) und Art. 91 ThürVerf verfassungsrechtlich garantierten kommunalen Selbstverwaltung stehen der Landesregierung in diesem Bereich nur begrenzte Einwirkungsmöglichkeiten zur Verfügung. Aus der Einordnung des Datenschutzes als Aufgabe der Kommunen im eigenen Wirkungskreis folgt, dass sich die staatliche Aufsicht über die Gemeinden und Gemeindeverbände im Bereich des Datenschutzes auf die Rechtsaufsicht i. S. des § 117 Abs. 1 Thüringer Kommunalordnung (ThürKO) beschränkt. Die vom TLfD ausgesprochenen Beanstandungen können die Aufsichtsbehörden deshalb lediglich veranlassen, innerhalb der Grenzen des rechtsaufsichtlichen Instrumentariums tätig zu werden, wenn die Kommunen berechtigten Beanstandungen nicht abhelfen.

Verstoßen die Kommunen gegen die ihnen nach dem ThürDSG obliegenden Verpflichtungen, wird dies nach § 39 Abs. 1 ThürDSG vom TLfD beanstandet. Die Pflicht zur Beseitigung berechtigter Beanstandungen liegt dann aber bei der verantwortlichen Stelle selbst. Die Aufsichtsbehörde ist lediglich zu informieren. Erst wenn nichts geschieht, kann der TLfD nach § 39 Abs. 2 ThürDSG auch die Aufsichtsbehörde auffordern.

Für das Handeln der Aufsichtsbehörden gilt grundsätzlich, dass sie die Gemeinden und Landkreise bei der Erfüllung ihrer Aufgaben gem. § 116 ThürKO beraten, fördern und unterstützen sollen.

Sie können darüber hinaus nach § 120 Abs. 1 ThürKO rechtswidrige Beschlüsse, Anordnungen und sonstige Maßnahmen der Gemeinde oder des Landkreises beanstanden und verlangen, dass diese aufgehoben werden. In eng begrenzten Ausnahmefällen besteht auch die Möglichkeit der Ersatzvornahme nach § 121 Abs. 1 ThürKO. Ein Weisungsrecht, wie es der Fachaufsicht im übertragenen Wirkungskreis nach § 120 Abs. 2 ThürKO zukommt, hat die Rechtsaufsicht jedoch nicht, sodass der Landesregierung insgesamt nur beschränkte Einwirkungsmöglichkeiten zur Verfügung stehen.

zu 5.5 Auskunftsrecht des Gemeinderats bzw. eines seiner Mitglieder zu privatrechtlichen Verträgen

Die Auffassung des TLfD, dass die im betreffenden Fall begehrte Auskunft nicht nach § 22 Abs. 3 ThürKO zu erteilen ist, ist zutreffend.

Die zusammenfassende Aussage, dass eine Offenbarung des Inhalts privatrechtlicher Verträge gegenüber einem Gemeinderatsmitglied unzulässig erfolgt, vernachlässigt nach Auffassung der Landesregierung jedoch die Regelungen des Thüringer Informationsfreiheitsgesetzes (ThürIFG), die neben der ThürKO als Rechtsgrundlage eines Auskunftsverlangens in Betracht kommen.

zu 5.9 ePass und neuer Personalausweis (nPA)

Der TLfD bemängelt, dass im Antragsverfahren für den neuen elektronischen Reisepass Fingerabdruckdaten bis zur Passübergabe an den Antragsteller vor Ort mehrere Wochen unverschlüsselt in den Kommunen und Rechenzentren vorliegen, da „in Thüringen“ entsprechende verbindliche Vorgaben fehlen.

In diesem Zusammenhang ist klarzustellen, dass diese verbindlichen Vorgaben nicht nur in Thüringen, sondern auch in den anderen Bundesländern fehlen. Die Zuständigkeit für die Erarbeitung derartiger Richtlinien liegt beim Bund und nicht bei den Ländern. Der TLfD sieht daher zwar zu Recht Handlungsbedarf, diesem muss allerdings der Bund nachkommen.

zu 5.10 Unzulässige Datenübermittlung an die Presse zu einem akademischen Grad

Die Darstellung des TLfD enthält kommunalverfassungsrechtliche Aussagen, die missverstanden werden können.

Es ist zutreffend, dass das Meldewesen zum übertragenen Wirkungskreis gehört und eine Befassung des Kreistags und seiner Ausschüsse mit diesen Angelegenheiten nicht zulässig ist, da es sich um Aufgaben des Landrats gem. § 107 Abs. 2 Nr. 2 ThürKO handelt. Allerdings erscheint die Aussage auf Seite 50, Mitte, „die Datenübermittlung des Bürgermeisters an den Landkreis“ sei „ohne Rechtsgrund“ erfolgt, rechtlich problematisch.

Im Bericht wird dargelegt, dass der Bürgermeister die Aufsichtsbehörde informiert hat. Nach § 111 Abs. 2 i. V. m. § 117 Abs. 2 ff. ThürKO ist das Landratsamt als untere Verwaltungsbehörde Fachaufsichtsbehörde in den Angelegenheiten des übertragenen Wirkungskreises und somit auch des Meldewesens. Das Landratsamt ist somit berechtigt und gegebenenfalls sogar verpflichtet, in diesen Angelegenheiten die Gemeindebehörde – auch in der Handhabung des Verwaltungsermessens – zu beraten und zu überwachen. Der Bürgermeister war somit berechtigt, in dieser Angelegenheit an die Fachaufsichtsbehörde zu berichten. Die Datenübermittlung erfolgte daher nicht ohne Rechtsgrund.

Zudem enthält die Darstellung auf Seite 50 gegen Ende des ersten Absatzes die Aussage "Auch gehören Auskunftserteilungen aus dem Melderegister nicht zu den Aufgaben eines Bürgermeisters, Rechtsamtes oder eines Pressesprechers." Diese

Behauptung ist unzutreffend, da der Bürgermeister gemäß § 29 Abs. 1 ThürKO die Gemeindeverwaltung leitet und die Geschäftsverteilung bestimmt. Wie jeder Behördenleiter ist er berechtigt, alle Angelegenheiten, die in der Gemeindeverwaltung bearbeitet und entschieden werden, selbst zu erledigen oder im Rahmen der Geschäftsverteilung zuzuweisen. Dies gilt auch für Alltagsgeschäfte im Bereich der laufenden Verwaltung. Somit ist er berechtigt, Angelegenheiten aus einer Organisationseinheit der Gemeindeverwaltung einer anderen Organisationseinheit (auch dem Rechtsamt oder dem Pressesprecher) zuzuordnen, solange diese wie das Melderecht dem übertragenen Wirkungskreis und damit dem Verantwortungsbereich des Bürgermeisters unterliegen.

zu 6.4 Nutzung von PC-Protokolldaten von Mitarbeitern

Die Empfehlungen des TLfD zur Nutzung von PC-Protokolldaten wurden beispielsweise im Geschäftsbereich des Thüringer Innenministeriums (TIM) umgesetzt. Die private Nutzung des dienstlichen Internetzugangs ist hier in einer Rahmendienstvereinbarung über die Nutzung des zentralen Internetzugangs und des Mailsystems Corporate Network (CN) des Freistaats Thüringen und einer Ergänzenden Dienstvereinbarung mit dem Örtlichen Personalrat geregelt. Diese sieht eine protokollierte Erfassung von Verkehrsdaten vor, die lediglich bei konkretem Verdacht auf einen Missbrauch des Internetzugangs in einem abgestuften Verfahren unter Beteiligung des Personalrates und des behördlichen Datenschutzbeauftragten personenbezogen ausgewertet werden darf.

zu 7.1 Novellierung des Polizeiaufgabengesetzes (Teil II)

Die Landesregierung sieht wie der TLfD die Notwendigkeit einer Überarbeitung des Polizeiaufgabengesetzes unter Berücksichtigung der jüngeren Rechtsprechung. Diese Novellierung ist deshalb bereits im Koalitionsvertrag vom Oktober 2009 (Zeilen 2029 bis 2033) vereinbart.

Mit Blick auf die zukünftige Regelung der Vorratsdatenspeicherung muss außerdem neben den bundesrechtlichen Vorgaben die Entwicklung des europarechtlichen Rahmens, der nach dem Inkrafttreten des Vertrags von Lissabon derzeit von der Kommission auf seine Vereinbarkeit mit der Europäischen Grundrechtecharta überprüft wird, beobachtet werden.

Im Hinblick auf die Befugnisse des Verfassungsschutzes teilt die Landesregierung die Auffassung des TLfD hingegen nicht.

Die materiell-rechtliche Regelungszuständigkeit für die Telekommunikationsüberwachung durch die Verfassungsschutzbehörden liegt beim Bundesgesetzgeber. Dieser hat hier mit § 3 a des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10) eine Bestimmung zum „Schutz des Kernbereichs privater Lebensgestaltung“ eingefügt. Den Ländern obliegt lediglich die Ausführung des G 10 durch die Ausgestaltung von Verfahrensregelungen. Die Befugnis zur Wohnraumüberwachung ist im Thüringer Verfassungsschutzgesetz

(ThürVSG) nicht (mehr) vorhanden, so dass spezielle Regelungen zum Kernbereichsschutz hier nicht erforderlich sind.

Die Forderung, den Kernbereichsschutz auch für solche Maßnahmen des Verfassungsschutzes zu regeln, die verdeckte Datenerhebungen durch den Verfassungsschutz außerhalb von Wohnungen oder im Rahmen des G 10-Anwendungsbereichs betreffen, wird ebenso abgelehnt.

Wohnraum- und Telekommunikationsüberwachung besitzen auf Grund des speziell betroffenen Schutzbereichs des Art. 13 GG bzw. des Art. 10 GG eine besondere Eingriffsqualität und -intensität, die sich gegenüber sonstigen Arten der verdeckten Nachrichtenbeschaffung heraushebt. Somit können die Maßstäbe, die das Bundesverfassungsgericht insbesondere zur Wohnraumüberwachung, aber auch zur Telekommunikationsüberwachung oder zur Online-Durchsuchung aufgestellt hat, nicht ohne Weiteres auf alle anderen Maßnahmen der verdeckten Nachrichtenbeschaffung übertragen werden. Vielmehr ist nach dem jeweiligen Schutzbereich zu differenzieren. Vertrauliche Kommunikation, die nicht dem Schutzbereich des Art. 13 GG, des Art. 10 GG oder des durch das Bundesverfassungsgericht neu geschaffenen Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme unterfällt, wird daher durch den zu beachtenden Verhältnismäßigkeitsgrundsatz in § 4 ThürVSG nicht nur in ausreichendem Maße geschützt, sondern ermöglicht außerdem einzelfallgerechtes Vorgehen, ohne schematische Lösungen vorzugeben.

zu 7.5 Fehlende Rechtsgrundlage für INPOL-Dateien

Am 8. Juni 2010 ist die „Verordnung über die Art der Daten, die nach den §§ 8 und 9 des Bundeskriminalamtgesetzes gespeichert werden dürfen (BKA-Daten-Verordnung – BKADV)“ im Bundesgesetzblatt (BGBl. I S. 716) verkündet worden.

Sie trat am 9. Juni 2010 in Kraft und das Bundesverwaltungsgericht hat sich in seiner Entscheidung in dem Verfahren Az. 6 C 5.09 bereits auf die Verordnung gestützt.

zu 7.6 Zugriffsprotokollierung und Kontrolle bei polizeilichen Dateien

Das TIM hat den Aufwand, das Datenfeld „Veranlasser“ als Pflichtfeld bei INPOL- und ZEVIS-Abfragen auszugestalten, geprüft. Der relativ komplexe Entwicklungsaufwand, die lange Dauer einer technischen Verfahrensänderung und der Umstand, dass eine Vielzahl derartiger Abfragen nicht auf fremde Veranlassung hin getätigt werden, weshalb eine Ausgestaltung des Datenfeldes als Pflichtfeld in vielen Fällen überflüssig wäre, haben zu der Einschätzung geführt, zum gegenwärtigen Zeitpunkt von einer entsprechenden Softwareänderung abzusehen.

Unabhängig hiervon wurden als Reaktion auf die zu Grunde liegenden Sachverhalte aber bereits

1. eine verbindliche organisatorische Regelung zur Nutzung des Feldes „Veranlasser“ getroffen und

2. die Verlängerung der Aufbewahrungsdauer der Aufzeichnungen im Sprechfunkverkehr auf sechs Monate (in Anlehnung an die Protokollierungsdauer beim Kraftfahrt-Bundesamt) veranlasst.

Diese Maßnahmen werden als ausreichend erachtet. Sollten die Erfahrungen mit den jetzt getroffenen organisatorischen Lösungen jedoch wider Erwarten die Notwendigkeit zur Etablierung einer weiteren technischen Lösung aufzeigen, könnte diese nachfolgend verwirklicht werden.

zu 9.1 Steuerbürokratieabbaugesetz und Bürgerentlastungsgesetz Krankenversicherung

Gemäß § 150 Abs. 1 Satz 2 und Abs. 6 Satz 1 in Verbindung mit § 1 der Steuerdaten-Übermittlungsverordnung (StDÜV) und § 87a Abs. 3 Abgabenordnung (AO) besteht die Möglichkeit, eine Steuererklärung elektronisch an das Finanzamt zu übermitteln, soweit der Zugang hierfür eröffnet worden ist. In Thüringen wurde ein solcher Zugang eröffnet und die Einkommensteuererklärung kann über das ElsterOnline-Portal mittels qualifizierter elektronischer Signatur übermittelt werden. Eine Übermittlung via E-Mail ist nicht zulässig.

Zu beachten ist allerdings, dass Steuerpflichtige in der Praxis regelmäßig nicht über eine Signaturerstellungseinheit (Hardware) zur Erstellung einer qualifizierten elektronischen Signatur verfügen. Deshalb sieht § 6 Abs. 1 StDÜV die Möglichkeit vor, anstelle der qualifizierten elektronischen Signatur ein anderes sicheres, durch das Bundesministerium der Finanzen (BMF) bestimmtes Verfahren, welches den Datenübermittler authentifiziert und die Anforderungen an Gewährleistung der Authentizität und Integrität der Daten erfüllt, zu nutzen. Die Nutzung dieses Authentifizierungsverfahrens ist zeitlich bis zum 31. Dezember 2011 begrenzt und zu evaluieren (§ 87 a Abs. 6 AO).

Im Rahmen des Verfahrens ELSTER wird das Alternativverfahren über das ELSTER-Online-Portal zur Nutzung angeboten und die folgenden Maßnahmen wurden unter der Federführung des Freistaats Bayern zur Bestätigung sowie zur Evaluierung der Sicherheit des alternativen „anderen sicheren Verfahrens“ durchgeführt:

- Zertifizierung der ELSTER-Clearingstellen Düsseldorf und München nach ISO 27001 durch das Bundesamt für Sicherheit in der Informationstechnik (BSI),
- Dokumentation der Clientkomponenten (ERiC, eSigner und eSiCl) angelehnt an Common Criteria for Information Technology Security Evaluation (CCITSE) EAL3,
- Wissenschaftliche Untersuchung der rechtlichen Situation durch den Lehrstuhl für Öffentliches Recht – Verwaltungs- und Steuerrecht – an der Universität Potsdam und das Institut für Betriebswirtschaftliche Prüfungs- und Steuerlehre der Freien Universität Berlin,
- Gutachten der secunet SwissIT AG, dass
 - angemessene Sicherheitsvorgaben existieren,
 - allen Bedrohungen mit angemessenen Maßnahmen begegnet wird und
 - die Sicherheit der Technik der bei ELSTER verwendeten technischen Verfahren denen der qualifizierten elektronischen Signatur entspricht.

Zudem wurde vom federführenden Freistaat Bayern die Vergabe des Datenschutz-Gütesiegels beim Unabhängigen Landeszentrum für Datenschutz in Schleswig-Holstein beantragt. Darüber hinaus beabsichtigt das BMF, den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) in den Evaluierungsprozess einzubeziehen.

Angesichts der vorgenannten Maßnahmen werden die Einlassungen des TLfD zur Sicherheit des „anderen sicheren Verfahrens“ als unbegründet angesehen. Zudem steht es dem Steuerpflichtigen frei, alternativ von der Möglichkeit der qualifizierten elektronischen Signatur Gebrauch zu machen, wenn seinerseits Zweifel an der Sicherheit des „anderen Verfahrens“ bestehen.

Das Gleiche gilt bei der verpflichtenden Einreichung der Steuererklärungsdaten mittels Datenfernübertragung im Sinne des § 150 Abs. 7 AO. Auch hier sind die übermittelten Daten grundsätzlich mit einer qualifizierten elektronischen Signatur zu versehen. Daneben soll die Möglichkeit bestehen, mittels eines anderen sicheren Verfahrens die Anforderungen an die Authentizität und Integrität der Daten zu gewährleisten.

zu 9.2 Haushaltsmanagementsystem (HAMASYS)

Fehlerkorrektur

Der mitgeteilte Sachverhalt betrifft im IT-Verfahren HAMASYS lediglich eine Anwendung („Posten bearbeiten“). Die weiteren Anwendungen sind bereits durch entsprechende Lese- und Schreibrechte von der Einsichtnahme anderer Stellen, insbesondere anderer Dienststellen, geschützt. Das Thüringer Finanzministerium (TFM) hat die Herstellerfirma der Software beauftragt, den geschilderten Mangel auch bei der verbleibenden Anwendung „Posten bearbeiten“ abzustellen.

Ab Verwendung der HAMASYS-Version 1.63 wurden die bereits bestehenden Rechte auch auf die seit der Versionsumstellung generierten Posten übertragen. Darüber hinaus hat der Softwarehersteller auf Veranlassung des TFM die Möglichkeit geprüft, diese Funktion auch auf Posten anzuwenden, die bereits vor der Versionsumstellung vorhanden waren. Die entsprechende Programmierung wurde sodann vom TFM in Auftrag gegeben und wird mit der HAMASYS-Version 1.67, die zum 30. September 2010 ausgeliefert wird, bereitgestellt.

Unabhängig von den benannten technischen Lösungen wurde für alle HAMASYS-Nutzer ein Merkblatt herausgegeben, das darauf hinweist, welche datenschutzrechtlichen Vorgaben zum Schutz personenbezogener Daten bei der Ausübung der Zugriffsrechte in HAMASYS beachtet werden müssen.

Die Anmerkung, dass der Anschluss weiterer Behörden an das Verfahren HAMASYS als bedenklich angesehen wird, ist als entbehrlich anzusehen, da bis auf den Thüringer Landtag (TLT) bereits alle anzubindenden Behörden mit dem Verfahren HAMASYS arbeiten.

Widerspruchsrecht/Einwilligung

Mit Schreiben vom 5. Februar 2008 hat das TFM die Ressorts darauf hingewiesen, dass jeder Betroffene gem. § 4 Abs. 6 ThürDSG ein „Widerspruchsrecht“ gegen die Verarbeitung seiner Daten hat. Übt er dieses aus, so ist gem. § 4 Abs. 6 ThürDSG zu prüfen, ob der Datenverarbeitung überwiegende schutzwürdige Gründe aus seiner besonderen Situation entgegenstehen. Die Prüfung dient also nicht dazu, auf Wunsch des Betroffenen die Rechtmäßigkeitsvoraussetzungen der Datenerhebung nochmals zu prüfen, da diese bereits geprüft wurden. Die Prüfung soll vielmehr unabhängig davon, eine zusätzlich Prüfung aufgrund der besonderen persönlichen Lage des Betroffenen ermöglichen, um vom Regelfall abweichenden Lebenslagen gerecht zu werden.

Darüber hinaus vertritt die Landesregierung die Auffassung, dass sich die Zulässigkeit der Verarbeitung und Nutzung der personenbezogenen Daten der Partner bereits aus den §§ 19 Abs. 1 und 20 Abs. 1 ThürDSG ergibt. Damit besteht keine Notwendigkeit, die vom TLfD angeregte Einwilligung aller Partner einzuholen.

Zugriffsrechte des Kompetenzzentrums

Die gewünschten Informationen bezüglich der Zugriffsrechte der Bediensteten des Kompetenzzentrums auf das Produktivsystem wurden dem TLfD bereits übersandt. Die Zugriffsrechte folgen dabei der Erforderlichkeit zur Aufgabenwahrnehmung der jeweiligen Bediensteten, wie dies nach datenschutzrechtlichen Grundsätzen üblich ist.

zu 9.3 Auskunftsanspruch im Steuerverfahren

Das Bundesverfassungsgericht hat in seinem Beschluss vom 10. März 2008 (1 BvR 2388/03) die Anwendbarkeit des § 19 BDSG im Besteuerungsverfahren bestätigt. Das Verfahren betraf eine Bundesbehörde. Eine entsprechende Aussage zur Auskunftserteilung durch Landesbehörden wurde im Beschluss nicht getroffen. Dennoch bestand auf der Ebene der obersten Finanzbehörden von Bund und Ländern Einigkeit, dass möglichst zeitnah eine gesetzliche Regelung zum Auskunftsanspruch im Besteuerungsverfahren in die AO aufgenommen werden sollte.

Um den Vorgaben des Bundesverfassungsgerichts bereits vorab Rechnung zu tragen, hat das BMF am 17. Dezember 2008 zunächst die vom TLfD benannte, mit den obersten Finanzbehörden der Länder abgestimmte, Verwaltungsanweisung erlassen.

Seit Anfang Juni 2010 existiert ein Vorschlag der zuständigen Referatsleiter der obersten Finanzbehörden des Bundes und der Länder für eine gesetzliche Neuregelung in der Abgabenordnung. Der Gesetzesvorschlag soll den Auskunftsanspruch im Besteuerungsverfahren unter Berücksichtigung des Auskunftsinteresses des Steuerpflichtigen einerseits und der ordnungsgemäßen Aufgabenerfüllung der Finanzverwaltung andererseits regeln.

Der Gesetzesvorschlag soll noch in dieser Legislaturperiode umgesetzt werden. Er wurde durch das BMF mit Schreiben vom 13. Juli 2010 vor der Einleitung des

förmlichen Gesetzgebungsverfahren zunächst dem BfDI zur Stellungnahme zugeleitet.

zu 9.6 Datenlöschung in gepfändeter IuK-Technik

Vor dem Eingang der Beschwerde bestand für die Thüringer Finanzämter folgende Weisungslage für die Verwertung gepfändeter Computer und die Löschung der entsprechenden Datenbestände:

„Bei der Verwertung von Computern ist zu beachten, dass deren Speichereinheit (Festplatte) in der Regel geschützte Daten und Programme enthält. Insbesondere ist die Weitergabe geschützter personenbezogener Daten im Rahmen der Verwertung des Computers aus datenschutzrechtlichen Gründen nicht statthaft. Aus diesem Grund sind alle auf der Festplatte gespeicherten Daten des Vollstreckungsschuldners vor der Verwertung unwiederbringlich zu löschen.

Dem Vollstreckungsschuldner ist vor der Verwertung des Computers unter Fristsetzung schriftlich anheim zu stellen, seinen Datenbestand zu kopieren und anschließend zu löschen. Diese Aufforderung sollte zweckmäßigerweise mit dem Hinweis verbunden werden, dass - falls er die hierfür gesetzte Frist nicht wahrht - das Finanzamt gehalten ist, den Datenbestand auf seine Kosten löschen zu lassen. Etwaige entstehende Kosten gehen zu Lasten des Verwertungserlöses (§ 344 Abs. 1 Nr. 8 AO).

Den Systembetreuern wurde durch das Referat IT-Grundsatzangelegenheiten der Oberfinanzdirektion Erfurt das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelte Festplatten-Löschprogramm VS-Clean Version 2.1 zum Löschen von Festplatten zur Verfügung gestellt.

Diese Software kann genutzt werden, um die Daten auf einem zur Verwertung vorgesehen PC unwiederbringlich zu löschen.“

Aufgrund der datenschutzrechtlichen Bedenken des TLfD zur bisherigen Verfahrensweise im Umgang mit gepfändeter IuK-Technik wurden die Finanzämter mit Verfügung vom 26. Mai 2009 wie folgt angewiesen:

„Bei der Verwertung von Computern ist zu beachten, dass deren Speichereinheit (Festplatte) in der Regel geschützte Daten und Programme enthält. Insbesondere ist die Weitergabe geschützter personenbezogener Daten im Rahmen der Verwertung des Computers aus datenschutzrechtlichen Gründen nicht statthaft. Aus diesem Grund sind alle auf der Festplatte gespeicherten Daten des Vollstreckungsschuldners vor der Verwertung unwiederbringlich zu löschen. Aus diesem Grund wird das Protokoll für die Vollziehungsbeamten um eine weitere Anlage erweitert.

Bereits bei der Pfändung von PCs oder Laptops ist der Schuldner darauf hinzuweisen, dass er seine personenbezogenen Daten bis zu einem bestimmten Termin zu löschen hat. Die Frist sollte in der Regel 14 Tage betragen. Meldet er sich bis zu diesem Zeitpunkt nicht beim Finanzamt, wird davon ausgegangen, dass keine personenbezogenen Daten mehr auf dem Gerät gespeichert sind.

Macht der Schuldner bei der Pfändung der Geräte Angaben dazu, dass sich auf der Festplatte noch personenbezogene Daten befinden, welche für ihn von Bedeutung sind, sind diese Angaben ebenfalls im Protokoll zu erfassen.

Hat sich der Schuldner bis zum angegebenen Datum nicht im Finanzamt gemeldet und hat er keine Angaben zu für ihn bedeutsamen Daten gemacht, kann die Festplatte mit dem Löschprogramm VS-Clean gelöscht werden.

Hat sich der Schuldner bis zum angegebenen Datum nicht im Finanzamt gemeldet und hat er Angaben zu für ihn bedeutsamen Daten gemacht, ist er nochmals unter Fristsetzung darauf hinzuweisen, dass er seine personenbezogenen Daten zu löschen hat. Kommt er dieser Aufforderung wiederum nicht nach, ist die Verwertung des Laptops bzw. Computers ohne die entsprechende Festplatte durchzuführen.“

Ein Absehen von der Verwertung gepfändeter IuK-Technik hält die Landesregierung im Hinblick auf den Grundsatz der Gleichmäßigkeit der Besteuerung für nicht vertretbar. Allerdings machen die Vollstreckungsstellen der Finanzämter auf Grund der datenschutzrechtlichen Problematik nur noch sehr zurückhaltend von der Pfändung von Datenträgern eines hohen oder unbekanntem Schutzbedarfs Gebrauch. Zudem wird bei der Verwertung gepfändeter IuK-Technik ein erhöhtes Augenmerk auf die Einhaltung der datenschutzrechtlichen Belange gelegt.

zu 9.7 Verwenden von Kundendaten der Sparkasse Mittelthüringen zu Werbezwecken

Die Sparkasse Mittelthüringen teilte mit, dass es sich bei dem angesprochenen Vorfall um einen Einzelfall gehandelt habe. Sie werde - wie im Bericht erwähnt - das erbetene Werbeverbot beachten und geeignete Qualitätssicherungsmaßnahmen vornehmen.

zu 10.2 Abfrage von Telekommunikations-Verkehrsdaten einschränken

Die im Fazit angesprochenen Forderungen sind an den Bundesgesetzgeber gerichtet.

In diesem Zusammenhang hat Thüringen den Beschluss der 81. Justizministerkonferenz vom 23./24. Juni 2010 in Hamburg unterstützt (TOP II.3 – „Gesetzliche Neuregelung der Vorratsdatenspeicherung“). Danach begrüßen die Justizministerinnen und Justizminister, dass auf der Grundlage der Entscheidung des Bundesverfassungsgerichts vom 2. März 2010 (1 BvR 256/08) nunmehr klare Maßstäbe für eine verfassungskonforme gesetzliche Regelung zur Nutzung der Telekommunikationsverkehrsdaten vorliegen. Sie bitten die Bundesministerin der Justiz, die Länder frühzeitig in die Verhandlungen zur Überarbeitung der Richtlinie 2006/24/EG einzubinden, um eine konstruktive Einflussnahme zu ermöglichen.

zu 10.3 Justizzahlstellenverfahren speichert längst erledigte Forderungen

Das Thüringer Finanzministerium beabsichtigt, dass vom TLfD bemängelte Kosteneinziehungsverfahren „KEVE“ schnellstmöglich durch ein neues, den aktuellen datenschutzrechtlichen Bestimmungen entsprechendes, Programm abgelöst wird.

Bereits im August 2009 sollte eine Entscheidung über die Ablösung des Verfahrens durch den Beitritt in den Länderentwicklungsverbund „KASH“ getroffen werden. Dies konnte jedoch wegen vergaberechtlicher Bedenken nicht unmittelbar umgesetzt werden. Es wird nunmehr angestrebt, das Problem schnellstmöglich einer einvernehmlichen Lösung zuzuführen.

zu 11.5 Arge ARGEEn?

Die im Tätigkeitsbericht geschilderte Problematik in der ARGE SGB II des Landkreises Saalfeld-Rudolstadt ist dem Thüringer Ministerium für Wirtschaft, Arbeit und Technologie (TMWAT) bekannt. Zum Teil war hier die Aufsichtszuständigkeit des Bundesministeriums für Arbeit und Soziales betroffen. Der Sachverhalt in der Grundsicherung für Arbeitsuchende musste daher mit der Regionaldirektion Sachsen-Anhalt-Thüringen der Bundesagentur für Arbeit aufgeklärt und besprochen werden. Die Landesregierung nimmt zustimmend zur Kenntnis, dass durch entsprechende Schulungsmaßnahmen und intensive Kommunikation auch seitens des TLfD die beanstandeten Defizite beseitigt werden konnten.

zu 12.3 Falsche Adressaten für Gasliefervertrag

Die Erkenntnisse des TLfD betreffen ein organisatorisches Versagen der Kundenverwaltung des betroffenen Unternehmens. Die Rechte der betroffenen Bürger wurden schon auf der Handlungsebene fahrlässig verletzt. Die Verstöße beruhen nicht auf einer falschen Bewertung datenschutzrechtlicher Belange.

zu 12.4 Intelligente Stromzähler

Die Landesregierung sieht die datenschutzrechtliche Problematik bei der Einführung intelligenter Stromzähler (SmartMeter) und stimmt auch mit deren Bewertung durch den TLfD überein.

Die möglichst breitflächige Einführung intelligenter Stromzähler ist energiepolitisch gewünscht und bildet ein Element der energiepolitischen Zielsetzung „grüner Motor“ der Landesregierung. Die Einführung wird aber nur gelingen, wenn der Bürger das System akzeptiert. Er muss deshalb darauf vertrauen können, dass seine Teilnahme freiwillig ist. Das bedeutet auch, dass er nicht durch wirtschaftliche Sanktionen wie ungünstige Alternativtarife in das System hinein gedrängt werden darf. Weiterhin ist erforderlich, dass keine Möglichkeit für die Versorgungsunternehmen besteht, das Kundenverhalten Einzelner zu erfassen, sofern diese sich gegen eine Teilnahme am SmartMetering entschieden haben.

zu 12.5 Videoüberwachung in Wohngebäuden

Der TLfD besitzt nur in begrenztem Umfang die Aufgabe, datenschutzrechtliche Prüfungen nach § 6 b BDSG durchzuführen, da dieser vorrangig für Behörden des Bundes und nicht-öffentliche Stellen gilt. Eine Ausnahme ist demgegenüber nur dann gegeben, wenn es sich um öffentliche Wettbewerbsunternehmen handelt, die wegen ihrer strukturellen Vergleichbarkeit zu nicht-öffentlichen Stellen nach § 26 ThürDSG dem BDSG unterfallen. Insoweit sind die Aussagen des TLfD zur Beurteilung einer Videoüberwachung in öffentlich zugänglichen Räumen nach § 6 b BDSG zutreffend.

Die Prüfung einer Videoüberwachung im nicht-öffentlich zugänglichen Innenraum obliegt hingegen nicht mehr dem TlFD. Es dürfte in Anbetracht der obergerichtlichen Rechtsprechung der Zivilgerichte zum Unterlassungsanspruch nach den §§ 823 und 1004 BGB zwar zutreffen, dass die permanente Überwachung des Innenraumes unzulässig ist. Das Bundesdatenschutzgesetz erfasst diesen Fall jedoch nicht, da es lediglich eine Regelung zur Videoüberwachung öffentlich zugänglicher Räume nach § 6b BDSG enthält, auf deren Prüfung der TlFD gem. § 26 ThürDSG beschränkt ist. Eine Prüfkompetenz darüber hinaus kann nicht auf § 28 BDSG gestützt werden, da die Vorschrift als Rechtsgrundlage für eine Videoüberwachung zu allgemein gehalten ist. Das BDSG bietet daher keinen Anknüpfungspunkt für eine Prüfung des TlFD im Innenbereich.

zu 15.1 Umsetzung der EU-Dienstleistungsrichtlinie in Thüringen THEA

Bei der Umsetzung der EU-Dienstleistungsrichtlinie in Thüringen hat das federführende TMWAT den TlFD einbezogen und seine Vorschläge und Hinweise umgesetzt. Es besteht Konsens mit dem TlFD, dass im Rahmen späterer Systemanpassungen auch die Wahrung datenschutzrechtlicher Belange über dessen Einbindung und Mitwirkung sichergestellt werden muss.

zu 15.2 Einsatz EiCoNeD in Thüringen

Die bisherige Konzeption sieht vor, wie bisher ein in sich geschlossenes Datennetz mit vielfältigen Sicherheitsstrukturen auszuschreiben. Standortübergreifende Anforderungen an den Datenschutz und die Datensicherheit sollen bei der Erstellung der Feinkonzepte berücksichtigt werden. Ein unberechtigter Zugriff durch Dritte auf die zu übertragenden Daten wird durch das geschlossene Datennetz maßgeblich erschwert. Eine zusätzliche Verschlüsselung der Daten- und Sprachdatenpakete stellt einen weiteren festen Bestandteil der Ausschreibung und der späteren Inbetriebnahme dar. Im Rahmen des weiteren Projektverlaufs wird eine enge Einbindung des TlFD erfolgen. Die Erstellung eines Sicherheitskonzeptes wird sukzessive zum Ausschreibungsverfahren bzw. zur Projektumsetzung erfolgen.

zu 15.3 Protokollierung von Zugriffen auf Internetangebote in der Thüringer Landesverwaltung

Entsprechend den Anforderungen im 5. Tätigkeitsbericht und in Absprache mit dem TlFD werden für das Zugriffsreporting die Log-Dateien täglich automatisiert anonymisiert (durch Löschung des 4. Oktetts der IP-Adresse) und in eine Datenbank eingelesen. Durch die Anonymisierung der IP-Adresse handelt es sich nicht mehr um ein personenbezogenes Datum. Die Speicherung der Log-Informationen in der Datenbank für eine ad-hoc-Reporterstellung (statistische Auswertungen) durch die jeweiligen Webseiteneigner ist rückwirkend für 2 Monate eingestellt. Die Auswertungen erfolgen kumuliert und verdichtet, d. h. ohne explizite Darstellung einer IP-Adresse.

zu 15.4 Einsatz BlackBerry in der Thüringer Landesverwaltung

Das Thüringer Landesrechenzentrum (TLRZ) bietet die Nutzung von BlackBerry innerhalb der Thüringer Landesverwaltung als zentralen Dienst an. Zur Gewährleistung eines sicheren Betriebs wurde dafür ein IT-Sicherheitskonzept entsprechend den Vorgaben des BSI erstellt.

Das TLRZ nutzt darüber hinaus die von der Herstellerfirma bereitgestellten jeweiligen aktuellen und zertifizierten Softwareversionen. Derzeit wird der BlackBerry Enterprise Server (BES) vom TLRZ in der Version 5.0 betrieben. Die BES-Software wurde von unabhängigen „Common Criteria“-Experten getestet und entspricht den Sicherheitsanforderungen des EAL (Evaluation Assurance Level) 4+, dass gemäß des Common Criteria Recognition Arrangements (CCRA) von 26 Ländern, u. a. Deutschland, anerkannt wird.

Die Common Criteria verkörpern den entsprechenden internationalen Standard zur Prüfung der spezifischen Sicherheitsanforderungen an ein IT-Produkt. Die EAL-Stufen der Common Criteria (ISO 15408) beschreiben präzise Anforderungen an eine IT-Sicherheitsprüfung. Mit wachsender EAL-Nummer steigen die Anforderungen an den zu prüfenden Umfang, an die Prüftiefe und an die Prüfmethode. Ziel einer Common Criteria-Evaluierung ist die Bestätigung, dass die vom Hersteller behauptete Sicherheitsfunktionalität wirksam ist. Da die Sicherheitsleistung insbesondere durch die Ausnutzbarkeit vorhandener Schwachstellen unwirksam werden kann, ist bei allen Evaluierungsaspekten die Analyse der Schwachstellen ein zentrales Prüfziel. Eine niedrigere EAL-Stufe kann vom Prüfumfang als Untermenge des Prüfaufwandes der nächst höheren Stufe angesehen werden.

Im Tätigkeitsbericht ist zutreffend festgestellt, dass das vom Fraunhofer SIT ausgestellte Zertifikat der BES-Software-Version 4.1 Ende 2010 ausläuft. Das TLRZ betreibt deshalb, wie bereits ausgeführt, den BES in der Version 5.0, für den die benannte EAL4+ - Prüfung vorliegt.

zu Anlage 5 Mehr Augenmaß bei der Novellierung des BKA-Gesetzes

Unter anderem fordert die EntschlieÙung der Datenschutzbeauftragten des Bundes und der Länder vom April 2008 eine Abgrenzung von Befugnissen der Polizei und der Verfassungsschutzbehörden. Weiter fordern die Datenschutzbeauftragten unter Bezugnahme auf die Entscheidung des Bundesverfassungsgerichts vom 27. Februar 2008 (1 BvR 370/07) zur Online-Durchsuchung eine Regelung zum Schutz des Kernbereichs privater Lebensgestaltung für Eingriffsmaßnahmen in allen Rechtsgebieten.

Das BKA-Gesetz wurde zwischenzeitlich durch das „Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt“ vom 25. Dezember 2008 grundlegend novelliert und in § 20k BKA-Gesetz eine Regelung zur Online-Durchsuchung geschaffen. Gegen das novellierte BKA-Gesetz sind mittlerweile unter den Aktenzeichen 1 BvR 966/09 und 1 BvR 1140/09 Verfassungsbeschwerden beim Bundesverfassungsgericht anhängig.

Die geforderte Aufgabenabgrenzung in Fragen des Verfassungsschutzes betrifft das Trennungsgebot. Dieses besagt, dass der Verfassungsschutz keine polizeilichen Zwangsbefugnisse haben darf. Die Zusammenarbeit von Verfassungsschutz und Polizei ist hiervon nicht betroffen, sondern sogar ausdrücklich im Grundgesetz festgelegt. Art. 73 Abs. 1 Nr. 10 b GG sieht vor, dass Bund und Länder „zum Schutze der freiheitlichen demokratischen Grundordnung, des Bestandes und der Sicherheit des Bundes oder eines Landes (Verfassungsschutz)“ zusammenarbeiten. Dies wird nicht auf bestimmte Behörden begrenzt und umfasst auch den Informationsaustausch. Befugnisse, die einen Verstoß gegen das Trennungsgebot begründen würden, werden dadurch nicht geschaffen. Die von den Datenschutzbeauftragten unterschwellig zum Ausdruck gebrachte Auffassung, Polizei und Verfassungsschutz seien im Hinblick auf Daten- bzw. Informationsaustausch zu trennen, wird daher nicht geteilt. Nach Art. 97 ThürVerf stehen dem Verfassungsschutz polizeiliche Befugnisse und Weisungen nicht zu.

Soweit die Forderung aufgestellt wird, den Kernbereichsschutz für alle Maßnahmen der Sicherheitsbehörden zu regeln, wird auf die Ausführungen zu Punkt 7.1 Bezug genommen.