Vorsitzenden des Innen- und Rechtsausschusses
des Schleswig-Holsteinischen Landtages
Herrn Werner Kalinka, MdL
Landeshaus

24105 Kiel

Innenministerium
des Landes
Schleswig-Holstein

Schleswig-Holsteinischer Landtag
Umdruck 16/1002

Minister

Kiel, 8. Juli 2006

28. Tätigkeitsbericht des Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Sehr geehrter Herr Vorsitzender,

zu den wesentlichen Punkten des Unabhängigen Landeszentrums für Datenschutz (ULD) in seinem 28. Tätigkeitsbericht gebe ich die nachfolgende Stellungnahme ab:

Die Stellungnahmen des Ministeriums für Justiz, Arbeit und Europa (Ziffern 4.3.1, 4.3.2, 4.5.1, 11.1, 11.2, 11.3), des Ministeriums für Bildung und Frauen (Ziffern 4.7.1, 4-7-2), des Finanzministeriums (Ziffern 4.8.2, 6.5, 6.6, 6.7, 6.9, 9, 9.1.1, 9.1.2, 12.2.2) und des Ministeriums für Soziales, Gesundheit, Familie, Jugend und Senioren (Ziffern 4.6.5, 4.6.6) wurden einbezogen.

4.1.1 E-Government im Meldewesen – Polizeiabrufverfahren

Bei der Übermittlung von Meldedaten im automatisierten Abrufverfahren hat das ULD bei der Prüfung einer Stadt Mängel bei der Ausgestaltung auch des Polizeiabrufverfahrens festgestellt.
Die vom ULD u.a. kritisierte nicht ausreichende Identitätsprüfung von gesuchten Personen im automatisierten Polizeiabrufverfahren ist rechtlich nicht eindeutig geregelt.
Das Verfahren wird seit 1986 mit den Funktionalitäten durch den Aufgabenvollzug der Landespolizei Schleswig-Holstein genutzt, und zwar nicht nur zum Abgleich von Personen, sondern auch zur Ermittlungsunterstützung.

Postfach 7125
24171 Kiel
Telefon (0431) 988-0
Telefax (0431)988-2833
e-mail: ralf.stegner@im.landsh.de
Internet:www.schleswig-holstein.de

Die 2004 erfolgte Novellierung des Landesmeldegesetzes führte zu Änderungen der Regelungen für die sog. Listenauskünfte im automatisierten Verfahren zur Identität der angefragten Person. In die Diskussion um den Umfang der Listenauskünfte wurde die Landespolizei allerdings erst jetzt einbezogen. Sie hat sofort reagiert und nachgewiesen, dass in bestimmten Fällen derartige Listenauskünfte für die polizeiliche Ermittlungsarbeit zwingend erforderlich sind. Die Landespolizei muss in der Lage sein, Abfragen aus dem Einwohnerinformationssystem (EIS-Abfragen) auch im Rahmen notwendiger Informationsverdichtungen durchführen zu können. Sie hat daher für eine klarstellende Gesetzesänderung geworben, die von dem für das Melderecht zuständigem Fachreferat umgesetzt werden soll.

4.2.1 Neues Polizeirecht – mehr Daten von Unverdächtigen

Nach Auffassung des ULD bedeute der Gesetzesentwurf der Landesregierung gerade wegen der weitergehenden Befugnisse im so genannten Gefahrenvorfeld eine grundsätzliche Wende im Polizeirecht. Das ULD sieht dies als verfassungsrechtlich bedenklich an und empfiehlt eine Nachbesserung.
Die vom ULD kritisierte Entwurfsfassung des neuen Polizeirechts ist nicht mehr aktuell. Die Anhörung der Verbände, im Rahmen dessen sich auch das ULD äußerte, hatte zu zahlreichen Änderungen im endgültigen Entwurf der Landesregierung geführt. Der Landtag hat den aktualisierten Gesetzentwurf der Landesregierung eines Gesetzes zur Anpassung gefahrenabwehrrechtlicher und verwaltungsverfahrensrechtlicher Bestimmungen (Landtagsdrucksache 16/670) nach der Erstdebatte am 23.03.2006 zur weiteren Beratung an den Innen- und Rechtsausschuss überwiesen. Der Ausschuss hat am 29.03.2006 beschlossen, eine schriftliche und im Anschluss daran eine mündliche Expertenanhörung durchzuführen. Das parlamentarische Verfahren ist derzeit noch nicht abgeschlossen.
Der Vorwurf des ULD, dass der Gesetzentwurf verfassungswidrig sei, wird jedoch weiterhin vom Innenministerium zurückgewiesen. Gerade die vom ULD als Beweis der Verfassungswidrigkeit angeführten jüngsten Entscheidungen des Bundesverfassungsgerichtes (BVerfG) zum sog. großen Lauschangriff vom 03.03.2006 und zur niedersächsischen Regelung präventiver Telefonüberwachung vom 27.07.2006 berücksichtigt der aktualisierte Gesetzentwurf.

4.2.2 INPOL SH

Das ULD kritisiert, dass INPOL SH weiterhin ohne ausreichende Errichtungsanordnung betrieben werde, und fordert das Innenministerium auf, eine bewertbare Darstellung vorzulegen.
Das Innenministerium hatte bereits die umfangreiche Stellungnahme des ULD vom 28.04.2005 zum Anlass genommen, die Errichtungsanordnung INPOL SH zu überarbeiten. Mit Schreiben vom 22.08.2005 übersandte das Innenministerium dem ULD eine geänderte Fassung der Errichtungsanordnung (Stand: 01.08.2005), in der die vom BVerfG geforderten verfahrensrechtlichen Vorkehrungen zur Sicherung des Rechts auf informationelle Selbstbestimmung enthalten sind. Gleichzeitig wurde angeregt, den begonnenen Dialog zur Optimierung der Errichtungsanordnung mit dem ULD fortzusetzen, um ggf. weitere noch offene Punkte rechtskonform und pragmatisch lösen zu können. Die erbetenen Formulierungsvorschläge sind vom ULD jedoch nicht erfolgt, so dass die jetzige Kritik nicht nachvollzogen werden kann.

4.2.3 @rtus

In der Frage der einschlägigen Rechtsgrundlage für das polizeiliche Vorgangsbearbeitungs- und –verwaltungssystem @rtus-VBS gib es zwischen dem Innenministerium und dem ULD unterschiedliche Rechtsauffassungen. Das Innenministerium hat entsprechend reagiert und die anstehende Novellierung des Landesverwaltungsgesetzes genutzt, um eine klarstellende Rechtsgrundlage für @rtus-VBS in § 189 Abs. 1 Landesverwaltungsgesetz (LVwG) zu schaffen. In diesem Zusammenhang wird nochmals darauf hingewiesen, dass @rtus-VBS der Zweckbestimmung entsprechend ein System ist, das zwar begrenzt ein Reporting zulässt, aber keine übergreifenden Recherchen oder Initiativermittlungen.

Mit der landesweiten Einführung von @rtus-VBS soll das Altsystem COMPAS-AWS[1] nach jetziger Planung bis spätestens Ende 2007 abgelöst werden. Aufgrund technischer Probleme ist eine Migration dieser Daten in @rtus-VBS jedoch nicht möglich. Da die Landespolizei Schleswig-Holstein nicht auf diese Daten verzichten kann, ist derzeit partiell ein Parallelbetrieb erforderlich. Für eine datenschutzgerechte Löschung dieser Daten wird ein entsprechendes Löschkonzept erstellt.

4.2.4 Protokollierung – eine unendliche Geschichte

Die nachvollziehbare Protokollierung von Zugriffen oder Änderungen in automatisierten Abrufverfahren ist nicht nur beim ULD, sondern auch bei der Landespolizei Schleswig-Holstein ein zentrales Thema, das gerade in der letzten Zeit aufgearbeitet und optimiert worden ist. Obwohl es gesetzlich noch nicht gefordert ist, erfolgt bei INPOL SH in der Landespolizei bereits eine automatische Vollprotokollierung aller Zugriffe und aller Änderungen. Die Protokolldaten werden für ein Jahr gespeichert und sind nur zweckgebunden abrufbar. Datensatzänderungen sind nur durch Mitarbeiterinnen und Mitarbeiter, die über eine spezielle Berechtigung verfügen, möglich. Damit ist die Authentizität der Daten in automatisierten Abrufverfahren grundsätzlich gewährleistet. Eine Vollprotokollierung ist aber kein sicherer Garant für die Authentizität der Daten, dafür ist nach wie vor die Sachbearbeitung als „menschliche“ Schnittstelle verantwortlich.
Da auch jeder Zugriff in den automatisierten Abrufverfahren INPOL SH und INPOL Z (INPOL Zentral als Schnittstelle zum Bundeskriminalamt – BKA) automatisch protokolliert und für ein Jahr gespeichert wird, kann auch die Rechtmäßigkeit des Datenabrufs überprüft werden.
Bei Zugriffen auf INPOL-Fall-Dateien (Dateien, die nach bestimmten Kategorien, z. B. Rauschgift, Menschenhandel, gegliedert sind) wird auf der Grundlage von § 11 Abs. 6 Bundeskriminalamtgesetz (BKAG) durchschnittlich jeder zehnte Abruf für Zwecke der Datenschutzkontrolle protokolliert.
Bei Änderungen von Daten, die nur mit einer speziellen Berechtigung möglich sind, werden in jedem Fall die Anwender, der Zeitpunkt und der Inhalt der Änderung automatisch protokolliert. Diese Daten sind vom BKA zweckgebunden abrufbar.
Der Zugriff auf die INPOL-Fall-Dateien beim BKA erfolgt über einen Server[2] im Polizeizentrum Eichhof. Dort werden die IP-Adresse, der Zeitpunkt des Zugriffs und das Ziel der Anfrage für einen Zeitraum von 6 Monaten in Dateien gespeichert. Bedingt

[1] AWS = Anwendungssoftware
[2] Proxy-Server für die http-Kommunikation mit INPOL Fall über eine gesicherte Leitung (CNPON)

durch die Vergabe einer „quasi festen“ [3] IP-Adresse besteht eine hohe Wahrscheinlichkeit, dass der PC ermittelt werden kann, von dem die Anfrage kam. Anhand der INPOL-Fall-Kennung, die beim BKA mitgeloggt wird, besteht dann die Möglichkeit der Feststellung des oder der Anfragenden.

Die Landespolizei wird prüfen, ob das derzeitige Protokollierungsverfahren bei INPOL-Fall durch interne technische Lösungen noch optimiert werden kann.

4.2.5 Auskunftserteilungen durch die Polizei

Der Umfang der Auskunftserteilung ans ULD durch die Polizei ist in der Vergangenheit intensiv mit dem ULD diskutiert worden. Die zunächst restriktive Sichtweise des Landeskriminalamtes (LKA) und des Innenministeriums, die das ULD bemängelt, ist nach Rücksprache mit dem BKA wie folgt verändert worden:
Künftig wird das LKA als zentrale Auskunftsstelle der Landespolizei Schleswig-Holstein neben den Auskünften aus INPOL-Verbunddateien, soweit die Landespolizei Schleswig-Holstein Datenbesitzer ist, dem ULD mitteilen, dass über den Petenten Daten auch bei anderen Verbundteilnehmern gespeichert sind. Das LKA wird das Auskunftsersuchen an das BKA als Zentralstelle für Auskünfte aus anderen INPOL- Verbunddateien weiterleiten. Dies ist mit dem BKA abgestimmt.
Die Speicherung von Petentendaten aus Anlass einer Anfrage erfolgt beim LKA 3 (Abteilung Staatsschutz) zum Zweck der Vorgangsverwaltung und Dokumentation. Sofern für einen Petenten bereits eine Personenakte beim Staatsschutz angelegt wurde, wird diese auch in der Datei „Innere Sicherheit Schleswig-Holstein“ (ISSH) registriert. Das LKA hatte in der Vergangenheit diese Speicherungen nicht dem Auskunftsersuchen des ULD zugeordnet und sie deshalb auch nicht mitgeteilt. Künftig wird das LKA auch über diese Datenspeicherungen zeitnah dem ULD Auskunft erteilen.

4.2.6 Rasterfahndung – nutzlos, aber verlängert

Das Gesetz zur Einführung des automatisierten Datenabgleichs vom 19.10.2001 (GVOBl. Schl.-H. Nr. 11, S. 166) stellte nach den Anschlägen des 11. September 2001 mit dem zunächst bis zum Ende des Jahres 2005 befristeten § 195a des Landesverwaltungsgesetzes (LVwG) die Rasterfahndung zu Gefahrenabwehrzwecken der schleswig-holsteinischen Polizei zur Verfügung.
Danach kann die Polizei erst nach richterlicher Anordnung von öffentlichen und nichtöffentlichen Stellen die Übermittlung von personenbezogenen Daten bestimmter Personengruppen aus den dortigen Dateien zum automatisierten Abgleich mit anderen Dateien nach fahndungsspezifischen Suchkriterien verlangen. Voraussetzung ist, dass entweder für den Bestand der staatlichen Ordnung eine erhebliche Gefahr besteht oder dass Straftaten von erheblicher Bedeutung begangen werden sollen, bei denen Schäden für Leben, Gesundheit oder Freiheit oder gleichgewichtige, erhebliche Schäden für die Umwelt zu erwarten sind. Die andauernde Gefährdung höchster Rechtsgüter durch den internationalen Terrorismus erfordert die unbefristete Fortgeltung der schleswig-holsteinischen Vorschrift als länderpolizeirechtliches Instrumentarium. Deshalb hat der Landtag mit dem Gesetz zur Änderung des Landesverwaltungsgesetzes und anderer Vorschriften vom 15.12.2005 (GVOBl. Schl.-H. Nr. 17, S. 542) die Befristung der Rasterfahndung aufgehoben.

[3] IP-Adresse wird vom Server fest zugewiesen, solange keine größeren Veränderungen im Netzwerk erfolgen.

Im Gegensatz zum ULD sieht das Innenministerium den Ausgang der letzten Rasterfahndung nicht als erfolglos an, weil das Ergebnis unter Gefahrenabwehrgesichtspunkten sowohl objektiv als auch subjektiv die wertvolle Erkenntnis erbracht hat, dass in Schleswig-Holstein keine sog. „Schläfer“ ermittelt wurden. Außerdem wird mit der Rasterfahndungsmaßnahme und –option Druck auf unerkannt gebliebene Schläfer ausgeübt und damit einem Schadenseintritt entgegengewirkt. Die weiterhin bestehende Gefahr terroristischer Anschläge rechtfertigt den Einsatz der Rasterfahndung. Es gibt kein anderes Mittel, das die gleiche Wirkung entfaltet, aber weniger stark in das informationelle Selbstbestimmungsrecht eingreift. Das ULD hatte die bisher einzige Rasterfahndung in Schleswig-Holstein datenschutzrechtlich begleitet. Mit dem ULD wurden Verfahrensregelungen über die Benachrichtigung der von Maßnahmen Betroffenen und zur Vernichtung der im Zusammenhang mit dem automatisierten Datenabgleich angefallen Daten und Unterlagen vereinbart. Diese Regelungen werden auch bei künftigen Maßnahmen nach § 195a LVwG zur Anwendung kommen.

Zu der vom ULD als „Geheimniskrämerei“ bewerteten Weigerung auf Herausgabe eines internen, für die Innenministerkonferenz erstellten Papiers ist anzumerken, dass sich das Innenministerium an die von der Innenministerkonferenz beschlossene Nichtfreigabe von Berichten und Beschlüssen gehalten hat.

Das ULD nimmt darüber hinaus die Entscheidung des BVerfG vom 04.04.2006 zur präventiven Rasterfahndung des nordrhein-westfälischen Polizeigesetzes (1 BvR 518/02) zum Anlass, die ersatzlose Streichung der entsprechenden schleswig-holsteinischen Norm (§ 195a LVwG) zu fordern (Presseinformation des ULD vom 23.05.2006). Das BVerfG hat bei der Durchführung der bundesweiten, nach den jeweiligen landesrechtlichen Bestimmungen durchgeführten, aber insoweit einheitlichen Rasterfahndungsmaßnahmen nach den Terroranschlägen des 11. September 2001 Subsumtions-, also Anwendungsfehler festgestellt und diese konkrete Maßnahme als rechtswidrig bezeichnet. Die Norm selbst ist vom höchsten deutschen Gericht nicht verworfen oder gar mit Gesetzeskraft „kassiert“ worden. Das BVerfG hat für seine Presseerklärung 40/2006 den darauf gerichteten Titel „Rasterfahndung nur bei konkreter Gefahr für höchste Rechtsgüter zulässig“ gewählt.

4.2.7 Beobachtungen von Versammlungen im Visier des ULD

Die Kritik des ULD, dass die Teilnahme einer Person an einer erlaubten Demonstration als „Hinzuspeicherung“ in eine bereits vorhandene Kriminalakte beim LKA einfließt, ist sachlich falsch dargestellt.
Die Teilnahme an einer erlaubten Demonstration wird im Einzelfall nur dann gespeichert, wenn es sich um eine politische Veranstaltung handelt, der Teilnehmer der Polizei als politisch motivierter Straftäter bekannt ist, über ihn bereits eine Personenakte von der Staatsschutzabteilung des LKA auf der Grundlage von § 189 Abs. 1 LVwG geführt wird und die Hinzuspeicherung unter Berücksichtigung bisheriger Erkenntnisse fachlich geboten ist. Die Hinzuspeicherung erfolgt ausschließlich in der Personenakte des polizeilichen Staatsschutzes, nicht aber in der ggf. zusätzlich vorhandenen Kriminalakte bei einer Polizeidirektion, die im Gegensatz zur Personenakte nicht so umfassend und außerdem von allen Polizeibeamtinnen und –beamten über INPOL SH abrufbar ist.
Die Beanstandung des ULD einer Hinzuspeicherung in einer Personenakte anlässlich der Teilnahme an einer angemeldeten Demonstration gegen die Hartz IV-Gesetze in Lübeck ist hingegen gerechtfertigt, weil bereits die Datenerhebung unzulässig war.

Mit Hilfe der Datei „Innere Sicherheit Schleswig-Holstein“ werden die Prüffristen der Personenakten der Staatsschutzabteilung des LKA überwacht. Die fehlende Errichtungsanordnung für diese Datei ist in Vorbereitung.

Für das Altsystem COMPAS-AWS gelten grundsätzlich auch die datenschutzrechtlichen Vorgaben, einschließlich der Löschungsfristen. Derzeit wird die 10-jährige Speicherfrist mit dem Ziel geprüft, sie mit den Regelungen von @rtus-VBS in Einklang zu bringen.

4.2.8 Lageberichte – gute Kooperation mit der Polizei

Im Gegensatz zur Rechtsauffassung des ULD sieht die Landespolizei bei der Nutzung der personenbezogenen Daten, die zu Zwecken der Strafverfolgung oder der Gefahrenabwehr erhoben worden sind, in Lageberichten die Zweckidentität dieser Daten als gegeben an. Die Landespolizei kann rechtmäßig erhobene Daten auf der Grundlage des § 188 Abs. 1 LVwG in Lageberichten nutzen, wenn gewährleistet ist, dass die personenbezogenen Daten nur an die operativ zuständigen Dienststellen zur Aufgabenwahrnehmung übermittelt werden. Sofern zur Information ein breiterer Empfängerkreis gewählt wird, werden die personenbezogenen Daten anonymisiert.
Gerade in der Frage der differenzierten Übermittlung besteht aber weiterer Handlungsbedarf. Deshalb wird diese Thematik vom Innenministerium mit dem Ziel aufgearbeitet, landesweit einen verbindlichen Rahmen festzulegen, der unter Berücksichtigung der Erforderlichkeit die Rechtmäßigkeit der Datenübermittlung sicherstellt.

Die Warndatei „Rechts“ wurde in Umsetzung einer Leitlinie des Innenministeriums zur Intensivierung der polizeilichen Maßnahmen gegen Rechtsextremismus und Fremdenfeindlichkeit eingerichtet. Die Kritik des ULD am Umfang der gespeicherten Daten wurde zum Anlass genommen, die Errichtungsanordnung dieser Datei zu überarbeiten.

4.2.9 Fußball-WM 2006 führt zur Durchleuchtung

Die datenschutzrechtliche Problematik des Akkreditierungsverfahrens ist im Rahmen der Gremienarbeit zur Innenministerkonferenz ausführlich mit allen Datenschutzbeauftragten der Länder und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit kontrovers diskutiert worden.
Erwähnenswert ist in diesem Zusammenhang die Aussage des ULD, dass – entgegen der vorherigen Rechtsauffassung – in der Konferenz der Datenschutzbeauftragten im März 2006 die Ansicht aller Innenminister geteilt und festgestellt wurde, dass das Recht auf informationelle Selbstbestimmung dispositiv ist, d.h. durch Einwilligung gestaltet werden kann.
Nach der Konferenz hat das ULD allerdings seine Argumentation geändert und erneut das „informierte Einwilligungsverfahren“ insgesamt als unvollständig und als zu unbestimmt in Zweifel gezogen. Diese Auffassung teilt das Innenministerium nicht. Nach Auswertung aller Erkenntnisse aus dem „Probelauf während des Confederation Cups 2005“ und unter Einarbeitung aller Datenschutzanforderungen in ein Belehrungsschreiben für die zu Akkreditierenden ist ein rechtlich in jeder Weise belastbares Verfahren mit der informierten Einwilligung in allen Ländern gefunden worden. Es gab bundesweit auch keine bekannt gewordenen Rechtsverfahren oder Schadensersatzforderungen von Arbeitnehmern oder Bewerbern, die auf erkenntnisbezogene arbeitsrechtliche Konsequenzen der Firmen zurückzuführen waren.

Schleswig-Holstein hat sich - wie vorgesehen - an dem Akkreditierungsverfahren beteiligt und so seinen Beitrag für eine sichere WM 2006 geleistet.

4.3.1 Neuregelung der DNA-Analyse zur Strafverfolgung

Mit dem Gesetz zur Novellierung der forensischen DNA-Analyse, das am 01.11.2005, in Kraft getreten ist, wurde insbesondere Folgendes geregelt:

- Die Voraussetzungen für eine DNA-Analyse zu Zwecken künftiger Strafverfolgung wurden unter Verzicht auf einen Anlasstatenkatalog dahingehend erweitert, dass die Maßnahme auch bei Beschuldigten zulässig wird, die wiederholt Straftaten auch von jeweils nicht erheblicher Bedeutung begangen haben und diese voraussichtlich wieder begehen werden, wenn diese Straftaten in ihrer Summe den Unrechtsgehalt einer Straftat von erheblicher Bedeutung erreichen (§ 81g Abs. 1 Satz 1 und 2 StPO).

- Bei einer Einwilligung der betroffenen Personen in eine DNA-Analyse ist keine gerichtliche Entscheidung erforderlich (§ 81g Abs. 3 StPO).

Beide Neuregelungen werden vom ULD kritisiert. Insbesondere die Einwilligungslösung wird dahingehend als problematisch angesehen, dass sich die Betroffenen im Strafverfahren in einer Drucksituation befänden, welche die Freiwilligkeit einer erklärten Einwilligung als zweifelhaft erscheinen lasse.
Die Einwendungen des ULD sind nach Auffassung des Ministeriums für Justiz, Arbeit und Europa nicht überzeugend. Die Streichung der Regelbeispiele in § 81g Abs. 1 StPO erfolgte, weil dem Missverständnis entgegen getreten werden sollte, nur besonders schwere Straftaten könnten eine DNA-Analyse für Zwecke künftiger Strafverfolgung rechtfertigen. Bedenken im Hinblick auf den Bestimmtheitsgrundsatz aus Art. 103 Abs. 2 GG bestehen nicht, da der unbestimmte Rechtsbegriff einer Straftat von erheblicher Bedeutung durch die dazu ergangene höchstrichterliche Rechtsprechung mittlerweile ausreichend konkretisiert ist (vgl. BVerfGE 103, 21).
Auch die Ermöglichung der DNA-Analyse, wenn der Beschuldigte wiederholt Straftaten begangen hat, die für sich genommen die Schwelle zur erheblichen Straftat nicht erreichen, aber in ihrer Gesamtheit einer Straftat von erheblicher Bedeutung gleichstehen (§ 81g Abs. 1 Satz 2 StPO), begegnet im Ergebnis keinen - insbesondere verfassungsrechtlichen - Bedenken. Erfasst sein dürften Fälle, die entweder im Bereich der mittleren Kriminalität liegen, ohne dass die ansonsten für eine Straftat von erheblicher Bedeutung erforderlichen Auswirkungen auf den Rechtsfrieden und das Gefühl der Rechtssicherheit der Bevölkerung (vgl. BVerfGE 103, 21) vorliegen oder die im unteren Bereich der Kriminalität liegen (*Senge* NJW 2005, 3028). Die unbestimmten Rechtsbegriffe sind ebenfalls durch die obergerichtliche Rechtsprechung hinreichend konkretisierbar.

Zum Wegfall des Richtervorbehalts ist richtig, dass die betroffenen Personen im Strafverfahren einer besonderen Drucksituation ausgesetzt sind. Dieser Lage wird jedoch dadurch Rechnung getragen, dass der Betroffene qualifiziert belehrt werden muss, damit die schriftlich erklärte Einwilligung Wirksamkeit erlangen kann. Die qualifizierte Belehrung umfasst nicht nur, dass Körperzellen vom Betroffenen benötigt würden, um einen molekulargenetischen Abgleich mit Spurenmaterial vorzunehmen, sondern auch Informationen über die weitere Nutzung und die voraussichtliche Speicherdauer. Die-

se Belehrung erfolgt in Schleswig-Holstein durch die „Hinweise zur Einwilligungserklärung (§ 81 g StPO)“ des LKA.
Dementsprechend hat Schleswig-Holstein das Gesetz zur Novellierung der forensischen DNA-Analyse im Gesetzgebungsverfahren unterstützt.

4.3.2 Warum waren Sie in der Nähe des Tatortes?

Grundsätzlich dient eine Funkzellenabfrage zur Ermittlung eines Täters. Jedoch ermöglicht sie auch die zwangsläufige Ermittlung bzw. Erfassung von an der Tat unbeteiligten Personen, zu der es aufgrund von wenig vorhandenen Daten (es sind häufig nur die Geo- und Zeitdaten bekannt) kommt.
Allerdings rechtfertigt allein der Umstand, dass von einem Handy zur tatrelevanten Zeit in Tatortnähe Mobilfunkverkehr geführt worden ist, nicht die Annahme, dass der Besitzer des betreffenden Handys auch in irgendeiner Art und Weise an der Tat beteiligt war. Mithin sind die durch die Funkzellenabfrage ermittelten Personen bei Nichtvorliegen weiterer Verdachtsmomente zunächst als Zeugen und nicht als Beschuldigte anzusehen.
Insoweit ist in den beiden Ausgangsfällen in Bad Segeberg und Ödendorf sowohl die von der Polizei vorgenommene Datennutzung als auch die Annahme der Zeugeneigenschaft der Betroffenen korrekt.
Insbesondere sind im Falle der schriftlichen Zeugenbefragung durch die Kriminalpolizei Bad Segeberg die angeschriebenen Personen über ihren rechtlichen Status nicht im Unklaren gelassen worden. Aus dem von der Kriminalpolizei erstellten Zeugenbefragungsbogen sowie dem dazugehörigen Anschreiben geht hervor, dass es sich um eine schriftliche Zeugenbefragung handelt. So war das Anschreiben zum Fragebogen mit den Worten „Die Kriminalpolizei bittet um Ihre Mithilfe“ überschrieben und mit einer dem Wortlaut der §§ 52 Abs. 1, 55 StPO entsprechenden Zeugenbelehrung versehen. Darüber hinaus befand sich der Hinweis „Zeugen-Anhörung“ auf dem Fragebogen.
Aus den genannten objektiven Umständen folgt, dass eine verständige Person von einer Befragung als Zeuge ausgehen musste.
Hierfür spricht auch, dass es nur sehr vereinzelt Nachfragen aus der Bevölkerung zum Fragebogen gegeben hat. Soweit im Mordfall in Ödendorf die durch die Funkzelle ermittelten Personen durch Beamte der zuständigen Kriminalpolizei angerufen worden sind, wurden auch diese Personen entsprechend belehrt.
Hinsichtlich der weiteren vertrauensvollen Zusammenarbeit zwischen der Staatsanwaltschaft und dem ULD erwartet auch das Ministerium für Justiz, Arbeit und Europa, dass der Dialog im Sinne eines bestmöglichen Datenschutzes unter Berücksichtigung der Strafverfolgungsinteressen der Ermittlungsbehörden fortgesetzt wird.

4.4.4 Protokollierungslücken bei der Polizei erleichtern unberechtigte ZEVIS-Abrufe

Bei dem vom ULD geschilderten Fall einer nicht nachvollziehbaren Datenabfrage beim Zentralen Verkehrsinformationssystem (ZEVIS) handelt es sich um einen Einzelfall. Dies ist natürlich für den Petenten sehr bedauerlich.
In diesem Zusammenhang aber von der „Spitze des Eisberges“ zu sprechen, ist übertrieben. Das Innenministerium hat diesen Vorfall zum Anlass genommen, die Verfahrensregelungen, u. a. durch technische Vorgaben, revisionssicherer zu machen.

4.5.1 Hartz IV

Das ULD hat angemerkt, dass die Bundesagentur für Arbeit (BA) die Überarbeitung der Antragsvordrucke im letzten Jahr zugesagt und auch durchgeführt hat, diese nun vorhandenen Antragsvordrucke bisher jedoch nicht zur Verfügung stehen. Zudem strebt das ULD eine „Paketlösung“ an, mit der sichergestellt wird, dass die neuen Vordrucke nur mit den entsprechenden Ausfüllhinweisen verwendet werden.
Die BA hat dazu mitgeteilt, dass bis spätestens 30.06.2006 die überarbeiteten Antragsvordrucke zusammen mit den Ausfüllhinweisen als „Paket“ in den Arbeitsgemeinschaften (Argen) herausgegeben werden sollen. Durch eine entsprechende Handlungsempfehlung werde den Argen diese Vorgehensweise von der BA empfohlen.
Schon im letzten Tätigkeitsbericht hat das ULD auf Mängel des eingesetzten EDV-Verfahrens aufmerksam gemacht. Nach wie vor seien keine ausreichenden Löschungsmöglichkeiten der Daten sowie keine eingeschränkten Zugriffsberechtigungen und Zugriffsprotokollierungen vorhanden. Zurzeit stünden die Daten der EDV-Verfahren allen bundesweiten Anwendern zur Verfügung.
Nach Auffassung der BA bedarf dieser Vorwurf der Konkretisierung, da es nicht zutreffend ist, dass in den EDV-Verfahren keine Löschungsmöglichkeiten vorgesehen sind. Hinsichtlich der eingeschränkten Zugriffsberechtigungen wird darauf hingewiesen, dass das neue Verfahren „Vermittlungs-, Beratungs- und Informationssystem“ (VerBis) diese Forderungen berücksichtigt. Für das Verfahren „Arbeitslosengeld 2 Leistungen zum Lebensunterhalt“ (A2LL) wird das Zugriffsberechtigungskonzept noch mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) abgestimmt.
Das ULD befürchtet, dass bei der Einführung neuer EDV-Verfahren die datenschutzgerechte Migration der Daten nicht gegeben ist, sondern veraltete Daten ungeprüft überspielt werden.
Die BA weist darauf hin, dass das neue Verfahren VerBis und die entsprechenden alten Verfahren coArbNT/COMPAS in vielen Bereichen funktional als auch im Hinblick auf die Datenstruktur sehr unterschiedliche Systeme sind. Aus diesem Grunde ließ es sich nicht vermeiden, dass Altfälle nicht automatisch, sondern nur manuell in VerBis nachgearbeitet und gelöscht werden können. Zudem wurden nach fachlicher Vorgabe eine Reihe besonderer Festlegungen für die Datenübernahme im Rahmen der Migration getroffen, damit sich ein Folgeaufwand im System VerBis auf ein möglichst geringes Maß reduziert.
Ein besonderes Projekt Datenqualitätsmanagement (DQM) befasst sich damit, Daten so aufzubereiten, dass sie qualitativ hochwertig in VerBis eingearbeitet werden können. Hierzu wurde u.a. festgelegt, Bewerber- und Stellendaten auf aktuellem Stand zu halten und offene Wiedervorlagen und Fehlermeldungen rechtzeitig abzuarbeiten.

Das ULD sieht die telefonische Befragung durch Callcenter als auch die Durchführung mancher Hausbesuche als rechtlich zweifelhafte Aktionen an. Diese Bereiche bedürften sensibler Vorgehensweise und strukturierter Konzepte, aus denen klare Kriterien sowohl für die Mitarbeiterinnen und Mitarbeiter als auch für die betroffenen Menschen hervorgehen.
Die BA verweist auf den Koalitionsvertrag der Regierungsparteien vom 11.11.2005, indem diese sich darauf verständigt hatten, eine gesetzliche Grundlage dafür zu schaffen, dass Leistungsempfänger zur Teilnahme an einer Telefonabfrage verpflichtet werden, in der die aktuellen Lebenssituationen überprüft werden. Im Januar 2006 wurde eine zweite telefonische Befragung von SGB II-Kunden gestartet, die unter

frühzeitiger Einbindung des BfDI vorbereitet und abgestimmt wurde. Insbesondere werden nun die Forderungen nach einem vorab postalisch versendeten Informationsschreiben und dem Hinweis auf die Freiwilligkeit an der Teilnahme bei der Befragung erfüllt.
Die Durchführung der telefonischen Befragung der SGB II-Kunden erfolgt nach einer klaren Struktur. Sie wird den Argen von der Zentrale der BA als vertragliche Leistung angeboten. Sofern ein Vertrag abgeschlossen wurde, werden die Anrufe nach einem vorgegebenen und mit dem BfDI abgestimmten Gesprächsleitfaden von BA- Mitarbeitern in Service Centern durchgeführt. Konsequenzen aus den Ergebnissen der Befragung sind den Argen vorbehalten.
Der aktuelle Gesetzentwurf zum SGB II-Fortentwicklungsgesetz sieht durch die Änderung des § 51 SGB II eine Ermächtigungsgrundlage für die Telefonbefragung wie geplant vor.
Hinsichtlich der Durchführung von Hausbesuchen bei ALG II-Empfängern teilt die BA mit, dass weder Handlungsempfehlungen oder Geschäftsanweisungen noch Mindeststandards festgelegt worden sind. Die BA stellt klar, dass keine Hausbesuche durch die BA veranlasst oder durchgeführt werden oder wurden. Auch hier verweist die BA auf das SGB II-Fortentwicklungsgesetz. Als weitere Maßnahme zur Bekämpfung von Leistungsmissbrauch soll die Einrichtung eines Außendienstes durch die Träger der Grundsicherung eingeführt werden.

Das ULD berichtet, dass Betroffene wiederholt geschildert haben, dass bereits in den Eingangsbereichen der Argen sehr persönliche Fragen gestellt und nicht auf Diskretion und Vertraulichkeit geachtet worden sei.
Das Ministerium für Justiz, Arbeit und Europa hat in seinen regelmäßigen Besprechungen mit den Geschäftsführern der Argen und Optionskommunen dieses Thema angesprochen. Es bestand einhellig die Auffassung, dass dieser Bereich heikel und somit mit großem Feingefühl behandelt werden muss. Entsprechend den jeweiligen Möglichkeiten vor Ort sind Diskretionsbereiche eingerichtet worden. Leider gab es zu Beginn der Umsetzung des SGB II oftmals räumliche Probleme, die aber im Laufe der Zeit weitgehend behoben werden konnten. Die Vertraulichkeit von persönlichen Daten ist allen Mitarbeiterinnen und Mitarbeitern bewusst und wird dementsprechend beachtet.

Aus Sicht des ULD ist die rechtliche Stellung der Argen und damit die Klärung der Zuständigkeit des Landesbeauftragten für Datenschutz klar. Das ULD sieht die Argen als eigenverantwortlich Daten verarbeitende Stellen, die der Kontrolle des ULD unterliegen.
Aus Sicht des Innenministeriums können die Arbeitsgemeinschaften nach § 44 b SGB II nicht als Behörden im Sinne des § 3 Abs. 2 LVwG angesehen werden. Nach § 3 Abs. 2 LVwG ist Behörde im Sinne des LVwG jede organisatorisch selbständige Stelle, die öffentlich-rechtliche Verwaltungstätigkeit ausübt. Diese Verwaltungstätigkeit nehmen die Behörden für die Träger der öffentlichen Verwaltung wahr. Gemäß § 2 Abs. 1 LVwG sind Träger der öffentlichen Verwaltung Land, Gemeinden, Kreise und Ämter. Mit der Gründung einer Arbeitsgemeinschaft nach § 44 b SGB II errichten die Kreise bzw. kreisfreien Städte als Träger der öffentlichen Verwaltung und gleichzeitig als Träger von Leistungen nach dem SGB II zusammen mit der Bundesagentur für Arbeit (Bundesverwaltung) Arbeitsgemeinschaften. Mit den Arbeitsgemeinschaften entstehen im Ergebnis keine neuen Behörden, sondern vielmehr liegt ein Rechtsinstitut eigener Art vor.

Die Regionaldirektion Nord hat mehrfach darauf aufmerksam gemacht, dass die BA auch im Rahmen des Datenschutzes eine getrennte Zuständigkeit sieht. Die Unterteilung und somit auch die Zuständigkeit der Datenschutzbeauftragten muss demnach nach dem für die Leistungsart jeweils zuständigen Träger (BA oder Kommune) vorgenommen werden.

4.6.5 Verkürzung der Aufbewahrungsfrist von Patientenakten auf zehn Jahre

Das ULD führt aus, die in der Vergangenheit übliche Aufbewahrung von Patientenakten über 30 Jahre sei damit begründet worden, dass die Verjährung zivilrechtlicher Ansprüche erst nach diesem Zeitraum eingetreten sei. Patientenakten könnten bereits nach zehn Jahren vernichtet werden, da mit der 2002 durchgeführten Schuldrechtsreform heute eine regelmäßige Verjährungsfrist von drei Jahren gelte.

Hier irrt das ULD. Ein Blick ins Gesetz führt zu der Erkenntnis, dass die maßgeblichen zivilrechtlichen Ansprüche gerade nicht der regelmäßigen Verjährungsfrist unterliegen. Nach § 199 Abs.2 BGB verjähren Schadensersatzansprüche, die auf der Verletzung des Lebens, des Körpers, der Gesundheit oder der Freiheit beruhen, nach wie vor in 30 Jahren von der Begehung der Handlung an. Darunter fallen auch und insbesondere Schadensersatzansprüche aufgrund von Behandlungsfehlern im Rahmen der Arzthaftung. Die in Kliniken praktizierte Aufbewahrung über einen Zeitraum von 30 Jahren korrespondiert mit dieser Regelung und ist daher beizubehalten.

4.6.6 Besuch vom Pflegeberater der AOK

Probleme im Zusammenhang mit dem Einsatz von Pflegeberatern der AOK Schleswig-Holstein sind bisher nicht an das Ministerium für Soziales, Gesundheit, Familie, Jugend und Senioren herangetragen worden.
Die AOK Schleswig-Holstein hat zu dem vom ULD dargestellten Fall mitgeteilt, dass die geschilderte Problematik auf die Anfänge des Einsatzes von Pflegeberaterinnen und Pflegeberatern der AOK in den Jahren 2004 und 2005 zurückgehe. Das beanstandete Vorgehen der Pflegeberater sei nach Diskussion und in engem Zusammenwirken mit dem ULD von der AOK bereits vor längerer Zeit abgestellt worden. Eine Beratung durch Pflegeberater der AOK erfolge lediglich auf Ersuchen der oder des Pflegebedürftigen bzw. ihrer Angehörigen. Hausbesuche würden nur durchgeführt, wenn Versicherte dies ausdrücklich wünschten. In der Folge sei die Zahl der Hausbesuche erheblich zurückgegangen. Eine Einsichtnahme in die Pflegedokumentation erfolge nur mit schriftlicher Einverständniserklärung der oder des Versicherten. Daher könne es sich nur um einen Einzelfall handeln, der natürlich für die Betroffene sehr bedauerlich ist.

4.7.1 Kindertageseinrichtungen kooperieren mit Grundschulen

Das ULD kritisiert, dass in der Vergangenheit in Einzelfällen im Zusammenhang mit den Maßnahmen zur Sprachstandfeststellung und Sprachförderung von einzuschulenden Kindern (sog. SPRINT-Maßnahmen), Daten dieser Kinder durch die Grundschulen ohne Einverständnis der Eltern und ohne rechtliche Grundlage bei den Kindertagesstätten abgefragt bzw. von dort an die Grundschulen übermittelt wurden.

Die Datenübermittlung zwischen Schulen und anderen öffentlichen Stellen ist in § 50 Abs. 3 Schulgesetz (SchulG) geregelt. Danach ist die Übermittlung personenbezoge-

ner Daten zwischen Schulen, Schulträgern und Schulaufsichtsbehörden an „andere öffentliche Stellen“ zulässig, wenn sie zur jeweiligen Aufgabenerfüllung erforderlich ist. Bei Kindertagesstätten handelt es sich nur dann um „öffentliche Stellen“, wenn sie in der Trägerschaft einer Gemeinde, eines Amtes, eines Zweckverbandes oder eines öffentlichen Trägers der Jugendhilfe stehen (§ 9 Abs. 1 Nr. 2 und 3 Kindertagesstättengesetz - KitaG) stehen. Keine „öffentliche Stellen“ im Sinne des § 50 Abs. 3 SchulG sind danach die von den anerkannten Trägern der freien Jugendpflege oder anderen Trägern (§ 9 Abs. 1 Nr. 1 und 4 KitaG) getragenen Kindertagesstätten. Die Übermittlung von Daten an diese - wie auch an öffentlichen Stellen - durch die Schule ist nach § 50 Abs. 3 S. 2 SchulG nur mit Einwilligung der Betroffenen zulässig. Die Übermittlung der Daten durch die Kindertagesstätten an die Schulen ist weder im SchulG noch im KitaG geregelt.
Vor diesem Hintergrund hat das Ministerium für Bildung und Frauen mit Erlass vom 14.10.2005 geregelt, dass die Daten der Kinder nur mit Einwilligung der Erziehungsberechtigten von der Kindertagesstätte - gleich in welcher Trägerschaft - an die Schule übermittelt werden dürfen. Ferner wurde geregelt, dass Informationen, die von den Kindertagesstätten bereits vor Inkrafttreten des Erlasses ohne Einverständnis der Erziehungsberechtigten weitergegeben wurden, nicht verwertet werden dürfen und unverzüglich zu löschen sind. Dem Erlass liegt eine Vorlage für eine standardisierte Einverständniserklärung der Erziehungsberechtigten bei. Mit diesen Regelungen wurden - auch aus Sicht des ULD – die Anforderungen an den Datenschutz erfüllt.

4.7.2 Videoüberwachung an Schulen

Auch das ULD erkennt ein Bedürfnis zur Videoüberwachung von schulischen Anlagen in eng begrenzten Ausnahmefällen an, z.B., wenn die Überwachung von Fahrradkellern zur Vermeidung von Diebstählen und Vandalismus notwendig ist. Es weist allerdings ausdrücklich darauf hin, dass ein Bedürfnis für die Videoüberwachung von Unterricht nicht bestehen kann.
Die Schulgebäude und -gelände unterliegen dem Hausrecht des Schulträgers, das die Schulleitung für diese ausübt (§ 82 Abs. 4 SchulG) und sind nicht dem Gemeingebrauch durch die Allgemeinheit zugänglich. Das Betreten des Schulgeländes oder der dortige Aufenthalt kommt nur im Zusammenhang mit den Aufgaben einer Schule in Betracht. Ausnahmen bilden lediglich die nachmittäglichen anderweitigen Nutzungen des Schulgeländes (z: B: für Fortbildungsveranstaltungen), die aber auch stets auf einen vom Schulträger individuell zugelassenen Nutzerkreis begrenzt sind. Eine Videoüberwachung von Schulgeländen ist demnach zur Wahrnehmung der Aufgaben der Schulen oder zur Ausübung des Hausrechts unter sorgfältiger Abwägung mit den Belangen der Benutzerinnen oder Benutzer zulässig. So kann beispielsweise eine Überwachung von einzelnen Flächen oder Gebäudeteilen zur Vermeidung von Vandalismus ausnahmsweise erforderlich sein, wenn diese nicht durch Personal beaufsichtigt werden können. Im Ergebnis teilt das Ministerium für Bildung und Frauen die Auffassung des ULD, dass eine Videoüberwachung schulischer Anlagen eine Ausnahme bleiben muss und erst in Betracht kommt, wenn alle pädagogischen Mittel zur Konfliktlösung gescheitert sind.

4.8.1 Verfassungsbeschwerde: Kontenabruf

Der IX. Senat des BFH hat mit seiner am 11.01.2006 veröffentlichten Entscheidung vom 29.11.2005 ausdrücklich betont, dass der Kontenabruf nicht nur verfassungsgemäß ist, sondern sogar verfassungsrechtlich geboten ist. Das Kontenabrufverfahren

ist nicht nur zur Verifikation geeignet; es ist wegen der Regelung über das sog. Bankgeheimnis (§ 30a Abgabenordnung - AO) auch verfassungsrechtlich notwendig, um das Erklärungsverhalten der Steuerpflichtigen zu überprüfen. Das BVerfG hat im einstweiligen Rechtsschutzverfahren die das Gesetz konkretisierenden Regelungen im Anwendungserlass ausdrücklich gebilligt.

4.8.2 Einsicht in Steuerakten für Betroffene

Nach der Rechtsprechung des Bundesfinanzhofes (BFH) muss jeder Bürger Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen. Die Herstellung steuerlicher Belastungsgleichheit ist nach Auffassung des BVerfG ein solches überwiegendes Allgemeininteresse.
Da in der Abgabenordnung kein Anspruch auf Akteneinsicht vorgesehen ist, steht die Entscheidung hierüber den Finanzbehörden zu. Sie entscheiden nach pflichtgemäßem Ermessen, ob und inwieweit sie einem Beteiligten in einem steuerlichen Verwaltungsverfahren Akteneinsicht, z.B. zur Kenntnisnahme entscheidungserheblicher Tatsachen und Beweisergebnisse, gewähren wollen und können (§ 364 AO). Die Beteiligten haben insofern nur einen Anspruch auf fehlerfreie Ermessensausübung. In dem vom ULD geschilderten Fall hat das zuständige Finanzamt nach umfangreicher Prüfung eine Ermessensentscheidung getroffen und dem Betroffenen schließlich Einsicht in seine Steuerakte gewährt. Die Prüfung als „bürgerfeindliche Praxis“ zu bezeichnen, hält das Finanzministerium für unangebracht.

6.1 Der Datenschutzzyklus

Die Teilziffer 6.1 übernimmt die Einleitung in das Gesamtthema Systemdatenschutz. Der Bericht suggeriert, dass die IT-Verantwortlichen ohne die tatkräftige - und kostenpflichtige - Unterstützung des ULD über den gesamten Zyklus der Verfahrensplanung und -einführung keine datenschutzgerechte Arbeit leisten können. Da die Landesverwaltung aber über gut ausgebildetes Personal verfügt, das sich seiner datenschutzrechtlichen Aufgaben durchaus bewusst ist, kann diese Auffassung aus der Sicht des ULD zwar nachvollzogen, in der Absolutheit der Aussage aber nicht unterstützt werden.

6.5 Datenschutzgerechte Protokollierung

Die Problematik der Protokollierung der Aktivitäten von Systemadministratoren und der Nutzung der Anwender der Fachverfahren ist ein seit langem bekanntes Thema. Vor dem Hintergrund der Feststellungen im aktuellen Tätigkeitsbericht, dass ein Standard für derartige Protokollierungen nicht definiert ist und die Anforderungen des ULD mit den derzeit am Markt gängigen Systemen nicht realisierbar sind - nach den Recherchen des ULD genügen weder Windows 2003 Server noch syslog-Architekturen auf UNIX-Servern diesen Anforderungen - erscheint die Debatte um eine rein technische Umsetzung der Anforderungen nach Auffassung des Finanzministeriums nicht zielführend.
Das gleiche gilt für den Vorschlag zum Aufbau dedizierter und mandantenfähiger Protokollserver. Hier ist weiterhin das Zusammenwirken von technischen und organisatorischen Maßnahmen zur Umsetzung der Anforderungen des Datenschutzes zwingend.

6.6 Dokumentenmanagementsystem elektronischer Akten

Die Arbeiten zur "schrittweisen Einführung der elektronischen Akte", für die das Finanzministerium ressortübergreifend zuständig ist, werden in intensiver Abstimmung mit dem ULD durchgeführt. Dazu gehört die Beteiligung des ULD schon im Rahmen der AG „3P“ (Begleitarbeitsgruppe für das Projekt „3P“ - Pflichtenheft, Produktauswahl, Pilotierung) ebenso wie die Abstimmung sämtlicher organisatorischer Konzepte mit dem ULD. Das Finanzministerium und das ULD gewinnen aus diesen Arbeiten Hinweise und Erkenntnisse, die dann z.B. auch in diesen Tätigkeitsbericht eingeflossen sind.

Im März d. J. haben die Datenschutzbeauftragten in bundesweiter Abstimmung eine "Orientierungshilfe der Arbeitsgruppe des Arbeitskreises eGovernment der Konferenz der Datenschutzbeauftragten des Bundes und der Länder - Datenschutz bei Dokumentenmanagementsystemen" herausgegeben (siehe z.B. http://www.datenschutz.thueringen.de/veroeffentlichungen/Orientierungshilfen/Datenschutz bei_Dokumentenmanagementsystemen.htm).Das Finanzministerium wird auch Erkenntnisse aus dieser Orientierungshilfe bei der Fertigstellung der Konzepte einbeziehen.

Nach Auffassung des ULD besteht die neue Qualität eines Dokumentenmanagementsystems (DMS) darin, dass die Tätigkeiten der Beschäftigten automatisiert und im Detail erfasst und ausgewertet werden können. Dies ergebe für sich und erst recht in der Kombination eine brisante Sammlung an Informationen über die Leistung und das Verhalten der Beschäftigten.
Das Finanzministerium bewertet die Eigenschaft eines DMS, bestimmte Informationen "mitzuschreiben", insbesondere aus datenschutzrechtlicher Sicht sehr viel positiver. Durch die Protokollierung und Historisierung an dezidierten Stellen (und sonst nirgendwo) können diese Informationen abschließend datenschutzrechtlich bewertet und die notwendigen Regelungen implementiert werden. Dies ist bei dezentralen fragmentierten Systemlandschaften so gut wie unmöglich. Die Schlussfolgerung des ULD hierzu trifft in der Formulierung nicht ganz die Intention des Finanzministeriums, nämlich den Datenschutz einschließlich des Mitarbeiterdatenschutzes zu beachten, um qualitativ hochwertige und rechtmäßige Datenverarbeitung zu betreiben und nicht, um - mit wem auch immer - Ärger zu vermeiden.

6.7 Clearingstellen sind nur eine Übergangslösung

Die Übermittlung der elektronischen Rückmeldung im Meldewesen zwischen den Meldeämtern muss zum 1. Januar 2007 nach bundeseinheitlichen Vorgaben funktionieren. Für die bundesländerübergreifende Datenübermittlung ist dabei die Verwendung von OSCI-Transport (Online Service Computer Interfaces-Transport) vorgegeben. Die Landesmeldeverordnung gibt vor, dass die Datenübermittlung über eine zentrale Vermittlungsstelle erfolgen muss. Diese so genannte Clearingstelle wird von Hamburg und Schleswig-Holstein gemeinsam im gesicherten Rechenzentrum bei Dataport betrieben. Die Darstellungen des ULD reduzieren die Betrachtung der Problematik auf ein rein technisches Problem.
Das organisatorische Problem, das mit der Problematik einer Datenübermittlung zwischen weit mehr als 10.000 Einwohnermeldeämtern in Deutschland verbunden ist, wird nicht in die Betrachtungen einbezogen.

Vor dem Hintergrund

- der Terminsetzung zum 1. Januar 2007,
- des bisher nur in Testversionen verfügbaren Deutschen Verwaltungsdienste Verzeichnisses (DVDV, als „Gelbe Seiten der elektronischen Verwaltungsdienste der gesamten deutschen Verwaltung“), auf das bei jeder Kommunikation zugegriffen werden muss und
- der Tatsache, dass es sich bei der bundesweiten OSCI-Transport-Infrastruktur um eine weitgehend neue Lösung handelt, dessen Funktionsfähigkeit in dieser Breite bisher nicht nachgewiesen ist,

hatte die Sicherstellung der elektronischen Übermittlung der Rückmeldung im Meldewesen für die Landesregierung die oberste Priorität. Die jetzt gefundene Struktur des für Hamburg und Schleswig-Holstein zentral organisierten länderübergreifenden Datenaustausches stellt für das Flächenland Schleswig-Holstein eine nach derzeitigem Stand der Technik angemessene und wirtschaftlich sinnvolle Lösung dar.
Derzeit wird die Bereitstellung einer Clearingstelle auch für andere zukünftige länderübergreifende Datenübermittlungen als hilfreich gesehen. Die gemeinschaftliche Nutzung dieser Infrastruktur durch mehrere Verwaltungsbereiche ist wirtschaftlich sinnvoll. Aus Sicht der Landesregierung stellen deshalb Clearingstellen nach derzeitigem Stand eine dauerhaft erforderliche Komponente der E-Government-Infrastruktur für Land und Kommunen dar.

6.9 IP-Telefonie

Die zentrale Steuerung der Sprachtelefonie durch das Finanzministerium bietet auch nach Auffassung des ULD administrative Vorteile. Die im Tätigkeitsbericht formulierten Bedenken sind unberechtigt, da in der Vorlage zum Regierungsbeschluss zur Einführung der IP-Telefonie die Sicherheitsproblematik dargestellt wurde. Diese beinhaltet auch ein Sicherheitskonzept zu erstellen, das die Thematik der Datensicherheit im Netzwerk und auf den Endgeräten behandelt.

9 Audit und Gütesiegel - Allgemeine Problematik

Während sich in den vergangenen Jahren die Behandlung des Themas auf eine Bewertung des Werkzeugs „Datenschutzaudit“ beschränkte, setzt sich der diesjährige Bericht auch inhaltlich mit laufenden Auditierungsverfahren des Landes auseinander.
Das Finanzministerium ist mit den Auditierungsverfahren „Landesnetz“ und „SAP-Modul KLR“ (Modul Kosten- und Leistungsrechnung) direkt betroffen.
Die Auditierungsverfahren werden vom ULD im Auftragsverhältnis durchgeführt. Auftraggeber für die beiden oben benannten Auditierungen ist das Finanzministerium. Das ULD erhält für die Durchführung der Auditierung ein Leistungsentgelt, das den Leistungsentgelten (hier Stundenentgelten) von Dataport entspricht. In den Anwendungsbestimmungen des ULD zum Datenschutzaudit ist geregelt, dass die Daten verarbeitende Stelle - also der Auftraggeber - über die Verwendung des Gutachtens (9.4) entscheidet.
Im aktuellen Tätigkeitsbericht setzt sich das ULD inhaltlich kritisch mit laufenden Auditierungsverfahren auseinander, eine Abstimmung mit den Auftraggebern ist nicht erfolgt. In der Wirkung wird das Problem dadurch verstärkt, dass die Berichte über die laufenden Auditierungsverfahren in ihrer Gestaltung nicht von den Berichten über Prüfungsverfahren zu unterscheiden sind. Eine Berichterstattung aus laufenden Auditie-

rungsverfahren, die das ULD für Auftraggeber gegen Bezahlung erbringt, wirkt sich unnötig negativ auf die laufenden Projekte aus.
Das ULD wird gebeten, zukünftig auf die inhaltliche Berichterstattung aus aktuell laufenden Auditierungsverfahren zu verzichten, andernfalls werden keine Finanzmittel für Auditierungsverfahren im IT-Haushalt (Kap. 1103) mehr bereitgestellt werden können.
Für den Fall zukünftiger Beauftragungen eines Auditierungsverfahrens ist darüber hinaus im Vorfeld eine exakte Klärung und Darstellung durch das ULD erforderlich, ob das ULD für die Erledigung eines Auditierungsverfahrens in einer komplizierten Infrastruktur personell und organisatorisch so aufgestellt ist, dass die Erledigung zeitnah erfolgen kann.

9.1.1 Landesnetz SH

Der im Tätigkeitsbericht vorgebrachten Suggestion, dass es sich beim Landesnetz um ein potentiell unsicheres Netz handelt, wird vom Finanzministerium ausdrücklich widersprochen. Zur Fortentwicklung des Landesnetzes hat das Finanzministerium das ULD mit der Durchführung eines Audits beauftragt. Zur Verwendung von Zwischenerkenntnissen des ULD, die nicht abschließend mit dem Finanzministerium als Auftraggeber behandelt wurden, kann derzeit keine Stellungnahme abgegeben werden. Zur Verwendung von Erkenntnisses, die im Rahmen eines beauftragten Audits gewonnen werden, wird auf die Stellungnahme zu Ziffer 9 verwiesen.

9.1.2 SAP R/3-Modul Kosten- und Leistungsrechnung

Das Finanzministerium hat als Auftraggeber mit dem ULD eine Vereinbarung über die Durchführung dieses Audits geschlossen. Das Auditverfahren befindet sich derzeit in der Phase der Bestandsaufnahme. Ein erster Bericht wurde vom ULD am 20.03.2006 an das Finanzministerium übergeben. In den Anwendungsbestimmungen des ULD zum Datenschutzaudit (9.3) ist geregelt, dass eine Veröffentlichung erst nach Verleihung des Datenschutzauditzeichens in Form eines Kurzgutachtens in einem Register des ULD erfolgt.
Die Veröffentlichung in diesem Tätigkeitsbericht erfolgt aus einem laufenden Verfahren, sie ist nicht mit dem Finanzministerium abgestimmt und kann daher nicht akzeptiert werden. Da es in der Landesverwaltung auch Bedenken zum Einsatz der Kosten- und Leistungsrechnung gibt, könnte die jetzige Darstellung vor Abschluss des Auditverfahrens negative Auswirkungen auf die Einführung der Kosten- und Leistungsrechnung haben.

11.1 Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten

Die vom Rat der EU-Justiz- und Innenminister am 21.02.2006 verabschiedete und an die Mitgliedstaaten gerichtete "Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15.03.2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG" muss spätestens 18 Monate nach ihrer Annahme in innerstaatliches Recht umgesetzt werden; also bis Ende August/September 2007.

Nach der Richtlinie müssen die Mitgliedstaaten die Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste und die Betreiber eines öffentlich zugänglichen

Kommunikationsnetzes verpflichten, die in Telefonaten, SMS-Kurzmitteilungen und der Internetnutzung erzeugten Daten (Verkehrs- und Standortdaten sowie alle damit in Zusammenhang stehenden Daten, die zur Feststellung des Teilnehmers oder Benutzers erforderlich sind) zu erheben und für einen bestimmten Zeitraum zu speichern. Es sollen demnach nicht die Kommunikationsinhalte (Daten, die Aufschluss über den Inhalt einer Kommunikation geben) gespeichert werden, sondern vor allem die sog. Verbindungsdaten. Ziel ist, mit Hilfe der Informationen über Quelle und Adressaten sowie die Dauer der Verbindung die Gesprächspartner vor allem in Fällen, in denen es um schwere Kriminalitätsformen geht, zurückzuverfolgen, zu identifizieren und zu lokalisieren.
Die Bewertung des ULD, wonach die Richtlinie eine "Richtungsentscheidung für eine überwachte europäische Informationsgesellschaft" darstellt, wird vom Ministerium für Justiz, Arbeit und Europa nicht geteilt. Die Richtlinie ist in ihrer jetzigen Ausgestaltung und gegenüber früheren Rechtsetzungsvorschlägen insgesamt ausgewogen und verhältnismäßig und berücksichtigt weitestgehend die Vorgaben des Bundesrates. Diese Einschätzung entspricht i.ü. - entgegen früheren Positionierungen - auch der der Mehrheit des Bundestages und des Europäischen Parlaments.
Die pauschale Behauptung, die Vorratsspeicherung von Daten sei verfassungswidrig, wird im Hinblick auf die verfassungsgerichtliche Rechtsprechung insbesondere zum Fernmeldegeheimnis nicht geteilt. Das BVerfG hat zwar wiederholt festgestellt, dass eine Erhebung personenbezogener Daten "auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken" verfassungswidrig wäre, allerdings hat es eine Vorratsspeicherung von Daten nicht generell verboten.

Die Entscheidungen des BVerfG, insbesondere zur "Volkszählung" (BVerfGE 65, 1 ff.), zur "Handy-Überwachung" (E 107, 299 ff.), zum "Lauschangriff" (E 109, 279 ff.), zum niedersächsischen Gefahrenabwehrgesetz (Entscheidung vom 27.07.2005, Az: 1 BvR 668/04, NJW 2005, 2603 ff.) sowie aktuell zur "Beschlagnahme von Verbindungsdaten" (Entscheidung vom 2.03.2006, Az: 2 BvR 2099/04) verlangen jedoch für die verfassungsmäßige Zulässigkeit der Vorratsdatenspeicherung eine bereichsspezifische, präzise und normenklare Begrenzung des Eingriffs sowie eine strikte Wahrung des Verhältnismäßigkeitsgrundsatzes. Dies besonders unter Beachtung insbesondere des Rechts auf informationelle Selbstbestimmung, des Fernmeldegeheimnises, der Berufsfreiheit sowie der Meinungs-, Informations-, Rundfunk- und Pressefreiheit.

In der "Handy-Überwachungs-Entscheidung" haben die Karlsruher Richter - unter Hinweis auf den Gesetzesvorbehalt in Artikel 10 Abs. 2 GG - betont, dass die Regelungen in §§ 100g und 100 h StPO, die bereits jetzt den Zugang der Strafverfolgungsbehörden zu den bei den Telekommunikationsunternehmen zu Abrechnungszwecken gespeicherten Daten ermöglichen, einen legitimen Zweck verfolgen, nämlich die Aufklärung und Verfolgung schwerer Straftaten.
Das BVerfG hat wiederholt die unabweisbaren Bedürfnisse einer wirksamen Strafverfolgung betont, das öffentliche Interesse an einer möglichst vollständigen Wahrheitsermittlung im Strafverfahren hervorgehoben und die wirksame Aufklärung gerade schwerer Straftaten als einen wesentlichen Auftrag eines rechtsstaatlichen Gemeinwesens bezeichnet. Insbesondere bei der Beschaffung von Beweismitteln für tatbestandsmäßiges Verhalten, zur Bestimmung des Standorts eines Beschuldigten und zur Abklärung, ob und bezüglich welcher Personen eine Telekommunikationsüberwachung Erfolg versprechend erscheint, ist die Auskunftsanordnung - auch nach Auffassung des BVerfG - "ein wirkungsvolles Ermittlungsinstrument". Ihre Eignung unterliegt

danach "keinen Zweifeln, wenn Auskunftsverlangen mit dem Ziel angeordnet werden, den Aufenthaltsort eines Beschuldigten in Erfahrung zu bringen".
Um insbesondere die Aufklärung schwerer Straftaten organisierter Kriminalität, bei gewerbsmäßiger Hehlerei, Raub, räuberischer Erpressung, Bandendiebstahl und die von Terrorakten zu ermöglichen oder nachhaltig zu verbessern, ist - auch nach Auffassung der staatsanwaltschaftlichen Praxis in Schleswig-Holstein - die Speicherung eines gewissen Umfangs von Daten ebenso unerlässlich wie eine Speicherfrist, die einen sachgerechten Zeitraum für Ermittlungsansätze eröffnet.
Die Landesregierung wird der Empfehlung des ULD daher nicht folgen, "auf allen Ebenen zu versuchen, diese aus Freiheitssicht folgenreiche Entscheidung rückgängig zu machen." Vielmehr wird sich die Landesregierung im Bundesrat bei der Umsetzung der Richtlinie in das innerstaatliche Recht für eine strikte Wahrung des Verhältnismäßigkeitsgrundsatzes sowie für eine interessengerechte Lösung einsetzen, die sowohl sicherheits- und datenschutzrechtliche als auch wirtschafts- und haushaltspolitische Belange berücksichtigt und gegeneinander abwägt.
Für diesen Abwägungsprozess sind die weiteren Empfehlungen des ULD (Wahl der kürzesten Speicherungsfrist von sechs Monaten, Eingrenzung der Speicheranlässe, inhaltliche Präzisierungen, etc.) eine geeignete Grundlage.

11.2 Grundsatz der Verfügbarkeit contra Zweckbindung

Der von der Kommission vorgelegte Vorschlag für einen Rahmenbeschluss des Rates über den Austausch von Informationen nach dem Grundsatz der Verfügbarkeit ist Teil des Haager Programms zum Ausbau eines Raumes der Freiheit, der Sicherheit und des Rechts. Er hat zum Ziel, den EU-weiten Austausch strafverfolgungsrelevanter Informationen zu vereinfachen.

Die Mitgliedstaaten sollen verpflichtet werden, den entsprechenden Behörden anderer Mitgliedstaaten und Europol bestimmte Informationen (DNS-Profile, Fingerabdrücke, ballistische Erkenntnisse, Kfz-Halterermittlungen, Tel.-Nummern und sonstige Verbindungsdaten sowie Mindestauskünfte zur Identifizierung von Personen aus Personenstandsregistern) online oder mittels Indexdaten und anschließender Informationserteilung zugänglich zu machen, wenn die Informationen für die ihnen übertragenen Aufgaben erforderlich sind und kein Ausnahmefall (Gefahr für laufende Ermittlungen, Schutz einer Informationsquelle, u.a.) vorliegt. Die Behörde, die die Informationen erhält, soll diese ausschließlich zu dem Zweck verwenden dürfen, für den sie bereitgestellt wurden. Ohne vorherige Genehmigung einer Justizbehörde des Mitgliedstaates, der die Information zur Verfügung gestellt hat, sollen sie nicht als Beweismittel für das Vorliegen einer Straftat verwendet werden dürfen.
Die Rechtsetzungsinitiative steht im Zusammenhang mit dem Vorschlag für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden.
Der Rahmenbeschluss ergänzt die europäische Datenschutz-Richtlinie von 1995, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit keine bzw. nur mittelbare Anwendung findet.
Im Einzelnen enthält der Rahmenbeschluss folgende Regelungen:

(1) Informations-, Auskunfts-, Berichtigungs-, Löschungs- und Sperrungsansprüche der Betroffenen können (nur dann) verweigert bzw. eingeschränkt erteilt werden, wenn dies z.B. "laufende Ermittlungen, Untersuchungen oder Verfahren oder die zu-

ständigen Behörden bei der ordnungsgemäßen Erfüllung ihrer Aufgaben behindern" würde (Artikel 19).

(2) Artikel 27 sieht die Verpflichtung der Mitgliedstaaten vor, dass jede Person im Falle der Verletzung der Rechte, die ihr nach diesem Rahmenbeschluss durch die für die betreffende Verarbeitung geltenden innerstaatlichen Rechtsvorschriften garantiert sind, bei Gericht Rechtsmittel einlegen kann.

(3) Nach Artikel 28 Nr. 1 kann jede Person, der wegen einer rechtswidrigen Verarbeitung ein Schaden entsteht, Schadensersatz von dem für die Verarbeitung Verantwortlichen erhalten, wobei jedoch eine Dispensmöglichkeit für den für die Verarbeitung Verantwortlichen eröffnet werden soll, wenn er nachweist, dass ihm der Umstand, durch den der Schaden eingetreten ist, nicht zur Last gelegt werden kann.

(4) Die Weitergabe personenbezogener Daten an Behörden aus Drittstaaten und an internationale Einrichtungen soll nur dann erfolgen, wenn dort ein gleichwertiger Datenschutz wie innerhalb der EU gewährleist wird. Ausnahmsweise sollen die Daten jedoch trotz des dortigen unzureichenden Datenschutzes weitergegeben werden, wenn dies zum Schutz der grundlegenden Interessen eines Mitgliedsstaats oder zur Abwehr einer drohenden ernsthaften Gefahr für die öffentliche Sicherheit notwendig ist (Artikel 15).

(5) Verbieten sollen die Mitgliedstaaten die Sammlung von Angaben über rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Mitgliedschaft in Gewerkschaften sowie zu Gesundheit und Sexualleben. Ausnahmen von dieser Regel sind u.a. erlaubt, wenn diese Daten für die Bekämpfung oder Vorbeugung von Straftaten "unabdingbar" sind, die betroffene Person ausdrücklich ihre Einwilligung zu der Datenverarbeitung erteilt hat oder nur bestimmte Personen einen Zugriff darauf haben (Artikel 6).

(6) Unabhängige öffentliche Kontrollstellen sollen die Anwendung der innerstaatlichen Bestimmungen zur Umsetzung des Rahmenbeschlusses in den Mitgliedstaten überwachen. Ihre "Untersuchungs- und Einwirkungsbefugnisse" dürfen jedoch weder die Vorschriften für Strafverfahren noch die Unabhängigkeit der Gerichte berühren (Erwägungsgrund 17 und Artikel 30 Nr. 9).

Nach Auffassung des Ministerium für Justiz, Arbeit und Europa ist der Rahmenbeschlussvorschlag "über den Austausch von Informationen nach dem Grundsatz der Verfügbarkeit" von entscheidender Bedeutung, um in einem Raum ohne Personenkontrollen an den Binnengrenzen schnellen Zugang zu Informationen aus anderen Mitgliedstaaten zu erhalten und dadurch Straftaten erfolgreich bekämpfen zu können.
Es wird die Einschätzung des ULD geteilt, dass für eine intensivierte polizeiliche Zusammenarbeit - wie beispielsweise durch den genannten Rahmenbeschlussvorschlag - auch datenschutzrechtliche Vorkehrungen erforderlich sind. Entgegen der Auffassung des ULD stellt der mit der Initiative verknüpfte Rahmenbeschlussvorschlag "über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden" einen bedeutenden Fortschritt für den Schutz personenbezogener Daten in einem wichtigen Bereich dar. Er gewährleistet einen angemessenen Datenschutz der Betroffenen und steht im Einklang mit dem Verhältnismäßigkeitsprinzip, so dass eine "grundlegende Überarbeitung" nicht erforderlich ist. Diese Auffassung wird i.ü. - trotz Kritik an einigen Einzelregelungen,

wie z.B. der konkreten Ausgestaltung des Zweckbindungsgebotes - vom Europäischen Datenschutzbeauftragten geteilt.
Die Landesregierung ist zuversichtlich, dass es auf EU-Ebene gelingt, eine interessengerechte Lösung zu erarbeiten, die auch die vom Europäischen Datenschutzbeauftragten vorgebrachten Bedenken berücksichtigt.

11.3 Das zweite Schengen – Der Vertrag von Prüm

Der Vertrag von Prüm, der den vertragsschließenden Ländern den gegenseitigen Zugriff auf DNA-Datenbanken, Fingerabdrucksammlungen und Kfz-Halter- und Fahrzeugregister ermöglicht, wird vom ULD kritisiert. Der Vertrag enthalte keine zeitgemäßen Standards und präzisen Vorgaben über die Verarbeitung personenbezogener Daten. Diese Einwendungen hält das Ministerium für Justiz, Arbeit und Europa sowie das Innenministerium nicht für überzeugend.

Im Vertragskapitel 7 des Prümer Vertrages sind ausreichende allgemeine Bestimmungen zum Datenschutz festgeschrieben. Insbesondere schreibt Art. 34 ein innerstaatlich zu fassendes datenschutzrechtliches Niveau fest, welches im Mindestmaß dem Übereinkommen des Europarates vom 28. Januar 1981 über den Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten und dem Zusatzprotokoll vom 08.11.2001 sowie der Empfehlung Nr. R (87) des Ministerkomitees des Europarates an die Mitgliedstaaten über die Nutzung personenbezogener Daten im Polizeibereich vom 17.09.1987 zu entsprechen hat. Dies gilt auch für Daten, die nicht automatisiert verarbeitet werden. Dieser Standard ist als ausreichend zu bezeichnen.
Dementsprechend hat Schleswig-Holstein zu den von der Bundesregierung vorgelegten Entwürfen eines Vertragsgesetzes sowie eines Gesetzes zur Umsetzung des Vertrages keine Einwendungen erhoben.

12.1 Die geplante Novelle des IFG

Die Aussagen des ULD zur geplanten Novelle des Informationsfreiheitsgesetz (IFG), die sich zurzeit in der Landtagsberatung befindet, sind geprägt von einer weiten Auslegung des IFG. Demgegenüber vertritt die Landesregierung eine engere Auffassung zur Anwendung des Gesetzes und hat dies im geplanten neuen IFG unzweifelhaft geregelt.
Weil die Einzelheiten zum Gesetzentwurf in den weiteren Landtagsdebatten beraten werden, weist das Innenministerium nur auf Folgendes hin:

- Der Gesetzentwurf regelt – im Gegensatz zur Auffassung des ULD - bei allgemeinen Verwaltungsinformationen, dass Informationsrechte nur dann bestehen sollen, wenn die Informationen im Rahmen „öffentlich-rechtlicher Verwaltungstätigkeit“ der Behörde entstanden sind. Dadurch sind Informationsansprüche ausgeschlossen, die aus dem Bereich des privatrechtlichen Behördenhandels erwachsen. Bei Umweltinformationen ist das privatrechtliche Handeln dagegen durch EG-Recht zwingend einzubeziehen.
- Das ULD kritisiert im Gesetzentwurf eine „durchgehende Unterscheidung“ zwischen Umwelt- und allgemeinen Verwaltungsinformationen. Diese Kritik greift bis auf die Regelung des Anwendungsbereiches in § 1 des Gesetzentwurfes nicht mehr, weil der Entwurf aufgrund der Ergebnisse der Anhörung diesbezüglich geändert wurde.

- Auch die kritisierte (bisher) fehlende Abwägungsklausel bei den Geschäfts- und Betriebsgeheimnissen ist aufgrund der Anhörung in den Gesetzentwurf eingefügt worden.

12.2.2 Informationszugang im Besteuerungsverfahren

Bei dem Verzicht des Gesetzgebers auf die Einräumung eines allgemeinen Auskunfts- und Akteneinsichtsrecht in der im Besteuerungsverfahren geltenden Abgabenordnung (AO) handelt es sich um einen absichtsvollen Regelungsverzicht. Der fehlende Anspruch auf Auskunft bzw. Akteneinsicht im außergerichtlichen Besteuerungsverfahren und eine insoweit der Finanzverwaltung eingeräumte Ermessensausübung verstoßen nicht gegen verfassungsrechtliche Grundsätze. Nach der Konzeption des Gesetzgebers soll die AO eine gerechte, gleichmäßige und für alle Beteiligten möglichst unbürokratische und zeitnahe Durchführung der Besteuerung sichern und hierbei einen gerechten Ausgleich zwischen den Belangen der Allgemeinheit und denen des Steuerpflichtigen schaffen. Dieser Anspruch wiegt gegenüber dem Zweck des IFG-SH, allen Bürgern freien Zugang zu den bei den Behörden vorhandenen Informationen zu gewährleisten, deutlich schwerer.
Die vom ULD vertretene Auffassung zum Informationszugang im Besteuerungsverfahren, nämlich, dass die Vorschriften der AO neben denen des IFG zur Anwendung kommen, wird vom Innenministerium und Finanzministerium nicht geteilt. Die bundesrechtliche Abgabenordung enthält abschließende Regelungen, die keinen Raum für parallele Informationsansprüche nach Landesrecht einräumen. Diese Auslegung der AO wird auch durch ein Urteil des Bundesfinanzhofes zum Verhältnis der AO zu Ansprüchen aus dem Datenschutzrecht gestützt (BFH v.04.06 2003, NVwZ 2004, S.302).

Mit freundlichen Grüßen

gez. Dr. Ralf Stegner