Schleswig-Holsteinischer Landtag
Umdruck 18/1469

Innenministerium
des Landes
Schleswig-Holstein

Staatssekretär

An die
Vorsitzende des
Innen- und Rechtsausschusses
des Schleswig-Holsteinischen Landtages
Frau Barbara Ostmeier, MdL
Landeshaus

24105 Kiel

29. Juli 2013

34. Tätigkeitsbericht des Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (Drs. 18/555)

Sehr geehrte Frau Vorsitzende,

zu den wesentlichen Punkten des Unabhängigen Landeszentrums für Datenschutz (ULD) in seinem 34. Tätigkeitsbericht gebe ich die nachfolgende Stellungnahme ab.

Die Stellungnahmen der Staatskanzlei (Ziffern 1.5 und 4.1.6), des Ministeriums für Justiz, Kultur und Europa (Ziffern 4.3.1 bis 4.3.8 und 4.3.10), des Ministeriums für Bildung und Wissenschaft (Ziffern 4.7.2, 4.7.3, 4.7.4 und 4.7.6), des Finanzministeriums (Ziffern 4.8.1, 4.8.2 und 12.4), des Ministeriums für Wirtschaft, Arbeit, Verkehr und Technologie (Ziffern 5.2 und 5.3) und des Ministeriums für Soziales, Gesundheit, Familie und Gleichstellung (Ziffern 4.6.3 und 4.6.6) wurden einbezogen.

1.5 Öffentliche Stellen und das Betreiben einer Facebook-Fanpage

Der Innen- und Rechtsausschuss hat sich in seiner Sitzung am 05.06.2013 darauf verständigt, dass zum Tätigkeitsbericht des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, Drucksache 18/555, von den Fraktionen Fragen formuliert werden sollen, die dem Innenministerium und dem ULD zur Berücksichtigung in deren Stellungnahmen zugeleitet werden sollen.
Die Fraktion BÜNDNIS 90/DIE GRÜNEN stellte zu Punkt 1.5 des Tätigkeitsberichts folgende Frage:
„Welche Konsequenzen ergeben sich aus der aktuellen Prism-Enthüllung durch die facebook-Nutzung durch die Staatskanzlei und weiteren Stellen der öffentlichen Verwaltung?“

Die Staatskanzlei hat auf die Frage der Fraktion BÜNDNIS 90/DIE GRÜNEN wie folgt Stellung genommen:

Postfach 71 25, 24171 Kiel | Telefon 0431 988-0 | Telefax 0431 988-2833 | Bernd.Kuepperbusch@im.landsh.de | www.landesregierung.schleswig-holstein.de

Außer der medialen Berichterstattung liegen der Landesregierung keine Erkenntnisse zu dem sog. NSA-Programm Prism vor.

Ministerpräsident Albig hat bereits im vergangenen Jahr gegenüber dem Datenschutzbeauftragten Dr. Thilo Weichert bekräftigt, dass die Landesregierung eine unmittelbare gesetzliche Verpflichtung, ihre Facebook-Fanseiten zu schließen, für das Land nicht sehe. Es sei das Unternehmen Facebook, das als Anbieter und Dienstleister den Datenschutz gewährleisten müsse.

Gleichwohl weist die Landesregierung sowohl auf ihrer Facebook-Fanseite als auch auf dem Landesportal schleswig-holstein.de deutlich darauf hin, dass Facebook Daten aufzeichnet und speichert.

Es ist auch Aufgabe von Politik, die Nutzer für den Umgang mit neuen Medien noch stärker zu sensibilisieren. Sie müssen lernen, verantwortungsvoll und kritisch mit den neuen Angeboten umzugehen.

Die Landesregierung wird ihren Facebook-Auftritt im Internet belassen.

4.1.6 KoPers - ein neues Personalmanagementsystem

Zu diesem Punkt teilt die Staatskanzlei mit, dass das Projekt KoPers im Tätigkeitsbericht überwiegend positiv dargestellt und u.a. als Beispiel für die in § 8 LDSG neu geschaffene Regelung genannt wird, nach der die Verantwortung für die Gewährleistung der Ordnungsmäßigkeit des automatisierten Verfahrens von der Verantwortung für die gespeicherten Daten abgetrennt und auf eine zentrale Stelle übertragen werden kann.

Der Hinweis des ULD, dass sich Einzelheiten zur Zusammenarbeit zwischen der zentralen und den beteiligten Stellen, zu den Verwaltungsabläufen bei Mängeln im Verfahren sowie zur Verantwortung für Personalentscheidungen gegenüber den Betroffenen in den nach der Landesverordnung für die Errichtung der zentralen Stelle vorgesehenen Nutzungsbestimmungen regeln lassen, zielt in die vom Projekt verfolgte Richtung. Das Beratungsangebot des ULD wird gern angenommen, das aktuell anlaufende Auditierungsverfahren ist hierfür beispielhaft.

Der mehrfache Hinweis bzw. die Empfehlung des ULD, aus seiner Sicht könne nur eine qualifizierte elektronische Signatur den Anforderungen an eine ausschließlich elektronisch geführte Personalakte angemessen genügen, kann auch als Forderung interpretiert werden. Hier wird in Zukunft noch zu klären sein, ob diese Forderung angesichts der damit verbundenen Kosten tatsächlich angemessen ist. Gespräche zwischen dem Projekt und ZIT laufen (ab 1.4.2013 hausintern).

4.2.1 @rtus beschäftigt die Polizei - und das ULD

Das polizeiliche Vorgangsbearbeitungssystem @rtus VBS wird kontinuierlich weiterentwickelt. Dieser Prozess wird vom ULD konstruktiv begleitet. Schwerpunkt der aktuellen Entwicklung ist die Nutzung als Lage- und Auswerteinstrument. Die fachliche Bewertung der Landespolizei führte innerhalb gesetzlicher Grenzen zu einer Verlängerung der Speicherfristen. Dem ULD wurde eine ergebnisoffene Evaluierung der verlängerten Fristen zuge-

sagt. Voraussetzung hierfür ist, dass die Verlängerung der Speicherfristen eine spürbare Auswirkung auf den Datenbestand bewirkt hat, um entsprechende Beispiele für die Erforderlichkeit gewinnen zu können. Die Evaluierung wird zum 31.12.2013 beendet.

4.2.2 Sicherheitsüberprüfungen

Das ULD führt in seinem Tätigkeitsbericht aus, dass die Landespolizei im Zusammenhang mit Großveranstaltungen Sicherheitsüberprüfungen ohne Rechtsgrundlage vornehme. Diese Darstellung ist falsch.

1. Zur Vorbereitung der Ministerpräsidentenkonferenz wurden Abstimmungsgespräche durch die Staatskanzlei, mit dem LKA, dem IM und dem ULD geführt.
   Die polizeiliche Gefahrenprognose für die Ministerpräsidentenkonferenz kam zu dem Ergebnis, dass eine polizeiliche Begleitung der Veranstaltung durch einen ständigen Objektschutz und durch eine polizeiliche Zugangskontrolle notwendig ist. Aufgrund dieser Bewertung ist das Polizeirecht anzuwenden. Dieses ermöglicht eine Identitätsfeststellung und Überprüfung von Personen, die sich an/in dem gefährdeten Objekt aufhalten. Eine Überprüfung aller relevanten Person vor Beginn der Veranstaltungen vor Ort wäre mit extremen Wartezeiten verbunden. Aus diesem Grunde wurden alle überprüfungsnotwendigen Personen, die sich erkennbar an den Veranstaltungstagen im gefährdeten Objekt aufhalten werden, im Vorweg überprüft. Mittels umfangreicher Merkblätter wurde den Betroffenen das Verfahren erläutert. Das ULD vertritt die Auffassung, dass Überprüfungen nicht im Vorwege vorgenommen werden können, weil dafür keine Rechtsgrundlage bestehe.
2. Zur Rechtsbewertung des ULD, dass eine Sicherheitsüberprüfung aufgrund einer Einwilligung nicht zulässig sei, wird auf die Stellungnahme zum 30. TB zu 4.2.3 (Umdruck 16/3362) verwiesen.

4.2.5 Umgang mit Auskunftssperren im Melderegister in Strafverfahren

Aufgrund einer Eingabe beim ULD wurde in Zusammenarbeit mit den Datenschutzbeauftragten der Landespolizei eine datenschutzrechtliche Kontrolle vorgenommen. Die vom Petenten des ULD vorgebrachte Vermutung bestätigte sich. Eine im Einwohnermelderegister vermerkte Auskunftssperre war nicht in den polizeilichen Vorgang übernommen worden. Dieses Versäumnis wurde umgehend behoben. Die Datenschutzbeauftragten der Landespolizei sorgten anhand des Beispiels für eine Sensibilisierung der Mitarbeiter der Landespolizei.

4.3.1 Der Staatstrojaner ohne rechtliche Grundlage

Bei der Quellen-TKÜ handelt es sich grundsätzlich um eine richterlich angeordnete Maßnahme auf Grundlage der §§ 100a, 100b der Strafprozessordnung (StPO). Danach ist – entsprechend den Vorgaben des Bundesverfassungsgerichts in seiner Entscheidung aus dem Jahre 2008 – allein die Überwachung und Aufzeichnung der bestehenden Telefonverbindung zulässig. Die Grenzen werden durch den richterlichen Beschluss vorgegeben. Ein darüber hinausgehender Zugriff auf die auf dem Rechner gespeicherten Inhalte im Sinne einer Online-Durchsuchung ist nicht zulässig.

Das MJKE teilt mit, dass die Quellen-TKÜ in Schleswig-Holstein bisher in wenigen Einzelfällen durch die Staatsanwaltschaft beantragt und durch richterlichen Beschluss nach §§ 100a, 100b StPO angeordnet worden ist. Es handelt sich keineswegs um eine Ermittlungsmaßnahme, die regelmäßig in zahlreichen Ermittlungsverfahren genutzt wird. Zum einen sind ihr rechtliche Grenzen gesetzt, da sie nur zulässig ist, wenn die engen Voraussetzungen des § 100a StPO vorliegen, zum anderen ist zu berücksichtigen, dass die Quellen-TKÜ durch das Bereithalten der erforderlichen Technik und Software eine sehr kostenintensive Ermittlungsmaßnahme darstellt.
Mit Blick auf die teilweise in der rechtswissenschaftlichen Literatur vertretene Auffassung, die Quellen-TKÜ könne nicht auf § 100a StPO gestützt werden und sei damit nicht zulässig, erscheint eine ausdrückliche gesetzliche Regelung der Quellen-TKÜ für Zwecke der Strafverfolgung zwar nicht notwendig, jedoch denkbar.

4.3.2 Anordnung von Blutproben - Richtervorbehalt stärken statt abschaffen

Die Erforderlichkeit des in § 81a Absatz 2 StPO normierten Richtervorbehalts ist seit Jahren Gegenstand intensiv geführter Erörterungen. Ein bereits am 5. November 2010 durch den Bundesrat eingebrachter Gesetzentwurf des Landes Niedersachsen (BR-Drs. 615/10) sieht vor, für Verkehrsstraftaten und Verkehrsordnungswidrigkeiten von dem grundsätzlichen Erfordernis einer richterlichen Anordnung der Blutentnahme zum Zwecke des Nachweises von Alkohol, Betäubungsmitteln oder Medikamenten im Blut in § 81a Absatz 2 StPO abzusehen und der Staatsanwaltschaft und ihren Ermittlungspersonen (Polizei) eine eigene gleichrangige Anordnungskompetenz einzuräumen. Die Beratungen in den parlamentarischen Gremien des Bundestages dauern an.

Für die Streichung des Richtervorbehalts in § 81a Absatz 2 StPO sprechen insbesondere folgende Gründe:

In den Fällen des § 81a Absatz 2 StPO ist eine eigenständige richterliche Prüfung des Sachverhalts regelmäßig nicht möglich. Nach Messung der Atemalkoholkonzentration oder bei Wahrnehmung deutlicher Ausfallerscheinungen durch die Polizei liegen regelmäßig bereits alle zureichenden tatsächlichen Anhaltspunkte vor, die den Verdacht einer Verkehrsstraftat begründen, zu dessen Überprüfung die Bestimmung der Blutbestandteile erforderlich ist. Der Richter wird in diesen Fällen die polizeiliche Entscheidung einer Blutprobenentnahme zur Bestimmung der Blutalkoholkonzentration nur bestätigen können. Das Instrument des Richtervorbehalts wird damit im Bereich des § 81a Absatz 2 StPO zu einer bloßen Formalie abgewertet.

4.3.3 MESTA - erste Fortschritte

Das staatsanwaltliche Informationssystem MESTA protokolliert jede Änderung der gespeicherten Daten. Nicht protokolliert wird bisher die reine MESTA-Datenabfrage für Auskunftszwecke. In der Erstellungsphase von MESTA Mitte der 90er-Jahre erschien eine derartige Lösung aus rein technischer Sicht nur mit unverhältnismäßig hohem Aufwand realisierbar zu sein. In Abstimmung mit dem für die - damaligen - Partnerländer beteiligten Landesdatenschutzbeauftragten von Hamburg wurde auch im Hinblick auf eine beschränkte Aussagekraft auf die Vollprotokollierung verzichtet. Nach fortgeschrittenem informationstechnischen Entwicklungsstand, wurde diese Entscheidung in den vergangenen Jahren wiederholt überprüft. Zuletzt wurden im Dezember 2012 Belastungstests bei einer

Staatsanwaltschaft durchgeführt. Ergebnis war, dass bei dem gegenwärtigen (und für die nahe Zukunft zu erwartenden) Ausstattungsstand eine Vollprotokollierung bei Aufrechterhaltung des Dienstbetriebs nicht möglich sein wird. Zeitgleich wurde Dataport mit dem Ergebnis konfrontiert und um eine Bewertung und ggf. um Lösungsvorschläge gebeten. Das weitere Vorgehen wird kurzfristig mit Dataport abgestimmt.

4.3.4 Sicherstellung von Datenträgern im Strafverfahren

Zur Sicherstellung von Datenträgern im Strafverfahren hat das MJKE folgende Angaben gemacht:
Die Sicherstellung und Beschlagnahme von Datenträgern ist zum Zwecke der Beweisführung in zahlreichen Ermittlungsverfahren erforderlich. Exemplarisch sind hier etwa Verfahren wegen Kinderpornografie oder Verfahren im Bereich der Wirtschaftskriminalität zu nennen.
Die Durchsuchung und Beschlagnahme von Datenträgern wird regelmäßig richterlich angeordnet. Bei Gefahr im Verzug erfolgt die Durchsuchung auf Anordnung der Staatsanwaltschaft und ihrer Ermittlungspersonen. Hier ist entsprechend § 98 Absatz 2 Satz 2 StPO der Antrag auf gerichtliche Entscheidung zulässig.
Die Auswertung der beschlagnahmten Datenträger ist äußerst zeitaufwendig und nimmt regelmäßig mehrere Monate, manchmal auch Jahre in Anspruch. Die Spiegelung der Daten ermöglicht eine frühzeitige Herausgabe des Rechners samt der auf dem Rechner befindlichen Originaldaten an den Beschuldigten. Eine vorherige Auswertung der Daten (vor Spiegelung) und Auswahl der zu spiegelnden Daten ist wegen hohen Zeitaufwands und knappen Personalressourcen nicht möglich.
Fälle, in denen Daten der Betroffenen durch die Ermittlungsbehörden rechtswidrig verwendet oder sonst missbraucht worden wären, sind nicht bekannt.

4.3.5 Therapieunterbringungsvollzugsgesetz

Das Therapieunterbringungsgesetz wurde durch die Landtagsfraktionen der CDU und der FDP in den Landtag eingebracht. Aufgrund eines laufenden gerichtlichen Verfahrens vor dem Schleswig-Holsteinischen Oberlandesgericht über die Frage einer Unterbringung nach dem Therapieunterbringungsgesetz des Bundes (ThUG) bestand Eilbedürftigkeit. Inhaltlich richten sich die Regelungen zum Akteneinsichtsrecht an dem bestehenden Maßregelvollzugsgesetz des Landes aus.

Die jetzige Regierungskoalition hat im Koalitionsvertrag die Überarbeitung des Therapieunterbringungsgesetzes angekündigt (Zeile 2317). Insbesondere durch den Staatsvertrag mit der Freien und Hansestadt Hamburg zur gemeinsamen Unterbringung ist eine Novellierung notwendig. Das ULD wird im Rahmen des Gesetzgebungsverfahrens beteiligt werden.

4.3.6 Sicherungsverwahrungsvollzugsgesetz

Das MJKE berichtet hierzu, dass der Text im 34. Tätigkeitsbericht noch den Stand vor der zweiten Kabinettsbefassung und inhaltlich damit den Stand der Stellungnahme des ULD im Anhörungsverfahren wiedergibt. Die Kritik des ULD ist nahezu vollständig in den Regierungsentwurf eingearbeitet worden, so dass die konkret benannten Kritikpunkte keine

Grundlage mehr haben. Es verbleiben aus Sicht des ULD einzig Bedenken bzgl. der Ermächtigung zum Auslesen von Datenspeichern (§ 118 SVVollzG-E), soweit diese die Verarbeitung von Daten erlaubt, die zum Kernbereich der privaten Lebensgestaltung des Untergebrachten gehören. Die Bedenken richten sich einerseits dagegen, dass der „Kernbereich privater Lebensgestaltung“ nach der Rechtsprechung des BVerfG einem absoluten Schutz vor hoheitlichen Eingriffen unterliegt, andererseits sei fraglich, ob die infrage kommenden Daten überhaupt dem Kernbereich privater Lebensgestaltung unterlägen oder wegen ihres Sozialbezuges zwar dem Schutz der privaten Lebensgestaltung unterliegen, aber außerhalb des Kernbereichs zu verorten sind. Das ULD hat hierzu eine Stellungnahme an den Innen- und Rechtsausschuss abgegeben, der jedoch an dieser Stelle keine Änderung des – am 01. Juni 2013 in Kraft getretenen – Gesetzes beschlossen hat.

4.3.7 Einführung eines bundesweiten Vollstreckungsportals

Seit dem 01. Januar 2013 sind die bislang bei den Amtsgerichten geführten Schuldnerverzeichnisse über ein zentrales Schuldnerportal bundesweit über das Internet abrufbar.

Die Suche ist gemäß § 8 Schuldnerverzeichnisführungsverordnung (SchuFV) jetzt so geregelt, dass die Übermittlung von Daten an den Nutzer erfolgt, wenn dieser mindestens folgende Suchkriterien angibt:

1. Den Namen und Vornamen des Schuldners oder die Firma des Schuldners und
2. den Sitz des zuständigen zentralen Vollstreckungsgerichts oder den Wohnsitz oder das Geburtsdatum des Schuldners oder den Ort, an dem der Schuldner seinen Sitz hat.

Vorbehaltlich der folgenden zwei Absätze wird nicht mehr als ein Datensatz übermittelt. Der Datensatz enthält die in § 882b Absatz 2 und 3 der Zivilprozessordnung angegebenen personenbezogenen Daten des Schuldners.

Sind zu einer Abfrage gemäß Absatz 2 mehrere Datensätze vorhanden, hat der Nutzer zusätzlich das Geburtsdatum des Schuldners einzugeben. Ergibt auch diese Abfrage mehrere Treffer, hat der Nutzer außerdem zu der Angabe gemäß Satz 1 den Geburtsort des Schuldners einzugeben; sind dann weiterhin mehrere Treffer vorhanden, sind diese zu übermitteln.

Kann der Nutzer abweichend von der Abfrage gemäß den Absätzen 2 und 3 Familiennamen, Vornamen, Geburtsdatum und Geburtsort des Schuldners sofort angeben, werden ihm sämtliche zu einem Schuldner vorhandene Datensätze übermittelt. Das Gleiche gilt, wenn der Schuldner keine natürliche Person ist und bei der Abfrage Name oder Firma und Sitz des Schuldners angegeben werden.

Die Bund-Länder-Kommission AG-Vollstreckungsportal hatte ursprünglich gefordert, dass für eine eindeutige Suche zwingend der Name, Vorname und das Geburtsdatum des Schuldners anzugeben sind. Davon war der Verordnungsgeber in seinem Entwurf, wie vom ULD beschrieben, abgewichen. Das Ergebnis nach einer entsprechenden Intervention durch das ULD ist die oben beschriebene Suche.

Derzeit ist es so, dass ein Schuldner nur dann im SV gefunden werden kann, wenn der Suchende exakt so sucht, wie der Schuldner im SV eingetragen ist. Auch dies war eine Vorgabe vom ULD.

In Bezug auf die Registrierung ist der Forderung des ULD, dass die Registrierung allein über den elektronischen Identitätsnachweis des neuen Personalausweises erfolgen soll, nicht nachgekommen worden.

Momentan muss sich der Nutzer online unter www.Vollstreckungsportal.de mit Name, Anschrift und E-Mail-Adresse anmelden und bekommt dann seine Zugangsdaten per Post nach Hause geschickt. Ein Identitätsnachweis findet folglich dadurch statt, dass die Post mit den Zugangsdaten auch nur denjenigen erreicht, der bei der Anmeldung die richtigen Daten angegeben hat.

Der Einsatz des E-Personalausweises wird alternativ zur o.g. Variante voraussichtlich ab Oktober 2013 möglich sein.

Grundsätzlich dürfen die Sicherheitsvorkehrungen nicht so weit gehen, dass eine vernünftige Suche im SV nicht mehr möglich ist. Damit würde dann der Sinn und Zweck dieser Reform - nämlich eine größere Sicherheit im Bereich des Zahlungsverkehrs in der Wirtschaft zu erreichen - verfehlt werden.

4.3.8 Dokumentation von Grundbucheinsicht

In Schleswig-Holstein stehen 99% der Grundbuchblätter in elektronischer Form zur Verfügung, das restliche 1% in Papierform. Für die Blätter in Papierform gilt der vom ULD zitierte Erlass, wonach Grundbucheinsichten auf einem Formular zu dokumentieren sind. Für elektronische Grundbuchblätter wurde dieser Erlass aufgehoben. Er war insoweit überflüssig, als dass Grundbucheinsichten in elektronischer Form mit Hilfe der technischen Möglichkeiten des automatisierten Abrufverfahrens erfolgen. In eben diesem Verfahren erfolgt eine automatische Protokollierung der Einsicht.

Für eine vollständige Protokollierung aller Einsichten ist die korrekte Handhabung erforderlich. Die Einsichtsprotokolle werden regelmäßig auf ihre Vollständigkeit hin überprüft. Auf fehlerhafte Protokollierungen werden die Grundbuchämter hingewiesen und angehalten, ihre Mitarbeiter entsprechend anzuweisen. Darüber hinaus werden regelmäßig Schulungen angeboten.

Die technischen und organisatorischen Möglichkeiten für eine vollständige Protokollierung sind folglich gegeben. Denkbar ist angesichts des geschilderten Falls, dass einigen Grundbuchamtsmitarbeitern u. U. die rechtliche Lage nicht präsent und somit nicht klar ist, dass auch mündliche Auskünfte zu erfassen sind und nicht nur diejenigen Auskünfte, bei denen die Auskunftssuchenden direkte Einsicht in das Grundbuchblatt erhalten. Hier könnten entsprechende Hinweise seitens der jeweiligen Behördenleitung die Lösung sein.

4.3.10 Protokollierung (auch) der lesenden Zugriffe im Justizvollzug

Das MJKE hatte bereits, unmittelbar nach Bekanntwerden des ersten benannten Falls, eine Verschärfung der organisatorischen Maßnahmen zum Datenschutz veranlasst. Demnach hat vor der Vergabe von Zugriffsberechtigungen auf personenbezogene Daten nunmehr eine Mitprüfung durch die behördlichen Datenschutzbeauftragten zu erfolgen.

Festgehalten werden muss zudem, dass die dem Wissenschaftler im ersten Fall eingeräumte Zugriffsberechtigung umfangreichen Einschränkungen unterlag. Im zweiten Fall konnten die Mitarbeiter, die eine unzulässige Verarbeitung personenbezogener Daten vorgenommen haben, ermittelt werden. Angemessene personalrechtliche Maßnahmen wurden durch die Dienststelle veranlasst.
In beiden Fällen ist der Darstellung des ULD dahingehend entgegenzutreten, dass durchaus bekannt war bzw. wurde, durch wen eine Datenverarbeitung stattgefunden hat.

Unabhängig hiervon, wurden die Anforderungen des ULD mit Blick auf § 5 Abs. 1 Ziffer 4 LDSG SH durch das Ministerium für Justiz, Kultur und Europa aufgegriffen. Im Rahmen der aktuellen Prüfungen erfolgt eine enge Abstimmung mit dem ULD.

4.6.3 Nationales Krebsregister und
4.6.4 Klinisches Krebsregister Schleswig-Holstein

Mit dem Krebsfrüherkennungs- und -registergesetz (KFRG) werden alle Länder verpflichtet, flächendeckende klinische Krebsregister aufzubauen. Schleswig-Holstein plant, das bestehende epidemiologische Krebsregister zu einem klinisch-epidemiologischen Krebsregister auszubauen.

Derzeitiger Sachstand: Beim bestehenden epidemiologischen Krebsregister gibt es eine Meldepflicht für alle Krebserkrankungen von Patienten aus Schleswig-Holstein. Die Registrierung klinischer Daten durch den Verein Klinisches Krebsregister Schleswig-Holstein e.V. (KKR - SH) erfolgt mit Einwilligung der betroffenen Personen.

Es ist beabsichtigt, für alle Meldungen (epidemiologische und klinische) eine gesetzlich geregelte Meldepflicht einzuführen. Damit soll eine Vollzähligkeit der Meldungen erreicht werden, die für belastbare Aussagen erforderlich ist. Außerdem erleichtert ein einheitliches Verfahren den Ärztinnen und Ärzten die Meldungen der Daten an die Vertrauensstelle.

4.6.6 Patientenarmbänder – Sicherheit auf Kosten des Patientengeheimnisses?

Patientenarmbänder sind – auch aus Sicht des Ministeriums für Soziales, Gesundheit, Familie und Gleichstellung – sehr empfehlenswert, weil sie letztlich der Patientensicherheit dienen.

Durch einen Vergleich der Patientenakte mit dem Armband ist es für Ärzte und Pflegepersonal einfacher, die Patienten schnell zu identifizieren, was unter anderem auch bei desorientierten und narkotisierten Patienten besonders wichtig ist.

Die Krankenhäuser betonen, dass es aus Datenschutzsicht keine Probleme gibt, auch weil alle Daten verschlüsselt seien.

Letztlich ist es aber Angelegenheit der Krankenhäuser selbst, die Modalitäten hinsichtlich der Armbänder zu regeln. Das Land besitzt keine Rechtsaufsichtsfunktion, aus der sich eine Erteilung von Auflagen ableiten ließe.

4.7.2 LanBSH mausert sich zur „Allzweckwaffe“ für mehr Effizienz und
4.7.3 Neue Möglichkeiten des EDV-Einsatzes in der Schule - neue Fragen

Die vom ULD geforderten Vorgaben betreffen Punkte, die bei der anstehenden Novelle der Datenschutzverordnung Schule (SchulDSVO) vom MBW berücksichtigt werden.

4.7.4 Handreichung für die Schulsozialarbeit

Der Bericht verweist in Kapitel 4.7.4 „Handreichung für die Schulsozialarbeit“ darauf, dass sich die gemeinsam mit dem Sozialministerium erarbeitete und 2011 veröffentlichte Broschüre „als sinnvolle Hilfe bei der täglichen Arbeit“ bewährt und zu „zahlreichen positiven Rückmeldungen“ geführt habe. Diese Aussage kann vom Fachreferat bestätigt werden: Die Handreichung wird in Schleswig-Holstein sowohl von Schulen als auch von Schulsozialarbeitern und deren Anstellungsträgern nachgefragt und ebenso von einschlägig Interessierten außerhalb des Landes.

Nicht bekannt sind dem MBW die an der Stelle ebenfalls erwähnten fortbestehenden „Unsicherheiten hinsichtlich der Zusammenarbeit zwischen Schule und Sozialarbeit“, die u.U. auf das „Fehlen hinreichend präziser Rechtsvorschriften“ zurückzuführen seien.
Wie das ULD selbst darlegt, sind in der gemeinsam entwickelten Broschüre die verschiedenen datenschutzrechtlichen Belange umfassend aufgearbeitet, so dass das ULD gebeten werden könnte, konkret zu erläutern, welche „eindeutigen Regelungen“ darüber hinaus erforderlich und ggf. in der SchulDSVO zu verankern seien. Diese können dann bei der anstehenden Novelle der SchulDSVO vom MBW berücksichtigt werden.

4.7.6 Tausche Fingerabdruck gegen Schulmittagessen

Dieses Kapitel regt insbesondere an, dass „Schulen, die die Einführung eines auf Fingerabdrücken basierenden Essenausgabesystems für ihre Mensen planen“, im Vorwege „prüfen“ sollen, „ob das System den Datenschutzanforderungen genügt“.
Hier wird seitens des MBW darauf verwiesen, dass über die Einführung und Gestaltung einer Mittagsverpflegung grundsätzlich die Schulträger im Rahmen ihrer Selbstverwaltungsaufgaben entscheiden.

4.8.1 Die Steuerverwaltung ohne Auskunftsanspruch

Die Ansicht des ULD, das einen Anspruch auf Akteneinsicht und Auskunftserteilung in einem laufenden Besteuerungsverfahren aus dem Informationszugangsgesetz SH (IZG SH) und dem LDSG SH ableitet, wird vom Finanzministerium nicht geteilt. Das vom ULD zitierte Urteil des OVG Schleswig vom 6.12.2012 bezieht sich auf die Gewährung um Akteneinsicht in einem abgeschlossenen Besteuerungsverfahren. Über die Frage, wie sich der allgemeine Informationszugangsanspruch des § 3 IZG SH zu dem Akteneinsichtsrecht eines Beteiligten währen eines laufenden Verwaltungsverfahrens [in Steuersachen] verhält, wurde ausdrücklich nicht entschieden.

Ein Auskunftsrecht im laufenden Besteuerungsverfahren kann entgegen der Auffassung des ULD nicht aus § 3 IZG SH bzw. § 27 LDSG SH abgeleitet werden. Zwar ist nach der Entscheidung des BVerfG vom 10.3.2008 fraglich, inwieweit der in der Abgabenordnung

(AO) bestehende Rechtsgrundsatz des absichtsvollen Regelungsverzichts weiterhin Gültigkeit entfaltet. Die obersten Finanzbehörden des Bundes und der Länder sehen die Notwendigkeit einer bundeseinheitlichen gesetzlichen Regelung für die Finanzverwaltung, die den weiteren landesrechtlichen Bestimmungen über ein Auskunftsrecht vorgeht. Sie haben inzwischen Eckwerte einer gesetzlichen Regelung eines den Anforderungen des BVerfG genügenden Auskunftsrechts in der AO entwickelt. Der Entwurf lehnt sich weitgehend an die Struktur des § 19 BDSG an, wobei an geeigneter Stelle jeweils besondere Belange des bereichsspezifischen Datenschutzes in der Finanzverwaltung zum Ausdruck kommen. Mit einem Inkrafttreten dieser Gesetzesänderung ist nicht vor 2014 zu rechnen.
Mit dem BMF-Schreiben vom 17.12.2008 – BStBl. Teil I, 9 – wurde im Vorgriff auf eine gesetzliche Regelung eine Verwaltungsanweisung geschaffen, die die Eckwerte der Entscheidung des BVerfG vom 10.3.2008 berücksichtigt. Eine Ermessensentscheidung über die Auskunftserteilung dem Grunde nach ist hierin nicht ersichtlich; dies gilt neben den Fällen des Ausschlusskatalogs der Nr. 7 auch bei fehlendem berechtigten Interesse gemäß Nr. 1 bis 3.
Die obersten Finanzbehörden des Bundes und der Länder beurteilen die Reichweite des BMF-Schreibens vom 17.12.2008 dahingehend, dass landesrechtliche Regelungen über einen Auskunftsanspruch im laufenden Besteuerungsverfahren unbeachtlich bleiben. Dies ergibt sich aus dem Grundsatz der Rechtseinheit im Verwaltungsverfahren in Steuersachen. Denn der Gesetzgeber hat mit Art. 108 GG die Notwendigkeit eines gesonderten Regelungsbedarfs der Kompetenzen im Bereich der Bundesauftragsverwaltung über die generellen Bestimmungen der Art. 84 und 85 GG hinaus zum Ausdruck gebracht.

4.8.2 Zusendung falscher Steuerunterlagen

Wie durch das Finanzministerium bereits zu vergleichbaren Feststellungen des ULD im 31. und 32. Tätigkeitsbericht ausgeführt, ist es im Veranlagungsverfahren als sog. Massenverfahren nicht ausgeschlossen, dass bei der Versendung von Steuerunterlagen durch mechanische Versehen oder ähnliche Flüchtigkeiten die beschriebenen Fehler eintreten. Die vom ULD nunmehr zitierten vier Einzelfälle in verschiedenen Finanzämtern bilden nach wie vor einen außergewöhnlich geringen Anteil an der Zahl der Steuerfälle mit Belegversand.
Die Bediensteten der Finanzämter werden regelmäßig auf die umfassende Wahrung des Steuergeheimnisses hingewiesen (Nr. 2 der Veranlagungsgrundsätze des FM), dies umfasst auch den sorgfältigen Umgang mit Dokumenten. Darüber hinaus wird in den Erläuterungen zu Nr. 3.4.4 der Geschäftsordnung für die Finanzämter (FAGO) auf den hohen Grad an Sorgfalt bei Versendung von Schriftstücken im Telefax-Verkehr hingewiesen.

5.2 Geldkarten mit Funkchips

Der Bericht des ULD stellt in Kapitel 5.2 „Geldkarten mit Funkchips“ seine Kritikpunkte an der neuen kontaktlosen Schnittstelle der Geldkarte dar, die im Folgenden vom MWVAT kommentiert werden.

Der Begriff "Geldkarten mit Funkchips" ist nicht hinreichend aussagekräftig gewählt. Aus diesem Grund erfolgt zunächst eine kurze Beschreibung des neuen Produkts kontaktlose Geldkarte bzw. „girogo“. Die Geldkarte hat keinen neuen Funkchip erhalten, sondern hat nach wie vor nur einen Chip, der nun auf zwei Arten angesprochen werden kann. Neu hinzugekommen ist, dass neben dem kontakthaften Zugriff auch ein kontaktloser Zugriff ge-

mäß der ISO Norm 14443 erlaubt wird. Die Norm sieht vor, dass bis zu einer Entfernung von 10 cm Daten über ein elektromagnetisches Feld zwischen Terminal und Karte ausgetauscht werden können. Handelsübliche Terminals ermöglichen kontaktlose Transaktionen nur über wenige Zentimeter (3 - 4 cm). Inhaltlich hat sich an der Geldkarte-Anwendung in der Chipkarte sonst nichts geändert.

Historie:
Die Deutsche Kreditwirtschaft (DK) befindet sich seit Anfang 2012 im regen Austausch mit den Datenschützern zum Thema „girogo“ (kontaktlose Geldkarte). In diesem Zusammenhang fanden neben einer technischen Präsentation im Arbeitskreis Technik der Datenschützer am 29.02.2012 auch mehrere Sitzungen mit dem Düsseldorfer Kreis (Düsseldorfer Kreis = informelle Vereinigung der obersten Aufsichtsbehörden, die in Deutschland die Einhaltung des Datenschutzes im nicht-öffentlichen Bereich überwachen) statt. Außerdem wurden Informationstermine mit mindestens drei Landesdatenschützern, u. a. auch mit Herrn Dr. Thilo Weichert, durchgeführt. In einer Pilotregion im Raum Hannover, Braunschweig und Wolfsburg wird seit Mitte April 2012 ein Pilotprojekt zum kontaktlosen Bezahlen durchgeführt. Die DK hat den Datenschützern sehr früh mitgeteilt, dass auf freiwilliger Basis pilotbegleitend ein sogenanntes Privacy Impact Assessment (PIA) erstellt wird und nach Abschluss des Piloten den Datenschützern übermittelt wird. Das Datenschutzmerkblatt, das vom Deutschen Sparkassen- und Giroverband (DSGV) erstellt wurde, ist dem Düsseldorfer Kreis und somit auch Herrn Dr. Weichert bereits im September letzten Jahres zur Verfügung gestellt worden. Der Düsseldorfer Kreis hat in seinem Beschluss zur NFC-Technik vom 18./19. September 2012 insbesondere deutlich zum Ausdruck gebracht, dass etwaigen datenschutzrechtlichen Bedenken durch eine Wahlmöglichkeit des Kunden zur Deaktivierung der Kontaktlosfunktion Rechnung getragen werden kann. Diese Anregungen aus dem Düsseldorfer Kreis sind aufgenommen worden.

Die DK hat auch in den Gesprächen mit den Datenschützern darauf hingewiesen, dass mit „girogo“ ein kontaktloses Verfahren pilotiert wird, dass datenschutzrechtlich besser abgesichert ist als kontaktlose Systeme, die sich bereits seit mehreren Jahren im Markt befinden. Somit war die Kreditwirtschaft überrascht bezüglich der ersten Reaktionen auf „girogo“, da keine Beanstandungen zu diesen Systemen bekannt geworden seien. Anscheinend sind diese Systeme, bei denen es sich nicht nur um kontaktlose Bezahlverfahren handelt, bisher bei den Datenschützern unbemerkt geblieben und tauchen auch im letzten Bericht von Herrn Dr. Weichert noch nicht auf.

Erster Kritikpunkt des ULD:
Im ersten Spiegelpunkt sind die gespeicherten Transaktionsdaten der letzten drei Ladetransaktionen und der letzten 15 Bezahltransaktionen angesprochen. Diese Daten dienen der Information des Kunden und müssen zur Kontrolle der korrekten Abwicklung der Transaktionen in der Karte protokolliert werden. Die Protokollierung erfolgt durch die Karte. Der Kunde kann mit einem zusätzlichen kleinen Gerät, einem sogenannten Taschenkartenleser, prüfen, ob die letzte(n) Transaktion(en) korrekt durchgeführt wurde(n). Um die Prüfung zu erleichtern und auch ohne zusätzliches Gerät für den Kunden zu ermöglichen, ist der kontaktlose Zugriff erlaubt worden. Damit lassen sich die Transaktionsdaten mit einem Smartphone mit NFC-Funktionalität auslesen, so dass kein zusätzlicher Taschenkartenleser benötigt wird.

In dem Bericht wird kritisiert, dass die Übermittlung dieser Daten ohne Einsatz von Kryptographie oder Passwörtern erfolgt. Aus Sicherheitsgründen werden keine Passwörter über die kontaktlose Schnittstelle übertragen, da ein Ausspähen möglich ist. Dies ist auch inter-

national akzeptierte und geübte Praxis. Die Verwendung von kryptographischen Schlüsseln setzt den Schutz dieses Schlüssels auf beiden Seiten, also der Chipkarte und dem lesenden Kundendevice, z. B. dem Taschenkartenleser oder dem Smartphone, voraus. In der Chipkarte kann man den Schlüssel ausreichend schützen. Eine ausreichende Hardwaresicherheit ist in einem Smartphone aber nicht möglich und selbst in einem separaten Device nicht wirtschaftlich umsetzbar.

Zu den gespeicherten Daten gehören nicht die gekauften Produkte selbst oder der Händlername, sondern nur die Höhe des Zahlbetrags. Der Händlername wird nicht protokolliert, sondern nur die technische Händlerkartennummer des vom Händler für die Zahlung verwendeten Sicherheitsmoduls (sogenannte Händlerkarte). Dies ist notwendig, damit im Falle einer Reklamation des Kunden von der Kreditwirtschaft der Begünstigte der Bezahltransaktion ermittelt werden kann. Eine Pflicht zur Protokollierung der erfolgten Abrufe dieser Daten ist für Chipkarten im Gesetz nicht angelegt. Im Geldkarte-System stellen die ergriffenen technisch-organisatorischen Sicherheitsmaßnahmen, wie etwa die äußerst geringe Lesedistanz durch Wahl der kontaktlosen Schnittstelle (ISO 14443) oder die sparsame Verwendung der ohnehin wenig aussagekräftigen Daten einen ausreichenden Schutz dar.

Eine Umsetzung einer Protokollierung, wie durch Herrn Dr. Weichert gefordert, würde kein zusätzliches Maß an Sicherheit bringen und hätte für den Kunden keinen Nutzen. Die Chipkarte könnte jeden kontaktlosen Zugriff auf die Daten in der Karte zählen. Der Kunde müsste selbst die Anzahl der Zugriffe im Rahmen von Bezahltransaktionen mitzählen, was er technisch nur durch Kontrolle des Zählers vor und nach jeder Bezahltransaktion könnte. Das erscheint nicht praktikabel.

Ebenfalls angesprochen wird die kontaktlos auslesbare eindeutige Kartennummer. Eindeutige Merkmale einer Karte könnten, so die Befürchtung der Datenschützer, zur De-Pseudonymisierung von Daten verwendet werden. Die eindeutige Kartennummer wird zur Identifizierung der Karte im System und zur Ableitung von kartenindividuellen Schlüsseln benötigt. Neben dieser eindeutigen Kartennummer muss nach Vorgabe der Deutschen Bundesbank ein ebenso eindeutiges Zertifikat über Kartendaten in der Karte vorhanden sein und bei Bezahltransaktionen in der Händlerkarte geprüft werden. Diese Maßnahme verhindert Totalfälschungen. Ob nun ein eindeutiges Merkmal auf der Karte gespeichert und kontaktlos gelesen werden kann oder zwei, stellt keinen Unterschied dar.

<u>Zweiter Kreditpunktpunkt des ULD:</u>
In diesem Spiegelpunkt wird die Möglichkeit zur Abschaltung der kontaktlosen Schnittstelle angesprochen. Eine fallweise Abschaltung der NFC-Schnittstelle ist datenschutzrechtlich nicht erforderlich. Diese Forderung steht auch im Widerspruch zu der Abstimmung im Rahmen der Arbeitsgemeinschaft „Kreditwirtschaft“ beim Düsseldorfer Kreis auf künftig wünschenswerte Verbesserungen der Kartentechnik. Die DK arbeitet an einer Ergänzung des Chipkartenbetriebssystem, die das Deaktivieren der kontaktlosen Schnittstelle im Feld erlaubt. Nach dem Deaktivieren der Schnittstelle können dann keine Daten mehr über die kontaktlose Schnittstelle gelesen werden. Bis zur Umsetzung dieser Funktion auf neuen Karten stellen Schutzhüllen eine gute Alternative dar. Befindet sich die Karte in einer Schutzhülle, wird das elektromagnetische Feld komplett von der Karte abgeschirmt und eine kontaktlose Kommunikation unterbunden. Der DSGV hat im Datenschutzmerkblatt für die Kunden und in seinem Rundschreiben an die Institute (Nr. 234 vom 13. Juni 2012) auf die Möglichkeiten der Schutzhüllen hingewiesen, diese sind effektiv und für den Kunden auch über den Deutschen Sparkassenverlag (DSV) beziehbar.

Bewertung:
Da bereits heute keine Rückschlüsse auf Sachverhalte der Intim- und Privatsphäre möglich sind und die bereits ergriffenen technisch und organisatorischen Maßnahmen als ausreichender Schutz angesehen werden, können Kunden „girogo“ weiter einsetzen. Die ausgesprochene Warnung, nur Transaktionen zuzulassen, die keinen Rückschluss auf die Intim- oder Privatsphäre zulassen, erscheint insoweit verfehlt.

„girogo“ wird weiterhin das Standardprodukt der Sparkassen sein. Durch Datenschützer gewünschte Änderungen wurden inzwischen auf den Weg gebracht (s. o.) und werden mit der nächsten Generation der SparkassenCard umgesetzt. Die Forderung nach einer Autorisierung von Auslesevorgängen geht über die datenschutzrechtlichen wie – technischen Anforderungen hinaus (s. o.). Eine Löschung einzelner Lade- und Bezahltransaktionen aus den LOG-Daten ist nicht vorgesehen. Dieser Umstand ist auch von den Datenschutzaufsichtsbehörden nie bemängelt worden. Der Kunde wird hier künftig die Möglichkeit haben, den kontaktlosen Zugriff auf die Karte und damit auch auf diese Daten durch Abschalten der Kontaktlosfunktion zu unterbinden (s. o.). Bis dahin besteht für Kunden, denen nach Einsatz der Karte Bedenken im Hinblick auf die Kontaktlostechnik kommen, die Möglichkeit, ihre Karte gegen eine neue, transaktionsdatenfreie Karte zu tauschen. Der DSGV wird hierzu per Rundschreiben informieren.

Der Kunde wird im Gegensatz zu den übrigen am Markt befindlichen Bezahlverfahren per NFC-Technik über das Merkblatt zur „girogo“ in allgemein verständlicher Form über die Funktionsweise des Kartenchips und insbesondere auch die Art der verarbeiten Daten sowie mögliche Risiken und Möglichkeiten zu deren Vermeidung informiert. Die Kunden werden mit dem Datenschutzmerkblatt, das auch dem Düsseldorfer Kreis zur Verfügung gestellt wurde, somit ausreichend informiert. Dieses Merkblatt wurde auch durch die Datenschützer sehr positiv aufgenommen. Weitergehende Informationen werden ebenfalls angeboten. Darüber hinaus steht den Kunden immer die Möglichkeit offen, eine Kontaktierung ihrer SparkassenCard über NFC mittels Schutzhülle zu unterbinden, der DSV bietet eine Schutzhülle an. Die Sparkassen sehen jedoch davon ab, dieses Produkt aktiv anzubieten.

Die DK hat den Datenschützern sehr früh mitgeteilt, dass auf freiwilliger Basis pilotbegleitend ein sogenanntes Privacy Impact Assessment (PIA) erstellt wird und nach Abschluss des Piloten den Datenschützern übermittelt wird. Soweit auf die Nutzung von NFC-Schnittstellen zu Zahlungen über Smartphones und mit Kreditkarten verwiesen wird, so sieht der DSGV hier die Anbieter derartiger Dienstleistungen bzw. die Kreditkartenunternehmen in der Pflicht. Die Kreditkartenunternehmen haben sich insoweit auch gegenüber dem AK-Kreditwirtschaft und dem AK-Technik des Düsseldorfer Kreises, in dem im Übrigen auch das ULD vertreten ist, zur Erstellung eines PIA bereit erklärt.

5.3 Elektronisches Lastschriftverfahren - der Kunde bezahlt mit seinen Daten

Das Elektronische Lastschriftverfahren (ELV) ist kein Verfahren der Kreditwirtschaft, sondern ein von Handels- und Dienstleistungsunternehmen in Deutschland getragenes Verfahren zur bargeldlosen Bezahlung an Kassenterminals. Man nennt diese Verfahren auch "wilde" Verfahren, welche individuell zwischen Händlern und Netzbetreiber vereinbart werden. Anhand der Daten auf der Bankkundenkarte wird eine Lastschrift nach dem Einzugsermächtigungsverfahren generiert. Beim ELV liest das Händlerterminal die Kontoinformationen für die Generierung der Lastschrift aus dem Magnetstreifen der Bankkarten aus.

Anders als für das kreditwirtschaftliche Verfahren electronic cash gibt es für das vom Handel initiierte und vertriebene ELV-Verfahren keine veröffentlichten Musterspezifikation und auch keine Zulassungsverfahren. Die Deutsche Kreditwirtschaft erhält über diese Verfahren keinerlei Kenntnis und hat auch keinerlei Einflussnahmen.

12.4 IZG-SH und Einsicht in Steuerakten

Zu diesem Punkt teilt das Finanzministerium folgendes mit:
Sofern sich der Auskunftsanspruch eines Bürgers auf ein abgeschlossenes Besteuerungsverfahren bezieht, wird der Auffassung des ULD zugestimmt wird, dass § 3 IZG SH zur Anwendung kommt.
Der Darlegung eines besonderen Interesses bedarf es nach dem IZG nicht; der Antrag muss jedoch erkennen lassen, zu welchen Informationen der Zugang begehrt wird. Im Übrigen wird auf die Ausführungen zu Punkt 4.8.1 verwiesen.

Mit freundlichen Grüßen

gez. Bernd Küpperbusch