Schleswig-Holsteinischer Landtag
Umdruck 16/2220

Innenministerium
des Landes
Schleswig-Holstein

Minister

An den
Vorsitzenden des
Innen- und Rechtsausschusses
beim Schleswig-Holsteinischen Landtag
Herrn Werner Kalinka, MdL
Landeshaus

24105 Kiel

12. Juli 2007

29. Tätigkeitsbericht des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein

Sehr geehrter Herr Vorsitzender,

zu den wesentlichen Punkten des Unabhängigen Landeszentrums für Datenschutz (ULD) in seinem 29. Tätigkeitsbericht gebe ich die nachfolgende Stellungnahme ab:

Die Stellungnahmen des Ministeriums für Justiz, Arbeit und Europa (Ziffern 4.3.1, 4.3.2, 4.3.3, 4.5.1, 4.5.2, 4.5.3, 4.5.5, 4.5.6, 4.5.8, 7.1, 12.4.6), des Ministeriums für Bildung und Frauen (Ziffern 4.7.1, 4.7.2), des Finanzministeriums (Ziffern 4.8.2, 6.3, 9.1.1), des Ministeriums für Wissenschaft, Wirtschaft und Verkehr (Ziffern 4.4.1, 5.1) und des Ministeriums für Soziales, Gesundheit, Familie, Jugend und Senioren (Ziffern 4.5.12, 12.4.5) wurden einbezogen.

4.1.3 Online-Meldedatenabruf lässt auf sich warten
Der dargestellte Sachverhalt entspricht seit längerem nicht dem aktuellen Stand. Mit Unterzeichnung des Vertrages vom 5./14. Februar 2007 hat das Innenministerium Dataport mit der Erweiterung der Funktionalität der Clearingstelle beauftragt. Ab dem 01. August 2007 nimmt das neue Polizeiabrufverfahren seinen Dienst auf. Damit werden die erwähnten datenschutzrechtlichen Beanstandungen ausgeräumt. Gleichzeitig ist die Eigenbestandskontrolle der Meldebehörden sowie die Sichtung der Protokollierungsdaten zu getätigten Abrufen möglich. Auch dies war eine datenschutzrechtliche Forderung.

Ab dem 28. September 2007 wird der automatisierte elektronische Datenabruf von Behörden und sonstigen öffentlichen Stellen bundesweit sowie die Erteilung der einfachen Melderegisterauskunft für private Stellen eröffnet. Ab Januar 2008 erfolgt die

Postfach 71 25, 24171 Kiel | Telefon 0431 9 88-0 | Telefax 0431 9 88-2833 | ralf.stegner@im.landsh.de |
www.landesregierung.schleswig-holstein.de |
E-Mail-Adressen: Kein Zugang für elektronisch signierte oder verschlüsselte Dokumente

gesetzlich vorgeschrieben Nachberichtspflicht für die Meldebehörden automatisiert. Dann werden Datenempfängern, denen unvollständige oder unrichtige Daten übermittelt wurden, automatisiert die korrekten Daten nachberichtet. Ab März 2008 kann die Anmeldung über die Nutzung des vorausgefüllten Meldescheines erfolgen. Dies bedeutet für die Bürger und die Meldebehörden gleichermaßen eine deutliche Vereinfachung. Das handschriftliche Ausfüllen des Anmeldescheins und manuelle Erfassen der Daten durch die Meldebehörde gehören dann der Vergangenheit an.
Mit einer Realisierung dieses umfassenden Konzepts in dem vorgesehenen Zeitrahmen ist Schleswig-Holstein im bundesweiten Vergleich im Meldewesen weit vom „Tabellenende“ entfernt, wenn auch manche Länder einzelne Funktionalitäten eventuell früher realisieren mögen.
Die beschriebenen weiteren Schritte und deren Umsetzungsfristen waren auch dem ULD schon bei Redaktionsschluss seit längerem bekannt und sind von ihm bereits in Informationsveranstaltungen des Innenministeriums für die Meldebehörden nachdrücklich als datenschutzrechtliche Verbesserungen gewürdigt worden.

4.1.6 Erhebung von Lichtbilddaten durch die Passbehörde

Nach gegenwärtiger Rechtslage ist der Passbewerber verpflichtet, bei der Antragstellung ein aktuelles Lichtbild abzugeben; hinsichtlich der Qualitätsanforderungen (Biometriefähigkeit) ist die von der Bundesdruckerei zur Verfügung gestellte Foto-Mustertafel für Personaldokumente zu beachten (§ 6 Abs. 2 i. V. m. § 4 Abs. 1 Satz 2 PassG, Nr.6.2.3 PassVwV).
In einigen Passbehörden können Antragsteller das erforderliche Lichtbild mit Hilfe eines dort vorhandenen Automaten herstellen lassen. Dabei handelt es sich um eine freiwillige Leistung der Behörde.
Die vom ULD vorgeschlagene verstärkte Nutzung der Möglichkeiten der Digitalfotografie durch die Passbehörden könnte vor dem Hintergrund der kommunalen Selbstverwaltung vom Innenministerium empfohlen werden. Eine Verpflichtung wäre nur durch Änderung des (Bundes-)Gesetzes möglich, da das Passwesen der ausschließlichen Gesetzgebung des Bundes unterfällt (Artikel 73 Abs. 1 Nr. 3 GG).
Nach § 21 Abs. 2 enthält das Passregister u. a. das Lichtbild des Passbewerbers. Sofern das Register noch nicht in automatisierter Form geführt wird, wird das vorgelegte Lichtbild - entgegen der Auffassung des ULD - dafür physisch benötigt.
Bei dem Vorschlag des ULD ist zudem zu bedenken, dass eine entsprechende Empfehlung durch das Innenministerium als Eingriff in die Berufsfreiheit der Berufsfotografen gewertet werden könnte. Hierzu verweise ich auf zahlreiche 1999 an den damaligen Innenminister gerichtete Eingaben von Inhabern von Fotofachgeschäften im Zusammenhang mit der Einführung des digitalen Antragsverfahrens für Pass und Personalausweis (DIGANT). Seinerzeit wurde die Befürchtung geäußert, die Einführung des Verfahrens würde in dem Bereich zu wirtschaftlichen Einbußen führen. Diese Befürchtung konnte zerstreut werden, da die Behörde in dem Verfahren herkömmliche Lichtbilder verwendet und die Herstellung eines Lichtbildes über eine digitale Kamera von der Bundesdruckerei GmbH nicht unterstützt wird.

Der Vollständigkeit halber weise ich darauf hin, dass das zum Passrecht Ausgeführte entsprechend für das **Ausweisrecht** gilt. Das Ausweiswesen wurde im Zuge der Föderalismusreform durch Gesetz vom 28. August 2006 (BGBl. I S. 2034) ebenfalls der ausschließlichen Gesetzgebung des Bundes zugeordnet (Artikel 73 Abs. 1 Nr. 3 GG). Derzeit wird für einen Personalausweis noch kein biometriefähiges Lichtbild benötigt. Allerdings bereitet das BMI gegenwärtig die Einführung des elektronischen Personalausweises vor.

4.1.11 Informationsansprüche des Gesamtpersonalrates

Die Ausführungen des ULD zu den Informationsansprüchen des Gesamtpersonalrats sind missverständlich. Richtig ist, dass der Gesamtpersonalrat im Gegensatz zu den örtlichen Personalräten und den Stufenvertretungen lediglich eine sehr eingeschränkte Zuständigkeit in mitbestimmungsrechtlichen Angelegenheiten hat. Im Rahmen dieser Zuständigkeit stehen ihm allerdings die gleichen Informationsrechte zu wie den anderen Personalräten (vgl. § 61 Abs. 2 i.V.m. § 49 Mitbestimmungsgesetz Schl.-H.).
Es ist rechtlich nicht ausgeschlossen, dass der Gesamtpersonalrat auch für Personalangelegenheiten zuständig sein kann. Dies könnte z.B. bei Beförderungsaktionen der Fall sein, wenn die „Hauptdienststelle“ entscheidungsbefugt ist und eine Auswahl zwischen allen Beamtinnen und Beamten sämtlicher ihr angehörenden „Einzeldienststellen“ vorgenommen würde (dienststellenübergreifende Maßnahmen). In diesen Fällen wäre der Gesamtpersonalrat zuständig, da er die einzige von allen Beschäftigten der „Einzeldienststellen“ legitimierte Personalvertretung ist. Ihm sind dann - entgegen der Ausführungen des ULD - sehr wohl alle für die Entscheidung relevanten Informationen zu überlassen, zu denen ggf. auch Personalaktendaten gehören können.
Ferner ist darauf hinzuweisen, dass nicht der Gesamtpersonalrat in der Pflicht ist, seinen Informationsbedarf gegenüber der Dienststellenleitung zu begründen, sondern die Dienststellenleitung von sich aus verpflichtet ist, dem (Gesamt-)Personalrat alle mitbestimmungsrechtlich relevanten Informationen zukommen zu lassen.
Im Ergebnis bestimmt sich der Umfang des Unterrichtungsanspruchs des Gesamtpersonalrats nach der Erforderlichkeit für seine Aufgabenerfüllung unter Berücksichtigung seiner Zuständigkeit im Verhältnis zu den örtlichen Personalräten und Stufenvertretungen.

4.2.1 Neues Polizeirecht – Verfassungsmäßigkeit weiter fraglich

Die Anregung des ULD, den Gesetzentwurf zum neuen Polizeirecht noch einmal gründlich zu überarbeiten, ist nur vor dem Hintergrund des Redaktionsschlusses am 15.02.2007 für den 29. Tätigkeitsbericht erklärbar. Denn der Landtag hat bereits am 22. 02. 2007 mehrheitlich den Gesetzentwurf der Landesregierung einer Polizeirechtsnovelle (Landtagsdrucksache 16/670) in der Fassung eines gemeinsamen Änderungsantrages der Fraktionen von CDU und SPD (Landtagsdrucksache 16/1246 vom 21.02.2007), im Übrigen in der Fassung der Ausschussempfehlung (Landtagsdrucksache 16/1163 vom 15.02.2007) beschlossen. Das Gesetz ist seit dem 27.04.2007 in Kraft (Gesetz vom 13.03.2007, GVOBl. Schl.-H. 2007, Nr. 9 S. 234).
Die vom ULD in seinem Bericht vorgetragenen verfassungsrechtlichen Bedenken, zwar gestützt durch vom Innen- und Rechtssausschuss angehörte Sachverständige und von der Opposition im Landtag, sind bekannt, aber nicht zutreffend.

Auf Hinweis des Wissenschaftlichen Dienstes wurden folgende zwei Forderungen des Gesetzentwurfes konkretisiert bzw. verändert, die eine mögliche Gefahr für die Verfassungsmäßigkeit hätten darstellen können:

- Bei einer von der Polizei aufgrund ihrer Eilkompetenz veranlassten heimlichen Datenerhebung muss statt innerhalb von drei Tagen nunmehr unverzüglich die richterliche Entscheidung nachgeholt werden.
- Das Aufenthaltsverbot ist mit dem Kriminalvorbehalt des Art. 11 Grundgesetz formuliert.

Alle anderen Änderungsvorschläge, die der Landtag beschlossen hat, sind verfassungsrechtlich zwar nicht notwendig; sie dienen aber einer noch größeren Normen-

klarheit und Bestimmtheit des Gesetzes und sollen den Zweiflern an der Verfassungskonformität entgegenkommen.
Zwischenzeitlich ist eine landesverfassungsgerichtliche Entscheidung ergangen, die die vom ULD und von anderen Kritikern unterstellte Verfassungsbedenklichkeit der präventiven Wohnraumüberwachungsnorm ad absurdum führt. Der Verfassungsgerichtshof Rheinland-Pfalz hat mit seinem Mitte März veröffentlichten Urteil - VGH B 1/06 - vom 29.01.2007 die Verfassungsbeschwerde zur Wohnraumüberwachung im rheinland-pfälzischen Polizei- und Ordnungsbehördengesetz (§ 29 POG RP) zurückgewiesen. § 29 POG RP verstößt nicht gegen Landes- und Bundes-Verfassungsrecht. Damit bestätigt der rheinland-pfälzische Verfassungsgerichtshof (VGH) in Koblenz auch den schleswig-holsteinischen Gesetzgeber. § 29 POG RP stand Pate für die vom Landtag am 22.02.2007 beschlossenen Anpassungen der §§ 185 Abs. 3, 186 und § 186a Landesverwaltungsgesetz (LVwG) an die auf das Gefahrenabwehrrecht notwendig zu übertragenden Vorgaben des Urteils des Bundesverfassungsgerichtes zur repressiven akustischen Wohnraumüberwachung vom 24.06.2005 (BGBl. I. S. 1841).
Der im Laufe des Gesetzgebungsverfahrens immer wieder erhobene Vorwurf einer „ins Auge springenden Verfassungswidrigkeit“, weil der Gesetzentwurf und die Änderungsvorschläge u. a. nicht hinreichend den absoluten Schutz des unantastbaren Kernbereichs privater Lebensgestaltung gewährleisteten und das Gebot der Normenklarheit und –bestimmtheit nicht berücksichtigten, ist durch die Rechtsprechung des VGH Koblenz nicht bestätigt worden. Der VGH Koblenz hat seine Entscheidung am unantastbaren Kernbereich privater Lebensgestaltung zur Sicherung der Menschenwürde, am Grundsatz der Verhältnismäßigkeit und am Gebot der Normenbestimmtheit und Normenklarheit gemessen.

4.2.2 Auskunft an Betroffene durch die Polizei

Das Thema der Auskunftserteilung an Betroffene wurde im Innen- und Rechtsausschuss umfassend behandelt, so dass auf eine Stellungnahme an dieser Stelle verzichtet werden kann. Daher nur soviel: Ein grundsätzlicher Konsens besteht zwischen allen Verfahrensbeteiligten, dass die im Jahr 2002 getroffene Vereinbarung zwischen dem Generalstaatsanwalt und dem ULD weiterhin Grundlage für die Beantwortung von Auskunftsersuchen sein wird.

4.2.3 @rtus

Bei der Überarbeitung des Landesverwaltungsgesetzes sind Klarstellungen zum Vorgangsbearbeitungs- und –verwaltungssystem @rtus-VBS ergänzt worden, so dass es für die polizeiliche Handhabung künftig eine zweifelsfreie gesetzliche Ermächtigung gibt. Dabei ist allerdings nicht – wie vom ULD dargestellt – das Recht der Technik gefolgt.
Mit der Kennzeichnung von Verwaltungsvorgängen und der Dokumentation des Zugriffs auf diesen Bestand, erfüllt die Landespolizei - entgegen der Auffassung des ULD - den gesetzlichen Rahmen.

4.2.4 INPOL-neu

Das ULD kritisiert die Zusammenarbeit bei der Fortentwicklung des Verbunddateisystem INPOL-neu. Da es vom Innenministerium vertrauliche Unterlagen aus der Arbeit von Untergremien der Innenministerkonferenz (IMK) zur Verfügung gestellt bekommen wollte, wurde es an den IMK-Vorsitzenden verwiesen. Das hat das ULD allerdings nicht gemacht, sondern kritisiert stattdessen die mangelnde Zusammenarbeit.

Inzwischen dürfte sich das Anliegen des ULD durch das Angebot des Bundeskriminalamtes (BKA) vom 02.03.2007 an die Datenschutzbeauftragten des Bundes und der Länder erledigt haben. Neben zwei jährlichen Informationsveranstaltungen werden vor zukünftigen Beschlussfassungen die Tagungsunterlagen und im Nachgang die Protokolle der AG Kripo an die Datenschutzbehörden des Bundes und der Länder übersandt.

4.2.5 Zuverlässigkeitsüberprüfungen bei Großveranstaltungen

Soweit vom ULD das Nichtvorliegen der Einwilligung der betroffenen Personen bei den Landesbehörden bemängelt wird, ist folgendes festzustellen: Herr des Verfahrens war das FIFA-Organisationskomitee. Mit diesem gab es feste Absprachen von Seiten der Behörden. Soweit keine Einwilligungserklärung der Betroffenen vorlag, durfte keine Akkreditierung eingeleitet werden, d.h. die Daten der Personen durften nicht in das automatisierte Verfahren, an dessen Endpunkt die Landesbehörden standen, eingestellt werden. Es bestand kein Anlass zu der Annahme, dass eine der beteiligten Stellen von diesen Absprachen abgewichen ist, so dass die Vorlage einer Einwilligungserklärung erforderlich geworden wäre.
Aus Sicht der Verfassungsschutzbehörde hat es im Rahmen der Akkreditierung auch keine Sicherheitsüberprüfungen gegeben. Soweit die Verfassungsschutzbehörde beteiligt wurde, handelte es sich um reine Erkenntnisanfragen des Bundeskriminalamtes, die über das Bundesamt für Verfassungsschutz an die Verfassungsschutzbehörde gerichtet wurden.

4.2.6 Antiterrordatei – Angriff auf das Trennungsgebot

Die auf Bundesrecht gestützte Errichtungsanordnung sichert die nötige Trennung zwischen Polizei- und Verfassungsschutzbehörden hinreichend, wobei sie über die notwendige operative Trennung hinaus sogar den regelmäßigen Informationsverbund einschränkt und sensible Informationen einer besonders strengen Erforderlichkeits- und Verhältnismäßigkeitsprüfung aussetzt. Das Trennungsgebot wird durch die Antiterrordatei nicht berührt.

4.2.8 ED-Daten aus Schleswig-Holstein beim Bundeskriminalamt

Die Datensätze von erkennungsdienstlich behandelten Personen (ED-Daten) werden zweifach erstellt. Gem. § 2 Bundeskriminalamtgesetz (BKAG) wird ein Datensatz dem BKA übersandt und dort übernommen. Der in Schleswig-Holstein verbleibende Datensatz wird in der Regel spätestens nach 5 Jahren vernichtet. Dieses wird dem BKA mitgeteilt. Die weitere Aufbewahrung des Datensatzes beim BKA regelt das BKAG; sie unterliegt dort der Kontrolle des Bundesdatenschutzbeauftragten.
Die Kritik des ULD richtet sich ausschließlich gegen das BKA. Das Landeskriminalamt SH hat seine Meldeverpflichtung gegenüber dem BKA datenschutzrechtlich erfüllt.

4.2.9 Beobachtung von Versammlungen im Visier des ULD – Teil II

<u>Hinzuspeicherung aus Anlass der erlaubten Teilnahme an Veranstaltungen</u>

Das Hinzuspeichern von Daten über eine erlaubte Teilnahme an Veranstaltungen setzt eine speicherungsfähige verbotene Anlasstat voraus. Es ist fachlich kurzsichtig, dass hinzugespeicherte „neutrale“ Erkenntnisse ohne polizeiliche Relevanz wären. Zur Beurteilung von Gefährdungen ist es oft wichtig zu wissen, ob sich jemand, der noch mit einer verbotenen Anlasstat (rechtmäßig) gespeichert ist, sich aus Milieus, Organisationen, Gruppen usw. zwischenzeitlich gelöst hat. Darüber hinaus geben Teilnahmen an erlaubten Veranstaltungen wichtige Zusatzinformationen.

Datei COMPAS
Ein Löschverfahren (differenzierte Fristen) für das Vorgangsbearbeitungssystem @rtus ist erstellt und vorgangsabhängig modifiziert worden.
Für das Altsystem COMPAS-AWS gelten grundsätzlich auch die datenschutzrechtlichen Vorgaben, einschließlich der Löschfristen. Derzeit wird die 10-jährige Speicherfrist mit dem Ziel geprüft, sie mit den Regelungen von @rtus-VBS in Einklang zu bringen. Datensätze aus COMPAS sind im LKA 3 ins System @rtus-VBS migriert worden. Bezüglich der Prüfung, Löschung und Nutzung der in @rtus migrierten Datenbestände informiert das LKA 3 das ULD fortlaufend.

Datei ISSH
Zurzeit wird die Abteilung im LKA, die das ISSH (Innere Sicherheit Schleswig-Holstein) Verfahren nutzt, mit dem Vorgangsbearbeitungssystem @rtus ausgerüstet. Wenn bei Inbetriebnahme von @rtus erkennbar wird, dass die Datei ISSH nicht mehr erforderlich ist, wird diese sofort abgeschaltet. Andernfalls wird im Falle der weiteren notwendigen Nutzung von ISSH eine Errichtungsanordnung umgehend erstellt werden. Eine Errichtungsanordnung für die Warndatei Rechts besteht bereits.

4.2.10 Eine unzulässige Datenübermittlung und ihre Folgen

Im Rahmen des Auswahlverfahrens für den Polizeidienst eines anderen Bundeslandes wurde von der Polizei Schleswig-Holstein eine MESTA Anfrage bei der Staatsanwaltschaft durchgeführt. Dieses – für die Petentin negative - Ergebnis wurde der anfragenden Stelle mitgeteilt. Die Anfrage bei der Staatsanwaltschaft war nicht zulässig.
Durch organisatorische Regelungen ist sichergestellt, dass zukünftig nur Auskünfte aus polizeilichen Dateien an andere Bundesländer gegeben werden.

4.3.1 Neuregelung der verdeckten Ermittlungsmaßnahmen im Strafverfahren

Die vom ULD insoweit angeführten Kritikpunkte gegen den Referentenentwurf der Bundesregierung werden vom Ministerium für Justiz, Arbeit und Europa aus folgenden Gründen nicht geteilt:

Anlasstatenkatalog für die Telekommunikations-Überwachung (TÜ)
Der Entwurf verlangt für die TÜ eine „schwere Straftat“ und berücksichtigt insoweit den Bestimmtheits- und Verhältnismäßigkeitsgrundsatz hinreichend. Der Katalog sondert Taten aus, die für eine TÜ wenig Relevanz haben und nimmt demgegenüber Delikte auf, deren Struktur die TÜ als Erfolg versprechendes Ermittlungsinstrumentarium erfordert, insbesondere Taten des Wirtschafts- und Korruptionsstrafrechts. Soweit Urkunden- und Betrugsdelikte erfasst sind, handelt es sich um besonders schwere Fälle bzw. um banden- und/oder gewerbsmäßige Begehungsformen.

Verkehrsdatenerhebung bei mittels Telekommunikation begangenen Delikten
Die Erfassung dieser Delikte ist notwendig, weil die Verkehrsdatenerhebung in vielen Fällen den einzig Erfolg versprechenden Ermittlungsansatz, insbesondere betreffend das sog. „Stalking“, darstellt. Der Grundsatz der Verhältnismäßigkeit wird dadurch gewahrt, dass zum einen nur vollendete Delikte erfasst werden und zum anderen eine strenge Subsidiaritätsklausel eingefügt ist.

Reichweite des sog. Kernbereichsschutzes
Nach Auffassung des ULD hat sich der Kernbereichsschutz auch auf - neben der akustischen Wohnraumüberwachung und der TÜ - weitere heimliche Ermittlungseingriffe zu beziehen. Dem ist entgegen zu halten, dass der Rechtsprechung des Bundes-

verfassungsgerichtes *(BVerfG)*, welche sich auf die beiden genannten Eingriffe beschränkt hat (vgl. *BVerfG* NJW 2004, 999; 2005, 2603), eine solche Reichweite nicht entnommen werden kann.

Schutz von Berufsgeheimnisträgern
Das ULD ist der Auffassung, dass die Differenzierung zwischen Geistlichen, Strafverteidigern und Abgeordneten (absolutes Beweiserhebungs- und -verwertungsverbot) sowie sonstigen Berufsgeheimnisträgern (nur relatives, von dem Ergebnis einer Güterabwägung abhängiges Verbot) grundlos sei; für die zweit genannte Gruppe seien die im Regierungsentwurf (RE) genannten Abwägungskriterien (§ 53b Abs. 2 Satz 1 StPO-RE: „Prüfung der Verhältnismäßigkeit unter Würdigung des öffentlichen Interesses an den von dieser Person wahrgenommenen Aufgaben und des Interesses an der Geheimhaltung der dieser Person anvertrauten oder bekannt gewordenen Tatsachen“) ohne objektiv messbaren Maßstab.
Dem ist entgegen zu halten, dass sich die Notwendigkeit für einen absoluten Schutz allein zu Gunsten der erstgenannten Gruppe aus der Rechtsprechung des *BVerfG* ergibt, welche nur für die Berufsgeheimnisträger der Geistlichen und Verteidiger eine Tätigkeit annimmt, die eine besondere Nähe zum Kernbereich privater Lebensgestaltung aufweist (vgl. BVerfGE109, 279, 322 f.). Die Erstreckung auf Abgeordnete dürfte sich aus Art. 47 GG ergeben. Der Einwand, die Abwägungsklausel für die zweit genannte Berufsgruppe ermögliche Willkür, ist zurück zu weisen: Es entspricht Jahrzehnte alter Rechtsprechung des *BVerfG* und des *BGH*, dass für die Entscheidung, ob ein Verwertungsverbot besteht, auf eine Abwägung zurück zu greifen ist, welche insbesondere die mit Verfassungsrang ausgestaltete Pflicht des Staates, für eine funktionstüchtige (Straf-)Rechtspflege zu sorgen, zu berücksichtigen hat (vgl. *BVerfG* NJW 2000, 3557; BGHSt 34, 39, 52).

Gesteigerte Begründungspflicht für den TÜ-Beschluss
Nach Auffassung des ULD müssten die qualifizierten Begründungspflichten, die für die akustische Wohnraumüberwachung bei den richterlichen Anordnungen vorgesehen sind, auch für die TÜ gelten.
Dem ist entgegen zu halten, dass eine Übertragung der für die akustische Wohnraumüberwachung geltenden Grundsätze (vgl. § 100 d Abs. 3 und 4 StPO: insbesondere sind danach Abwägungs- und Verhältnismäßigkeitserwägungen anzugeben) auf die TÜ deshalb nicht in Betracht kommt, weil die Grundrechtsbetroffenheit und somit die Eingriffsvoraussetzungen hier insgesamt geringer sind. Es kommt hinzu, dass die Gerichte schon auf Grund der Rechtsprechung des *BVerfG* zum notwendigen Inhalt von Durchsuchungsbeschlüssen (vgl. BVerfGE 107, 299, 325) zur entsprechenden Sorgfalt angehalten sind.

4.3.2 Nicht eingeleitete Strafverfahren – dennoch gespeichert

Nach Auffassung des ULD bedürfen die Vergabe von Löschfristen, die technische Ausgestaltung der Löschungen und die Protokollierung in MESTA – im Automationssystem der Staatsanwaltschaft - einer vertieften Prüfung.

Löschfristen und Vorgangsverwaltung in MESTA (Mehrländer-Staatsanwaltschafts-Automation): Die Löschfristen für zukünftige Verfahren und die Vorgangsverwaltung entsprechen grundsätzlich den gesetzlichen Vorgaben – nur hinsichtlich der Verjährung (§ 489 Abs. 3 letzter Satz StPO) wurde eine Abweichung vorgenommen, indem die verjährungsunterbrechenden strafprozessualen Maßnahmen in der Fristvorbelegung unberücksichtigt bleiben. Dies wirkt sich allerdings nur zugunsten des Gespei-

cherten, weil verkürzend, aus. Hintergrund ist die gewünschte und in der Praxis erforderliche weitgehend automatische Berechnung, bei der in MESTA nicht gespeicherte Informationen (z. B. Datum der ersten Beschuldigtenvernehmung) berücksichtigt werden müssten.

Zur Frage der Speicherung bei Verfahren, die mangels Anfangsverdachts eingestellt wurden, gilt, dass auch hier die Daten nach § 483 StPO zunächst zu erfassen sind. Diese müssen auch zur Vorgangsverwaltung so lange zur Verfügung stehen, wie die Akten aufzubewahren sind. Soweit es die Speicherung von Daten für zukünftige Verfahren betrifft, ist § 484 StPO (Datenverarbeitung für Zwecke künftiger Strafverfahren) einschlägig. § 484 Abs. 1 StPO lässt die Speicherung bestimmter Daten für künftige Verfahren ohne Rücksicht auf die Art der Erledigung zu, wobei aber immer die Notwendigkeit einer Speicherung zu prüfen ist. Der hiernach zulässige Umfang der aufzubewahrenden Daten begrenzt die Dateien weitgehend auf sog. Aktenhinweisesysteme.
Von der darüber hinausgehenden gesetzlichen Möglichkeit der Speicherung für künftige Verfahren nach § 484 Abs. 2 StPO macht Schleswig-Holstein keinen Gebrauch. Auch Vorgänge, die mangels zureichender tatsächlicher Anhaltspunkte nicht zur Einleitung eines Ermittlungsverfahrens führen, können für künftige Verfahren bedeutsam sein: Beispielhaft sei erwähnt, dass zu einem späteren Zeitpunkt ergänzende Tatsachen bekannt werden, dass ein neues Verfahren wegen Vortäuschens einer Straftat oder wegen falscher Verdächtigung eingeleitet werden muss, oder dass aus der Ballung mehrerer Vorgänge mit jeweils nicht ausreichenden tatsächlichen Anhaltspunkten Rückschlüsse gezogen werden können, die später zur Verfahrenseinleitung führen. Die für MESTA gefundene Regelung stellt einen Kompromiss dar. Zugunsten Betroffener werden Fristunterbrechungen nicht berücksichtigt und weitergehende Daten für Zwecke künftiger Verfahren nicht länger gespeichert. Andererseits wird nicht jedes Verfahren für die Frage der weiteren Speicherung einer Einzelfallentscheidung unterzogen. Eine solche wäre bei der personellen Ausstattung der Staatsanwaltschaften nicht zu leisten. (Vorzeitige) Löschungen im Sinne der Reduzierung der Daten auf die reine Aktenverwaltung (§ 485 StPO) erfolgen nur, wenn besonderer Anlass besteht, z. B. nach Prüfung auf Antrag.
Grundsätzlich sind Art und Umfang der staatsanwaltschaftlichen Datenspeicherung ein von vielen Einflussgrößen geprägter Kompromiss: Die Entscheidung für eine Generalklausel und damit der Verzicht auf eine stark ausdifferenzierte Regelung entspricht den Bedürfnissen der Praxis. Verzichtet wurde darauf, die verschiedenen Arten der einzelnen Dateien festzulegen sowie durch eine Aufzählung von Datenfeldern gesetzlich die Daten zu umschreiben, die gespeichert werden dürfen. Eine bewertende Bestandsaufnahme der in der staatsanwaltschaftlichen und polizeilichen Praxis geführten Daten hat gezeigt, dass eine solche gesetzliche Eingrenzung, bedingt durch die Unterschiedlichkeit der möglichen und notwendigen Datenfelder, die sich wiederum regelmäßig nach den fall- bzw. deliktsspezifischen Bedürfnissen der speichernden Stelle richtet, nicht möglich ist. Mit den MESTA-Partnerländern wurden die Löschregelungen zuletzt in 2005 überarbeitet. Die Löschmechanismen unterliegen der laufenden Kontrolle durch die 5-Länder-Fachgruppe.
Protokollierung:
Aus technischer Sicht war bei der Schaffung von MESTA eine Voll-Protokollierung nicht durchführbar. Hierüber hatte es seinerzeit lange Diskussionen mit dem Hamburgischen Datenschutzbeauftragten gegeben, der auch für seine Kollegen der anderen Länder an der MESTA-Einrichtung beteiligt war. Ob nach heutigen technischen Bedingungen neben der bestehenden Änderungs-Protokollierung auch eine reine

Auskunfts-Protokollierung (ohne unvertretbare Kostensteigerung und Performance-Einbußen) möglich ist, dürfte prüfenswert sein. Diese Prüfung könnte in die anlaufende Programm-Überarbeitung (MESTA 2010) einbezogen werden.

4.3.3 Kontrollbefugnis bei der Staatsanwaltschaft

Zwischen dem ULD und dem Generalstaatsanwalt bestehen über die Frage der richtigen Darstellung der datenschutzrechtlichen Kontrolle vom 20. April 2006 bei der Staatsanwaltschaft Kiel, insbesondere über die Frage, ob dem ULD die Akteneinsicht verweigert wurde, unterschiedliche Auffassungen. Nach Darstellung des Generalstaatsanwalts hat das ULD seine Prüfung im vorliegenden Fall von vornherein selbst begrenzt, so dass die gewährte Akteneinsicht dem Begehren der Prüfer entsprach. Mithin ist vom ULD geäußerte Kritik am Vorgehen der Staatsanwaltschaft nicht gerechtfertigt.

Ergänzend hierzu ist anzumerken, dass zwischen dem ULD und dem Generalstaatsanwalt die übereinstimmende Rechtsauffassung besteht, dass das ULD nicht berechtigt ist, strafprozessuale Zwangsmaßnahmen einer Strafverfolgungsbehörde einer Rechtmäßigkeitsprüfung nach Datenschutzrecht zu unterziehen. Der Prüfvorgang des ULD ist damit auf die Datenverarbeitung (z. B. die Eintragung des Verfahrens, die Speicherung von Daten usw.) zu beschränken.

Der Generalstaatsanwalt ist daran anknüpfend der Auffassung, dass dem ULD damit ein vollständiges Akteneinsichtsrecht gemäß der Strafprozessordnung nicht zusteht. Dennoch räumt der Generalstaatsanwalt dem ULD ein, die kompletten Akten im Rahmen des Prüfvorganges in den Räumen der Staatsanwaltschaft zu sichten, um zu überprüfen, welche Bereiche von ihrer Kontrollbefugnis umfasst sind und welche nicht.

Durch diese Art der Akteneinsicht vor Ort in die gesamte Akte können sich die Prüfer des ULD ein umfassendes Bild auch über die reine Datengewinnung und Datenverarbeitung hinaus verschaffen.

Mithin scheint die Kritik des ULD am Vorgehen der Staatsanwaltschaft im vorliegenden Einzelfall auf einem Missverständnis zu beruhen. So hat das ULD nach Ansicht des Generalstaatsanwalts im betroffenen Verfahren durch Begrenzung seines Prüfbegehrens die beschränkte Akteneinsicht selbst veranlasst, da anderenfalls dem ULD durch die Staatsanwaltschaft eine für die Erfüllung seiner gesetzlichen Aufgaben ein ausreichendes Akteneinsichtsrecht eingeräumt worden wäre.

4.4.1 StVG-Übermittlungsnorm verunsichert Polizei und Fahrerlaubnisbehörden

Mit dem ULD besteht insoweit Übereinstimmung, dass unter die Vorschrift des § 2 Abs. 12 Straßenverkehrsgesetz (StVG) nur solche Mitteilungen fallen, die auf nicht nur vorübergehende Eignungs- oder Befähigungsmängel zum Führen von Kraftfahrzeugen schließen lassen, und diese von den Fahrerlaubnisbehörden nur dann gespeichert werden dürfen, wenn nach den Umständen des Einzelfalles mit hoher Wahrscheinlichkeit in absehbarer Zeit mit einer Antragstellung zu rechnen ist (Hentschel Straßenverkehrsrecht, Beck, 37. Auflage, Erl. zu § 2 StVG; Bouska/Laeverenz Fahrerlaubnisrecht, 3. Auflage, Erl. zu § 2 Abs. 12 StVG).

Das Fahrerlaubnisrecht ist bundesrechtlich geregelt und dient als „besonderes Gefahrenabwehrrecht“ dem Schutz der Allgemeinheit vor Gefahren, die von ungeeigneten Kraftfahrzeugführern ausgehen. Bei der Feststellung der Eignung oder Befähigung kommt es auf ein „Verschulden“ des Betreffenden nicht an. Der Zweck der Gefahrenabwehr liegt auch der Vorschrift des § 2 Abs. 12 StVG zugrunde. Fahrerlaubnisrechtlich angeordnete Maßnahmen zur Aufklärung von Eignungszweifeln, wie z. B. die Anordnung, ein medizinisch-psychologisches Gutachten einer amtlich anerkannten Be-

gutachtungsstelle für Fahreignung beizubringen oder die Versagung einer Fahrerlaubnis wegen festgestellter Nichteignung, sind keine Sanktionen oder Strafen sondern Gefahren abwehrende Maßnahmen. Deshalb steht die Übermittlung eignungsrelevanter Informationen und Tatsachen, die die Polizei bei Jugendlichen festgestellt hat, sowie die Speicherung und Verwendung dieser Tatsachen durch die Fahrerlaubnisbehörden auch nicht im Widerspruch zu den Intentionen des Jugendgerichtsgesetzes. Weder wird den Jugendlichen durch fahrerlaubnisrechtliche Gefahrenabwehr ihr Handeln angelastet, noch wird ihnen die Zukunft versperrt.
Bereits mit Stellungnahme vom 21.07.2005 wurde das ULD anlässlich eines konkreten Einzelfalles ausführlich über diese Rechtsauffassung des Ministeriums für Wissenschaft, Wirtschaft und Verkehr informiert. Diese Stellungnahme ist auch dem Innenministerium zugegangen.

4.5.1 Datenschutzkontrollzuständigkeit über die Arbeitsgemeinschaften (ARGEn)

Auf der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26. bis 27.11.2006 wurde Einvernehmen erzielt, dass die Landesdatenschutzbeauftragten die vollumfängliche datenschutzrechtliche Kontrollkompetenz für die ARGEn haben, während der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BFDI) für die zentralen IT-Verfahren der Bundesagentur für Arbeit (BA) zuständig ist. Diese Auffassung wird vom Bundesministerium für Arbeit und Soziales, dem Land Schleswig-Holstein und der Regionaldirektion (RD) Nord der BA geteilt. Mit dieser Regelung sind die Irritationen über die Zuständigkeit bei der Datenschutzkontrolle beseitigt. Seit bekannt werden dieser Regelung hat es keine Fälle mehr gegeben, in denen dem ULD Auskünfte und Informationen aufgrund angenommener Unzuständigkeit verweigert worden wären.

4.5.2 Viel Ärger um die ARGE Lübeck

Die Prüfung der ARGE Lübeck erfolgte bereits im November 2005. Mit Klärung der Zuständigkeit des ULD als Datenschutzkontrollbehörde hat sich kein Träger mehr den Auskunfts- und Informationsersuchen des ULD verweigert.
Auch das ULD wird aktiver Bestandteil des schleswig-holsteinischen Netzwerkes zur Umsetzung des SGB II. Die Träger nehmen die Anmerkungen und Anregungen konstruktiv auf, um das gemeinsame Ziel, eine verbesserte Umsetzung des SGB II zu verfolgen. Hierzu gehören auch die Wahrnehmung von Informations- und Fortbildungsangeboten des ULD.

4.5.3 Hausbesuche? Wenn überhaupt, dann bitte datenschutzgerecht!

Nach Auskunft der RD Nord wurde zur Durchführung von Hausbesuchern mittlerweile ein detaillierter Leitfaden entwickelt und zur Verfügung gestellt. Die Ausarbeitungen des ULD zu dieser Thematik sind den Trägern bekannt. Im Rahmen der Netzwerk-Steuerungsgruppe arbeitet das Ministerium für Justiz, Arbeit und Europa mit den Partnern an Mindeststandards für den Außendienst (Ergebnis aus dem Dialog mit der Sozialgerichtsbarkeit).

4.5.5 Vermittlungsvorschlag – Einwilligung zwecks Übermittlung an potentiellen Arbeitgeber?

Das ULD kritisiert, dass die Träger in Anlehnung an eine gängige Praxis der Bundesagentur für Arbeit (BA) mit Arbeitgebern Daten über Bewerber austauschen, ohne diese davon rechtzeitig in Kenntnis zu setzen.
Hierzu teilt die RD Nord mit:

„Es ist nicht Ziel der BA, Arbeitgeber für Kontrollzwecke zu benutzen, es ist vielmehr erklärte Geschäftspolitik, eine hohe Qualität der Vermittlungstätigkeit zu gewährleisten. Dies schließt Telefonate mit Bewerbern zur Vorabklärung der Eignung durch Vermittler zur Überprüfung der Passgenauigkeit mit ein. Zum Umgang mit persönlichen Daten gibt es explizite Erklärungen in den Merkblättern SGB III und SGB II. Die Kunden unterschreiben im Leistungsantrag, dass sie den Inhalt des Merkblattes zur Kenntnis genommen haben. Auf die gesetzlich festgelegten Regelungen in §§ 67 ff. SGB X (SGB Verwaltungsverfahren – Schutz der Sozialdaten) *i.V.m. § 35 SGB I* (SGB Allg. Teil – Sozialgeheimnis) *sei ausdrücklich hingewiesen.“*

4.5.6 Die Ortsabwesenheitsklausel

Das ULD kritisiert eine uneinheitliche Praxis in den ARGEn zu der in den Eingliederungsvereinbarungen festgeschriebenen Verpflichtung, dass sich Arbeitssuchende nur nach Absprache und mit Zustimmung des persönlichen Ansprechpartners außerhalb des zeit- und ortsnahen Bereiches aufzuhalten haben.
Die RD Nord erklärt hierzu, dass *seit dem 01.08.2006 eine gesetzliche Regelung vorliegt, die diese Verpflichtung beinhaltet, die somit nicht mehr in der Eingliederungsvereinbarung festgehalten werden muss. Auf § 7 Abs. 4a SGB II* (Berechtigte – Ortsabwesenheit) *wird ausdrücklich hingewiesen.*

4.5.8 Beschäftigungsorientiertes Fallmanagement im SGB II

Laut ULD gäbe es in Deutschland keine Behörde, die so viele so sensible Informationen von so vielen Menschen sammelte wie die ARGEn und die BA. Es stelle sich die Frage, ob alle erhobenen Daten (durch Vordruck) auch tatsächlich erforderlich seien?
Die RD Nord nimmt hierzu wie folgt Stellung:*„Zielgerichtetes Fallmanagement im SGB II ist Grundlage einer erfolgreichen Arbeitsvermittlung. Dazu müssen im Rahmen eines Profilings Daten zur beruflichen, familiären und sozialen Situation erhoben werden. In diesem Zusammenhang werden selbstverständlich nur Daten erhoben, die zur Erfüllung der Aufgabe – Vermittlung in Arbeit – erforderlich sind. Dem wird in den angewandten IT-Verfahren Rechnung getragen. Diese finden mit Zustimmung des Bundesdatenschutzbeauftragten Anwendung.“*

4.5.12 Neue Instrumente bei der Eingliederungshilfe

Bei den im Rahmen von Fortbildungsveranstaltungen durchgeführten Workshops "Zielgruppenmanagement" bzw. "Anbietermanagement" ging es inhaltlich um die Erarbeitung von Erhebungsrastern, Inhalten, Verknüpfungen und Codierungen als Vorarbeiten für die Erstellung entsprechender Datenbanken. In diese Aktivitäten sowie auch in die Präsentation der erarbeiteten Ergebnisse war das ULD eingebunden. Die eigentlich datenschutzrelevante Fortführung dieses Themas (Aufbau von Datenbanken) liegt allerdings in der Zuständigkeit der Kommunen und damit nicht im Zugriff des Ministeriums für Soziales, Gesundheit, Familie, Jugend und Senioren. Den Kommunen (Arbeitsgemeinschaften der Kreise und kreisfreien Städte) wird in den nächsten Kontaktgesprächen die Anregung des ULD mit der Bitte um Beachtung zur Kenntnis gegeben werden.

4.7.1 Ist der „gläserne Schüler“ geplant?

In diesem Abschnitt setzt sich das ULD mit der von der Kultusministerkonferenz (KMK) diskutierten Datengewinnungsstrategie - der „Einführung einer bundesweiten Schuldatenbank“ – auseinander, wobei an mehreren Stellen inhaltlich nicht zutreffend argumentiert wird.

- Das ULD behauptet, der Schüler-Identifikationsnummer (ID) würden bestimmte Daten zugeordnet, z. B. Nationalität, Muttersprache, Elternhaus, zu sämtlichen Schuljahren Art der Schule, Wiederholungen, Schwerpunkte und Ziele der Ausbildung. Darüber könne die gesamte Schulkarriere nachvollzogen und bewertet werden.
  Richtigstellung: Im Kerndatensatz (Beschluss der KMK vom 8.5.2003) wird beschrieben, welche Daten von der Schule erhoben und über eine Kennnummer (Schüler-ID) pseudonymisiert an das statistische Landesamt weitergegeben werden. Die beispielhaft erwähnten Daten über das Elternhaus werden im Kerndatensatz nicht erhoben.

- Es wird dargelegt, dass mit Hilfe der Schüler-ID eine Verknüpfung von Person zu den erfassten Daten möglich sei.
  Richtigstellung: Bevor jedoch die mit der Schüler-ID verknüpften Daten an das statistische Landesamt weitergegeben werden, erfolgt eine erneute Verschlüsselung, die zur Schüler-ID eine Datensatznummer generiert. Bei dem vorgesehenen Verschlüsselungsalgorithmus handelt es sich um eine Einwegverschlüsselung. Das bedeutet, dass zwar die Daten einer Person mittels der Schüler-ID/Datensatznummer stets ein und demselben Datensatz zugeordnet werden, dass aber umgekehrt einem mit einer ID versehenen Datensatz einzelne Personen nicht zugeordnet werden können. Durch die zweimalige Pseudonymisierung (erstmalig durch die Vergabe der Datensatznummer, danach durch die Einweg- Verschlüsselung) kann aus der ID nicht auf personenbezogene Daten geschlossen werden.

- Es wird dargelegt, die mit den zu erhebenden Daten verfolgten Ziele seien nicht klar.
  Dem ist entgegenzuhalten, dass als Zwecke mehrfach folgende genannt wurden:
  - Gezieltes Steuerungswissen für Bildungsverwaltung und Bildungspolitik, insbesondere hinsichtlich atypischer Bildungsverläufe,
  - Bildungsberichterstattung,
  - Durchführung von Leistungsvergleichsuntersuchungen und
  - Erleichterung bei der Erstellung von Statistiken.

- Es wird behauptet, die erforderlichen Daten könnten auch mit Hilfe bestehender wissenschaftlicher Studien, z.B. PISA, erhoben werden.
  Für viele Fragestellungen reichen Stichprobenerhebungen tatsächlich aus. In diesen Fällen reicht entweder der einmalige Erkenntnisgewinn für den angestrebten Zweck oder die Strukturen sind so homogen, dass eine Stichprobe repräsentative Ergebnisse ermöglicht. Die Bevölkerungsdichte und -struktur und damit die Zusammensetzung der Schülerschaft ist in Deutschland jedoch heterogen. Zur Planung und Weiterentwicklung von Schulstrukturen und Bildungsangeboten reichen Stichproben also häufig nicht aus, da sie nur einen kleinen Ausschnitt abbilden. Um repräsentative Ergebnisse erzielen zu können, müsste man in kurzen Zeitabständen sehr große Stichproben ziehen. Die Aussagekraft von (bundesweiten) Durchschnittswerten ist also für die Steuerung, Weiterentwicklung und Evaluation von bildungspolitischen Maßnahmen sehr begrenzt. Dies trifft bei den unterschiedlichen Bildungssystemen in den Ländern umso mehr zu. Zusätzlich ist eine höhere Verfügbarkeit, Zuverlässigkeit, Aktualität und größere Vollständigkeit der Daten gewährleistet.

- Die Behauptung, das MBF wolle sich an einer zentralen Schülerdatenbank beteiligen, entspricht nicht den Tatsachen. Eine zentrale Datenbank ist zwar von der Wissenschaft und dem Statistischen Bundesamt gewünscht, bislang aber in der KMK weder diskutiert noch beschlossen worden.

- Die in der Bezeichnung „persönliche Identifikationsnummer“ enthaltene Verknüpfung zwischen der ID und der Person ist irreführend und nicht korrekt, da es eben eine solche Verbindung von Datensätzen, die an die Statistik geliefert werden, zu den Schülerinnen und Schülern nicht geben wird.

4.7.2 Informationstechnologie an Schulen

Das Ministerium für Bildung und Frauen nimmt erfreut zur Kenntnis, dass das ULD den Einsatz von Standardsystemkonzepten in Schule und Unterricht unterstützt. Gemeinsam mit den Kommunalen Landesverbänden hat das Ministerium die Modellprojekte des Bundesministeriums für Bildung und Forschung „sh21 Basis“ und „Landesnetz Bildung“ unter Einbeziehung des ULD Systemlösungen erarbeitet, die im Pilotbetrieb zu einer deutlichen Entlastung von Schulverwaltung und Lehrkörper geführt haben.
Das Ministerium wird, bevor die Ergebnisse der Projekte flächendeckend verfügbar gemacht werden, die Fragen zu Datenschutz und Datensicherheit mit dem ULD abstimmen.

4.8.2 Data Center Steuern

Die Datenschutzbeauftragten der beteiligten Länder haben unter der Federführung des Landesdatenschutzbeauftragten aus Mecklenburg-Vorpommern dem Data Center Steuern (DCS-Projekt) Hinweise auf datenschutzrechtliche Belange für die Gestaltung des Vertragsverhältnisses mit Dataport gegeben. Diese lagen dem DCS-Teilprojekt 5 vor und sind in die Ausgestaltung des Servicescheins IT-Sicherheit mit eingeflossen. Das Gesamtvertragswerk unter Einschluss dieses Servicescheins ist mittlerweile von allen beteiligten Ländern unterzeichnet worden.
Darüber hinaus hat das DCS-Teilprojekt 5 den Auftrag, das im Tätigkeitsbericht angesprochene Sicherheitskonzept des Auftragnehmers gemeinsam mit Dataport zu erstellen. Die Landesdatenschutzbeauftragten wurden und werden in speziellen Informationsveranstaltungen (zuletzt am 1.3.2007, weitere Veranstaltung geplant im August 2007) über den Fortgang im Projekt informiert.

5.1 Auslandsüberweisungen aus Schleswig-Holstein über Brüssel an die CIA

Die Kritik des ULD hinsichtlich der Weitergabe von Überweisungsdaten (auch bei Überweisungen innerhalb der EU) bei einer Auslandsüberweisung durch SWIFT (Society for Worldwide Interbank Financial Telecommunication) an US-Geheimdienste und sonstige US-Behörden ist nachvollziehbar. Die Möglichkeiten der Einflussnahme der Kreditwirtschaft erscheinen indes begrenzt, zumal SWIFT – wie vom ULD konstatiert – Quasimonopolist auf dem Gebiet der internationalen Geldüberweisungen ist und die USA vermutlich großen Druck auf SWIFT ausüben können. Das ULD fordert in diesem Zusammenhang den Aufbau alternativer Infrastrukturen für Auslandsüberweisungen.
Zwischenzeitlich soll SWIFT beabsichtigen, künftig alle europäischen Transaktionen ausschließlich über Rechenzentren in Europa abzuwickeln und damit eine Spiegelung dieser Daten in die USA zu vermeiden. Die Implementierungsphase zur Umsetzung der hierfür erforderlichen Technik würde allerdings nach Einschätzung von SWIFT 3

bis 5 Jahre dauern, wobei man aber bemüht sei, den Zeitraum so kurz wie möglich zu halten.
Die konkreten Beschlüsse von SWIFT sind daher abzuwarten. Die Banken sind aber während der Übergangsphase weiterhin gefordert, die Information der betroffenen Kunden über die derzeitige Verfahrensweise zu optimieren.

Die Börsen-Zeitung berichtete unlängst, dass die US-Regierung schriftlich zugesichert habe, SWIFT- Informationen ausschließlich im Kampf gegen den internationalen Terrorismus (und nicht gegen Wirtschaftsspionage) einzusetzen. Dies sei von der EU gegen erheblichen Widerstand der US-Regierung durchgesetzt worden. Mehr sei nach Aussage von Finanzminister Steinbrück (vor dem EU-Parlament) nicht zu erreichen gewesen, berichtete die Börsen-Zeitung in dem Artikel vom 27.06.2007 weiter.

6.1 Transparenz und Revisionssicherheit: Basis jedes Datenschutzmanagements

Ziel ist, eine Prozessorganisation basierend auf Best-Practice-Referenzmodellen im Geschäftsbereich des Innenministeriums einzurichten. Die Prozessorganisation wird dabei gestaltet durch ein zu bildendes Prozessmanagement. Dieses schafft die Möglichkeit und den Rahmen dafür, langfristig und kontinuierlich Prozessverbesserungen vornehmen zu können. Mit der Einführung der Prozessorganisation werden im Detail folgende Ziele angestrebt:

- Standardisierte Dokumentation von Prozessen,
- Erzeugung von Transparenz über Prozesse,
- Definition von Standardprozessen,
- Beschreibung von Prozessschnittstellen (Kommunikationsbeziehungen),
- Aufbau einer auf Referenzmodellen basierenden Prozessarchitektur sowie
- Zuweisung der Verantwortung für die Steuerung von Prozessen und der von Prozessen erzeugten (Dienst-)Leistung.

Aufgrund des erheblichen Aufwandes, der bei einer sofortigen und vollständigen Einführung eines Geschäftsprozessmanagements notwendig, aber derzeit nicht leistbar ist, sollen vorerst die bestehenden Grundlagen erweitert und dann erste, ausgewählte Prozesse betrachtet werden.
Im Rahmen der Einführung von Elementen des Geschäftsprozessmanagements werden auch die bisherigen Aktivitäten hinsichtlich eines Datenschutzmanagementsystems weiter verfolgt. So wurden bereits erste Maßnahmen ergriffen um den Verpflichtungen hinsichtlich der Transparenz bei der Planung, der Einführung und dem Betrieb von IT-Verfahren nachzukommen:
In einer Verfahrensakte wird die in der Datenschutzverordnung des Landes geforderte Verfahrensdokumentation zusammengestellt, wobei für jedes IT-Verfahren ein entsprechendes Sicherheitskonzept vorliegen muss. Derzeit ist die erforderliche Transparenz bei der Verarbeitung personenbezogener Daten formal vorhanden, allerdings sind in der Praxis Verbesserungen erforderlich. Der Prozessgedanke steht bei den vorhandenen IT-Konzepten noch nicht im Vordergrund. Eine zeitnahe Fortschreibung der IT- und Sicherheitskonzepte aufgrund von Veränderungen der Abläufe erfolgt noch sehr selten.
Bezüglich der Revisionsfähigkeit der Verfahren ist man sich ebenfalls der Notwendigkeit entsprechender Prüfungen bewusst und hat bereits erste Maßnahmen ergriffen. Jedes IT-Verfahren soll vor der Freigabe hinsichtlich der Einhaltung der Vorgaben in der Verfahrensakte, dem Datenschutz- und dem Sicherheitskonzept überprüft werden.

Allerdings sind Maßnahmen zur Sicherstellung der Revisionssicherheit wie z.B. Protokollierung oder zur Manipulationssicherheit zurzeit nur ansatzweise implementiert.
Zwar sind den IT-Verantwortlichen in den Geschäftsbereichen und der Leitungsebene die Vorteile dieser Qualitätskriterien bewusst. Allerdings wird nicht immer mit dem notwendigen Nachdruck für deren Umsetzung gesorgt.
Weiteres Verbesserungspotential im Hinblick auf eine transparente und revisionsfähige Datenverarbeitung sieht das Innenministerium in dem bereits eingeschlagenen Weg zu einem Geschäftsprozessmanagement.

6.2 ISO 27001 – der neue Grundschutz

Die Basis des IT-Sicherheitsprozesses, welcher im Innenministerium und in dessen nachgeordneten Bereichen sukzessive implementiert wird, sind die BSI-Standards 100-1 bis 100-3. Der BSI-Standard 100-1 "Managementsysteme für Informationssicherheit" (ISMS) ist vollständig kompatibel zum ISO-Standard 27001 und definiert die allgemeinen Anforderungen an ein ISMS.

ISMS und DSMS können theoretisch unabhängig voneinander erfolgen, allerdings ermöglicht eine Integration beider Managementsysteme die Nutzung von Synergien, da teilweise redundanter Aufwand entfällt. Im IT-Sicherheitsprozess bei der Landespolizei-SH (Projekt "IT-SM LaPo-SH") wird dies bereits ansatzweise verfolgt und zwar dort, wo die behördlichen Datenschutzbeauftragten die Aufgaben der IT-Sicherheitskoordination übernehmen. Die IT-Sicherheitskoordination führt, sowohl in regelmäßigen als auch anlassbezogenen Kontrollen, eine Überprüfung der Sicherheitsmaßnahmen durch. Die qualitative Dokumentation der Sicherheitsmaßnahmen erfolgt mit Hilfe des Grundschutz-Tools des Bundesamtes für Sicherheit in der Informationstechnik (GS-Tool des BSI). Ausgangspunkt für den IT-Sicherheitsprozess im Bereich der Landespolizei war im Jahr 2003 die Einführung von INPOL-SH und die damit verbundene Selbstverpflichtung der Teilnehmer am polizeilichen Informationsverbund zur Konformität zum IT-Grundschutz des BSI.

Der Kontakt zum ULD zur Thematik wurde bereits initiiert. Weitere Gespräche mit dem ULD zur Zertifizierung des IT-Managements/IT-Sicherheitsprozesses im Geschäftsbereich des Innenministeriums sollen im 2.Quartal 2007 erfolgen. Darüber hinaus werden seitens des Innenministeriums weitere Impulse aus dem vom ULD zu erarbeitenden Vorgehensmuster zur Umsetzung der DSVO in Verbindung mit der Norm ISO 27001 erwartet.

6.3 Verzeichnisdienste I: Active Directory

Die kritische Auseinandersetzung mit dem Microsoft Active Directory (AD) ist in der Entwicklung des landesweiten Verzeichnisdienstes erfolgt. Die Ergebnisse des Landes sind deckungsgleich mit den Ermittlungen seitens des ULD. Die Protokollierung in einem derartigen System ist umfassend, jedoch nicht revisionssicher. Der Hersteller bietet diese Funktion nicht an und in absehbarer Zeit ist auch mit keiner Umsetzung dieser Funktionalität zu rechnen. Die gewünschte Protokollierung bezieht sich auf Tätigkeiten eigener Administratoren (also Landesbediensteter) sowie auf Administratoren von Dienstleistern. Da herstellerseitig keine Umsetzung möglich ist, wurde im Rahmen des KITZ-Datenschutzaudits aktuell untersucht, welche Tools die Revisionssicherheit des AD verbessern können.
Ein erstes Fazit ist bereits erkennbar. Es gibt am Markt kein Tool, welches diese Funktionalität auf Knopfdruck bereitstellt. Erst die Kombination mehrerer Werkzeuge

sowie die Einrichtung einer Produktionsumgebung für die Revisionsfunktionalität verbessern diesen Zustand.
Fazit:
Die verbesserte Protokollierung ist auch im Landesbereich wünschenswert. Sie stellt sicher, dass Änderungen am gemeinsamen System nachvollzogen werden können. Diskussionspunkte mit Ressorts, welche bisher noch nicht am Landesstandard teilnehmen, könnten neu diskutiert werden.
Es bleibt dabei die Frage, wie viel uns dieser Zuwachs an Funktionalität wert ist, bzw. wo die Grenze ist, um rechtliche Anforderungen zu erfüllen. Nach der ersten Berechnung ist jedoch mit einer erheblichen Zunahme der Kosten für die Zentrale IKOTECH III Kopfstelle im Land - rund 40 – 50 % - zu rechnen. Nach 6 Jahren Betrieb IKOTECH III und keinem Vorfall über unberechtigte Administrationsvorgänge, ist diese Frage sicher angemessen.
Es bleibt als generelle Aussage bestehen: Sofern dem Administrator (oder Dienstleister) nicht vertraut wird, sollte kein gemeinsames System betreiben werden.

6.6 Fehlermanagement über die Clearingstelle

Das ULD hat das Sicherheitskonzept zur Clearingstelle gemeinsam mit dem hamburgischen Datenschutzbeauftragten am 25. Januar 2007 abgenommen. Zuvor waren die Datenschützer der Länder Hamburg und Schleswig-Holstein in den Prozess „Sicherheitskonzept Clearingstelle“ seit langem eingebunden.
Bereits im Sommer 2006 hatte das ULD das Landesnetz als sicheres geschlossenes Netz auditiert, in dem Daten sogar unverschlüsselt übermittelt werden können. Trotzdem werden die Daten der Meldebehörde auf dem Weg zur Clearingstelle als weitere Sicherheitsmaßnahme verschlüsselt. Beide in der Kommunikation der Meldebehörden zum Einsatz kommenden Infrastrukturmaßnahmen arbeiten aus datenschutzrechtlicher Sicht einwandfrei.
Darüber hinaus bietet die Clearingstelle dauerhaft zusätzliche datenschutzrechtliche Sicherheitsaspekte. So werden sämtliche Sender- und Empfänger-Zertifikate sowie die Tatsache der Nachrichtenintegrität in der Kommunikation zwischen Sender- und Empfänger-Meldebehörde geprüft. Eingehende XMeld-Nachrichten werden zusätzlich auf OSCI-XMeld-Schemakonformität (technisches Datengerüst) und Virenbefall hin geprüft. Durch die hier möglichen technischen Prüfungen seitens der Clearingstelle wird echter Datenschutz praktiziert.
In der Kommunikation ohne Clearingstelle, d.h. ohne Nutzung der Synergien, die ein gemeinsamer Dienstleister bieten kann, ist dies - wie die Praxis gezeigt hat - im selben Umfang wirtschaftlich nicht zu bewerkstelligen.
Dies gilt insbesondere auch für die Kommunikation auf Basis von OSCI-Transport [1], das als Technik zwar eine abgesicherte Ende-zu-Ende-Sicherheit ermöglicht. Diese wird aber nur gewährleistet, wenn diverse durch diese Technik mögliche Prüfungen (Gültigkeit von Zertifikaten, Übereinstimmung von fachlich gewünschtem Empfänger aus dem Inhalt der XMeld-Nachricht und benutztem Zertifikat, etc), auch wirklich durchgeführt werden.
Damit bietet die bloße Anwendung von OSCI-Transport in der Praxis nur scheinbar die gewünschte Absicherung einer direkten Ende-zu-Ende-Verschlüsselung.
Um trotzdem diesem Sicherheitsniveau nahe zu kommen, soll die Clearingstelle als reiner Dienstleister der Verwaltung Auftragsdatenverarbeitung durchführen. Um dies auch datenschutzrechtlich möglich zu machen, wurde bei der Konzeption der Clea-

[1] OSCI = Online Service Computer Interface, OSCI-Transport ist ein Protokollstandard zur vertraulichen und sicheren Übermittlung von Nachrichten in einer auf das deutsche Signaturgesetz abgestimmten Sicherheitsumgebung

ringstelle in Zusammenarbeit mit dem ULD darauf geachtet, dass die Verantwortung für die verarbeiteten Daten jederzeit klar definiert ist und bei jeweils der beauftragenden Meldebehörde liegt.
In einer solchen Konstellation bildet die Meldebehörde zusammen mit allen von ihr genutzten „Rechenzentren“ – also auch der Clearingstelle – quasi das eine Ende der Kommunikation. So wird die Clearingstelle bei Dataport quasi nur als verlängerter Arm der Meldebehörde tätig, d.h. es gibt quasi keine Unterbrechung der Ende-zu-Ende-Absicherung.

7.1 Vorratsdatenspeicherung

Die vom ULD insoweit angeführten Kritikpunkte gegen den Entwurf werden hier nicht geteilt:
Die Umsetzung der sog. „Vorratsdatenspeicherung“ im Entwurf unterliegt keinen durchgreifenden verfassungsrechtlichen Bedenken, da die Daten zu bestimmten Zwecken gespeichert werden sollen. Eine sechsmonatige Speicherpflicht ist jedenfalls nach den Erhebungen des BKA notwendig, um das angestrebte Ziel zu erreichen. Die Verkehrsdatenerhebung ist schon nach geltendem Recht auch den Diensten und zu Zwecken der Gefahrenabwehr möglich (vgl. nur §§ 8 a Abs. 2 Nr. 4 und 5 BVerfSchG, § 2 a BNDG, § 4 a MADG, § 185 a Abs. 1, 2 Nr. 2 LVwG). Der Schutz besonderer Vertrauensverhältnisse erfolgt in ausreichendem Maße durch § 53b StPO-E.

9.1.1 Landesnetz Schleswig-Holstein (LN-SH)

Der positive Bericht des ULD zum Landesnetz ist das Ergebnis der qualifizierten Arbeitsergebnisse aus der Mitte 2006 abgeschlossenen umfangreichen Generaldokumentation und einer damit einher gegangenen engen und kooperativen Zusammenarbeit zwischen Finanzministerium, Dataport, T-Systems und dem ULD, welches mit seinem Sachverstand an vielen Stellen richtungweisende Impulse gesetzt hat.
Von Vorteil ist das Audit vor allem in der Diskussion mit dem kommunalen Bereich, da die gerne als „Anschlussverhinderungsgrund“ genutzte Sicherheitsthematik nicht mehr greift.
Das System ist heute „rund“, wird aber auch durch neue Aufgaben gefordert, wie z.B. die Umsetzung der EU-Dienstleistungsrichtlinie oder Maßnahmen aus der Aufgabenkritik. Insofern gilt auch hier „Stillstand ist gleich Rückschritt“. Um den Betrieb, die technische Qualität und die Sicherheit aufrechterhalten zu können, obliegt es dem Finanzministerium, dieses durch eine dauerhafte Bereitstellung von personellen Ressourcen auch für die Weiterentwicklung und das Controlling zu gewährleisten.

Das ULD beschreibt neben der erfolgreichen Auditierung des Verwaltungsnetzes auch dessen Revisionswerkzeuge. In dem Zuständigkeitsbereich des Innenministeriums wird das Revisionstool "LNRC" (Landesnetz Router Controll) noch nicht in allen Geschäftsbereichen genutzt. Eine abschließende Bewertung ist für das Innenministerium zum jetzigen Zeitpunkt nicht möglich, da die im Sicherheitskonzept des Finanzministeriums beschriebenen Restrisiken noch nicht darauf hin bewertet werden konnten, ob das vom LN garantierte Sicherheitsniveau auch für alle Geschäftsbereiche des Innenministeriums ausreichend ist.
Im Bereich der Landespolizei gilt darüber hinaus die IT-Sicherheitspolicy für den polizeilichen Informationsverbund CNP (CNP-Policy) als strategische Leitlinie. Eine Verschlüsselung der im Rahmen von Fachanwendungen zu transportierenden Daten ist hier deshalb erforderlich, aber zurzeit noch nicht umgesetzt.

12.4.5 Gebührenerhebung im Sozialbereich

In derartigen Fällen besitzt das Ministerium für Soziales, Gesundheit, Familie, Jugend und Senioren keine originäre Zuständigkeit. Es handelt sich um eine Aufgabenwahrnehmung in kommunaler Selbstverwaltung. Vorsorglich ist jedoch bei einzelnen Kommunen eine telefonische Abfrage zu diesem Thema erfolgt, mit dem Ergebnis, dass dort nur in ausgesprochen seltenen Fällen Kopien gefertigt werden (z.B. bei Verlust des Bescheides zur Kostenübernahme für eine Maßnahme), diese dann aber durchweg unentgeltlich erfolgten. In besonderen Fällen, z.B. für Rechtsanwälte in Klageverfahren, werden schon einmal Auszüge aus Fallakten kopiert, für die dann auch Gebühren, z.B. 0,50 € pro Seite, verlangt wurden.

12.4.6 Beanstandung der ARGE unumgänglich

Das ULD beanstandet, dass mit Blick auf die unsichere Rechtslage hinsichtlich der Zuständigkeit des ULD sowie der Anwendbarkeit des Informationsfreiheitsgesetzes Schleswig-Holstein (IFG-SH) Informationen durch die ARGEn nicht zugänglich gemacht worden seien.
Diese in der Vergangenheit aufgetretene Problematik (s. auch Ziff.4.5.1) wurde im Sinne des ULD gelöst, indem die Zuständigkeit des ULD und Anwendbarkeit des IFG-SH geklärt wurden.

Mit freundlichen Grüßen

gez. Dr. Ralf Stegner