Schleswig-Holsteinischer Landtag
Umdruck 16/3362

Innenministerium
des Landes
Schleswig-Holstein

Minister

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

24105 Kiel

Kiel, den 17. Juli 2008

30. Tätigkeitsbericht des Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein

Sehr geehrter Herr Vorsitzender,

zu den wesentlichen Punkten des Unabhängigen Landeszentrums für Datenschutz (ULD) in seinem 30. Tätigkeitsbericht gebe ich die nachfolgende Stellungnahme ab:

Die Stellungnahmen des Ministeriums für Bildung und Frauen (Ziffern 4.7.2, 4.7.3), des Finanzministeriums (Ziffern 4.8.2, 4.8.3, 6.3, 6.4, 6.6, 6.8.1, 7.2, 10.4), des Ministeriums für Wissenschaft, Wirtschaft und Verkehr (Ziffern 4.4.2, 4.6.7, 5.3, 5.6.1, 5.6.3, 5.6.8, 8.6, 9.1.8) und des Ministeriums für Soziales, Gesundheit, Familie, Jugend und Senioren (Ziffern 4.6.1, 4.6.2, 4.6.4, 4.6.5, 4.6.6) wurden einbezogen.

4.1.1 Online-Meldedatenabruf mit Mängeln gestartet

Die noch ausstehenden technischen Verfahrensbeschreibungen liegen zwischenzeitlich vor und werden nochmals aktualisiert. Auf Basis der vorhandenen Unterlagen ist mittlerweile das Test- und Freigabeverfahren zum Datenabruf für Behörden und der einfachen Melderegisterauskunft in der Stadt Reinbek als koordinierende Meldebehörde erfolgt.

Die kritisierte Authentisierung im Datenabruf für Behörden wird der Forderung des ULD entsprechend nun über eine Prüfung der erfassten IP-Adresse des Rechners, von dem auf Daten zugegriffen werden soll, gewährleistet. Damit wird sichergestellt, dass eine Datenübermittlung nur an Rechner von teilnehmenden Behörden erfolgt. Die IP-Adresse des Rechners wird protokolliert.

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

Der festgestellte Mangel im Polizeiabrufverfahren wird mit dem nächsten Change-Request (Änderungsanforderung) behoben. Im Übrigen hat das Innenministerium dem ULD zugesichert, dass eine klarstellende Regelung zur so genannten Listenauskunft in das Landesmeldegesetz schnellstmöglich aufgenommen wird.

Bei der Melderegisterauskunft an Private kritisiert das ULD das Authentifizierungsverfahren. Dies stellt allerdings kein datenschutzrechtliches Problem, sondern lediglich ein Umsetzungserfordernis in der technischen Abwicklung dar. Die Art und Weise der Authentifizierung durch persönliche Vorsprache in einer Meldebehörde der Wahl soll lediglich sicherstellen, dass die Gebühr für die einfache Melderegisterauskunft zweifelsfrei der anfragenden Person zugeordnet werden kann. In Hamburg wird dieses Authentifizierungsverfahren seit längerem ohne Beanstandung des Hamburger Datenschutzbeauftragten betrieben.

4.1.3 Fragwürdige Sicherheit bei den neuen biometrischen Pässen

Die hier beschriebenen Datenschutzrisiken hatte das ULD schriftlich dem Bundesministerium des Innern (BMI) vorgetragen.
Das BMI geht in seinem Antwortschreiben an das ULD ausführlich auf die beschriebenen Angriffssituationen ein. Zusammenfassend wird festgestellt, dass die geschilderten Situationen zwar technisch vorstellbar seien. Der Informationsgewinn stehe jedoch in keinem Verhältnis zum erforderlichen Aufwand eines möglichen Angreifers, zumal der Erfolg als vergleichsweise gering eingestuft werde. Daher sei aus der Sicht des BMI die Verwendung einer Schutzhülle für den Reisepass nicht erforderlich.

4.1.7 Unsicherheiten der Zielvereinbarungen für die leistungsorientierte Bezahlung

Der Bericht verkennt die unterschiedlichen Sachstände in der Landesverwaltung und in der Kommunalverwaltung und enthält darüber hinaus problematische rechtliche Ausführungen.
In der Landesverwaltung gibt es keine leistungsorientierte Bezahlung in Verbindung mit einer Beurteilung oder einer Zielvereinbarung. Ferner ist die Behauptung, im Landesbereich würden "praktisch nach jeder Beurteilungsrunde neue Beurteilungsrichtlinien erlassen", unzutreffend. Zutreffend ist, dass jede Regelbeurteilungsaktion evaluiert wird und die Konsequenzen gemeinsam mit den Spitzenorganisationen der Gewerkschaften, mit denen die Beurteilungsrichtlinien nach § 59 des Mitbestimmungsgesetzes Schleswig-Holstein vereinbart worden sind, erörtert und entschieden werden. Die Beurteilungsrichtlinien 1995 sind bislang einmal, im Jahr 2000, neu gefasst und im Jahr 2002 geringfügig geändert worden; nach den Regelbeurteilungen 2003 und 2005 sind keine Änderungen erfolgt.

Die Kernfrage, inwieweit Zielvereinbarungen für einzelne oder mehrere Mitarbeiter zur Personalakte genommen werden sollten, bezieht sich zurzeit allenfalls auf den kommunalen Bereich.
Grundsätzlich stellen Zielvereinbarungen keine dem Personalaktenrecht zuzurechnenden Daten (Personalaktendaten) dar. Sie sind vielmehr als ein organisationsintern zwischen Führungskraft und Mitarbeiter/in einzusetzendes Instrument zur **tatsächlichen** Erreichung der gemeinsam vereinbarten Arbeitsziele zu betrachten. Als solches stehen sie, **rechtlich** gesehen, in keinem unmittelbaren inneren Zusammenhang mit dem Dienstverhältnis. Ein solcher innerer Zusammenhang besteht allerdings hinsichtlich der **Ergebnisse** von Zielvereinbarungen, soweit diese als Grundlage für eine leistungsbezogene Bezahlung (LOB) herangezogen werden. Nur insoweit kann von Personalaktendaten gesprochen werden.

Entsprechendes gilt für Zielvereinbarungen, die gemeinsam mit mehreren Mitarbeiterinnen bzw. Mitarbeitern abgeschlossen werden. Dabei liegt es in der Natur der Sache, dass die Gewährung von LOB mit den Mitgliedern des Teams kommuniziert werden muss. Ein absolutes Schweigegebot wäre mit dem notwendigen kommunikativen Prozess nicht zu vereinbaren.
Zielvereinbarungen unterliegen damit als solche grundsätzlich lediglich der allgemeinen Verschwiegenheitspflicht nach § 77 Landesbeamtengesetz (LBG) und entsprechenden tarifrechtlichen Regelungen, welche allerdings nicht für "Mitteilungen im dienstlichen Verkehr" gelten. Die für Personalaktendaten geregelten höheren Anforderungen an die Vertraulichkeit gelten somit grundsätzlich nicht, sondern, wie dargelegt, nur hinsichtlich der Ergebnisse von Zielvereinbarungen, soweit diese die Grundlage für LOB bilden. Die entsprechenden Schnittstellen sind von dem eingesetzten Bewertungssystem abhängig und können deshalb nur im Einzelfall definiert werden.
Deshalb kann der im Tätigkeitsbericht getroffenen Bewertung und der Ablehnung gemeinschaftlicher Zielvereinbarungen nicht gefolgt werden.
Dem Innenministerium liegen derzeit keine Erkenntnisse über Probleme der Kommunen mit der Behandlung von Zielvereinbarungen im Zusammenhang mit LOB vor.

4.1.8 Kernpunkte des betrieblichen Eingliederungsmanagements

Das ULD schlägt vor, mit der Durchführung des Eingliederungsmanagements einen von der Personalverwaltung unabhängigen Mitarbeiter zu beauftragen, um Interessenkonflikte, die bei der Offenbarung besonders sensibler Daten durch die Betroffenen im Verfahren entstehen können, von vorneherein auszuschließen. Es begründet diesen Vorschlag unter anderem mit dem bei der Beihilfe nach § 106 b LBG praktizieren Verfahren (eigene getrennt aufbewahrte Teilakte, Bearbeitung durch von der übrigen Personalverwaltung getrennte Organisationseinheit).

Im Innenministerium wird nach Zustimmung der oder des Betroffenen ein schlankes Verfahren unter Einbeziehung der notwendigen Beteiligten (Mitarbeiterin oder Mitarbeiter, ggf. behandelnde Ärztin oder behandelnder Arzt, ggf. arbeitsmedizinischer Dienst, ggf. Betriebliche Suchthilfe, Vorgesetzte, Personalreferat, ggf. Betriebsarzt und Vertretungsgremien) praktiziert.
In der Regel wird ein Rückkehrgespräch mit der Mitarbeiterin oder dem Mitarbeiter geführt und dabei nach dem Eingliederungsbedarf gefragt. Häufig ist bei langfristigen Erkrankungen die Erkrankung bereits bekannt (Rückenbeschwerden, Herzinfarkt, Krebserkrankung etc.). In den Gesprächen zur Rückkehr geht es vor allem um notwendige Veränderungen am Arbeitsplatz (z. B. Hilfsmittel), um Aufgabenveränderungen oder einen anderen Arbeitsplatz. Dabei werden nur in Ausnahmefällen weitere sensible Daten abgefragt.
Bis auf wenige atypische Fälle wird nicht einmal die konkrete Erkrankung für die Personalakte festgehalten. Ziel ist es, möglichst erfolgreich wiedereinzugliedern und eine weitere Arbeitsunfähigkeit zu verhindern. Dazu sind Erkenntnisse des Personalreferates und der Vorgesetzten zwingend erforderlich (z. B. Hilfsangebote, Hilfsmittel, Arbeitsbelastung, Möglichkeiten zur Veränderung des Arbeitsplatzes, Übertragung eines neuen Arbeitsplatzes).
Die Schaffung einer „Extrastelle“ für einen unabhängigen Mitarbeiter, der von allen Beteiligten die notwendigen Daten abfragen, bewerten und dann wieder mit allen, ggf. auch mehrfach, besprechen muss, erscheint in der Praxis nicht sinnvoll und führt zu zusätzlichem Verwaltungsaufwand.

Im Unterschied zur Beihilfe, bei der es vorrangig um die Erstattung von Aufwendungen und nicht um Auswirkungen auf den konkreten Arbeitsplatz geht, handelt es sich beim betrieblichen Eingliederungsmanagement um einen originären Bereich der Personalverwaltung, nämlich die Ermittlung/ das Erkennen der Ursachen von Erkrankungen und deren Vermeidung. Dies gilt umso mehr, wenn Umstände eintreten, die Auswirkungen auf die Arbeitsleistung haben.
Selbst ohne das betriebliche Eingliederungsmanagement werden bei Fragen zur Arbeitsleistung dem Personalreferat und den Vorgesetzten sensible Daten, auch aus dem Umfeld, der oder des Betroffenen bekannt. Bei Suchtproblemen gibt es eigene Dienstvereinbarungen, die ebenfalls Vorgesetzte und Personalverwaltung miteinbeziehen.

Wenngleich die Ressorts kein einheitliches - aber ein weitgehend abgestimmtes - Eingliederungsverfahren haben, so vertreten jedoch alle Mitglieder der Personalreferentenkonferenz die Meinung, dass das vom ULD skizzierte Verfahren kein gangbarer Weg ist. Das betriebliche Eingliederungsmanagement ist ein Instrument der Fürsorge und nicht der Personalkontrolle, die Ressorts werden daher auch zukünftig wie bisher verfahren.

4.2.1 Neues Polizeirecht – Verfassung und Auslegung

Die Auffassung des ULD, dass die Vorschriften zur vorbeugenden Verbrechensbekämpfung, also zur Verhütung von Straftaten (§ 179 Abs. 2 LVwG in Verbindung mit § 189 Abs. 3 LVwG), und zur lagebildabhängigen Kontrolle nach § 180 Abs. 3 LVwG „zu weit“ geraten seien, wird vom Innenministerium nicht geteilt. Die Ankündigung des ULD, bei seinen kommenden Kontrollen eine verhältnismäßige, d. h. restriktive Gesetzesanwendung einzufordern, wird nicht erforderlich sein. Die Landespolizei beachtet die von der Verfassung vorgegebene Verhältnismäßigkeit bei der Ausführung von Gesetzen.

Kontrollen nach § 180 Abs. 3 Landesverwaltungsgesetz (LVwG) setzen auf Tatsachen gestützte und damit gerichtlich nachprüfbare Lagebilder und die Verhältnismäßigkeit der Maßnahme voraus.

Mit der durch das Gesetz vom 13.04.2007 erfolgten – und schon im Gesetzgebungsverfahren vom ULD bemängelten - Erweiterung im § 179 Abs. 2 LVwG ist keine inhaltliche Änderung vollzogen worden. Die Änderung hat lediglich die vom Gesetzgeber 1992 nicht gewollten Abgrenzungsschwierigkeiten für die Praxis behoben. Die Norm hebt nun deutlicher als bisher hervor, dass es um Datenerhebungen im Zusammenhang mit gefahrenrechtlich zu beurteilenden Sachverhalten geht, denen ein hohes Schadenspotenzial zugerechnet werden kann und die sich bei ungehindertem Fortgang zu erheblichen Straftaten unterhalb der Verbrechensebene entwickeln könnten.

Die Speicherung der von den Normadressaten des § 179 Abs. 2 LVwG erhobenen Daten richtet sich nach § 189 Abs. 3 LVwG. Die Speicherung muss dabei zur Aufklärung des die Erhebung der Daten begründenden Sachverhaltes erforderlich sein. Allerdings ist die Speicherung auf den für die Erhebung Anlass gebenden Sachverhalt beschränkt. Die gegenüber den allgemeinen Speicher- und Prüffristen verfügten Beschränkungen tragen der Tatsache Rechnung, dass es sich bei den Adressaten einer Datenerhebung nach § 179 Abs. 2 LVwG regelmäßig weder um einen Störer noch um einen strafprozessual Verdächtigen handelt.

Das Bundesverfassungsgericht hat in seiner Entscheidung vom 11.03.2008 (Aktenzeichen: 1 BvR 1254/07) die Regelung des automatisierten Abgleichs der mit technischen Mitteln erhoben Kraftfahrzeugkennzeichen mit dem polizeilichen Fahndungsbestand (sog. Kfz-Kennzeichen-Scanning) gem. § 184 Abs. 5 LVwG mit dem Grundrecht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG für nichtig

erklärt. Den Einsatz der Kennzeichenlesegeräte hat das Innenministerium daraufhin unmittelbar nach Urteilsverkündung gestoppt.

4.2.2 Verweigerungshaltung bei Antiterrordatei (ATD)

Im Zusammenhang mit der Verfassungsbeschwerde gegen die Antiterrordatei übersandte das ULD dem Landeskriminalamt (LKA) einen umfangreichen Fragenkatalog. Nicht alle Fragen konnten beantwortet werden, weil das ULD ausdrücklich nicht im Rahmen seiner Kontrollbefugnisse, sondern zur Weitergabe der Informationen an die Öffentlichkeit informiert werden wollte. Weil die gewünschten Informationen jedoch durch den VS-Verschlussgrad bis zur Stufe „geheim“ geschützt waren, durften sie nicht veröffentlicht werden.
Um deutlich zu machen, dass es keine grundsätzliche Verweigerungshaltung des Innenministeriums gibt, wurde im Antwortschreiben an das ULD auf das gesetzlich festgeschriebene datenschutzrechtliche Kontrollrecht des ULD, das eine umfassende Beantwortung der Fragen ermöglichen würde, besonders hingewiesen.
Das Auskunftsverfahren zur Antiterrordatei wird zurzeit auf der Grundlage eines Entwurfes einer Lenkungsgruppe unter Federführung des Bundeskriminalamtes (BKA) durchgeführt. Der Abstimmungsprozess aller an der ATD teilnehmenden Behörden, sowie unter Beteiligung der Datenschutzbeauftragten der Länder und des Bundes, ist noch nicht abgeschlossen.

4.2.3 Zuverlässigkeitsüberprüfungen – Neuer Standard am Gesetzgeber vorbei?

Sowohl nach Auffassung des Bundesverfassungsgerichts im Volkszählungsurteil als auch nach den Kommentierungen zum Grundgesetz bestehen keine Grundrechtsbeeinträchtigungen bei der Verarbeitung von personenbezogenen Daten auf der Grundlage einer Einwilligung des Betroffenen. Der Betroffene hat das Recht, seine dispositive Verantwortung (wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden) jederzeit auszuüben. Nach § 177 Abs. 1 LVwG ist die Verarbeitung von personenbezogenen Daten möglich, soweit dies durch Gesetz zugelassen ist oder der Betroffene eingewilligt hat. Der Vorwurf, Zuverlässigkeits- und Sicherheitsüberprüfungen „am Gesetzgeber vorbei“ durchzuführen, ist insofern nicht gerechtfertigt. Die formelle Ausgestaltung der Einwilligung richtet sich nach § 12 Landesdatenschutzgesetz, da das Landesverwaltungsgesetz keine Regelungen enthält. Besondere Anforderungen, wie die Festlegung des konkreten Verwendungszweckes, das rechtsverbindliche Vorliegen der Einwilligung vor der Datenverarbeitung und die Aufklärung über die Bedeutung der Einwilligung, werden erfüllt. Das Verfahren der „informierten Einwilligung“ wurde bisher beim Confederation Cup 2005, bei der Fußball WM und beim Tag der Deutschen Einheit in Schleswig-Holstein angewandt. Es sind keine Rechtsverfahren oder Schadensersatzforderungen von Arbeitnehmern oder Betroffenen bekannt geworden (s. auch Stellungnahme zum 28. Tätigkeitsbericht des ULD, Ziffer 4.2.9 und Stellungnahme zum 29. Tätigkeitsbericht des ULD, Ziffer 4.2.5).

4.2.4 Online-Durchsuchung

Das Bundesverfassungsgericht hat in seiner das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer System statuierenden Entscheidung vom 27.02.2008 (1 BvR 370/07; 1 BvR 595/07) zum nordrhein-westfälischen Verfassungsschutzgesetz die Maßnahme der Online-Durchsuchung als solche in Grenzen für mit der Verfassung vereinbar bezeichnet und Voraussetzungen für die Gesetzgebung formuliert.

Die Bundesjustizministerin prüft derzeit, ob die Strafprozessordnung geändert werden soll. Für den Bereich der Prävention sieht der Gesetzentwurf des Bundesinnenministerium zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt den verdeckten Zugriff auf informationstechnische Systeme vor. Die Innenminister und –senatoren halten den Gesetzentwurf im Gefahrenbereich des internationalen Terrorismus einstimmig für erforderlich.

4.2.5 Auskunftsverfahren bei der Polizei

Die grundsätzliche fallbezogene Ausgestaltung des Auskunftsverfahrens wurde letztmalig am 08.06.2007 in einem gemeinsamen Gespräch zwischen Polizei und ULD diskutiert. Verfahrensmängel, wie im 28. und 29. Tätigkeitsbericht des ULD angesprochen, waren bereits abgestellt.
Die im „13 Punkte Papier“ des ULD (vom 14.07.2005) angesprochenen Problembereiche wurden, bis auf die Bearbeitung des Auskunftsersuchens als Verwaltungsvorgang, einvernehmlich geregelt. Eine Verfahrensbeschreibung des Innenministeriums schafft nun Klarheit und Transparenz. Der Polizei steht neben dem Vorgangsbearbeitungssystem @rtus kein weiteres System für allgemeine polizeiinterne Verwaltungsvorgänge zur Verfügung. Das Landespolizeiamt bemüht sich, auch für diesen letzten Punkt eine praktikable Lösung herbeizuführen.
§ 198 Abs. 3 LVwG regelt die Verweigerung von Auskünften. Eine abstrakte Regelung kann hier nicht getroffen werden, weil immer der konkrete Einzelfall zu betrachten ist. Bei der Bewertung werden die zwischen dem Generalstaatsanwalt und dem ULD vereinbarten Grundsätze aus dem Jahre 2002 zugrunde gelegt. Die Überprüfung eines konkreten Falles durch den Innen- und Rechtsausschuss hatte im Jahr 2006/2007 die Bewertung der Polizei bestätigt.

4.2.6 Kontrolle beim Staatsschutz des LKA

Die vom ULD genannten „amtsinternen“ Dateien „Indexdatei Kalender“, „Innere Sicherheit Schleswig-Holstein (ISSH)“ und „Warndatei Rechts“ sind zur Aufgabenerfüllung des polizeilichen Staatsschutzes weiterhin erforderlich.
Eine neue Errichtungsanordnung „Indexdatei Kalender“ wurde zwischenzeitlich mit dem ULD abgestimmt und festgeschrieben. Errichtungsanordnungen zu den Dateien „Innere Sicherheit Schleswig-Holstein (ISSH)“ und „Warndatei Rechts“ wurden im Landeskriminalamt (LKA) abgestimmt. Der Abstimmungsprozess mit dem ULD hat begonnen.
Eine strenge Bedarfsprüfung der vom Vorgangsbearbeitungssytem „Compas“ nach „@rtus“ zu übernehmenden Datenbestände ist erfolgreich abgeschlossen.

4.2.7 Protokollierung bei polizeilicher Datenverarbeitung

Der geforderte Umfang der Protokollierung wird seit Jahren bei INPOL-SH angewandt. Die Anregung, sie als Modell zu nehmen und so Synergien zu gewinnen, ist angekommen.

4.2.8 @rtus – die neue Datei der Polizei in Schleswig-Holstein

In der Errichtungsanordnung zu @rtus VBS stehen zahlreiche Anregungen des ULD. Das Regelwerk braucht bundesweit keinen Vergleich zu scheuen. Details der Vorgangsbearbeitung und Vorgangsverwaltung sind weitestgehend mit ULD abgestimmt.
Zu Fristbeginn, Speicherdauer und Löschkonzepten hat das Innenministerium dem ULD seine Rechtsauffassung übermittelt und Lösungen aufgezeigt. Der Reaktion wird entgegengesehen.

Zugriffsberechtigungen werden zukünftig vom Landespolizeiamt (LPA) eingerichtet, der Erlass befindet sich derzeit in der Mitzeichnung.

4.4.2 Fachaufsicht über Kfz-Zulassungsbehörden auf Tauchstation

Ab 1. September 2008 ist vorgesehen, dass die Kfz-Zulassungsbehörden neben bereits bestehenden anderen Möglichkeiten in einem Online-Dialogverfahren registerpflichtige Daten an das Zentrale Fahrzeugregister (ZFZR) übermitteln können. Dieses Verfahren wird von den Fahrerlaubnisbehörden bereits seit einigen Jahren praktiziert.
Das ULD hatte die Einrichtung und den Betrieb von Kopfstellen im Rahmen seiner beratenden Funktion geprüft und Unzulänglichkeiten festgestellt. Neben informellen Gesprächen vor Ort hat es zusammen mit dem Kraftfahrt-Bundesamt (KBA) Hinweise für die Zulassungs- und Fahrerlaubnisbehörden erarbeitet und das Ministerium für Wissenschaft, Wirtschaft und Verkehr (MWV) als oberste Fachaufsichtsbehörde unterrichtet. Da die Standards für die Datenübermittlung nach den §§ 24 Abs. 2 und 33 Abs. 3 der Verordnung über die Zulassung von Fahrzeugen zum Straßenverkehr (FZV) vom KBA festgelegt werden, hat das MWV das KBA entsprechend unterrichtet.
Nach Auffassung des MWV unterliegt der Datenschutz nicht der straßenverkehrsrechtlichen Fachaufsicht, auch dann nicht, wenn die Datenschutzbestimmungen im Straßenverkehrsgesetz (StVG) oder in auf dessen Grundlage erlassenen Rechtsverordnungen des Bundesministeriums für Verkehr, Bau und Stadtentwicklung (BMVBS) enthalten sind. Straßenverkehrsrechtlich wurden keine Mängel dargelegt.
Das MWV hat das ULD im August letzten Jahres darauf hingewiesen, dass die angesprochene Problematik der IT-Anbindung der Fahrerlaubnis- und Zulassungsbehörden an das KBA nicht in die hiesige Zuständigkeit falle und somit auch nicht der Fachaufsicht unterliege.
Es hat auch den Hinweis gegeben, die Beanstandungen entsprechend der Aufgabenstellung des ULD gemäß dem LDSG den betroffenen Behörden bekannt zu machen.

4.6.1. Neues von der elektronischen Gesundheitskarte

Der Bewertung des ULD ist zuzustimmen. Insbesondere ist zu begrüßen, dass das ULD ausdrücklich feststellt, dass zur Ermöglichung der Nutzung der elektronischen Gesundheitskarte (eGK) durch besonders ältere und multimorbide Versicherte es unbedenklich sei, für diesen Personenkreis eine sog. Default-PIN fest in die eGK einzuprogrammieren.
Das ULD stellt im Bericht ausdrücklich fest, dass die Sicherheit des Gesamtsystems durch eine solche Ergänzung nicht beeinträchtigt wäre. Hohe Standards bei der Datensicherheit seien grundsätzlich zu begrüßen, aber sie dürften nicht gegen die mit dieser Technik befassten Nutzer eingesetzt werden. Vielmehr sei eine Möglichkeit erforderlich, die Technik hinreichend sicher, aber auch ohne übermäßige Anforderungen an das Verfahren, anzuwenden.
Bedauerlicherweise scheint das ULD allerdings seine Meinung geändert zu haben, wie aus einem dem Ministerium für Soziales, Gesundheit, Familie, Jugend und Senioren vorliegenden Vermerk des ULD vom 17.04 2008 hervorgeht. Dort wird nun festgestellt: „Das Risiko einer Default–PIN ist aus Datenschutzsicht nicht hinnehmbar.“ Die barrierefreie Nutzung der eGK gerade für den angesprochenen Personenkreis, der zu den Hauptnutzern der eGK gehören dürfte, ist damit in Frage gestellt.

4.6.2 Mammografie-Screening

Die Darstellung zum Mammographie-Screening ist teilweise unzutreffend bzw. missverständlich, deshalb hier einige Hinweise zur Richtigstellung:

- Die Kooperationsgemeinschaft Mammographie-Screening verfolgt nicht das Anliegen der Mortalitätsevaluation. Die Bewertung der Frage, ob sich das Screening im Hinblick auf die Reduzierung der Brustkrebs-Sterblichkeit lohnt, ist also nicht Aufgabe der Kooperationsgemeinschaft.

- Die Untersuchung der Frage, ob die Brustkrebs-Mortalität unter den Screening-Teilnehmerinnen niedriger ist als bei den Nicht-Teilnehmerinnen, kann nur mithilfe von Krebsregister-Daten untersucht werden. Voraussetzung ist dafür, dass das Krebsregister für jeden Brustkrebsfall die Information darüber erhält, ob der Tumor im Screening entdeckt worden ist oder nicht.

- Mortalitätsdaten gehen über die Todesbescheinigungen bei der Vertrauensstelle ein. Verarbeitet werden sie auch in der Registerstelle. Dort wird im Todesfall dem epidemiologischen Datensatz die Angabe über das Sterbedatum hinzugefügt. Zur Unterstützung der klinischen Forschung dürfen Angaben zum Sterbedatum von der Registerstelle auf Antrag an ein Klinikregister übermittelt werden (§ 6 Abs. 6 Landeskrebsregistergesetz, LKRG) und damit das Krebsregister verlassen.

- Die Krebsfrüherkennungsrichtlinien (KFÜ-Richtlinien) sehen für Qualitätssicherungszwecke einen Abgleich der Screening-Daten mit Krebsregister-Daten vor. Dieser Abgleich soll lt. Richtlinien allein auf den Kontrollnummern beruhen. Mittlerweile hat sich herausgestellt, dass für einen "treffsicheren" Abgleich unbedingt weitere Daten (z.B. Geburtsdatum, Anschrift) erforderlich sind. Die KFÜ-Richtlinien müssen deshalb überarbeitet werden. Das geschieht bereits.

- Auch die statistische Zahl von Intervallkarzinomen lässt sich nicht einfach, sondern nur mit einem um mehrere Angaben erweiterten Abgleich der Screening-Daten mit Krebsregister-Daten ermitteln.

- In den KFÜ-Richtlinien ist es nicht vorgesehen, dass Angaben zu einer Brustkrebs-Erkrankung, die im Krebsregister gespeichert sind, an die Zentrale Stelle übermittelt werden. Die KFÜ-Richtlinien sehen hingegen vor, dass das Krebsregister an die Zentrale Stelle die Kontrollnummern derjenigen Frauen übermittelt, für die im Krebsregister eine Brustkrebs-Erkrankung registriert ist. Von dem Programmverantwortlichen Arzt der Screening-Einheit soll dann die betroffene Frau gefragt werden, ob sie damit einverstanden ist, dass die ärztlichen Unterlagen aus dem Screening (z.B. Röntgenaufnahme) zur Begutachtung an das Referenzzentrum übermittelt werden.

- Zu den Aufgaben des Krebsregisters SH gehört es auch, zu der Bewertung der Qualität präventiver und therapeutischer Maßnahmen beizutragen (§ 1 Abs. 3 LKRG).

Das ULD kommt zu dem Schluss, dass der Abgleich mit dem Krebsregister nur mit Einwilligung der betroffenen Frauen stattfinden soll. Der Begriff "individualisierte Qualitätskontrolle" erweckt den Eindruck, als ginge es dabei einzig und allein um die betroffene Frau. Tatsächlich dient diese Qualitätssicherungsmaßnahme allen am Screening teilnehmenden Frauen. Denn alle Teilnehmerinnen profitieren davon, wenn sichergestellt ist, dass die Screening-Röntgenärzte möglichst wenig Tumore übersehen. Bevor auf Landesebene die Entscheidung getroffen wird, ob der Abgleich für alle Teilnehmerinnen oder lediglich für die Teilnehmerinnen mit Einwilligung durchgeführt wird, müsste eine Abwägung stattfinden zwischen dem zu erwartenden allgemeinen Nutzen (Erkennung "diagnoseschwacher"

Screening-Einheiten und Nachschulung) und dem möglichen Schaden für einzelne Patientinnen.
Selbstverständlich kann der Abgleich zwischen Screening-Daten und Krebsregister-Daten erst dann erfolgen, wenn die KFÜ-Richtlinien überarbeitet worden sind und eine hohe Treffsicherheit erlauben.

4.6.4 Patientenakten und Computer im Müll und
4.6.5 Aufbewahrungsfristen bei Patientenakten

Nach § 10 der Berufsordnung der Ärztekammer Schleswig-Holstein, nach § 12 der Berufsordnung der Psychotherapeutenkammer als auch nach § 12 der Berufsordnung der Zahnärztekammer sind sowohl (Zahn-)Ärztinnen und Ärzte als auch Psychotherapeutinnen und Psychotherapeuten verpflichtet, die in Ausübung des Berufes gemachten Feststellungen und getroffenen Maßnahmen zu dokumentieren und für die Dauer von 10 Jahren nach Abschluss der Behandlung ordnungsgemäß aufzubewahren.
Sofern es im Einzelfall aus medizinischen Gründen im Interesse der Patientin oder des Patienten (z.B. bei Krebserkrankungen) erforderlich ist, Patientendaten weiterhin aufzubewahren, kann auch eine längere Aufbewahrung der Daten erfolgen. Die/der behandelnde Ärztin/Arzt trifft diese Entscheidung in begründeten Einzelfällen vor Ort.

Alle (Zahn-)Ärztinnen und Ärzte bzw. Psychotherapeutinnen und Psychotherapeuten haben dafür Sorge zu tragen, dass bei Praxisübergabe, im Falle von längerer Krankheit oder Abwesenheit, die Aufzeichnungen in gehörige Obhut gegeben und im Falle des Ablaufes der Aufbewahrungszeit unter Beachtung der gesetzlichen Bestimmungen des Datenschutzes vernichtet werden.
Verstöße gegen die Berufsordnungen werden von den Heilberufekammern berufsrechtlich geahndet.
Die Kammern bieten auf Nachfrage ihren Mitgliedern eine entsprechende Beratung im Einzelfall an und informieren in den Kammermitteilungen. Sofern die Gefahr besteht, dass Patientendaten nicht mehr ordnungsgemäß aufbewahrt werden (z.B. bei verwaisten Praxen, Todesfall/Insolvenz), übernimmt im Einzelfall die zuständige Kammer die Dokumentationspflicht der Ärztin oder des Arztes und bewahrt das Datenmaterial selbst auf, um das Ansehen des Berufsstandes zu wahren.
Auf Nachfrage des Sozialministeriums teilten die Kammern mit, dass ihnen keine Häufung von Verstößen gegen die Dokumentationspflichten der jeweiligen Berufsordnungen bekannt sei. Ein Einzelfall aus jüngster Vergangenheit ist von der Psychotherapeutenkammer entsprechend berufsrechtlich geahndet worden.

4.6.6 Novellierung Maßregelvollzugsgesetz

Im Rahmen der Fachaufsicht durch die oberste Landesgesundheitsbehörde über den Maßregelvollzug wird auf die Einhaltung und Beachtung der datenschutzrechtlichen Regelungen im Maßregelvollzug im Interesse der Patientinnen und Patienten hingewirkt und so für eine datenschutzfreundliche Anwendung der neuen Vorschriften gesorgt.

4.6.7 Das Universitätsklinikum Schleswig-Holstein und der Datenschutz

Das Universitätsklinikum Schleswig-Holstein (UK S-H) befindet sich im Rahmen der Sanierungsmaßnahmen in einer mehrjährigen dynamischen Reorganisationsphase, die insbesondere die Einführung eines klinikweiten Informationssystems und die Verselbstständigung von einzelnen Organisationseinheiten in Privatrechtsform beinhaltet. Hieraus ergeben sich vielfältige datenschutzrelevante und gesetzlich geforderte sowie zudem risikobehaftete Fragestellungen, die einer qualifizierten und fachkundigen Begleitung durch den behördlichen Datenschutzbeauftragten bedürfen.

Der 30. Tätigkeitsbericht des ULD sowie der Bericht des Datenschutzteams des UK S-H haben den Vorstand des UK S-H veranlasst, die materiell-rechtliche Ausstattung des behördlichen Datenschutzbeauftragten den tatsächlichen, gestiegenen Notwendigkeiten anzupassen.
Der Datenschutzbeauftragte des UK S-H hat mit dem ULD bereits über ein Modell des sog. Konzerndatenschutzbeauftragten gesprochen. Mit maßvollen zusätzlichen Ressourcen könnten damit nicht nur die Tochtergesellschaften datenschutzkonform gestaltet werden, sondern auch die zusätzlich notwendigen Regelungsbedarfe im Bereich Informationstechnik.
Unter Ausnutzung der mit diesem Organisationsmodell einhergehenden Synergien wird dem UK S-H die Fortsetzung eines adäquaten kontinuierlichen Datenschutzmanagements möglich sein.

4.7.2 Wissensdefizite bei Schulleiterinnen, Schulleitern und Schulsekretärinnen

Der Bereich des Datenschutzes findet gerade im Umgang der Schulen mit den neuen Informationstechnologien bei den Schulleitungen hervorgehobene Beachtung. Das Datenschutzrecht mit seiner Vielzahl an Regelungen in verschiedenen Gesetzen und Verordnungen ist aber in der Tat nicht auf den ersten Blick leicht bzw. vollständig beherrschbar. Daher ist nicht auszuschließen, dass teilweise entsprechende Informationsdefizite bestehen. Datenschutzrechtliche Eingaben und Anfragen lassen in ihrer Häufigkeit und auch in ihrer Qualität aber nicht die Folgerung eines regelmäßig bestehenden Kenntnisdefizits zu. Gleichwohl bietet das Institut für Qualitätsentwicklung an Schulen Schleswig-Holstein (IQSH) in Kooperation mit dem ULD ab dem 2. Schulhalbjahr 2007/08 verstärkt datenschutzrechtliche Fortbildungen für Schulleiterinnen und Schulleiter wie folgt an:

- Schulleitungen Gymnasium: jeweils eine Doppelveranstaltung im 2. Halbjahr 2007/08 und im 1. Halbjahr 2008/09,
- Schulleitungen Grundschulen: ab dem 2. Halbjahr 2008/09,
- Schulleitungen Regional- und Gemeinschaftsschulen: ab Sommer 2009.

Die Anmerkung des ULD hat also bereits zum jetzigen Zeitpunkt durch das Ministerium für Bildung und Frauen Berücksichtigung gefunden. Für die Schulträger kann allerdings nicht gesprochen werden.

4.7.3 Zentrale Schülerdatenbank

Das ULD erklärt, aus den jährlich verschlüsselten Schülerdatensätzen ließe sich „ohne größeres Zusatzwissen“ die hinter dem einzelnen Datensatz stehende Person feststellen. Dies ist nicht zutreffend.
Es gibt innerhalb der Kultusministerkonferenz (KMK) bislang noch keine Festlegung, in welcher Form und an welchem Ort die Daten verschlüsselt und gespeichert werden sollen. Fest steht: Bei einer Speicherung außerhalb der Schule werden die persönlichen Daten der Schüler, wie Name und Anschrift, nicht gespeichert. Stattdessen erhält der einzelne Datensatz eine Kennnummer, die mittels einer Hashwert-Funktion ein weiteres Mal verschlüsselt werden soll. Diese Art der Verschlüsselung ist ein anerkanntes Verfahren, weil es eine Rückverfolgung auf den Ursprungsdatensatz praktisch unmöglich macht. Die verbleibende und rein theoretische Möglichkeit einer Rückidentifizierung der Datensatznummer wird durch die Ausgestaltung des Verfahrens zudem ausgeschlossen.
Letztlich muss noch beachtet werden, dass sich die KMK darin einig ist, Datensätze nur an gesicherten Orten (z.B. Statistische Ämter) zu speichern, so dass ein unbefugter Zugriff ohnehin nicht erfolgen kann.

Das ULD erklärt, die KMK plane, „für nicht näher definierte Zwecke die in den Bundesländern gespeicherten Daten temporär zusammenzuführen“. Dies ist ebenso nicht zutreffend.

1. Die KMK ist nicht bereit, einzelne Datensätze oder Reihen von einzelnen Datensätze weiter zu geben. Sofern überhaupt eine Weitergabe von Informationen erfolgt, dann nur in Form von Summendaten und in Form von Inhaltsclustern (leicht aggregierte Daten).
2. Die KMK hat den möglichen Adressatenkreis eindeutig auf die Bildungsforschung und Bildungspolitik begrenzt. Für private oder gar kommerzielle Zwecke werden keine Daten weitergegeben. Durch diese Eingrenzung ergibt sich zugleich auch der Begründungszusammenhang, warum nicht mit Stichproben gearbeitet werden kann. Diesbezüglich wurde bereits zum 29. Tätigkeitsbericht des ULD (Ziffer 4.7.1) vom Ministerium für Bildung und Frauen wie folgt Stellung genommen:
   „*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.“*

4.8.2 Speicherung von Lohnsteuerabzugsmerkmalen - Bundes-Steuerdatei

Im Rahmen des Gesetzgebungsverfahrens zum Jahressteuergesetz 2008 wurde der Datenschutz bereits thematisiert.
Der Datensicherheit wird u.a. durch die strikte Zweckbindung, die gesetzlich in § 139b Abgabenordnung (AO) verankert ist, Rechnung getragen. Damit wird sichergestellt, dass nur Berechtigte Zugriff auf den Datenpool haben.
Ein weiteres Sicherheitsmerkmal ist das sog. Authentifizierungsverfahren. Dieses wird bereits seit Einführung des Verfahrens ElsterLohn I (elektronische Lohnsteuerbescheinigung) erfolgreich genutzt.
Zukünftig muss sich der Arbeitgeber, wenn er Daten abrufen will, mit Eingabe der Identifikationsnummer und des Geburtsdatums des Arbeitnehmers sowie der Wirtschafts-Identifikationsnummer des Arbeitgebers authentifizieren.
Das Bundeszentralamt für Steuern ist zudem über die Steuerdatenübermittlungsverordnung verpflichtet, die Sicherheitsmaßnahmen ständig zu aktualisieren. Es führt umfangreiche Kontrollen durch. Es arbeitet mit dem Bundesamt für Sicherheit in der Informationstechnik und dem TÜV Informationstechnik (TÜViT) zusammen und lässt die Sicherheit des Zugriffschutzes auch durch unabhängige Gutachter testen.
Das Verfahren ElsterLohn II (elektronische Lohnsteuerkarte) wird daher als mit dem Datenschutz vereinbar angesehen.

4.8.3 Insolvenzhinweis als Adresszusatz

Eine dem Datenschutz gerecht werdende landesweit einheitliche Handhabung bei der Adressierung in Insolvenzfällen wurde zwischenzeitlich wie folgt umgesetzt:

Nach Einführung der neuen Software EOSS (Evolutionär orientierte Steuer-Software) in der schleswig-holsteinischen Steuerverwaltung werden keine Insolvenzvermerke mehr im Adressfeld aufgenommen. Vielmehr werden in laufenden Insolvenzverfahren ausnahmslos die Insolvenzverwalter als Empfangsbevollmächtigte gespeichert.

5.3 Heuschrecken – Erschrecken nach dem Darlehensverkauf

Das ULD nimmt Stellung zur Thematik des Verkaufs von Darlehensforderungen durch Kreditinstitute. Anlass für die Prüfung durch das ULD waren Darlehensverkäufe von zwei Sparkassen sowie hiermit im Zusammenhang stehende Kundenbeschwerden.
Die Thematik hat bundesweit ein erhebliches Medienecho gefunden und eine intensive Diskussion ausgelöst, da der Verkauf von Darlehensforderungen zu Refinanzierungszwecken in der Kreditwirtschaft insgesamt von einiger Bedeutung ist. Große Verunsicherung haben bei den Verbrauchern insbesondere Berichte hervorgerufen, nach einem Kreditverkauf könne auch bei ordnungsgemäß bedienten Darlehen die Zwangsvollstreckung in das Eigenheim drohen. Von Seiten des Verbraucherschutzes ist hierzu allerdings bereits klargestellt worden, dass bisher kein derartiger Fall in der Praxis bekannt geworden ist.

Der Bundesrat hat am 4. Juli 2008 mit den Stimmen Schleswig-Holsteins dem Risikobegrenzungsgesetz (Bundestags-Drucksachen 16/7438,16/7718,16/9778) zugestimmt. Dieses Gesetz regelt u. a., dass sich der Kreditkäufer alle Vereinbarungen der Sicherungsabrede entgegenhalten lassen muss. Der Entwurf eines Gesetzes zur Begrenzung der Risiken des Kreditverkaufs (Kreditnehmerschutzgesetz, BR-Drucksache 152/08 (B)) des Bundesrates hat sich damit erledigt.
Auf Seiten der Kreditwirtschaft wird befürchtet, dass zu weit gehende Anforderungen in diesem Bereich die Refinanzierung der Institute erschweren und deutlich verteuern könnten.
Zu der vom ULD in seinem Bericht erwähnten Frage, inwieweit bei Verkauf von Darlehensforderungen durch Sparkassen gegen § 203 Abs. 2 Nr. 1 Strafgesetzbuch (StGB) verstoßen werde, liegt bereits eine Entscheidung des OLG Schleswig vom 18.10.2007 (5 U 19/07 WM 2007 S. 2103 ff.) vor, in der ausgeführt wird, dass die Übertragung notleidender Darlehensforderungen an ein privatrechtliches Kreditinstitut nicht „unbefugt“ erfolgt. Ein Abtretungsverbot bei Sparkassen könnte die Refinanzierungsmöglichkeiten dieser Institute möglicherweise in existenzbedrohender Weise einschränken und würde daher gegenüber den privatrechtlichen Banken eine unzulässige Ungleichbehandlung darstellen.

Im Rahmen seiner datenschutzrechtlichen Bewertung von Darlehensverkäufen betont das ULD zunächst das „Übermittlungsverbot“, wenn der Datenweitergabe an den Käufer schutzwürdige Betroffeneninteressen entgegenstehen. Diese Aussage stellt die datenschutzrechtliche Rechtslage allerdings verkürzt dar. Gemäß § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) besteht für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ein Verbot mit Erlaubnisvorbehalt. Dies bedeutet, dass die Zulässigkeit einer Datenverarbeitung, soweit sie dem Bundesdatenschutzgesetz unterliegt, grundsätzlich einer Rechtsgrundlage bedarf. Sind die Tatbestandsvoraussetzungen einer Erlaubnisnorm erfüllt, besteht demnach gerade *kein* Übermittlungsverbot.
Sofern nicht im Einzelfall eine ausdrückliche Einwilligung des Betroffenen vorliegt, kommt für den Fall des Verkaufs von Darlehensforderungen durch Kreditinstitute § 28 Abs. 1 Satz 1 Nr. 2 BDSG als gesetzliche Grundlage für die in diesem Zusammenhang erforderlichen Datenübermittlungen in Betracht. Hiernach ist die Weitergabe personenbezogener Daten zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass die schutzwürdigen Interessen des Betroffenen an dem Ausschluss der Verarbeitung (Übermittlung) überwiegen. Eine

Unzulässigkeit der Datenweitergabe ist hiernach nicht schon dann gegeben, wenn schutzwürdige Interessen auf der Betroffenenseite überhaupt bestehen. Es ist vielmehr eine Abwägung mit den „berechtigten Interessen“ der speichernden Stelle – hier des Kreditinstituts – vorzunehmen.
Gerade bei notleidenden Krediten haben Kreditinstitute aber ein ganz erhebliches Interesse an einer bestmöglichen Verwertung von Forderung und Sicherheiten, u. U. auch an einem Verkauf der Forderung (und der dabei erforderlichen Datenübermittlung). Ein notleidender Kredit liegt nach dem allgemeinen Verständnis dann vor, wenn ein Kredit aufgrund von Vertragsverletzungen des Kreditnehmers gekündigt wurde oder jedenfalls auf der Grundlage der getroffenen Vereinbarungen jederzeit außerordentlich gekündigt werden könnte (vgl. Nobbe ZIP 2008 S. 97).
In einer solchen Situation kann ein Kreditinstitut mit einem Verkauf der Forderung zum einen das Kreditrisiko auf Erwerber übertragen und damit hinsichtlich des aufsichtsrechtlich vorzuhaltenden Eigenkapitals eine Entlastung erreichen. Damit können auch Spielräume für die Gewährung neuer Darlehen geschaffen werden, was nicht nur im Interesse des Instituts sondern auch anderer – an einem Kredit interessierten - Kunden liegen kann. Darüber hinaus kann mit einem Verkauf der Forderung die kostenintensive Betreuung des notleidenden Engagements sowie ggf. die aufwändige Durchführung von Vollstreckungsmaßnahmen vermieden und dem Institut zudem kurzfristig Liquidität zugeführt werden.

Dem gegenüber stehen die aus dem Vertragsverhältnis mit dem Kreditinstitut resultierenden Geheimhaltungsinteressen des Kunden. Da bei notleidenden Krediten der Kunde aber gerade seinen eigenen vertraglichen Pflichten nicht nachgekommen ist, erscheint dieses Interesse in dieser Situation zumindest nicht überwiegend schutzwürdig. Nach verbreiteter Auffassung in der juristischen Literatur wird ein Kreditinstitut in einer solchen Situation daher auch als berechtigt angesehen, den Kredit sowie die hierzu gewährten Sicherheiten ohne Mitwirkung des Kunden zu veräußern (vgl. Nobbe ZIP 2008 S. 104, Bruchner/ Krepold in: Schimansky/Bunte/Lwowski, Bankrechtshandbuch, 3. Aufl. 2007 Bd. I, § 39 Rn. 60).
Das ULD stellt in seinem Bericht lediglich fest, dass bei einem notleidenden Kredit das schutzwürdige Interesse des Kunden geringer zu bewerten sei, als wenn Zins und Tilgung bisher korrekt bedient wurden; mögliche berechtigte Interessen auf der Seite des Kreditinstituts sowie eine Interessenabwägung finden keine Erwähnung. Da im Ergebnis hinsichtlich der Datenübermittlung bei notleidenden Krediten aber keine Beanstandung erfolgt, ist davon auszugehen, dass das ULD die Veräußerung von notleidenden Krediten für datenschutzrechtlich grundsätzlich zulässig hält.
Das ULD führt unter Hinweis auf die neueste Rechtsprechung des Bundesverfassungsgerichtes aus, dass datenschutzrechtliche Verstöße im Rahmen des Verkaufs von Darlehensforderungen dazu führen können, dass das Grundgeschäft selbst unwirksam ist. Hierzu ist anzumerken, dass das Bundesverfassungsgericht in seinem Beschluss vom 11. Juli 2007 (I BVR 1025/07 WM 2007, S. 1694 ff.) bei Abtretung von Kreditforderungen regelmäßig gerade nicht von einer Nichtigkeit des Grundgeschäfts ausgeht und insoweit die Entscheidung des Bundesgerichtshofs vom 27.2.2007 (WM 2007 S. 643 ff.) bestätigt.

Bei Abtretung von Kreditforderungen sei eine einzelfallbezogene Abwägung der Interessen verfassungsrechtlich nicht geboten. Bei anderen Forderungen, durch deren Abtretung typischerweise Geheimhaltungsinteressen des Schuldners schwerwiegend beeinträchtigt würden, könne dies anders sein, soweit Informationen über vertrauliche oder gar intime Umstände aus dem Leben des Schuldners wiedergeben würden oder durch gezielte Informationssammlung ein umfassender Einblick in die Verhältnisse des Betroffenen verschafft werde. Es sei jedoch nicht ersichtlich, dass dies im Fall einer Übertragung von Dar-

lehensforderungen der Fall sei, wenn im Zusammenhang mit der Abtretung die Auskunftspflicht des § 402 BGB erfüllt wird.
Im Hinblick auf den Verkauf von Darlehensforderungen in das Ausland führt das ULD aus, dass der Datenschutz einer Datenübermittlung dann nicht entgegenstehe, sofern für den Kreditnehmer hinreichend Transparenz bestehe und bei dem neuen Gläubiger adäquate Datenschutzregelungen bestehen. Nicht nachvollziehbar erscheint insoweit, unter welchen Voraussetzungen der Transparenzaspekt Einfluss auf die Zulässigkeit einer Datenübermittlung haben soll.
Das Bundesdatenschutzgesetz sieht für bestimmte Fallkonstellationen eine Benachrichtigungspflicht vor, die in § 33 BDSG detailliert geregelt wird. Gemäß § 33 Abs. 1 BDSG ist zur Benachrichtigung des Betroffenen verpflichtet, wer erstmals personenbezogene Daten für eigene Zwecke ohne Kenntnis des Betroffenen speichert. Zu benachrichtigen ist über den Umstand der Speicherung selbst, die Art der Daten, die Zweckbestimmung der Erhebung, die Verarbeitung oder Nutzung und die Identität der verantwortlichen Stelle. Mit der Benachrichtigung wird der Betroffene in die Lage versetzt, seine Rechte nach dem Bundesdatenschutzgesetz gegenüber der betreffenden Stelle geltend zu machen. Mit der Benachrichtigung können somit die schutzwürdigen Interessen des Kunden hinsichtlich seiner Datenschutzrechte gewahrt werden.
Für den Fall eines Verkaufs von Darlehensforderungen trifft diese Verpflichtung den Käufer der Darlehensforderung als Empfänger der Informationen, soweit er diese erstmals für eigene Zwecke speichert. Die Zulässigkeit der Datenübermittlung gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG auf Seiten des Veräußerers wird von dieser Verpflichtung des Datenempfängers nicht berührt. Insbesondere ist die Zulässigkeit der Datenübermittlung durch den Verkäufer der Darlehensforderung nicht von der Erfüllung der Benachrichtigungspflicht durch den Käufer abhängig.
Erfolgt der Verkauf einer Darlehensforderung in das Ausland, hängt die datenschutzrechtliche Bewertung davon ab, ob es sich um eine Datenübermittlung in andere Mitgliedsstaaten der Europäischen Union oder andere Vertragsstaaten des Abkommens über den europäischen Wirtschaftsraum handelt oder um eine Übermittlung in andere Drittstaaten.
Im erst genannten Fall kann die Datenübermittlung gemäß § 4 b Abs. 1 BDSG ebenso wie eine Übermittlung innerhalb Deutschlands auf § 28 Abs. 1 Satz 1 Nr. 2 BDSG gestützt werden.
Besondere – über die gesetzlichen Vorschriften hinausgehende - Transparenzanforderungen sind ebenso wie bei einer Datenübermittlung im Inland nicht ersichtlich und auch nicht erforderlich, da auf Grund der gesetzlichen Regelungen ein angemessenes Datenschutzniveau hier vorausgesetzt werden kann.
Eine Datenübermittlung an Stellen außerhalb des in § 4 b Abs. 1 BDSG genannten Bereiches ist gemäß § 4 b Abs. 2 Satz 2 BDSG unzulässig, wenn der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Dies ist insbesondere dann der Fall, wenn bei den betreffenden Stellen im Ausland ein angemessenes Datenschutzniveau nicht gewährleistet ist. Nur in einem solchen Fall wären zur Wahrung der schutzwürdigen Interessen der Betroffenen ggf. weiter gehende Garantien zum Datenschutz notwendig. Nicht nachvollziehbar erscheint hingegen, warum derartige Zusatzanforderungen auch bei einer Datenübermittlung gemäß § 4 b Abs. 1 BDSG genannten Bereiches geboten sein sollte.

5.6.1 Wer hört mit? Aufzeichnungen von Telefongesprächen im Bankgeschäft

In seinen Ausführungen zu Aufzeichnungen von Telefongesprächen im Bankgeschäft weist das ULD auf die Strafvorschrift des § 201 Abs. 1 Nr. 1 StGB hin. Demnach macht sich strafbar, wer unbefugt das nicht öffentlich gesprochene Wort auf einen Tonträger aufnimmt. Bei Telefongesprächen im Bankgeschäft ist dieser Aspekt sowohl für die Aufzeich-

nung der Kundenäußerungen als auch für diejenigen der von der Bank angestellten Mitarbeiter relevant. Unstreitig ist, dass zur Vermeidung der Strafbarkeit einer Aufzeichnung von Gesprächen die Einwilligung der Betroffenen erforderlich ist.

Die Aufzeichnung von Telefongesprächen kann in der Praxis zum einen bei Einzelvertragsabschlüssen über das Telefon in Betracht kommen (Fernabsatzgeschäft). Häufig kommt sie aber auch im Rahmen von Servicevereinbarungen zum Einsatz, wenn die Kunden ggf. unter Einbindung von Sicherungsmedien (z.B. Geheimzahl, Kennwort) im Rahmen einer bestehenden Geschäftsbeziehung Einzelaufträge auch telefonisch abwickeln können. In diesen Fällen ist die ausdrückliche Einwilligung in die Telefonaufzeichnung regelmäßig schon Bestandteil der schriftlichen Vereinbarung mit dem Kunden. Die Aufzeichnung dient dabei nicht nur den Dokumentations- und Beweisinteressen des jeweiligen Unternehmens, sondern auch dem Schutz des Kunden, der ein Interesse daran hat, dass nachvollziehbar bleibt, wer in seinem Namen bestimmte Aufträge erteilt hat. Es trifft zu, dass ein Kunde, der eine solche Serviceleistung nutzen möchte, letztlich vor der Entscheidung steht, entweder der Aufzeichnung zukünftiger Telefonate zuzustimmen oder aber auf die Inanspruchnahme der angebotenen Dienstleistung zu verzichten. Hierbei ist aber zu berücksichtigten, dass sich die telefonische Kontaktaufnahme in der Regel als Zusatzdienstleistung darstellt, über deren Inanspruchnahme der Kunde frei entscheiden kann.

Zudem muss berücksichtigt werden, dass gerade im Finanzdienstleistungssektor für die jeweiligen Institute eine Vielzahl von zivil- und aufsichtsrechtlichen Vorgaben besteht, die die diese dazu zwingen, die Erledigung ihrer Pflichten gegenüber den Kunden nachvollziehbar zu dokumentieren. Wenn man den Kunden dabei die heute übliche Nutzung des Telefons ermöglichen möchte, gibt es zur Anfertigung von Tonbandaufnahmen praktischerweise kaum eine Alternative.

Das ULD weist darauf hin, dass die Erklärung einer Einwilligung in die Aufzeichnung eines Telefongespräches zwar nicht unbedingt schriftlich, jedoch *ausdrücklich* erfolgen müsse. Hierzu ist anzumerken, dass gemäß § 4 a Abs. 1 Satz 2 BDSG neben der schriftlichen Einwilligung auch eine „andere Form“ angemessen sein kann.
Diese Regelung enthält keine Einschränkung dahingehend, dass „angemessen“ immer nur eine ausdrückliche Einwilligung sein kann. Sowohl in der datenschutzrechtlichen Literatur (vgl. Schaffland/Wiltfang § 4 a BDSG, Rn. 4ff.) als auch in der Literatur zu § 201 StGB (vgl. Tröndle/Fischer, STGB, 54. Aufl. 2007, § 201 StGB Rn. 10) wird unter bestimmten Umständen auch eine konkludente Zustimmung für ausreichend erachtet. Allein aus Beweiszwecken und damit im eigenen Interesse wird ein Unternehmen aber in der Regel ohnehin eine dokumentierte Einwilligung des Kunden einholen. Überzogen erscheint demgegenüber die Forderung des ULD, dass ein bereits erteiltes Einverständnis zu Beginn des Mitschnitts nochmals ausdrücklich bestätigt werden sollte.

5.6.3 Datenschutz im Tank und
5.6.8 Der Wolf im Schafspelz

Die Bundesregierung hat am 14.03.2008 ihren Gesetzentwurf zur Bekämpfung unerlaubter Telefonwerbung vorgelegt.
Mit dem vorliegenden Gesetzentwurf soll es Verbrauchern ermöglicht werden, sich mittels Widerrufs von bestimmten, am Telefon geschlossenen Verträgen zu lösen. Darüber hinaus sollen Verstöße gegen das bestehende Verbot der unerlaubten Telefonwerbung künftig mit einem Bußgeld geahndet werden können. Schließlich soll die Rufnummernunterdrückung bei einem Werbeanruf verboten werden und Verstöße hiergegen sollen ebenfalls mit einem Bußgeld belegt werden können.

Die erforderlichen Änderungen sollen im Bürgerlichen Gesetzbuch (BGB), Gesetz gegen den unlauteren Wettbewerb (UWG) und Telekommunikationsgesetz (TKG) vorgenommen werden.
Als zuständige Behörde zur Verfolgung der zwei neuen Bußgeldregelungen ist die Bundesnetzagentur vorgesehen.
Darüber hinaus hat Baden-Württemberg einen Gesetzentwurf zur Stärkung des Kundenschutzes bei unlauterer Telefonwerbung in den Bundesrat eingebracht.
Der Entwurf nimmt eine Forderung der letzten Verbraucherschutzministerkonferenz auf. Nach dem Entwurf ist vorgesehen, dass Verträge, die durch eine unlautere Telefonwerbung abgeschlossen werden, zukünftig erst wirksam werden, wenn der Kunde das Vertragsangebot nochmals schriftlich bestätigt hat. Weiterhin soll der Unternehmer zukünftig die Beweislast dafür tragen, dass keine unzumutbare Belästigung vorgelegen hat.
Durch diese Gesetzentwürfe wird die Stellung der Verbraucher verstärkt. Es wird davon ausgegangen, dass hierdurch sog. „cold-calls“ zurückgehen werden.

6.3 NSI - Neue Steuerung

Ziel der NSI-Kommission als ressortübergreifendes Beratungsgremium ist die Unterstützung der Entwicklung und des Einsatzes von neuen Steuerungsinstrumenten (NSI) in der Landesverwaltung Schleswig-Holstein. Die erste Aufgabe der NSI-Kommission ist laut Kabinettsbeschluss vom 10. Juli 2007 die Bestandsaufnahme der Kosten- und Leistungsrechnung (KLR) in der Landesverwaltung Schleswig-Holstein. Es ist insbesondere geplant, den Einsatz der KLR auf der Basis der Ergebnisse der Bestandsaufnahme dahin gehend zu optimieren, dass die landesweite Standardisierung des Einsatzes der KLR differenziert nach den Anwendungsbereichen und Aufgaben in den Ressorts erfolgt, und zwar mit dem Ziel, einen wirtschaftlichen und effektiven Einsatz der Kosten- und Leistungsrechnung in der Landesverwaltung sicherzustellen. In das Konzept zur Bestandsaufnahme sind die Beratungen des ULD für den Datenschutz eingeflossen. Die NSI-Kommission hat zurzeit nicht die Aufgabe, ein Kennzahlen- und Indikatorensystem zu entwickeln.

6.4 SOA (Serviceorientierte Architekturen)

Der SOA-Ansatz wird bei der Umsetzung des haushaltskonformen ressortübergreifenden Inventarisierungs- und Bestandsführungsverfahren (Ham.s.t.er) berücksichtigt.
In der erreichten Realisierungsstufe 2 ist Ham.s.t.er eine Client-Serveranwendung, basierend auf Web-Services. Der einheitliche Ham.s.t.er-Client ist einziger Nutzer der angebotenen Services, die ausschließlich aus dem Landesnetz verfügbar und nicht öffentlich zugänglich sind. Für diese Web-Services ist WS-Security sehr konsequent umgesetzt, alle Nachrichten werden mit Ende-zu-Ende-Verschlüsselung verschickt und es wird eine Authentisierung nach WS-Security durchgeführt.
Zurzeit werden in Ham.s.t.er alle Daten zentral in einer Datenbank gehalten und die Zugriffsrechte der Nutzer werden in dieser Datenbank direkt modelliert. Sobald in den folgenden Realisierungsstufen die geplanten Schnittstellen zu anderen Anwendungen umgesetzt werden, wird für die zugreifenden Services in den entsprechenden Policies detailliert beschrieben, wer welche Zugriffsrechte auf welche Daten bekommt.

6.6 Sicherheitslücken im FHH-Netz: Auswirkungen auf Schleswig-Holstein

Die Schwachstellen wurden von Dataport erkannt. Die zukünftige Konzeption wurde von Dataport bereits kommuniziert. Das Finanzministerium begrüßt das geplante Vorgehen, da es sich an der Sicherheitsstruktur von Schleswig-Holstein orientiert. Bei zukünftigen Eigenentwicklungen wird deshalb auf Transparenz und frühzeitige Beteiligung des ULD geachtet.

6.8.1 Querschnittsprüfung “Landesnetz”

Das Finanzministerium würde es sehr begrüßen, wenn sich der kommunale Bereich noch mehr für den Landesnetzanschluss Typ 1 entscheiden könnte, da hier infolge der Standardisierung weniger Verwaltungsaufwand und Fehlerquellen vorhanden sind.

6.8.4 Universität Flensburg

Die Prüfung des ULD hat zu folgenden Beanstandungen geführt:

- Beanstandung der Dokumentationslage,
- Mängel in der technischen Konfiguration universitätsweit eingesetzter PC’s und Server sowie des Netzwerks
- die Hochschule verfügt über kein funktionierendes Datenschutzmanagementsystem,
- Intransparenz der Verfahren.

Die Universität und das ULD haben ein gemeinsamen Vorgehen vereinbart, in dem in Zusammenarbeit vor allem mit der Universität Lübeck landesweit geltende Standards für IT-Sicherheit und IT-Management an den Hochschulen erarbeitet werden sollen. Dem Bericht des ULD kann in diesem Punkt zugestimmt werden.
In mehreren Kontakten zwischen der Fachhochschule Lübeck, der Musikhochschule Lübeck und der Universität Flensburg ist vereinbart worden, das Sicherheitskonzept der Fachhochschule Kiel als Basis für ein abgestimmtes Konzept der Hochschulen in Schleswig-Holstein zu nutzen. Die Fachhochschule Lübeck organisiert zeitnah (Anfang Juni) ein Arbeitstreffen in Lübeck.
Die personelle Ausstattung der Universität Flensburg im IT-Bereich kann nur unter massiver Zuhilfenahme von studentischen Hilfskräften (bis hin zum Postmaster) das operative Geschäft gerade sicherstellen. Ein Abzug von Personal für die Entwicklung und Umsetzung eines Sicherheitskonzeptes würde das operative Geschäft erheblich beeinträchtigen. Die Universität Flensburg muss nach den Beratungen zwischen den Hochschulen des Landes nach einer Lösung suchen.

7.2 Datenschutzgestaltung von Webseiten

Das Finanzministerium als Betreiber des IT-Verfahrens Content Management System (CMS-II) und die Staatskanzlei als verantwortliche Stelle für den Internetauftritt des Landes arbeiten fortlaufend und mit beratender Unterstützung durch das ULD an der datenschutzgerechten Ausgestaltung von Technik und Organisation des IT-Verfahrens und des Internetangebots.

8.6 e-Region PLUS

Im Bereich IT-und Medienwirtschaft spielen datenschutzrechtliche Aspekte eine immer größere Rolle. Der frühe Kontakt zum ULD soll die Projektträger bei der Entwicklung ihrer Projekte unterstützen. Zum einen, da sich datenschutzrechtliche Belange bei der frühen Entwicklung besser einbinden lassen, zum anderen, um mögliche Wettbewerbsvorteile zu nutzen.
Speziell bei dem Projekt „Boatsecure“ hat sich hierdurch ein eindeutiger Wettbewerbsvorteil gegenüber vergleichbaren Produkten auf dem Markt entwickelt. Für das Projekt „SPITAL“ wurden durch den Kontakt zum ULD komplexere Sachverhalte für die Entwicklung des Projektes deutlich, die ansonsten nicht berücksichtigt worden wären und zu Nachteilen geführt hätten.

Ziffer 9.1.8: Christian-Albrechts-Universität
Die Christian-Albrechts-Universität zu Kiel hat in der zentralen EDV-Verwaltung eine wissenschaftliche Hilfskraft eingestellt. In Abstimmungen mit dem ULD ist zunächst die Erarbeitung einer Dienstanweisung zum Einsatz einer trouble-ticket-software für den Dienstleistungs-Support vorgesehen. Das Auditverfahren soll auch aus Sicht der CAU in 2008 abgeschlossen werden.
Dem Bericht des ULD kann daher zugestimmt werden.

10.4 Sicherheit bei Netzwerkgeräten
Die Vorschläge des ULD zur Netzwerksicherheit werden vom Finanzministerium befürwortet und unterstützt. Die derzeit zur Einführung der Internet-Protokoll-Telefonie (IP-Telefonie) ergriffenen Maßnahmen zur Qualitätssicherung und zur Erhöhung der Zugriffsicherheit in lokalen Netzen entsprechen im Wesentlichen diesen Vorschlägen. Im Rahmen eines laufenden Auditverfahrens befinden sich die notwendigen Maßnahmen zwischen dem Finanzministerium und dem ULD in Abstimmung.

Mit freundlichen Grüßen

gez. Lothar Hay