LANDTAG MECKLENBURG-VORPOMMERN **Drucksache 5/1440**
5. Wahlperiode **22.04.2008**

UNTERRICHTUNG

durch den Landesbeauftragten für den Datenschutz

Achter Tätigkeitsbericht gemäß § 33 Absatz 1 des Landesdatenschutzgesetzes von Mecklenburg-Vorpommern (DSG M-V),

Erster Tätigkeitsbericht zum Informationsfreiheitsgesetz Mecklenburg-Vorpommern

und

Dritter Tätigkeitsbericht gemäß § 38 Absatz 1 des Bundesdatenschutzgesetzes (BDSG)

Zugeleitet mit Schreiben des Landesbeauftragten für den Datenschutz vom 17. April 2008.

Vorwort

Das Datenschutzgesetz von Mecklenburg-Vorpommern sieht vor, dass der Landesbeauftragte für den Datenschutz dem Landtag und der Landesregierung für jeweils zwei Kalenderjahre einen Tätigkeitsbericht vorlegt. Der vorliegende Achte Tätigkeitsbericht umfasst den Zeitraum vom 1. Januar 2006 bis 31. Dezember 2007.
Wie in den vorherigen Berichten habe ich Vorgänge ausgewählt, die einen Gesamteindruck von der Tätigkeit meiner Behörde vermitteln. Einige Beiträge schließen an Sachverhalte aus den letzten Tätigkeitsberichten an. Insofern könnte es nützlich sein, in dem einen oder anderen Fall noch einmal auf diese Berichte zurückzugreifen.
Für die konstruktive und angenehme Zusammenarbeit danke ich meinen Amtskolleginnen und Amtskollegen beim Bund und in den Ländern. Ein weiterer Dank gilt meinen Mitarbeiterinnen und Mitarbeitern für die engagierte, zuverlässige und sachkundige Arbeit im Berichtszeitraum sowie bei der Erarbeitung der einzelnen Beiträge dieses Berichtes.

Karsten Neumann
Landesbeauftragter für den Datenschutz
Mecklenburg-Vorpommern

Inhaltsverzeichnis

Seite

Seite

Seite

0. Einleitung

Der Berichtszeitraum war geprägt von einer Fülle öffentlicher Diskussionen des Datenschutzrechtes, wie es sie wohl seit Jahrzehnten nicht gab. Dies spiegelt sich in allen Tätigkeitsfeldern meiner Behörde wider. Die im Bericht beschriebenen Einzelfälle meiner Tätigkeit sowohl als Landesdatenschutzbeauftragter mit der Zuständigkeit für Fragen des Datenschutzes im Verhältnis zwischen Bürger und Verwaltung als auch in meiner Funktion als Aufsichtsbehörde im Verhältnis zwischen Bürger und Unternehmen und genauso in der neuen Funktion als Landesbeauftragter für Informationsfreiheit verdeutlichen dies nachdrücklich.

Bungee-Jumping am seidenen Faden

Die Innenpolitik auf Bundes- und Landesebene hat auf vielfältige Weise den Versuch unternommen, das Verhältnis zwischen den bürgerlichen Freiheitsrechten und einem vermeintlichen Recht auf Sicherheit auf der Grundlage eines terroristischen Gefährdungsszenarios zugunsten der Sicherheit zu verschieben. In der Art eines gesetzgeberischen Bungee-Jumping wurden die Werteentscheidungen des Grundgesetzes nicht nur ausgereizt. Vielmehr wurden hierbei wiederholt Grenzen überschritten, die dann erst die Verfassungsgerichte in einer Fülle von Entscheidungen wiederherstellen mussten (siehe Punkte 2.1.1, 2.2.1). Die dabei aufgezeigten äußersten Grenzen sollten durch den Gesetzgeber jedoch nicht ausgefüllt, sondern der Geist respektiert und der Verfassungsauftrag in seiner Gänze erfüllt werden. Diese Aufgabe darf nicht länger auf die Verfassungsgerichte delegiert werden, sondern muss in der parlamentarischen Beratung in eine selbstbewusste Verteidigung grundrechtlicher Positionen münden.
„Es ist keine Freiheit ohne Sicherheit“, stellte Wilhelm von Humboldt (Wilh. v. Humboldt, Ideen zu einem Versuch, die Grenzen der Wirksamkeit des Staates zu bestimmen, Reclam 1991, S. 118 f.) zu Recht fest, jedoch nicht, ohne zu ergänzen, es könne zur Erhaltung der Sicherheit „das nicht notwendig sein, was gerade die Freiheit und mithin auch die Sicherheit aufhebt.“ Die mit der Behauptung eines „Rechtes auf Sicherheit“ einhergehende Überforderung der polizeilichen präventiven Möglichkeiten wird gesetzgeberisch versucht zu bewältigen, indem immer mehr Befugnisse erweitert, rechtsstaatliche Beschränkungen verringert und datenschutzrechtliche Grundsätze untergraben werden. Die „Gewöhnung“ hieran setzt schnell ein und führt mittlerweile dazu, dass beispielsweise sogenannte Massen-Gen-Tests längst nicht mehr freiwillig sind (siehe Punkt 2.1.4) oder ein vermeintlicher Exhibitionist eine terroristische Gefahr begründet und ohne Verurteilung in seiner Berufsfreiheit eingeschränkt wird (siehe Punkt 2.2.2). Bürgerinnen und Bürger werden vor die unlösbare Aufgabe gestellt, sich von gefährdeten Orten und gefährlichen Personen fernzuhalten, die sie aber gar nicht kennen können, wenn sie nicht zum Gegenstand polizeilicher Überprüfungen werden wollen (siehe Punkt 2.2.4). Einer Kontrolle der Rechtmäßigkeit solcher Maßnahmen entzieht sich dann die verantwortliche Stelle, indem sie die Daten vor einer angekündigten Kontrolle des vom Parlament hierzu berufenen Datenschutzbeauftragten „aus Datenschutzgründen“ löscht (siehe Punkt 2.2.4).

Das datenschutzrechtliche Konzept der unabhängigen Kontrolle steht jedoch vor weiteren Problemen. Beflügelt durch das vorgenannte Verfahren der Schaffung datenschutzrechtlich bedenklicher Gesetze nach dem Motto „Wo kein Kläger, da kein Richter“ und in der Hoffung, dass die betroffenen Bürgerinnen und Bürger sich schon nicht wehren werden, und wenn doch, dann den Gang durch die Instanzen doch nicht durchhalten können, werden auch immer wieder Empfehlungen nicht umgesetzt, die der Landesbeauftragte für den Datenschutz im Zusammenhang mit Beanstandungen gibt. Hier ist der Gesetzgeber aufgefordert, den Tätigkeitsbericht für ernsthafte Auseinandersetzungen und gegebenenfalls auch für rechtliche Korrekturen zum Anlass zu nehmen (siehe Punkte 2.5.6, 2.12.3 und 2.15.1).

Organisierte Verantwortungslosigkeit

Datenschutzrechtlich besonders risikobehaftet sind zentrale elektronische Verfahren, die dann aber in dezentraler Verantwortung umgesetzt werden müssen. Hier bleibt oft den Landes- oder Kommunalbehörden faktisch kaum eine Möglichkeit, sich den datenschutzrechtlichen Vorgaben des Gesetzgebers entsprechend zu verhalten (siehe Punkte 2.4.7, 2.5.6). Gerade im Bereich der koordinierten Entwicklung von E-Government-Verfahren muss es selbstverständlich werden, dass die zentralen Sicherheitsanforderungen bereits durch den Entwickler erfüllt werden. Nur so können die Anwender in die Lage versetzt werden, die daraus resultierenden Maßnahmen auch umzusetzen (siehe Punkte 2.4.7, 2.5.6). Dass ein solches Vorgehen praktikabel ist, hat sich bei der Einführung des Verfahrens zur elektronischen Melderegisterauskunft gezeigt.

Im kommunalen Bereich beobachte ich mit Sorge die gleiche Tendenz wie im nicht-öffentlichen Bereich, dass die verantwortlichen Stellen über kein oder kein ausreichendes technisches und rechtliches Know-how verfügen, um die gesetzlichen Anforderungen erfüllen zu können. Der kommunale Zweckverband E-Government geht hier den richtigen Weg, indem erstmals eine hauptberufliche Datenschutzbeauftragte eingestellt wurde, die dann mehrere Kommunen kompetent beraten kann (siehe Punkt 2.4.1).

Auch die zentrale Entwicklung technischer Basiskomponenten kann dazu beitragen, zentrale elektronische Verfahren datenschutzgerecht einzuführen und zu betreiben. Besonders wichtig erscheint mir die im E-Government-Masterplan beschriebene Basiskomponente „Verschlüsselung/Signatur“. Sie kann entscheidend dazu beitragen, datenschutzrechtliche und sicherheitstechnische Standards für viele weitere Anwendungen zu schaffen. Hier ist das Land aufgefordert, unabhängig von der Entwicklung einzelner Verfahren den vollständigen Aufbau dieser Basiskomponente abzuschließen. Das Fehlen einer solchen Basiskomponente würde dazu führen, dass ich den Einsatz unsicherer Verfahren beanstanden und deren Start untersagen müsste, selbst wenn der Einsatz der Signaturkomponente bereits geplant wäre (siehe Punkt 2.15.2).

Modernisierung des Datenschutzrechtes erforderlich

Die Herausforderungen der technischen Entwicklungen und vor allem die wachsende Anwendungsbreite informationstechnischer Systeme stellt den Gesetzgeber vor die akute Aufgabe, das rechtliche Instrumentarium zum Schutz der Menschenwürde im Informationszeitalter auf seine Wirksamkeit und Zukunftsfestigkeit hin zu überprüfen. Im März 2007 hatte ich die Gelegenheit, als Sachverständiger vor dem Innenausschuss des Deutschen Bundestages die wichtigsten Herausforderungen aufzuzeigen (siehe Anlage 3). Auf Landesebene könnte ein wichtiger Schritt zur Modernisierung des Datenschutzrechts gegangen werden, indem die gesetzliche Erlaubnis zur Durchführung des sogenannten Datenschutz-Audits auch umgesetzt würde. Dann wäre es endlich möglich, informationstechnische Produkte von unabhängigen Fachleuten auf ihre Datenschutzkonformität prüfen zu lassen. Diese Auditierungen werden vor allem von solchen Unternehmen verstärkt angefragt, die ihren Kunden Dienstleistungen in besonders sensiblen Bereichen anbieten. Darüber hinaus ist aber auch wichtig, öffentlichen und privaten Kunden ein überzeugendes Mittel zum Schutz der eigenen Privatsphäre oder zur Einhaltung der datenschutzrechtlichen Anforderungen an ihre Tätigkeit an die Hand zu geben (siehe Punkt 2.15.1). Der Staat muss auf dem Weg in das viel zitierte Informationszeitalter seiner Verantwortung für die Schaffung einer Infrastruktur gerecht werden, indem er die Vertraulichkeit und Integrität informationstechnischer Systeme gewährleistet. Angesichts der jahrelangen Weigerung der Landesregierung, den bereits 2002 formulierten gesetzgeberischen Willen umzusetzen, ist eine Gesetzesänderung zur Schaffung einer unmittelbaren Ermächtigung überfällig (siehe Punkt 2.15.1).

Die Datenschutzbeauftragen versuchen mit vielen Initiativen, diese Diskussion voranzutreiben und nicht allein aus einer „Mahner“-Position heraus, sondern als Experten ihr Wissen und ihre Erfahrungen in diese politische Diskussion einzubringen. Dem dienen nicht zuletzt unsere Vortragstätigkeit, sowie die inzwischen erfolgreiche Reihe „Datenschutz vor Ort“ und die gesamte Öffentlichkeitsarbeit. Erneut versucht dieser - inzwischen achte - Tätigkeitsbericht, diese Diskussion als ernsthafte und folgenreiche Debatte der politisch und gesellschaftlich Verantwortlichen anzuregen.

1. Empfehlungen

1.1 Zusammenfassung aller Empfehlungen

1. Ich empfehle der Landesregierung und dem Landtag, Zuverlässigkeitsüberprüfungen bei (Groß-)Veranstaltungen auf eine spezifische gesetzliche Grundlage zu stellen.
2. Ich empfehle der Landesregierung, die neu eingefügten und befristeten Befugnisse gründlich zu evaluieren und auf ihre Erforderlichkeit hin zu überprüfen.
3. Ich empfehle der Landesregierung, meine Vorschläge bei der nächsten Novellierung des Sicherheits- und Ordnungsgesetzes zu berücksichtigen.
4. Ich empfehle der Landesregierung, gesetzlich die Durchführung von Maßnahmen der Verkehrsüberwachung mittels Videotechnik zu regeln.
5. Ich empfehle dem Landtag erneut, für die elektronische Vorgangsbearbeitung bei der Verfassungsschutzbehörde eine gesetzliche Grundlage zu schaffen, und der Landesregierung, ein umfassendes Sicherheitskonzept für das Verfahren zu erstellen und vollständig umzusetzen.
6. Ich empfehle der Landesregierung, im Rahmen der Kommunalaufsicht verstärkt auf die Einhaltung von Datenschutzvorschriften aus dem Telekommunikations- und Medienrecht zu dringen. Dabei sollte die 2007 überarbeitete Orientierungshilfe „Datenschutzgerechte Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz“ der Datenschutzbeauftragten des Bundes und der Länder beachtet werden. Besondere Aufmerksamkeit ist geboten, wenn kommunale Vertretungen die technische Infrastruktur der Stadt- und Gemeindeverwaltungen mit nutzen.
7. Ich empfehle der Landesregierung, künftig die Kommunen bei der Einführung zentraler E-Government-Verfahren frühzeitig bei der Umsetzung datenschutzrechtlicher Anforderungen und die Passbehörden des Landes bei der Umsetzung der datenschutzrechtlichen und der sicherheitstechnischen Vorgaben beim Betrieb des Passantragsverfahrens zu unterstützen.
8. Ich empfehle dem Landtag, im Kommunalabgabengesetz eine Klarstellung dahingehend aufzunehmen, dass die Ermittlung von Steuerpflichtigen nicht im Wege einer Auskunftspflicht Dritter erfolgen darf.
9. Ich empfehle der Landesregierung, in geeigneter Weise sicherzustellen, dass die Grundsätze des Trennungsgebotes und der Zweckbindung der Verwendung von Personalaktendaten eingehalten werden. Dabei sollte gesetzlich geregelt werden, dass Mitarbeiter von Finanzämtern generell in einem anderen Finanzamt veranlagt werden, um so der Gefahr einer unzulässigen Verwendung von Beschäftigtendaten im Rahmen von Steuerstrafverfahren strukturell begegnen zu können.
10. Ich empfehle der Landesregierung, sich umgehend um die Schaffung einer verfassungsgemäßen Rechtsgrundlage zu bemühen und bis dahin das Verfahren LUNA 2.0 einzustellen.
11. Ich empfehle der Landesregierung, bei ihren Planungen für neue E-Government-Verfahren und der Weiterentwicklung bestehender Verfahren den Unterschied zwischen Signatur und Authentisierung genau zu beachten und nicht aus Kostengründen auf ungeeignete oder weniger sichere Verfahren auszuweichen. Die Landesregierung sollte insbesondere ihren Einfluss auf die Entwicklung der Software in der Finanzverwaltung in diesem Sinne nutzen. Darüber hinaus sollte sie sich dafür einsetzen, die Ausnahmebestimmung in § 87 a AO nicht weiter zu verlängern.

12. Ich empfehle daher der Landesregierung, die öffentlichen Stellen des Landes für die datenschutzrechtlichen Aspekte bei der privaten Nutzung von Internetdiensten zu sensibilisieren. Dies betrifft vor allem auch die Notwendigkeit, die entsprechenden Bedingungen (Kontrollmöglichkeiten, Protokollierungen) für eine solche Nutzung für alle Mitarbeiter transparent zu regeln.
13. Ich empfehle der Landesregierung erneut, dem ELENA-Verfahrensgesetz im Bundesrat nur dann zuzustimmen, wenn die Verfassungsmäßigkeit des Verfahrens nachgewiesen, die Sicherheit der Daten garantiert und eine Kontrolle durch unabhängige Stellen gewährleistet ist.
14. Ich empfehle der Landesregierung, die flächendeckende Verfügbarkeit von Kartenlesern und Signaturkarten für die qualifizierte elektronische Signatur voranzutreiben und somit die Basiskomponente Signatur/Verschlüsselung des E-Government-Masterplans umzusetzen.
15. Ich empfehle der Landesregierung, dafür Sorge zu tragen, dass ich über jede Planung einer schulischen Videoüberwachung analog zu § 32 Abs. 3 Satz 6 DSG M-V frühzeitig unterrichtet werde.
16. Ich empfehle dem Landtag klarzustellen, dass keinem Mitarbeiter wegen der Anrufung des Landesbeauftragten für den Datenschutz oder des behördlichen Datenschutzbeauftragten Nachteile entstehen dürfen.
17. Ich empfehle dem Landtag, durch eine Änderung des § 5 Abs. 2 Landesdatenschutzgesetz (DSG M-V) die erforderliche gesetzliche Grundlage für die Durchführung eines Auditierungsverfahrens zu schaffen.
18. Ich empfehle der Landesregierung, ihre Beschlüsse zur Basiskomponente Signatur entschlossen umzusetzen. Sie sollte sich darüber hinaus für eine stärkere Verbreitung der qualifizierten elektronischen Signatur einsetzen und ihren Einfluss im Bundesrat in diesem Sinne ausüben. In Mecklenburg-Vorpommern sollte sie Anwendungen der qualifizierten elektronischen Signatur sowohl in der Verwaltung als auch in der Wirtschaft fördern.
19. Ich empfehle dem Landtag, die technische Entwicklung von RFID-Systemen aufmerksam zu beobachten und sofort gesetzgeberisch aktiv zu werden, wenn die rechtlichen Schutzmechanismen den neuen Risiken nicht mehr gerecht werden.
20. Ich empfehle der Landesregierung, Informationssicherheits- und Datenschutzfragen künftig in engem Zusammenhang zu bearbeiten und die vom BSI beschriebenen Managementprozesse bei der Planung, der Einrichtung, dem Betrieb und nach der Außerbetriebnahme von IT-Verfahren vollständig umzusetzen.

1.2 Umsetzung der Empfehlungen des 7. Tätigkeitsberichts

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungs-punkt
1	Ich empfehle dem Landtag, im Rahmen einer Änderung der Geschäftsordnung des Landtages mit Beginn der nächsten Legislaturperiode das Rede- und Zutrittsrecht des Landesbeauftragten für den Datenschutz analog der Rechte der Bürgerbeauftragten zu gestalten, um so die Einbeziehung der Sachkompetenz meiner Behörde in Beratungsgegenstände der Fachausschüsse zu ermöglichen.	Der Empfehlung wurde nicht gefolgt.	A.0
2	Ich empfehle daher der Landesregierung, bei einer Überarbeitung der GGO II die förmliche Beteiligung des Landesbeauftragten für den Datenschutz im Stadium des Referentenentwurfes zu Gesetzen und zu Verordnungen mit aufzunehmen.	Der Empfehlung wurde nicht gefolgt.	A.0
3	Ich empfehle der Landesregierung, beim Verfahren zur Befreiung von der Rundfunkgebührenpflicht den Gesetzesvorschlag der Datenschutzbeauftragten des Bundes und der Länder zu befürworten und damit ein datenschutzgerechtes Verfahren zu unterstützen.	Die Landesregierung ist meiner Empfehlung nachgekommen.	A.1.I
4	Ich empfehle daher dem Landtag, die Ankündigung der Landesregierung und der Koalitionsfraktionen, noch vor Ende dieser Legislaturperiode ein Informationsfreiheitsgesetz für Mecklenburg-Vorpommern zu beschließen, umgehend umzusetzen.	Der Empfehlung wurde gefolgt. Das IFG M-V ist verabschiedet worden.	A.1.II.1.2
5	Ich empfehle daher der Landesregierung, auf der Grundlage der bisher geleisteten Vorarbeiten umgehend eine Verordnung nach § 5 Abs. 2 Landesdatenschutzgesetz (DSG M-V) zu erlassen.	Die Landesregierung hat die Verordnung nach wie vor nicht erlassen (siehe auch Punkt 2.15.1 und Anhang 8).	A.1.II.1.3

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungs-punkt
6	Ich empfehle der Landesregierung, für die neuen elektronischen Verfahren im Meldewesen - insbesondere für die elektronische Melderegisterauskunft - angemessene technische und organisatorische Vorkehrungen zu treffen und bei der Novellierung des Landesmeldegesetzes zu normieren.	Die neuen elektronischen Verfahren im Meldewesen wurden weitgehend unter Berücksichtigung der Empfehlungen der Datenschutzbeauftragten realisiert (siehe auch Punkt 2.4.3). Die Verordnung zum Landesmeldegesetz steht allerdings noch aus.	A.1.II.1.4
7	Ich empfehle der Landesregierung sicherzustellen, dass die erforderlichen Abschottungsmaßnahmen eingehalten werden. Neben der oben genannten technischen Abschottung sind dies vor allem die personelle Trennung zwischen Mitarbeitern des Statistischen Amtes und denen aus anderen Abteilungen des Landesamtes für innere Verwaltung, die bauliche Abschottung mit entsprechender Schlüsselverwaltung, die Verpflichtung der Mitarbeiter des Statistischen Amtes auf Wahrung der statistischen Geheimhaltung auch gegenüber dem Leiter des Landesamtes für innere Verwaltung und die Verarbeitung statistischer Einzeldaten im Auftrag nur aufgrund einer schriftlichen Verfügung des Leiters des Statistischen Amtes.	Die Dienstanweisung zur organisatorischen, räumlichen und personellen Absicherung des Statistischen Amtes ist in der Form, wie sie mit dem LfD erarbeitet wurde, ergangen. Die Dienstanweisung zur Gewährleistung der Datensicherheit beim ADV-Einsatz und bei der Erledigung von Aufgaben der amtlichen Statistik im LAIV ist mir bislang lediglich im Entwurf zwecks Bewertung aus datenschutzrechtlicher Sicht zugeleitet worden.	A.1.II.1.5
8	Ich empfehle dem Landtag, eine Klarstellung dahingehend vorzunehmen, dass auch in diesem Bereich dem Trennungsgebot Rechnung getragen wird.	Der Empfehlung wurde nicht gefolgt.	A.1.II.1.7
9	Ich empfehle der Landesregierung, Datenschutz- und IT-Sicherheitsaspekte der Landesfirewall im IT-Sicherheitsrahmenkonzept angemessen zu berücksichtigen und die hierfür erforderlichen Ressourcen zur Verfügung zu stellen, um das hohe Sicherheitsniveau auch weiterhin gewährleisten zu können.	In der Landesverwaltung wurde ein wirkungsvolles Informationssicherheits- und Datenschutzmanagement-system eingerichtet (siehe Punkt 2.15.5). In diesem Zusammenhang wurde auch die Landesfirewall den aktuellen Bedürfnissen bezüglich Verfügbarkeit, Durchsatz und Sicherheit angepasst.	A.1.II.1.9

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt
10	Ich empfehle der Landesregierung, bereits bei den Planungen zur IP-Telefonie die Empfehlungen der Datenschutzbeauftragten zu berücksichtigen, um künftig auch bei der Nutzung dieser modernen Kommunikationstechnologie das Fernmeldegeheimnis wahren zu können.	Die Landesregierung hat in ihrem Corporate Network mit dem Pilotbetrieb der IP-Telefonie begonnen. Das mir vorliegende IT-Sicherheitskonzept sieht unter anderem vor, die Verkehrs- und Inhaltsdaten innerhalb des Landesnetzes zu verschlüsseln.	A.1.II.1.10
11	Ich empfehle der Landesregierung, dem Landtag und den weiteren öffentlichen Stellen des Landes, die „Orientierungshilfe zu Datenschutzfragen bei der Präsentation öffentlicher Stellen im Internet“ zu nutzen, um bestehende oder geplante Internetportale zu prüfen (www.datenschutz-mv.de). Bei der Ausgestaltung der Internetportale sind die Prinzipien der Transparenz und der Datenvermeidung in vollem Umfang umzusetzen.	Die Landesregierung hat zugesagt, die Empfehlung umzusetzen.	A.1.II.1.11
12	Ich empfehle der Landesregierung, bei der Planung und beim Betrieb der landeseigenen Virtuellen Poststelle die Hinweise der Broschüre „Die virtuelle Poststelle im datenschutzgerechten Einsatz“ zu berücksichtigen. Für die datenschutzgerechte Ausgestaltung dieser zentralen E-Government-Komponente sind die Handlungsempfehlungen der Kapitel 8 und 9 besonders hilfreich.	Ein Teil der zentralen E-Government-Komponenten wird im Projekt Meldewesen eingesetzt. Hier wurden die datenschutzrechtlichen Empfehlungen weitgehend umgesetzt.	A.1.II.1.12
13	Ich empfehle der Landesregierung, gegebenenfalls zu überprüfen, ob sich an der aktuellen Sicherheitslage in Mecklenburg-Vorpommern seit dem Jahre 2000 etwas geändert hat. Ansonsten ist gegenüber den kommunalen Behörden klarzustellen, dass Videoüberwachungsanlagen auf öffentlichen Straßen und Plätzen nur bei Vorliegen der gesetzlichen Voraussetzungen zulässig sind. Bei entsprechenden Planungen sind die behördlichen Datenschutzbeauftragten frühzeitig einzubeziehen.	Die Empfehlung ist - soweit bekannt - nicht umgesetzt worden. Vielmehr ist das Sicherheits- und Ordnungsgesetz in diesem Punkt noch verschärft worden.	A.1.II.2.1

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungs-punkt
14	Ich empfehle dem Landtag, meine Vorschläge zur Sicherstellung ordnungsgemäßer Akten-/Datenübermittlung bei Aufgabenübertragungen und Verwaltungsfusionen im Gesetzgebungsverfahren zu berücksichtigen, um so bei der Verwaltungsmodernisierung die notwendige Rechtssicherheit in Datenschutzfragen zu erhalten.	Im Gesetz zur Modernisierung der Verwaltung des Landes Mecklenburg-Vorpommern wurde nur der Vorschlag umgesetzt, dass der Vorsitzende des Aufbaustabs für die Freigabe von Verfahren verantwortlich ist. Durch Urteil des Landesverfassungsgerichts vom 26.07.2007 wurde wegen der Unvereinbarkeit der Vorschriften über die Kreisgebietsreform mit der Verfassung des Landes M-V das Verwaltungsmodernisierungsgesetz bis auf wenige Ausnahmen als gegenstandslos erklärt.	A.1.II.2.2
15	Ich empfehle der Landesregierung sowie allen öffentlichen Stellen des Landes, im Rahmen der regelmäßigen Belehrungen ihre Mitarbeiter darauf hinzuweisen, dass Gesprächsteilnehmer generell vor Betätigen der Freisprechtaste beziehungsweise sonstigen Mithörens durch weitere Personen um ihr Einverständnis zu bitten sind. Diese Verfahrensweise ist verbindlich zu regeln.	Eine verbindliche Regelung hierzu ist bisher nicht erfolgt.	A.1.II.2.3
16	Ich empfehle der Landesregierung, im Rahmen der Kommunalaufsicht verstärkt darüber zu wachen, dass verdeckte Beobachtungen von Sozialleistungsempfängern nicht durchgeführt oder angeordnet werden.	Die Landesregierung sieht keinen Bedarf für einen entsprechenden Runderlass, da es sich nur um Einzelfälle handelt.	A.1.II.2.4
17	Ich empfehle der Landesregierung, im Rahmen der Kommunalaufsicht die Hinweise für die Durchführung von Hausbesuchen bei Sozialleistungsempfängern in den Landkreisen und kreisfreien Städten bekannt zu geben.	Handelungsbedarf wird hier nicht gesehen, da es zu der Problematik „Hausbesuche“ bereits umfangreiche Rechtsprechung gibt, sodass den Sozialhilfeträgern hinlänglich bekannt ist, unter welchen engen Voraussetzungen Hausbesuche erforderlich und zulässig sind.	A.1.II.2.5

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungs-punkt
18	Ich empfehle der Landesregierung, die Ausführungshinweise des Finanzministeriums und die Vollzugshinweise für die Durchführung des Wohngeldgesetzes des Ministeriums für Arbeit, Bau und Landesentwicklung um eine Regelung für den Fall zu ergänzen, wie mit dem Ergebnis des Kontenabrufes verfahren werden soll, wenn sich der Anlass für einen Kontenabruf im laufenden Verwaltungsverfahren erledigt hat.	Hierzu hat sich die Landesregierung nicht geäußert.	A.1.II.2.6
19	Der Landesregierung empfehle ich, bei der Novellierung der Vorschriften der Kommunalverfassung Mecklenburg-Vorpommern über die Informations- und Prüfungsrechte der Gemeinde bei Unternehmen oder Einrichtungen des privaten Rechts klarstellende Regelungen zur Zulässigkeit der Datenübermittlung an die Gemeinde-/Stadtvertreter im Rahmen ihrer Kontrollfunktion aufzunehmen.	Die Landesregierung greift die Empfehlung nicht auf. Sie ist der Auffassung, dass die Regelungen der KV M-V zur Auskunftsverpflichtung ausreichend sind.	A.1.II.2.7
20	Ich empfehle der Landesregierung, die Gemeindevertretungen darauf hinzuweisen, dass Tonbandmitschnitte zur Protokollerstellung während einer Einwohnerfragestunde nur zulässig sind, wenn die Betroffenen hierüber in geeigneter Weise aufgeklärt wurden.	Die Landesregierung regte lediglich den Städte- und Gemeindetag an, zu dieser Thematik einen Beitrag in dem Publikationsorgan „Der Überblick“ zu veröffentlichen.	A.1.II.2.8
21	Ich empfehle der Landesregierung zu prüfen, ob zum Umgang mit personenbezogenen Daten im Rahmen von Bürgerbegehren Regelungen in die Kommunalverfassung aufgenommen werden sollten, um hier mehr Rechtssicherheit zu erreichen.	Diese Empfehlung soll im Rahmen der anstehenden Novellierung der Durchführungsverordnung zur KV M-V einbezogen und gegebenenfalls mit den kommunalen Landesverbänden erörtert werden.	A.1.II.2.9

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt
22	Ich empfehle der Landesregierung sowie allen weiteren öffentlichen Stellen, darauf zu achten, dass bei Privatisierungen öffentlicher Unternehmen die von der Bundesbeauftragten für die Unterlagen des Staatssicherdienstes übermittelten Daten vor dem Betriebsübergang datenschutzgerecht vernichtet werden. Im Übrigen dürfen die Unterlagen nur bis Ende des Jahres 2006 für die Überprüfung von Mitarbeitern des öffentlichen Dienstes genutzt werden. Vor diesem Hintergrund ist dafür zu sorgen, dass die in den Personalakten enthaltenen Daten danach durch alle personalbearbeitenden Dienststellen gelöscht werden.	Für die Empfehlung einer datenschutzgerechten Vernichtung der betreffenden Daten wurde keine Grundlage gesehen.	A.1.II.2.10
23	Ich empfehle der Landesregierung vor dem Hintergrund weiterer Fusionen im kommunalen Bereich, dafür Sorge zu tragen, dass die ordnungsgemäße Übergabe von Aktenbeständen sowie die Verantwortlichkeiten, die Fristen, die Archivierung beziehungsweise die Vernichtung der Unterlagen verbindlich geregelt wird.	Eine verbindliche Regelung ist nicht erfolgt.	A.1.II.2.11
24	Ich empfehle der Landesregierung, die Ausländerbehörden darauf hinzuweisen, dass das Vorliegen der Voraussetzungen für die Speicherung im Schengener Informationssystem in jedem Einzelfall genau zu prüfen und zu dokumentieren ist.	Das Innenministerium hat meine Empfehlung aufgegriffen und die Ausländerbehörden ausdrücklich auf ihre Prüf- und Dokumentationspflichten hingewiesen.	A.1.II.2.12
25	Ich empfehle der Landesregierung, die Meldebehörden auf ihre Dokumentationspflichten bei erweiterten Melderegisterauskünften hinzuweisen, deren Einhaltung im Rahmen der Fachaufsicht zu prüfen und bei einer Neugestaltung des Verfahrens die Dokumentationspflichten zu berücksichtigen.	Ein entsprechender Hinweis an die Meldebehörden des Landes ist bisher nicht erfolgt.	A.1.II.2.13

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungs-punkt
26	Ich empfehle den öffentlichen Stellen des Landes, vor der Beschaffung einer Videoüberwachungsanlage den behördlichen Datenschutzbeauftragten zu beteiligen sowie die technischen Anforderungen mit Hilfe des Schutzprofils zu beschreiben. Anbieter sollten bereits im Vergabeverfahren aufgefordert werden, die Kompatibilität ihrer Anlage mit den Anforderungen des Schutzprofils möglichst durch eine Zertifizierung nachzuweisen.	Bei den Planungen zu Videoüberwachungsanlagen wurden die technischen Anforderungen in keinem mir bekannten Fall mit Hilfe des Schutzprofils beschrieben. Nach Common Criteria zertifizierte Videoüberwachungsanlagen sind mir nicht bekannt.	A.1.II.2.17
27	Ich empfehle der Landesregierung und dem Landtag, ein Akkreditierungsverfahren bei Großveranstaltungen, die besondere Sicherheitsmaßnahmen erfordern, auf eine generelle gesetzliche Grundlage zu stellen.	Die Empfehlung ist im Gesetzgebungsverfahren zum Sicherheits- und Ordnungsgesetz unseres Landes nicht umgesetzt worden.	A.1.II.3.1
28	Ich empfehle der Landesregierung Vorkehrungen zu treffen, damit sowohl die Staatsanwaltschaften als auch die Polizei aktuelle Ausgänge zu Ermittlungsverfahren mitteilen und die sich daran anschließende Korrektur von Eintragungen in Dateien und Verzeichnissen durchgeführt wird. Dies ist den Betroffenen auch in jedem Fall mitzuteilen.	Das Justizministerium hat zugesichert, den Generalstaatsanwalt zu bitten, weiter für eine Sensibilisierung der Staatsanwaltschaften in diesem Bereich Sorge zu tragen, um eine Erfassung der Daten zum Verfahrensausgang in jedem Fall zu gewährleisten.	A.1.II.3.2

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt
29	Ich empfehle der Landesregierung, der Novellierung des Pass- und Personalausweisgesetzes im Bundesrat nur zuzustimmen, wenn gewährleistet ist, dass bei der Einführung biometrischer Ausweisdokumente die biometrischen Merkmale ausschließlich von den für die Passkontrollen zuständigen Behörden für hoheitliche Zwecke genutzt werden können, die in Ausweisen gespeicherten Daten mit den biometrischen Merkmalen nicht als Referenzdaten genutzt werden, um Daten aus unterschiedlichen Systemen und Kontexten zusammenzuführen, die für die Ausstellung und das Auslesen verwendeten Geräte nach internationalen Standards von einer unabhängigen Stelle zertifiziert werden und Verfahren festgelegt werden, die einen Datenmissbrauch beim Erfassen der Referenzdaten und im weiteren Verfahren verhindern.	Obwohl bislang nicht fest steht, dass die weitere Funktion des elektronischen Personalausweises zur online-Identifikation sinnvoll, für die potenziellen Nutzerinnen und Nutzer vorteilhaft und datenschutzrechtlich unbedenklich wäre, hat die Landesregierung den entsprechenden Novellierungen des Pass- und des Personalsausweisgesetzes zugestimmt.	A.1.II.3.3
30	Ich empfehle der Landesregierung, gegenüber den Staatsanwaltschaften und den Polizeidienststellen klarzustellen, dass eine Übermittlung personenbezogener Daten an einen öffentlichen Arbeitgeber nur aufgrund einer normenklaren gesetzlichen Grundlage zulässig ist.	Es wurde keine Erforderlichkeit gesehen, die Staatsanwaltschaften auf den ohnehin zu beachtenden Datenschutz hinzuweisen, da entsprechende Regelungen in den §§ 474 ff. StPO und den Nrn. 182 ff. RiStBv enthalten sind.	A.1.II.3.4
31	Ich empfehle dem Landtag und der Landesregierung, für den Übergang zu einem papierlosen Büro bei der Verfassungsschutzbehörde eine gesetzliche Grundlage zu schaffen, wie das beispielsweise beim Verfassungsschutz im Land Brandenburg praktiziert wurde.	Es wurde angekündigt, dass dem Landesbeauftragten für den Datenschutz Anfang 2008 der Entwurf zur Änderung des Landesverfassungsschutzgesetzes zur Stellungnahme übersandt wird.	A.1.II.3.5

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungs-punkt
32	Ich empfehle der Landesregierung, bei der Überarbeitung der Richtlinie für das DNA-Verfahren der Landespolizei Mecklenburg-Vorpommern und der Richtlinie für die Staatsanwaltschaften des Landes die datenschutzrechtlichen Aspekte zu beachten, mich hieran rechtzeitig zu beteiligen und im Übrigen eine Evaluierung der Neuregelungen vorzunehmen.	Die Empfehlung wurde teilweise umgesetzt.	A.1.III.1
33	Ich empfehle der Landesregierung und dem Landtag, sich im Rahmen der Länderbeteiligung bei einer erneuten Bundesinitiative für eine datenschutzfreundliche Ausgestaltung der gesetzlichen Regelungen des Vollzugs der Untersuchungshaft einzusetzen, mich frühzeitig hieran zu beteiligen und im Rahmen der eigenen Zuständigkeit für eine Beachtung - auch des Rechtes auf informationelle Selbstbestimmung von Untersuchungsgefangenen - Sorge zu tragen.	Im Zuge der Föderalismusreform ist die Gesetzeskompetenz für den Untersuchungshaftvollzug auf die Länder übergegangen. Bisher ist das Gesetzgebungsvorhaben - soweit bekannt - von den Ländern noch nicht wieder aufgegriffen worden.	A.1.III.2
34	Ich empfehle der Landesregierung, gegenüber den Staatsanwaltschaften und den Polizeidienststellen in geeigneter Weise klarzustellen, dass bei Presseanfragen zu laufenden Verfahren die Betroffenen, die hiervon noch keine Kenntnis haben, generell vorab zu unterrichten sind. Ferner rege ich an, diesen Sachverhalt auch ausdrücklich in der Allgemeinen Verwaltungsvorschrift des Landes Mecklenburg-Vorpommern für die Zusammenarbeit der Justizbehörden mit den Medien zu regeln.	Der Generalstaatsanwalt hat zugesagt, die Thematik mit den Leitenden Oberstaatsanwälten auf einer Dienstberatung zu erörtern.	A.1.III.4

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungs-punkt
35	Ich empfehle der Landesregierung, die Gerichtsvollzieher bei der Umsetzung der Verwaltungsvorschrift zum Einsatz von EDV-Technik im Gerichtsvollzieherbüro zu unterstützen. Gerichtsvollzieher, die moderne Informations- und Kommunikationstechnik im dienstlichen Umfeld nutzen möchten, sollten auch die ergänzenden Hinweise der „Orientierungshilfe zum datenschutzgerechten Anschluss an Internet und Online-Banking bei Gerichtsvollziehern“ beachten, um ein Mindestmaß an Sicherheit für die auf ihren IT-Systemen gespeicherten Daten zu gewährleisten.	Die Landesregierung hat den Hinweis aufgenommen und zugesagt, die Gerichtsvollzieher weiter bei der Umsetzung der genannten Verwaltungsvorschrift zu unterstützen.	A.1.III.5
36	Ich empfehle der Landesregierung, die verfassungs- und datenschutzrechtlichen Aspekte bei der Vorratsdatenspeicherung in der Telekommunikation zu berücksichtigen und sich im Bundesrat gegen eine Speicherung von Daten, wie sie im Entwurf der Richtlinie der Europäischen Kommission vorgesehen ist, auszusprechen.	Das Gesetz hat inzwischen den Bundesrat ohne Widerspruch passiert.	A.1.III.6
37	Ich empfehle der Landesregierung, mich auch weiterhin frühzeitig bei der Gestaltung der länderübergreifenden Steuerdatenverarbeitung zu beteiligen. Wenn der Staatsvertrag wie vorgesehen verabschiedet wird, verbleibt für Dataport und die Steuerverwaltungen die Aufgabe, die Vorschriften zum Steuergeheimnis technisch und organisatorisch umzusetzen. So muss das Data Center Steuern von den anderen Teilen von Dataport abgeschottet werden, und die Steuerverwaltungen der beteiligten Länder dürfen nicht auf Daten eines anderen Bundeslandes zugreifen können.	Die Landesregierung berücksichtigt meine Empfehlungen.	A.1.IV.1

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt
38	Ich empfehle der Landesregierung, beim bargeldlosen Zahlungsverkehr in der Landesverwaltung auf Scoring-Verfahren beim Betrieb der Zahlungsverkehrsplattform generell zu verzichten. Darüber hinaus ist bei der weiteren Entwicklung des Verfahrens der Grundsatz der Datenvermeidung zu berücksichtigen.	Die Landesregierung hat zugesagt, meiner Empfehlung zu folgen.	A.1.IV.2
39	Ich empfehle der Landesregierung, die Daten der Mitarbeiterinnen und Mitarbeiter, die im Zuge der Strukturreform der Landesverwaltung dem Personalüberhang zugeordnet werden, nur in dem Rahmen zu nutzen, wie es für die Personalverwaltung notwendig ist. Ein unbeschränkter Zugriff auf diese Daten durch Personalstellen aller Ressorts wäre mit den datenschutzrechtlichen Bestimmungen nicht vereinbar.	Es wurde in Zusammenarbeit mit dem Landesbeauftragten eine Dienstanweisung erarbeitet.	A.1.IV.3
40	Ich empfehle der Landesregierung anzuordnen, dass die Finanzämter betroffene Geheimnisträger auf die Möglichkeit hinweisen, sich an den Landesbeauftragten für den Datenschutz zu wenden, wenn ihnen nachteilige steuerliche Entscheidungen drohen, sofern sie die Bekanntgabe personenbezogener Daten ihrer Mandanten/Patienten/Kunden verweigern.	Die Problematik ist mit den Sachgebietsleitern der Betriebsprüfungsstellen der Finanzämter ausführlich erörtert worden, sodass die Landesregierung davon ausgeht, dass einer Berücksichtigung der notariellen Verschwiegenheit im Steuerverfahren ausreichend Rechnung getragen worden sei. Hinsichtlich des vom LfD angesprochenen Falls sei die Betriebsprüfung unter Berücksichtigung der Verschwiegenheitspflicht des Notars beendet worden.	A.1.IV.4
41	Ich empfehle der Landesregierung, gegenüber den Sparkassen und anderen öffentlichen Einrichtungen bei Kundenbefragungen auf die Einhaltung datenschutzrechtlicher Bestimmungen hinzuweisen und deren Einhaltung zu prüfen.	Die Empfehlung ist vom Finanzministerium aufgegriffen und in einem Schreiben den Sparkassen des Landes Mecklenburg-Vorpommern bekannt gemacht worden.	A.1.IV.6

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt
42	Ich empfehle der Landesregierung, im Rahmen des noch immer ausstehenden Wasserverkehrs- und Hafenanlagensicherheitsgesetzes (WVHaSiG), die datenschutzrechtlich bedeutsame Zuverlässigkeitsüberprüfung, welche umfangreiche Abfragemöglichkeiten zu bestimmten Hafenmitarbeitern bei Polizei und gegebenenfalls weiteren Sicherheitsbehörden erlaubt, gesetzlich zu regeln und mich hieran frühzeitig zu beteiligen.	Der Empfehlung wurde gefolgt.	A.1.V.1
43	Ich empfehle der Landesregierung, im Rahmen der Tourismusförderung insbesondere Unternehmen und Kurverwaltungen für einen datenschutzgerechten Umgang mit den Daten ihrer Gäste zu sensibilisieren. Das gilt insbesondere bei der Einführung elektronischer Systeme.	Die Landesregierung stimmt meiner fachlichen Beurteilung zu, unternimmt aber keine besonderen Schritte, um die Tourismuswirtschaft zu Fragen des Datenschutzes zu informieren bzw. zu sensibilisieren. Die Unternehmen trügen selbst die Verantwortung für die Einhaltung der sie betreffenden Gesetze.	A.1.V.3
44	Ich empfehle der Landesregierung und allen anderen öffentlichen Stellen in Mecklenburg-Vorpommern, bei Auskunftsbegehren aufgrund eines berechtigten oder rechtlichen Interesses genau zu prüfen, ob dem Wunsch entsprochen werden kann.	Entsprechend der Empfehlung wird die Landesregierung die widerstreitenden Interessen nach Maßgabe des § 15 Abs. 1 Landesdatenschutzgesetz prüfen lassen.	A.1.VI.1
45	Die Landesregierung und die anderen öffentlichen Stellen sollten auch bei anderen Projekten, bei denen Vorteile für betroffene Personen unabdingbar mit Datenverarbeitungen verbunden sind, umfassend darüber aufklären und eine Einwilligung nur dort vorsehen, wo die Betroffenen tatsächlich Alternativen haben.	Die Empfehlung wurde aufgenommen.	A.1.VI.2

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungs-punkt
46	Ich empfehle der Landesregierung, Forschungsprojekte mit personenbezogenen oder aus diesen gewonnenen Daten nur zu genehmigen, wenn dazu ein datenschutzrechtliches Votum des jeweiligen behördlichen Datenschutzbeauftragten vorliegt.	Die Landesregierung teilt meine Rechtsauffassung.	A.1.VII.1
47	Ich empfehle der Landesregierung, unverzüglich das Datenschutz- und Datensicherheitskonzept für das Schulberichtssystem nachzureichen und die offenen Punkte zu klären. Künftig sollten Verfahren zur Datenverarbeitung erst in Betrieb genommen werden, wenn ein solches Konzept geprüft vorliegt.	Ein IT-Sicherheitskonzept wurde erarbeitet.	A.1.VII.2
48	Ich empfehle der Landesregierung gegenüber den Wohngeldstellen im Land klarzustellen, dass bei der Berechnung des Wohngeldes die Höhe des Vermögens nicht erhoben werden darf.	Meiner Empfehlung wurde gefolgt.	A.1.VIII.1
49	Ich empfehle der Landesregierung, dem JobCard-Verfahrensgesetz im Bundesrat nur dann zuzustimmen, wenn die Verfassungsmäßigkeit des Verfahrens nachgewiesen, die Sicherheit der Daten garantiert und eine Kontrolle durch unabhängige Stellen gewährleistet ist.	Die Landesregierung stimmt meiner Empfehlung grundsätzlich zu. Das Gesetz zur Einführung des Elektronischen Einkommensnachweises (ELENA - ehemals JobCard) wurde dem Bundesrat im Berichtszeitraum noch nicht vorgelegt.	A.1.VIII.2
50	Ich empfehle der Landesregierung, die Stellung der ARGEn in Mecklenburg-Vorpommern als eigenverantwortliche datenverarbeitende Stellen zu stärken, eine datenschutzgerechte Verarbeitung von Sozialdaten in den ARGEn zu fördern und die Kontrollkompetenz durch den Landesbeauftragten für den Datenschutz klarzustellen.	Meiner Empfehlung wurde insoweit gefolgt, als dass die Eigenverantwortlichkeit der ARGEn im Hinblick eines eigenen behördlichen Datenschutzbeauftragten geprüft wird. Im Ergebnis war beabsichtigt, mit dem Bundesministerium für Arbeit und Soziales Kontakt aufzunehmen, um die anstehenden Probleme einvernehmlich zu lösen.	A.1.VIII.3

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungs-punkt
51	Ich empfehle der Landesregierung, im Rahmen ihrer Fachaufsicht den datenschutzrechtlichen Vorgaben des § 21 LKHG M-V Beachtung zu schenken und die Krankenhäuser bei der Umsetzung der Vorgaben zu unterstützen, indem beispielsweise Maßnahmen zur Datensicherheit, wie Investitionen, behandelt werden.	Dem Sozialministerium sind Probleme bei der Rechtsanwendung im Bereich der Plankrankenhäuser nicht bekannt. Das Sozialministerium hat die Krankenhausaufsicht entsprechend dem Landeskrankenhausgesetz. Dies beinhaltet nicht die Fachaufsicht.	A.1.IX.2
52	Ich empfehle der Landesregierung, sich in der Gesundheitsministerkonferenz dafür einsetzen, dass der Umfang der zu verarbeitenden Daten im Rahmen von Disease-Management-Programmen kritisch auf die Erforderlichkeit hin untersucht wird.	Die Empfehlung wurde umgesetzt.	A.1.IX.4
53	Ich empfehle der Landesregierung, sofern sie weiterhin die Notwendigkeit sieht, zwischen dem Disease-Management-Programm „Brustkrebs“ und dem Krebsregister Daten auszutauschen, Verfahrensregelungen zu erlassen, die das Recht der Frauen auf informationelle Selbstbestimmung respektieren und dennoch dazu beitragen, dass Doppelmeldungen vermieden werden.	Die Landesregierung wird sich für entsprechende Regelungen einsetzen.	A.1.IX.5
54	Ich empfehle der Landesregierung, die Ärzte in der Wahrnehmung ihrer Auskunftspflichten und sonstigen datenschutzrechtlichen Verpflichtungen durch Schulungs- oder Informationsmaßnahmen zu unterstützen und Maßnahmen zur Stärkung der Patientenrechte zu ergreifen.	Die Empfehlung wurde umgesetzt.	A.1.IX.6
55	Ich empfehle der Landesregierung, mich bei der Planung von Forschungsprogrammen unter Einbeziehung von Patientenakten frühzeitig zu beteiligen bzw. darauf hinzuwirken und die Initiative der 67. Konferenz der Datenschutzbeauftragten zur Einführung eines Forschungsgeheimnisses aufzugreifen.	Die Landesregierung setzt sich für eine rechtzeitige Beteiligung des Landesdatenschutzbeauftragten bei Forschungsvorhaben ein.	A.1.IX.11

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt
56	Ich empfehle der Landesregierung, gegenüber den Gesundheitsämtern klarzustellen, dass aus den bei ihnen vorhandenen Patientenakten Auskünfte an Dritte nur mit einer Schweigepflichtentbindungserklärung des jeweiligen Patienten zulässig sind, aus der Umfang und Tragweite hervorgehen müssen.	Die Empfehlung wurde zustimmend zur Kenntnis genommen.	A.1.IX.12
57	Ich empfehle der Landesregierung, bei der Vergabe von Forschungsvorhaben auf die datenschutzrechtlichen Bestimmungen des § 34 Landesdatenschutzgesetzes Mecklenburg-Vorpommern hinzuweisen.	Der Empfehlung wurde gefolgt.	A.1.X.2

2. Öffentlicher Bereich

2.1 Rechtswesen

2.1.1 Klares „Nein“ zur heimlichen Online-Durchsuchung

Der Bundesgerichtshof (BGH) hat sich in seinem Beschluss vom 31. Januar 2007 erstmalig mit der Rechtmäßigkeit von sogenannten Online-Durchsuchungen nach der Strafprozessordnung befasst. Unter Online-Durchsuchungen versteht man den heimlichen Zugriff staatlicher Sicherheitsbehörden auf (personenbezogene) Daten, die in technischen Informationssystemen gespeichert sind. Dies geschieht mittels Installation von Überwachungssoftware etwa mit Hilfe des Internet oder durch die Versendung von E-Mails unter dem Namen einer anderen Behörde. Da viele Menschen auf ihrem Computer sehr private Informationen ablegen, beispielsweise Fotografien, Reiseberichte, Tagebuchaufzeichnungen und persönliche Briefe, wiegt der Eingriff in Grundrechte besonders schwer. So hat der BGH die Auffassung der Datenschutzbeauftragten des Bundes und der Länder bestätigt, dass eine heimliche Online-Durchsuchung im Bereich der Strafverfolgung rechtswidrig ist. Weder die Bestimmungen zur Wohnungsdurchsuchung noch die zur Telekommunikationsüberwachung können zur Rechtfertigung der heimlichen Durchsuchung und Ausforschung privater Computer herangezogen werden.

Seit diesem Zeitpunkt fordert insbesondere das Bundesinnenministerium spezielle Eingriffsgrundlagen, um die Online-Durchsuchung auf einfachgesetzlicher Ebene in der Strafprozessordnung und gegebenenfalls durch Änderung des Grundgesetzes zu legitimieren. Auch im Verfassungsschutzgesetz von Nordrhein-Westfalen ist die Online-Durchsuchung bereits Realität. Am 10. Oktober 2007 verhandelte das Bundesverfassungsgericht über mehrere Verfassungsbeschwerden. Der 1. Senat machte deutlich, dass das Gesetz unpräzise formuliert sei und damit wohl nicht dem Gebot der Normenklarheit entspreche.

Die Datenschutzbeauftragten des Bundes und der Länder haben daher in ihrer Entschließung vom 25./26. Oktober 2007 in Saalfeld (siehe Anlage 1.20) auf Folgendes hingewiesen:

- Bei dem geforderten heimlichen Zugriff auf informationstechnische Systeme geht es nicht nur um „Online-Durchsicht“ als einmalige Durchsuchung und die damit verbundene Übertragung von Festplatteninhalten an die Strafverfolgungs- und Sicherheitsbehörden, sondern auch um die anhaltende Überwachung, um das Ausspähen von Passworten und die Protokollierung aller elektronischen Aktivitäten.
- Es sollen auch Computernetze, Mobiltelefone und Notebooks in die heimliche Durchsuchung einbezogen werden.
- Die Feststellung des Computers einer Zielperson ist technisch ohne Zusatzinformationen nicht ohne Weiteres möglich. Daher ist die Gefahr sehr groß, dass von einer solchen Maßnahme eine Vielzahl von - auch unverdächtigen - Nutzern betroffen sein wird.
- Außerdem steht fest, dass sich der unantastbare Kernbereich privater Lebensgestaltung nicht schützen lässt. Ein automatisierter Kernbereichsschutz ist nicht realisierbar.
- Darüber hinaus wird selbst von Befürwortern der Online-Durchsuchung eingeräumt, dass sich mit Hilfe der entsprechenden Software die auf den Festplatten gespeicherten Inhalte manipulieren lassen, was die Beweiseignung der gewonnenen Erkenntnisse infrage stellt.

Zudem zeigen die bisherigen Erfahrungen, dass sich Maßnahmen, die zunächst nur für einen bestimmten Zweck, beispielsweise zur Terrorbekämpfung, eingesetzt werden sollten, schnell zu einem Standardinstrument der Sicherheitsbehörden entwickelt haben.

Daher bekräftigen die Datenschutzbeauftragten des Bundes und der Länder ihre im Rahmen der 73. Konferenz im März 2007 (siehe Anlage 1.15) erhobene Forderung an die Bundesregierung, die Landesregierungen und die Parlamente, auf die Einführung der repressiven und präventiven Online-Durchsuchung zu verzichten. Sie halten es für zwingend notwendig, dass das Urteil des Bundesverfassungsgerichts in dem Verfahren gegen die im Verfassungsschutzgesetz Nordrhein-Westfalens festgeschriebenen Online-Durchsuchungen abgewartet wird.

2.1.2 Vorratsdatenspeicherung

In meinem Siebten Tätigkeitsbericht habe ich über den Entwurf einer Richtlinie über die Vorratsspeicherung von Daten berichtet (Siebter Tätigkeitsbericht, Punkt III.6), wonach alle Telekommunikations- und Internetanbieter verpflichtet werden, eine Vielzahl von Daten über jeden einzelnen Kommunikationsvorgang über einen längeren Zeitraum zu speichern, ohne dass diese Daten für betriebliche Zwecke, zum Beispiel für die Abrechnung, erforderlich sind. Diese Richtlinie wurde im Februar 2007 von den Justizministern der EU mehrheitlich beschlossen. Obwohl beim Europäischen Gerichtshof gegenwärtig eine Nichtigkeitsklage gegen diese Richtlinie anhängig ist und in der Sachverständigenanhörung des Rechtsausschusses des Deutschen Bundestages am 21. September 2007 überwiegend negative Stellungnahmen zu verzeichnen waren, welche die verfassungsrechtlichen Probleme der geplanten Vorratsspeicherung verdeutlicht haben, wird diese Richtlinie mit dem „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ in deutsches Recht umgesetzt. Der Deutsche Bundestag hat dieses Gesetz am 9. November 2007 beschlossen.

Der Gesetzesentwurf verpflichtet alle Erbringer von öffentlich zugänglichen Telekommunikationsdiensten für Endnutzer, sämtliche Angaben über die Kommunikationsverbindungen ihrer Kunden für die Dauer von sechs Monaten zu speichern. Dies betrifft Anbieter öffentlich zugänglicher Telefondienste (auch Internet-Telefondienste), Anbieter von Diensten elektronischer Post und Anbieter von Internetzugangsdiensten. Nach der Gesetzesbegründung der Bundesregierung folgt hieraus zugleich, dass für den nicht öffentlichen Bereich keine Speicherungspflichten bestehen. Hierunter fallen zum Beispiel unternehmensinterne Netze, Nebenstellenanlagen oder E-Mail-Server von Universitäten ausschließlich für dort immatrikulierte Studierendende oder Bedienstete sowie die Telematikinfrastruktur im Gesundheitswesen.

Zu den umfangreichen Verkehrsdaten der Telefon- und Internetnutzung gehören zum Beispiel Rufnummern oder sonstige Kennungen des anrufenden oder angerufenen Anschlusses, elektronisches Postfach, IP-Adressen, Beginn und Ende der Verbindung und Standorte, wie die genaue Bezeichnung der genutzten Funkzellen.

Aufgrund einer solch weitreichenden Speicherung ist es möglich, Verhaltens- und Bewegungsprofile von Menschen ohne jeden Verdacht einer Straftat zu erstellen. So können Informationen über Geschäftsbeziehungen oder Kontakte zu Ärzten, Psychologen etc. über alle Bürger gesammelt werden. Damit geht einher, dass Berufsgeheimnisse ausgehöhlt werden und journalistische Quellen nicht mehr geschützt sind.

Da eine solche Speicherung der Verkehrs- und Standortdaten aller Teilnehmer elektronischer Kommunikationsdienste pauschal und ohne jeden konkreten Anhaltspunkt für eine konkrete Straftat erfolgen soll, ist sie unverhältnismäßig und somit verfassungsrechtlich bedenklich. Sie verstößt gegen das grundgesetzlich verankerte Fernmeldegeheimnis, das Recht auf informationelle Selbstbestimmung und widerspricht der Rechtsprechung des Bundesverfassungsgerichts, das die Speicherung von Daten auf Vorrat zu nicht hinreichend bestimmbaren Zwecken für verfassungswidrig erklärt hat (Bundesverfassungsgerichtsentscheidung 65, 1, 46 f). Hinzu kommt, dass der Gesetzgeber auch über die europarechtlichen Vorgaben hinausgeht, indem er eine Vorratsspeicherung nicht auf den Zweck der Ermittlung, Feststellung und Verfolgung schwerer Straftaten begrenzt, sondern die Speicherung der Verkehrsdaten auch bei minderschweren Straftaten vorgibt und so dem Grundsatz einer möglichst verfassungsschonenden Umsetzung der Richtlinie nicht ausreichend Rechnung trägt. Außerdem reihen sich neben die Liste der schweren Straftaten auch die Straftaten, die mittels Telekommunikation begangen worden sind.

Auf diese datenschutzrechtlichen Bedenken haben die Datenschutzbeauftragten des Bundes und der Länder unter anderem am 8./9. März 2007 in Erfurt in einer Entschließung der 73. Datenschutzkonferenz (siehe Anlage 1.17) hingewiesen.

Das Gesetz hat inzwischen den Bundesrat ohne Widerspruch passiert.

2.1.3 Entwurf eines Jugendstrafvollzugsgesetzes

Bisher gab es noch kein spezifisches Gesetz für den Jugendstrafvollzug. Dies hat das Bundesverfassungsgericht in seinem Urteil vom 31. Mai 2006 als verfassungswidrig bewertet und den Gesetzgeber aufgefordert, bis zum 31. Dezember 2007 ein entsprechendes Gesetz vorzulegen. Neun Bundesländer, darunter auch Mecklenburg-Vorpommern, haben einen weitgehend einheitlichen Gesetzentwurf erarbeitet.

Gegenüber dem Justizministerium unseres Landes habe ich Folgendes empfohlen:

Es muss auch jugendlichen Strafgefangenen möglich sein, sich an Institutionen wie Volksvertretungen des Bundes und der Länder, das Europäische Parlament oder den Datenschutzbeauftragten zu wenden. Die Wahrnehmung dieser Rechte kann bei jugendlichen Strafgefangenen nicht von der Zustimmung des Personensorgeberechtigen abhängig gemacht werden, wie dies der Gesetzentwurf vorsieht.

Im Hinblick auf die Bedeutung des Grundrechts des Briefgeheimnisses [Art. 10 Grundgesetz (GG)] und des Grundrechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) sollte geregelt werden, dass eine Überwachung des Schriftwechsels und der Ferngespräche nur in Einzelfällen zulässig ist.

Der Zweck und die Voraussetzungen für eine Durchsuchung von Hafträumen sind im Gesetzestext selbst zu regeln.

Nach dem Gesetzentwurf sind gespeicherte personenbezogene Daten in Dateien aus erkennungsdienstlicher Behandlung spätestens nach zwei Jahren zu löschen. Eine weitere Aufbewahrung von erkennungsdienstlichen Unterlagen (ED-Unterlagen) in der Gefangenenpersonalakte ist jedoch aus Datenschutzgründen nicht erforderlich. Die gespeicherten Daten sollten nach der Entlassung oder Verlegung gelöscht werden.

Als besondere Sicherungsmaßnahme soll die „Beobachtung der Gefangenen, auch mit technischen Hilfsmitteln“ zulässig sein. Soweit hierunter auch die Videoüberwachung zu fassen sein sollte, sollten sowohl diese Maßnahme selbst als auch ihre Rahmenbedingungen normenklar im Gesetzestext selbst zum Ausdruck gebracht werden.

Die Einrichtung eines automatisierten Verfahrens, das die Übermittlung oder den Abruf personenbezogener Daten ermöglicht, sollte nur im erforderlichen Umfang eingeführt werden.

Nach dem Gesetzentwurf haben sich beispielsweise Ärzte, Berufspsychologen und Sozialarbeiter gegenüber dem Anstaltsleiter immer schon dann zu offenbaren, wenn und soweit dies für die Aufgabenwahrnehmung der Strafvollzugsbehörde erforderlich ist. Dies bedeutet, dass Erkenntnisse aus der psychologischen Betreuung unmittelbar in Vollzugsentscheidungen aller Art einfließen. Aus datenschutzrechtlicher Sicht müsste jedoch zumindest den Anstaltsärzten und -psychologen eine Abwägungsbefugnis eingeräumt werden, ob Zwecke des Vollzugs die jeweils konkret in Rede stehende Durchbrechung ihrer beruflichen Schweigepflicht rechtfertigen.

Das Justizministerium hat nicht alle meine Empfehlungen in den Gesetzestext übernommen. Korrekturen und Klarstellungen in der Gesetzesbegründung reichen jedoch nicht aus, wie unsere Erfahrungen mit der Gesetzesauslegung durch die Behörden in Mecklenburg-Vorpommern belegen.

2.1.4 DNA-Massentests

Zwei Petenten haben sich im Zusammenhang mit dem Ermittlungsverfahren im Mordfall Simone K. aus folgendem Grund an mich gewandt:

Ein Amtsgericht hatte in der Form eines Serienbriefes mehrere Personen aufgefordert, bis zu einem bestimmten Zeitpunkt zu einem Antrag der Staatsanwaltschaft Stellung zu nehmen, ihnen eine Blutprobe zum Zweck der DNA-analytischen Untersuchung zu entnehmen und das Ergebnis der Untersuchung mit dem DNA-Identifizierungsmuster der am Tatort sichergestellten Spuren zu vergleichen.

Entgegen den Darstellungen des Justizministeriums aus dem Jahre 2004 und gleichlautenden Auskünften im Rahmen eines von mir durchgeführten Kontroll- und Informationsbesuches bei der zuständigen Kriminalpolizeiinspektion im Januar 2005 zu den Massengentests auf freiwilliger Grundlage wurden nunmehr durch die Staatsanwaltschaft zwangsweise Probenentnahmen beantragt, ohne dass es erkennbar weitere Anhaltspunkte als die Nichtteilnahme an der freiwilligen Untersuchung gab.

So stützt sich das Schreiben des Amtsgerichts auf die Ausführungen der zuständigen Staatsanwaltschaft, dass die Betroffenen nicht der freiwilligen Abgabe einer Mundspeichelprobe im Rahmen eines DNA-Massentests zugestimmt haben und zum Tatzeitpunkt in den Bereichen der damaligen Ämter Bad-Sülze, Tribsees, Richtenberg, Niepars, Altenpleen amtlich gemeldet waren.

Auch nachdem molekulargenetische Reihenuntersuchungen durch § 81 h Strafprozessordnung (StPO) auf eine ausdrückliche gesetzliche Grundlage gestellt worden sind, dürfen Personen, die ihre Einwilligung zur Abgabe einer Speichelprobe versagt haben, nicht zwangsweise zu einer Blutprobe herangezogen werden. Aus meiner Sicht müssen weitere verdachtsbegründende Kriterien in Bezug auf den Strafvorwurf hinzukommen, als das bereits dem DNA-Massentest zugrunde liegende Prüfungsmerkmal, dass die betreffende Person zum Tatzeitpunkt in dem festgesetzten geografischen Bereich gemeldet war und einer bestimmten Altersgruppe angehört. Derartige weitere Verdachtsmomente hatte die Staatsanwaltschaft jedoch nicht vorgetragen.

Die Staatsanwaltschaft stützt sich in ihrer Argumentation auf § 81 c Abs. 2 StPO. Danach sind bei anderen Personen als Beschuldigten Untersuchungen zur Feststellung der Abstammung und die Entnahme von Blutproben ohne Einwilligung des zu Untersuchenden zulässig, wenn kein Nachteil für seine Gesundheit zu befürchten und die Maßnahme zur Erforschung der Wahrheit unerlässlich ist. Diese Vorschrift kann - seit Einführung des § 81 h StPO - meines Erachtens nicht mehr isoliert herangezogen werden; andernfalls wäre das Prinzip der Freiwilligkeit reine Makulatur.

Einige Petenten haben - soweit mir bekannt ist - hinsichtlich des Beschlusses des Amtsgerichts, welches die Entnahme einer Blutprobe zum Zweck der DNA-analytischen Untersuchung anordnete, Beschwerde eingelegt. Ich habe das Justizministerium als Fachaufsichtsbehörde gebeten, mir die Entscheidungen des Beschwerdegerichts zu übersenden. Eine Antwort steht noch aus.

2.2 Polizei

2.2.1 Entscheidung des Bundesverfassungsgerichts zur Rasterfahndung

Das Bundesverfassungsgericht hat sich in seinem Beschluss vom 4. April 2006 zur Rasterfahndung geäußert. Dabei bezog es sich auf die in § 31 Polizeigesetz Nordrhein-Westfalen geregelte präventive polizeiliche Rasterfahndung. Das Gericht hat klargestellt, dass diese Art der Rasterfahndung mit dem Grundrecht auf informationelle Selbstbestimmung nur vereinbar ist, wenn eine konkrete Gefahr für hochrangige Rechtsgüter - wie den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person - gegeben ist.

Zum Gefahrenbegriff hat das Bundesverfassungsgericht ausgeführt, dass die Schwelle für eine konkrete Gefahr nicht unterschritten werden darf. Eine allgemeine Bedrohungslage, wie sie im Hinblick auf terroristische Anschläge seit dem 11. September 2001 durchgehend bestanden habe, oder außenpolitische Spannungslagen reichen für die Anordnung der Rasterfahndung nicht aus.

Die der Gefahrenfeststellung zugrunde gelegten Annahmen und Schlussfolgerungen müssen vielmehr nach Auffassung des höchsten deutschen Gerichts auf weiteren konkreten Tatsachen beruhen, etwa solchen, die auf die Vorbereitung oder Durchführung terroristischer Anschläge hindeuten. Solche konkreten Tatsachen hatten jedoch nicht vorgelegen. Damit war klar, dass auch die in Mecklenburg-Vorpommern nach den Anschlägen vom 11. September 2001 durchgeführte Rasterfahndung nicht den Vorgaben des Bundesverfassungsgerichts entsprach.

Zum Zeitpunkt des Gerichtsbeschlusses befand sich der entsprechende Paragraph des Sicherheits- und Ordnungsgesetzes unseres Landes (SOG M-V) gerade im Gesetzgebungsverfahren. Er sah jedoch das Vorliegen einer konkreten Gefahr nicht vor, sondern vielmehr eine Ausweitung der Rasterfahndung. Deshalb habe ich dem Innenausschuss und den Fraktionen des Landtages folgende Empfehlungen gegeben:

- die Einfügung des Erfordernisses der „konkreten“ Gefahr,
- die Herausnahme des Tatbestandsmerkmals „zur Bekämpfung von Straftaten von erheblicher Bedeutung im Sinne des § 49 Nr. 1 und Nr. 3 SOG M-V“,
- die Aufnahme der Verpflichtung zur Benachrichtigung der Betroffenen,
- das Einfügen eines Richtervorbehalts.

Der Landtag ist den ersten beiden Empfehlungen gefolgt. Eine Benachrichtigung Betroffener und ein Richtervorbehalt sind jedoch nicht in den Gesetzestext mit aufgenommen worden. Das halte ich auch weiterhin für verfassungsrechtlich bedenklich.

2.2.2 Zuverlässigkeitsüberprüfungen im Rahmen der Fußball-WM 2006

Während der Fußball-WM 2006 mussten sich Personen, die aus beruflichen Gründen Zugang zu bestimmten Stadionbereichen benötigten (Pressemitarbeiter, Freiwillige und Servicebedienstete aller Art), einer „Zuverlässigkeitsüberprüfung“ durch die Polizeibehörde und die Verfassungsschutzbehörde ihres Bundeslandes unterziehen. Für derart intensive Überprüfungen gibt es noch immer keine gesetzliche Grundlage. Vielmehr wird mit sogenannten informierten Einwilligungserklärungen gearbeitet. Über die Problematik der „Freiwilligkeit“ einer derartigen Einwilligung habe ich bereits in meinem Siebten Tätigkeitsbericht, Punkt 3.1, berichtet.

Beim Landeskriminalamt Mecklenburg-Vorpommern (LKA M-V) habe ich die Akten zu den abgelehnten Personen geprüft: Bei insgesamt 824 Personenüberprüfungen gab es 11 Ablehnungen. Die Entscheidungen entsprachen im Wesentlichen den in den Datenschutzinformationen genannten Ablehnungskriterien. Sie wurden teilweise darauf gestützt, dass die Betroffenen in der Vergangenheit wegen Verbrechen und Vergehen rechtskräftig verurteilt worden waren. In diesen Fällen waren die negativen Voten nachvollziehbar. In anderen Fällen wurden die Ablehnungen auf den Tatbestand der „wiederholten Tatbegehung ohne gerichtliche Verurteilung unter Würdigung der Gesamterkenntnisse“ gestützt.

Gemessen an der ursprünglichen Zielsetzung des Akkreditierungsverfahrens, die Gefahr von Terroranschlägen durch „Innentäter“ in den Fußballstadien zu vermeiden, ist festzustellen, dass bei den Ablehnungsgründen eher Fälle der leichten und mittleren Kriminalität vorherrschten. So wurde beispielsweise auch ein Bewerber, der als zeitlich befristeter Mitarbeiter im Cateringbereich geführt wurde, aufgrund von laufenden Ermittlungen wegen angeblicher exhibitionistischer Handlungen vom LKA M-V abgelehnt.

Des Weiteren habe ich kritisiert, dass eine auf den Einzelfall bezogene schriftliche Dokumentation, welche Gefahr von dem einzelnen Bewerber anlässlich des Einsatzes bei einer Großveranstaltung wie der Fußball-WM 2006 ausgehe, in den Akten fehlt.

1. **Ich empfehle der Landesregierung und dem Landtag, Zuverlässigkeitsüberprüfungen bei (Groß-)Veranstaltungen auf eine spezifische gesetzliche Grundlage zu stellen.**

2.2.3 SOG M-V verabschiedet - trotz datenschutzrechtlicher Bedenken

Der Entwurf eines Vierten Gesetzes zur Änderung des Sicherheits- und Ordnungsgesetzes (SOG M-V) hatte mir im April 2006 zur Stellungnahme vorgelegen. Er enthielt erhebliche Ausweitungen polizeilicher Befugnisse. Exemplarisch möchte ich an dieser Stelle nur drei Bereiche herausgreifen:

- die erhebliche Erweiterung der Videoüberwachung,
- die präventive Telekommunikationsüberwachung,
- den Einsatz eines Automatischen Kfz-Kennzeichen-Lesesystems (AKLS).

In meiner Stellungnahme gegenüber dem Innenministerium unseres Landes und anlässlich der Anhörung vor dem Innen- und Rechtsausschuss des Landtages bin ich auf die datenschutzrechtlichen Aspekte der Änderungen eingegangen. Trotz zahlreicher Bedenken auch anderer Sachverständiger ist das Gesetz nahezu unverändert verabschiedet worden.

Erhebliche Erweiterung der Videoüberwachung

Nach der Neuregelung ist der Einsatz von Videoüberwachungstechnik nunmehr auch bei der wiederholten Begehung von einfachen und mittelschweren Straftaten rechtmäßig. Vorher waren Bildaufzeichnungen nur zulässig, wenn im Einzelfall Anhaltspunkte für die Begehung von Straftaten von erheblicher Bedeutung bestanden. Durch den zusätzlichen Wegfall der weiteren Einschränkung „im Einzelfall“ wird die Schwelle für die Überwachung öffentlich zugänglicher Orte erheblich gesenkt. Einziges - in die Gesetzesbegründung verbannte - Korrektiv ist das Erfordernis, dass die so genannten Kriminalitätsschwerpunkte aufgrund von objektiv nachvollziehbaren ortsbezogenen Lageerkenntnissen zu ermitteln sind.

Als Grund für die Ausweitung der Videoüberwachung benennt die Landesregierung eine geänderte sicherheitspolitische Lage nach den terroristischen Anschlägen in London am 7. Juli 2005. Diese Begründung ist aus meiner Sicht nicht tragfähig, da es in Mecklenburg-Vorpommern keine Kriminalitätsschwerpunkte gibt, die mit denen gewisser Orte und Plätze in einer Millionenmetropole wie London vergleichbar wären.

Zu beachten ist, dass es auch nach den Ausführungen des Bundesverfassungsgerichts im sogenannten Volkszählungsurteil grundsätzlich möglich sein muss, dass sich Bürgerinnen und Bürger frei von staatlicher Beobachtung auf öffentlichen Straßen und Plätzen bewegen können müssen. Nur so sind sie in der Lage, ihre Grundrechte selbstbestimmt in Anspruch zu nehmen. Die Videoüberwachung im öffentlichen Raum betrifft ganz überwiegend völlig unverdächtige Personen und setzt diese der Gefahr der Ausforschung von Lebensgewohnheiten und einem ständig wachsenden Anpassungsdruck aus, ohne dass dem ein adäquater Sicherheitsgewinn gegenübersteht.

Noch zusätzlich wird die Schwelle für eine Videoüberwachung in oder an bestimmten Objekten, wie Verkehrs- oder Versorgungsanlagen und -einrichtungen, öffentlichen Verkehrsmitteln, Amtsgebäuden oder in deren unmittelbarer Nähe gesenkt. Es reicht aus, dass an oder in Objekten dieser Art lediglich Straftaten begangen werden „sollen“; es müssen folglich nicht polizeiliche Lageerkenntnisse den Nachweis erbringen, dass es tatsächlich solche Straftaten gegeben hat und Anhaltspunkte bestehen, dass auch künftig mit der Begehung von Straftaten zu rechnen ist. An diesen gefährdeten Objekten sind sogar Tonaufzeichnungen zulässig, was neben der Bildaufzeichnung noch eine zusätzliche Eingriffsqualität darstellt.

Die Bestimmung, dass der Landesbeauftragte für den Datenschutz unverzüglich von der Anordnung einer Videoüberwachungsmaßnahme zu unterrichten ist, verschafft diesem zwar einen besseren Überblick und eine sofortige Kontrollmöglichkeit, welche und wie viele Überwachungsmaßnahmen im Land angeordnet werden; es ändert aber nichts an der „Tatbestandsseite“, die gerade eine Videoüberwachung unter sehr unscharfen und ausufernd definierten Voraussetzungen zulässt.

Ich halte die Regelung für nicht verfassungsgemäß, da sie den Grundsatz der Verhältnismäßigkeit von polizeilichen Maßnahmen nicht wahrt.

Präventive Telekommunikationsüberwachung

Erstmalig ist in das Sicherheits- und Ordnungsgesetz (SOG M-V) die präventive Telekommunikationsüberwachung eingeführt worden. Bisher gab es eine solche Überwachung nur im Bereich der Strafverfolgung, also in den Fällen, wo bereits ein Ermittlungsverfahren wegen Straftaten von erheblicher Bedeutung gegen einen Beschuldigten lief.

Aus datenschutzrechtlicher Sicht ist es kritisch, eingriffsintensive Maßnahmen immer mehr in das Vorfeld zu verlagern. Der Gesetzestext enthält jetzt eine Formulierung, wonach Daten, bei denen sich nach der Auswertung herausstellt, dass sie dem Kernbereich privater Lebensgestaltung zuzuordnen sind, nicht verwendet werden dürfen, sondern zu löschen sind. Nach der Rechtsprechung des Bundesverfassungsgerichts im Beschluss vom 3. März 2004 zum Außenwirtschaftsgesetz ist es nicht ausreichend, lediglich ein Verwendungsverbot und ein Löschungsgebot zu formulieren. Vielmehr ist bereits die Anordnung der Telekommunikationsüberwachung nicht zulässig, wenn anzunehmen ist, dass bei der Durchführung dieser Maßnahme mit einem Eingriff in den Kernbereich privater Lebensgestaltung zu rechnen ist. Ebenso ist die Maßnahme zu unterbrechen, wenn der Kernbereich tangiert ist. Der Gesetzgeber ist meiner Empfehlung dazu nicht gefolgt.

Einsatz eines automatisierten Kfz-Kennzeichen-Lesesystems (AKLS)

Die Datenschutzbeauftragten des Bundes und der Länder sehen einen anlassfreien und lageunabhängigen Einsatz von automatisierten Kfz-Kennzeichen-Lesesystemen im Straßenverkehr mit Sorge, weil sich diese Maßnahmen zu einem weiteren Schritt zur Überwachung aller Bürgerinnen und Bürger entwickeln können. Es ist zu befürchten, dass mit dem Einsatz der automatisierten Kfz-Kennzeichenerfassung eine neue Infrastruktur geschaffen wird, die künftig noch weit tiefergreifende Eingriffe in das Persönlichkeitsrecht ermöglicht.

Diese Technik erfasst die Kfz-Kennzeichen aller an den Erfassungsgeräten vorbeifahrenden Verkehrsteilnehmer und gleicht sie mit polizeilichen Fahndungsbeständen ab. Schon dieser Abgleich führt zu einem Eingriff in das Recht auf informationelle Selbstbestimmung von Personen, die überwiegend keinen Anlass für eine polizeiliche Verarbeitung ihrer personenbezogenen Daten gegeben haben.

Mit der neuen Vorschrift können Kraftfahrzeuge nicht nur mit dem Fahndungsbestand abgeglichen werden. Der Datenabgleich ist auch mit anderen polizeilichen Dateien erlaubt, „soweit die Dateien zur Abwehr von im Einzelfall oder im Hinblick auf bestimmte Ereignisse allgemein bestehende Gefahren errichtet wurden und der Abgleich zur Abwehr einer solchen Gefahr erforderlich ist“. Diese Voraussetzungen sind viel zu unkonkret, als dass sie eine Einschränkung darstellen. Damit kann der Abgleich mit nahezu jeder Datei durchgeführt werden.

In meiner Stellungnahme hatte ich auch auf die tragenden Gründe des Landesverfassungsgerichts Mecklenburg-Vorpommern zur Schleierfahndung hingewiesen. Dort war eine flächendeckende Überwachung von Bürgern auf Straßen ohne besonderen Anlass als verfassungswidrig abgelehnt worden. Aus den genannten Gründen habe ich auch die Regelung zur Kfz-Kennzeichenerfassung für rechtswidrig erachtet.

2. Ich empfehle der Landesregierung, die neu eingefügten und befristeten Befugnisse gründlich zu evaluieren und auf ihre Erforderlichkeit hin zu überprüfen.

2.2.4 Datenschutz und G8-Gipfel

Der G8-Gipfel im Juni 2007 in Heiligendamm hat nicht nur die Sicherheitsbehörden, sondern auch den Landesbeauftragten für den Datenschutz stark beansprucht.

Ich bin dreimal zu einem Kontroll- und Informationsbesuch bei der Besonderen Aufbauorganisation für den G8-Gipfel (BAO KAVALA) in Waldeck gewesen: am 8. Mai, am 1. Juni und am 20. Juni 2007. Die Kontrollberichte sind im Internet unter www.datenschutz-mv.de abrufbar.

1. Polizeiliche Anhalte- und Sichtkontrollen

Gemäß § 27 a Abs. 1 Nr. 1 Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommern (SOG M-V) darf die Polizei im öffentlichen Verkehrsraum zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung (§ 49) Personen kurzfristig anhalten und mitgeführte Fahrzeuge, insbesondere deren Kofferräume und Ladeflächen, in Augenschein nehmen. Maßnahmen nach Satz 1 Nr. 1 werden durch den Behördenleiter angeordnet, soweit polizeiliche Lageerkenntnisse dies rechtfertigen; die Anordnung ist in örtlicher und zeitlicher Hinsicht zu beschränken.

Die Einsatzbefehle Nr. 1 vom 27. März 2007 und Nr. 2 vom 18. Mai 2007, welche die Anordnung nach § 27 a SOG M-V enthalten, sind mir von der BAO KAVALA übersandt worden. Die örtliche und zeitliche Beschränkung der Maßnahme ist dort enthalten. Auch gehe ich davon aus, dass nach dem polizeilichen Lagebild im Vorfeld und bei der Durchführung des G8-Gipfels hinreichende Erkenntnisse vorlagen, die Straftaten von erheblicher Bedeutung erwarten ließen. Zum Umfang der Maßnahme (es darf lediglich **kurzfristig** angehalten werden; die Kofferräume und Ladeflächen dürfen lediglich **in Augenschein** genommen werden) habe ich aufgrund der mir vorliegenden Petitionen den Eindruck, dass hier häufig die Grenzen des Zulässigen überschritten worden sind.

Das Landesverfassungsgericht hat in seinem Urteil zur sogenannten Schleierfahndung vom 21. Oktober 1999 ausdrücklich betont, dass bei Bürgern, die sich nichts haben zu schulden kommen lassen, grundsätzlich nicht der Kofferraum **durchsucht** werden darf. Infolge des Urteils ist die Norm des § 27 a in das Sicherheits- und Ordnungsgesetz eingefügt worden. Nach mir vorliegenden Informationen sind Personen und Fahrzeuge häufig stundenlang und auch mehrmals täglich durchsucht worden. Dies geschah unter anderem auch durch Polizeieinheiten anderer Bundesländer, denen offensichtlich die spezifischen Besonderheiten des hiesigen Sicherheits- und Ordnungsgesetzes nicht immer geläufig waren.

2. Identitätsfeststellungen gemäß § 29 Abs. 1 Satz 2 Nr. 3 SOG M-V

Nach den mir von der BAO KAVALA übersandten Unterlagen gab es in der Einsatzphase III insgesamt 187 Objekte mit besonderen Schutzmaßnahmen im Sinne des § 29 Abs. 1 Satz 2 Nr. 3 SOG M-V.

Als Objekte werden hier eine Vielzahl von gefährdeten Orten aufgelistet: vom Amtsgericht Rostock über die Firma X GmbH, verschiedene Relaisstellenstandorte der WEMAG, ein Bauunternehmen bis hin zum 13 km langen Sicherheitszaun.

An all diesen 187 Orten und deren Umgebung mussten Personen damit rechnen, dass sie einer Identitätsfeststellung unterzogen werden. Jede Person - dies ist ein Grundsatz in unserem Rechtsstaat - muss sich darauf einstellen können, wann und unter welchen Voraussetzungen sie mit polizeilichen Maßnahmen rechnen muss. Dies sollten sie im Gesetz nachlesen können. Wenn jedoch mehr oder weniger der gesamte Norden unseres Landes mit „gefährdeten Orten“ belegt ist, ist es einer Person schier unmöglich, ihr Verhalten so darauf einzustellen, dass sie nicht einer Identitätsfeststellung unterzogen wird.

Es gab, als der Sicherheitszaun errichtet wurde, viele „Schaulustige“, die sich den Zaun einfach nur ansehen wollten. Hier konnte sich der normale Bürger noch vorstellen, dass der Sicherheitszaun ein gefährdetes Objekt im Sinne des § 29 Abs. 1 Satz 2 Nr. 3 SOG M-V ist und dass man hier nach dem Personalausweis gefragt wird. Musste er aber auch damit rechnen, dass er - ohne dass weitere Anhaltspunkte hinzukommen - durchsucht wird? Die Frage muss bejaht werden.

Nach § 53 Abs. 1 Nr. 3 SOG M-V kann eine Person durchsucht werden, wenn eine Identitätsfeststellung aufgrund des § 29 Abs. 1 Satz 2 Nr. 1, 2 oder 3 (gefährdeter Ort) zulässig ist. Der Sicherheitszaun, auch technische Sperre genannt, ist ein gefährdetes Objekt im Sinne dieser Vorschrift. Die unmittelbare Koppelung der Vorschriften über Identitätsfeststellung und Durchsuchung einer Person, ohne dass hinsichtlich der höheren Eingriffsintensität der Durchsuchung weitere rechtliche Hürden aufgestellt werden, führt zu einem tiefen Eingriff in die Persönlichkeitsrechte. Damit ist es für die Durchsuchung einer Person nicht erforderlich, beispielsweise festzustellen, dass Anhaltspunkte für eine Straftat vorliegen bzw. die Maßnahme zur Abwendung einer im Einzelnen bevorstehenden Gefahr dient.

Als Datenschutzbeauftragter des Landes Mecklenburg-Vorpommern halte ich diese gesetzestechnische Koppelung für äußerst problematisch, da die Durchsuchung im Verhältnis zur Identitätsfeststellung einen tiefergehenden Eingriff in die Persönlichkeitssphäre und damit in das Recht auf informationelle Selbstbestimmung darstellt. Die Maßnahmen können daher auch auf einfache Besucher und Spaziergänger angewandt werden, die sich an oder in der Nähe eines gefährdeten Objekts aufhalten. Angesichts der 187 gefährdeten Objekte, die nicht öffentlich bekannt oder in irgendeiner Weise gekennzeichnet waren, war es auch unbescholtenen Bürgern nicht möglich, sich Identitätsfeststellungen und Durchsuchungen zu entziehen.

Ich habe hierzu eine Petition von Personen vorliegen, die sich dieser oben geschilderten Maßnahme und einer Durchsuchung ihres PKW’s unterziehen mussten, als sie den Zaun besichtigten. Die Petenten haben nach Auskunft der BAO KAVALA Widerspruch gegen die Maßnahmen eingelegt. In der Erwiderung der BAO KAVALA hieß es zur Begründung, die Personen hätten sich angesichts der polizeilichen Maßnahmen aggressiv und unkooperativ gezeigt.

3. Automatisiertes Kfz-Kennzeichen-Lesesystem (AKLS) nach § 43 a SOG M-V

Die BAO KAVALA stützte den automatisierten Kfz-Kennzeichenabgleich auf § 43 a Abs. 2 SOG M-V, da ein Abgleich mit dem Fahndungsbestand (§ 43a Abs. 1 SOG M-V) aus technischen Gründen nicht in Betracht gekommen sei. Danach ist der Abgleich erhobener Kennzeichendaten mit anderen polizeilichen Dateien nur zulässig, soweit die Dateien zur Abwehr von im Einzelfall oder im Hinblick auf bestimmte Ereignisse allgemein bestehende Gefahren errichtet wurden und der Abgleich zur Abwehr einer solchen Gefahr erforderlich ist. Es wurde vorgetragen, dass mit den Dateien Auskunftsdatei „Störer“ (lokale Datei der BAO KAVALA), PB 07 (verdeckte polizeiliche Registrierung) und Gewalttäter links (INPOL-Anwendung) abgeglichen worden sei. Das Ereignis, welches zu schützen war, war die Sicherheit des G8-Gipfels.

Durch den Einsatz des automatisierten Kfz-Kennzeichen-Lesesystems (AKLS) sollte verhindert werden, dass Gewalttäter und Störer anreisen und den Gipfel stören. Ob der Datenabgleich gerade mit den vorgenannten Dateien auch erforderlich war, ist nach der Gesetzesbegründung (Landtagsdrucksache 4/2116 vom 22. Februar 2006, S. 39) stets im Zusammenhang mit dem Errichtungszweck der Datei zu sehen. Es mag sein, dass die Dateien grundsätzlich im Zusammenhang mit dem zu schützenden Ereignis zum Datenabgleich geeignet waren. Das wäre dann der Fall, wenn bestimmte Kriterien einschlägig sind; jedenfalls müssten in den Dateien auch Halterdaten enthalten sein, sonst würde der Abgleich nicht funktionieren. Aus datenschutzrechtlicher Sicht kann ich das jedoch nicht (mehr) beurteilen, da mir die einzelnen Datenbestände nicht zur Verfügung gestellt wurden. Die Daten aus der Auskunftsdatei „Störer“ waren zum Zeitpunkt meines dritten Kontrollbesuches am 20. Juni 2007 bereits gelöscht. Die Datenbestände der Dateien PB 07 und Gewalttäter-links, mit denen abgeglichen worden sein soll, sind mir ebenfalls nicht bekannt. Mündlich wurde mir berichtet, dass die KfZ-Kennzeichen mit rund 1.000 gespeicherten Daten abgeglichen worden seien. Dabei habe es bei den vier Trefferfällen keinen aus der Datei PB 07 gegeben. Diese Fälle wurden jedoch nicht als so gravierend eingestuft, als dass sich weitere polizeiliche Maßnahmen hätten anschließen müssen.

Insgesamt stellt der Einsatz eines AKLS einen Eingriff in das Recht auf informationelle Selbstbestimmung im Sinne des Artikels 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 Grundgesetz (GG) dar. Eingriffe in dieses Grundrecht sind nur zulässig, wenn diese im überwiegenden Allgemeininteresse erfolgen und dem rechtsstaatlichen Gebot der Normenklarheit und Normenbestimmtheit sowie dem Grundsatz der Verhältnismäßigkeit genügen. Insofern müsste der Einsatz bei der BAO KAVALA auch so dokumentiert sein, dass er sowohl aus polizeilicher Sicht als auch aus datenschutzrechtlicher Sicht gerade in Bezug auf seine Grundrechtsrelevanz überprüft werden kann. Dies war mir unter den gegebenen Voraussetzungen nicht möglich.

Bei dem AKLS handelt es sich um ein Datenverarbeitungsverfahren im Sinne des § 47 Abs. 2 SOG M-V in Verbindung mit § 18 Abs. 1 DSG M-V. Somit ist hierfür eine Verfahrensbeschreibung zu erstellen. Inwieweit dieses Verfahren dabei auf Dateien zurückgreift, in denen bereits personenbezogene Daten gespeichert sind, ist dabei unerheblich.

Nach § 18 Abs. 1 DSG M-V ist dabei jede datenverarbeitende Stelle zur Führung eines Verfahrensverzeichnisses, welches aus Beschreibungen für alle automatisierten und nicht-automatisierten Verfahren besteht, verpflichtet. Im § 18 Abs. 1 DSG M-V ist festgelegt, welche Angaben das Verfahrensverzeichnis enthalten muss.

Ebenso ist offen, ob dieses automatisierte Verfahren nach § 19 DSG M-V auch freigegeben worden ist. Nach § 19 Abs. 1 DSG M-V bedarf die Einrichtung oder wesentliche Änderung eines automatisierten Verfahrens zur Verarbeitung personenbezogener Daten der Freigabe durch den Leiter der datenverarbeitenden Stelle oder eines dafür beauftragten Vertreter. Unter Datenverarbeitung fallen dabei alle Formen der Verarbeitung von Daten einschließlich der Erhebung und Nutzung. Die Freigabe hat schriftlich zu erfolgen. Die Freigabe ist Voraussetzung dafür, dass die Verarbeitung personenbezogener Daten mit einem bestimmten Verfahren begonnen werden darf.

Am 25. Juli 2007 hat mir die BAO KAVALA das Verfahrensverzeichnis und die datenschutzrechtliche Freigabeerklärung übersandt. Das Verfahrensverzeichnis datiert vom 18. Juli 2007, die Freigabeerklärung vom 23. Juli 2007. Mithin sind beide Dokumente erst mehr als einen Monat nach dem G8-Gipfel angefertigt worden und verfehlen somit den Zweck, zu dem die Dokumente nach den einschlägigen gesetzlichen Vorschriften erstellt werden müssen. Dies ist eine eklatante Verletzung datenschutzrechtlicher Grundsätze. Da die Daten inzwischen gelöscht sind (die Löschung erfolgte offenbar schon vor dem Anlegen des Verfahrensverzeichnisses), wird jede datenschutzrechtliche Prüfung obsolet.

Nur der Vollständigkeit halber möchte ich darauf hinweisen, dass ich den Vertretern der BAO KAVALA ausdrücklich anlässlich meines dritten Kontroll- und Informationsbesuches gesagt hatte, dass ich mir den Einsatz des AKLS gern in der Einsatzphase vor Ort an der Autobahn ansehen würde. Dies wurde mir allerdings mit der Begründung verweigert, dass das in der heißen Einsatzphase nicht möglich sei. Dies hatte ich hingenommen im Hinblick darauf, dass das System zu einem späteren Zeitpunkt einer datenschutzrechtlichen Prüfung unterzogen werden kann. Diese wurde jedoch durch die Löschung der Daten vereitelt.

4. Observationen

Die BAO KAVALA hat mir im Nachgang zu meinen Kontroll- und Informationsbesuchen mit Datum vom 25. Juni 2007 die Anordnungen zu elf durchgeführten Observationen übersandt.

Gemäß § 33 Abs. 1 Nr. 1 SOG M-V ist ein besonderes Mittel der Datenerhebung die planmäßig angelegte Beobachtung, die innerhalb einer Woche länger als 24 Stunden oder über den Zeitraum einer Woche hinaus vorgesehen ist oder tatsächlich durchgeführt wird (Observation). Gemäß Abs. 2 kann das Mittel der Observation nur angewandt werden, wenn Tatsachen die Annahme der Begehung von Straftaten von erheblicher Bedeutung rechtfertigen und die Aufklärung des Sachverhaltes zum Zwecke der Verhütung solcher Straftaten oder ihrer möglichen Verfolgung auf andere Weise nicht möglich ist.

In den vorliegenden Fällen wurde von der 2. Alternative in zeitlicher Hinsicht Gebrauch gemacht, das heißt, die Observation dauerte länger als eine Woche. Es war immerhin in den vorliegenden Fällen eine Observationsdauer von rund sechs bis sieben Wochen angeordnet worden. Wie intensiv die Personen tatsächlich observiert worden sind, lässt sich aus den Anordnungen nicht entnehmen und ist vom Gesetzestext her auch nicht genau definiert. Dies ist aus datenschutzrechtlicher Sicht ein großes Manko und sollte bei der nächsten Novellierung auf jeden Fall zeitlich konkretisiert werden. Es ist aus rechtsstaatlichen Gründen nicht vermittelbar, warum hier keine zeitliche Obergrenze festgelegt wird.

Gleichzeitig wurde hinsichtlich der observierten Personen gemäß § 33 Abs. 1 Nr. 2 SOG M-V der verdeckte Einsatz technischer Mittel, insbesondere solcher zur Bild- und Tonüberwachung oder Bild- und Tonaufzeichnung angeordnet.

Materiell-rechtliche Voraussetzung einer heimlichen Observation sind Tatsachen, die die Annahme der Begehung von Straftaten von erheblicher Bedeutung rechtfertigen, und die Aufklärung des Sachverhaltes zum Zwecke der Verhütung solcher Straftaten oder ihrer möglichen Verfolgung darf auf andere Weise nicht möglich sein. Die Polizei darf jedoch nicht nur Daten über den vorgenannten Personenkreis erheben, sondern auch über solche, die „mit den vorgenannten Personen hierzu in Verbindung stehen".

Bei den elf observierten Personen handelt es sich um solche, gegen die bereits vor dem G8-Gipfel Strafverfahren geführt worden waren; dies reicht von Verfahren wegen Bildung einer terroristischen Vereinigung bis hin zu Hausfriedensbruch, Nötigung und Diebstahl. Jedoch endeten nicht alle Strafverfahren mit einer Verurteilung. Einige Verfahren sind aktuell noch anhängig. Teilweise sind die Personen auch in einschlägigen Dateien wie „Straftäter linksmotiviert" in INPOL erfasst.

Dann gibt es wiederum andere Personen, die zu den vorstehend genannten Personen in Verbindung stehen. Dies sind zum Beispiel Personen, die Attac-Mitglied sind und an verschiedenen Veranstaltungen wie Camp Inski, Bürgerveranstaltung Bad Doberan oder dem Treffen „Camp AG" und Demonstrationen teilgenommen haben. Auch in einem solchen Fall lautet die in § 33 Abs. 1 Nr. 1 aufzustellende Prognoseentscheidung des Polizeiführers, dass die Annahme aufgestellt werden kann, dass sich eine Person X aufgrund der bisherigen Erkenntnisse und der Verbindung zu oben genannten Personen an Straftaten von erheblicher Bedeutung gemäß § 49 beteiligen wird.

Besonders bei den sogenannten „Verbindungspersonen" steht die Prognoseentscheidung sehr häufig auf äußerst wackeligen Füßen. Diese Personen haben sich in der Vergangenheit nicht strafbar gemacht, aber aufgrund ihrer Verbindungen zu Personen, gegen die Strafverfahren laufen oder gelaufen sind oder die in einschlägigen Dateien gespeichert sind, ebenfalls eine „negative Prognose" bekommen und wurden damit ebenfalls in den Kreis derjenigen Personen einbezogen, die einer Observation unterzogen wurden.

Der Einsatz von heimlichen Ermittlungsmaßnahmen gerade bei „Verbindungspersonen" (die Bezeichnung bezieht sich auf eine Verbindung zum Verdächtigen), auch „Kontakt- und Begleitpersonen" genannt, ist aus Sicht der Datenschutzbeauftragten des Bundes und der Länder besonders kritikwürdig, weil hier häufig jede Tatsachenbasis fehlt, die eine derart eingriffsintensive Maßnahme wie die Observation über mehrere Wochen und der gleichzeitige verdeckte Einsatz technischer Mittel, insbesondere solcher zur Bild- und Tonaufzeichnung, rechtfertigt.

Des Weiteren fehlt in den Anordnungen zur Observation eine **Feststellung** darüber, dass in den betreffenden Observationsfällen die Aufklärung des Sachverhaltes zum Zwecke der Verhütung solcher Straftaten oder ihrer möglichen Verfolgung auf andere Weise nicht möglich ist. Der Gesetzgeber sieht das Mittel der langfristigen Observation lediglich als „ultima ratio" vor. Gerade angesichts polizeilicher Großereignisse mit einer langen „Vorlaufzeit" wird man fordern müssen, dass die (schriftliche) Dokumentation die gesetzlichen Tatbestandsvoraussetzungen ausfüllt.

Schwerwiegende Bedenken bestehen insbesondere im Hinblick auf die fehlende rechtliche Nachprüfbarkeit dieser heimlichen Ermittlungsmaßnahmen - sowohl für den Datenschutzbeauftragten als auch für die Betroffenen selbst. Nach § 34 Abs. 6 SOG M-V ist die an sich rechtsstaatlich erforderliche Unterrichtung des Betroffenen (siehe Abs. 5 Satz 1) dann nicht geboten, wenn keine Aufzeichnungen mit personenbezogenen Daten erstellt oder sie unverzüglich nach Beendigung der Maßnahmen vernichtet worden sind. Die BAO KAVALA hatte mir anlässlich meiner Kontrolle am 20. Juni 2007 mitgeteilt, dass die Aufzeichnungen unverzüglich vernichtet worden seien, da sie für Strafverfolgungszwecke nicht mehr benötigt werden.

Den Personen, die im Vorfeld und während des Gipfels offenbar keine Straftaten von erheblicher Bedeutung begangen haben (trotz gegenteiliger polizeilicher Prognose) - ansonsten hätten die Daten zu Zwecken der Strafverfolgung aufbewahrt werden müssen -, wird jede Möglichkeit nachträglichen gerichtlichen Rechtsschutzes genommen. Dies ist besonders gravierend, da sie für einen langen Zeitraum, rund sechs bis sieben Wochen observiert wurden und sich dies hinsichtlich der tatsächlich observierten Stundenzahl nicht verifizieren lässt. Im Grunde genommen ist somit dieser Personenkreis, bei dem sich kein strafrechtliches Ermittlungsverfahren nach § 33 Abs. 6 Satz 2 SOG M-V anschließt, schlechter gestellt als derjenige, der eine Straftat von erheblicher Bedeutung während des Gipfels begeht, gefasst wird und dann im Zuge des Strafverfahrens durch Einbringung der Beweismittel von seiner Observation erfährt. Ich habe erhebliche Zweifel daran, dass das hier praktizierte Verfahren angesichts der Rechtsprechung des Bundesverfassungsgerichts zu verdeckt durchgeführten Ermittlungsmaßnahmen gerade in Bezug auf die Benachrichtigung Betroffener noch verfassungskonform ist.

Die Möglichkeiten der datenschutzrechtlichen Überprüfung derartiger Observationen sind ebenfalls im Gesetz völlig unzureichend geregelt. Hätte ich bei meinen Kontrollbesuchen bei der BAO KAVALA nicht ausdrücklich nach Observationsanordnungen gefragt, hätte ich nie davon erfahren. Da die personenbezogenen Unterlagen sofort vernichtet worden sind, wäre auch die eigentlich vorgesehene Unterrichtung des Datenschutzbeauftragten nach fünf Jahren, für den Fall, dass die Unterrichtung des Betroffenen fünf Jahre lang - aus Gründen des Schutzes von nicht offen oder verdeckt ermittelnden Polizeibeamten - nicht geschieht, gemäß Abs. 6 in Verbindung mit Abs. 5 nicht erfolgt.

Ich stelle daher fest, dass das in § 34 SOG M-V geregelte Verfahren beim Einsatz heimlicher Ermittlungsmethoden rechtsstaatlichen Anforderungen nicht genügt, und sehe daher dringenden gesetzgeberischen Handlungsbedarf.

3. Ich empfehle der Landesregierung, meine Vorschläge bei der nächsten Novellierung des Sicherheits- und Ordnungsgesetzes zu berücksichtigen.

2.2.5 Videoüberwachung - „East Coast Corner“ in Rostock

Seit der Novellierung des Sicherheits- und Ordnungsgesetzes Mecklenburg-Vorpommern (SOG M-V) vom 10. Juli 2006 ist der Landesbeauftragte für den Datenschutz unverzüglich über Anordnungen zur Videoüberwachung zu unterrichten. Die Polizeidirektion Rostock hat mich dementsprechend schriftlich darüber informiert, dass sie den Bereich rund um das Ladengeschäft „East Coast Corner“ überwacht.

Das überwachte Gebiet umfasst Ladenstraßen, Wohngebietsstraßen sowie Wohn- und Geschäftshäuser. Das Warensortiment von „East Cost Corner“ spricht in erster Linie Personen an, die der rechten Szene zuzurechnen sind. Das Geschäft wird von zwei Personen betrieben, die ebenfalls dem rechtsextremistischen Spektrum angehören. Seit der Geschäftseröffnung kam es mehrfach zu gewalttätigen Auseinandersetzungen, Veranstaltungen und spontanen Kundgebungen. Die Vertreter der Polizeidirektion legten dar, dass die Lage mit herkömmlichen Mitteln nicht mehr „in den Griff“ zu bekommen gewesen sei. In Internetforen seien unter anderem auch Äußerungen gefallen wie „Der Laden soll brennen.“ Da sich das Ladengeschäft in einem Mehrfamilienhaus befindet, waren aus polizeilicher Sicht auch die Anwohner zu schützen. Der Einsatz der Videokamera wurde für einen befristeten Zeitraum angeordnet.

Die Videoüberwachung wird auf § 32 Absatz 3 Satz 3 SOG M-V gestützt. Danach dürfen Bild- und Tonaufzeichnungen offen an oder in bestimmten sogenannten gefährdeten Objekten angefertigt werden, soweit Tatsachen die Annahme rechtfertigen, dass an oder in Objekten dieser Art Straftaten begangen werden sollen, durch die Personen, diese Objekte oder andere darin befindliche Sachen gefährdet sind.

Grundsätzlich stellt die dauerhafte Videoüberwachung einen Eingriff in das allgemeine Persönlichkeitsrecht und damit auch in das Grundrecht auf informationelle Selbstbestimmung dar. Es handelt sich um eine Maßnahme von großer Streubreite, bei der in der Regel auch eine Vielzahl von sich normgerecht verhaltenden Passanten oder Bewohnern betroffen sein kann. Die Maßnahme ist somit nur dann rechtmäßig, wenn sie auch verhältnismäßig ist. Aufgrund mehrerer Petitionen habe ich einen Kontroll- und Informationsbesuch vor Ort durchgeführt. Bei der Präsentation der Videoüberwachungsanlage stellte sich heraus, dass es für den diensthabenden Polizisten durchaus technisch möglich war, in die Wohnungen von Personen hineinzuzoomen, die ungefähr 130 Meter vom Kamerastandort entfernt waren. Es wäre durchaus möglich gewesen, eine Person, die am Fenster steht, zu erkennen.

Das Bundesverfassungsgericht hat in mehreren Entscheidungen den besonderen Schutz des Kernbereichs privater Lebensgestaltung in der eigenen Wohnung betont. Ebenso gibt es eine höchstrichterliche Rechtsprechung, dass Personen an ihrem Arbeitsplatz nicht ohne Grund und ohne ihr Wissen permanent videografiert werden dürfen.

Aus datenschutzrechtlicher Sicht habe ich vorgeschlagen, geeignete technisch-organisatorische Maßnahmen zu treffen, um Eingriffe in das Grundrecht auf informationelle Selbstbestimmung auszuschließen. Unter anderem habe ich empfohlen,

- bestimmte Bereiche wie Privatwohnungen oder Dienstgebäude auszublenden bzw. zu schwärzen,
- den videoüberwachten Bereich mit Hinweisschildern zu kennzeichnen und dabei auch die verantwortliche Behörde anzugeben,
- ein Zugriffsrechtekonzept zu erstellen und umzusetzen, dem zu entnehmen ist, welche Personen welche Zugriffsmöglichkeiten zum System und insbesondere zu den gespeicherten Videodaten haben,
- die zeitliche Befristung der Videoüberwachung zu nutzen, um zu überprüfen, was aus den bisher aufgelisteten strafrechtsrelevanten „Aktivitäten“ geworden ist,
- die Anlage nachträglich auf Konformität mit dem Schutzprofil „Software zur Verarbeitung von personenbezogenen Bilddaten“ zu überprüfen. In diesem Dokument wird beispielsweise beschrieben, wie Aufzeichnungsgeräte für Bild-, Protokoll- und Konfigurationsdaten auszugestalten sind und welche Eigenschaften die Bediengeräte für Nutzer, Administratoren und Revisoren einer solchen Anlage haben müssen (siehe auch Siebter Tätigkeitsbericht, Punkt A.1.II.2.17).

Die Polizeidirektion Rostock hat diese Empfehlungen bis auf die letzte bereits umgesetzt. Sie hat darüber hinaus zugesagt, für künftig zu installierende Videoüberwachungsanlagen das erwähnte Schutzprofil zu berücksichtigen.

2.2.6 Verkehrsüberwachung mittels Videotechnik

Petenten haben mich gebeten, die Zulässigkeit des Einsatzes von Videotechnik bei polizeilichen Verkehrsüberwachungen zu prüfen.

In einem Fall konnte ich feststellen, dass aus einem am Straßenrand abgestellten Fahrzeug alle vorbeifahrenden Fahrzeuge videografiert wurden, um Verstöße gegen die Gurtanlegepflicht und das Handyverbot erfassen und nachfolgend ahnden zu können. Die zuständige Polizeidirektion informierte mich, dass diese Bildaufzeichnung ohne Vorliegen eines konkreten Anfangsverdachtes erfolgte und damit alle Verkehrsteilnehmer betraf.

Bei dieser Verkehrsüberwachung wurde nicht zwischen Verkehrssündern und sich ordnungsgemäß verhaltenden Verkehrsteilnehmern unterschieden. In der Annahme, dass durch die Aufnahmen ahndungswürdige Verstöße erfasst werden, wurde eine Datenerhebung auf Vorrat durchgeführt. Eine verdachtslose Aufzeichnung von Bildern ist rechtswidrig. Daher hat die Polizeidirektion sie eingestellt. Das Innenministerium hat den Vorfall zum Anlass genommen, um die übrigen Polizeidirektionen des Landes noch einmal auf die rechtliche Situation hinzuweisen.

In einem anderen Fall wurde bei einer Verkehrsüberwachung ein Fahrzeugführer videografiert, wobei hier ein begründeter Verdacht eines Verstoßes gegen die Gurtanlegepflicht vorlag. Für die Verfolgung von Verkehrsordnungswidrigkeiten dürfen gemäß § 100 f Abs. 1 Nr. 1 Strafprozessordnung (StPO) in Verbindung mit § 46 des Gesetzes über Ordnungswidrigkeiten (OWiG) Bildaufzeichnungen gegen den Willen des Betroffenen vorgenommen werden, soweit die Erforschung des Sachverhalts auf andere Weise weniger Erfolg versprechend oder erschwert wäre. Der Begriff des Beschuldigten setzt einen bestehenden Anfangsverdacht gegen den Betroffenen voraus.

Sofern Bilder von Personen aufgezeichnet werden, bei denen ein Anfangsverdacht vorliegt, ist indes der Grundsatz der Verhältnismäßigkeit zu beachten. Danach muss die Maßnahme nicht nur zur Erreichung des angestrebten Zwecks geeignet und erforderlich sein, sondern es darf der mit ihr verbundene Eingriff nicht außer Verhältnis zu dem bestehenden Tatverdacht stehen.

Eine Datenerhebung mittels Bildaufzeichnungen dürfte bei Bußgeldverfahren nur für nicht geringfügige Ordnungswidrigkeiten in Betracht kommen. Ob dieses bei der Ahndung von Verstößen gegen die Gurtanlegepflicht oder das Handyverbot der Fall ist, ist aus meiner Sicht fraglich.

Selbst wenn ein konkreter Anfangsverdacht vorliegt und nur die betreffende Person videografiert wird, dürfte der § 100 f Abs. 1 Nr. 1 StPO in Verbindung mit § 46 OWiG somit als Rechtsgrundlage entfallen.

Unser Innenministerium schloss sich meiner Auffassung insoweit an, dass Videoaufzeichnungen ohne Vorliegen eines konkreten Anfangsverdachtes unzulässig sind. Die Frage nach der konkreten Rechtsgrundlage bei einem bestehenden Anfangsverdacht blieb bisher unbeantwortet.

4. Ich empfehle der Landesregierung, gesetzlich die Durchführung von Maßnahmen der Verkehrsüberwachung mittels Videotechnik zu regeln.

2.3 Verfassungsschutz

2.3.1 Papierloses Büro beim Verfassungsschutz

Die Verfassungsschutzbehörde stellte die überwiegend papiergebundene Arbeitsweise auf eine elektronische Bearbeitung um. Ich habe die Behörde bereits im letzten Berichtszeitraum darauf hingewiesen, dass eine elektronische Verarbeitung von personenbezogenen Daten in besonderem Maße in das Recht der Betroffenen auf informationelle Selbstbestimmung eingreift und dass für das Vorhaben eine gesetzliche Grundlage erforderlich ist (siehe Siebter Tätigkeitsbericht, Punkt A.1.II.3.5).

Im Frühjahr 2006 wurde mir das elektronische Vorgangsbearbeitungssystem im Rahmen einer Präsentation vorgeführt. Entgegen der Aussage der Behörde, das Verfahren befinde sich im Testbetrieb, musste ich feststellen, dass mit dem Verfahren bereits seit zwei Jahren im Echtbetrieb gearbeitet wurde. Dies verwundert besonders, da die Verfassungsschutzbehörde meine Auffassung teilt, dass eine spezielle Rechtsgrundlage zwar erforderlich, aber noch nicht vorhanden ist.

Zudem habe ich während der Präsentation festgestellt, dass die erforderlichen technischen und organisatorischen Maßnahmen nur unzureichend umgesetzt waren. Durch das vollständige Scannen der eingehenden Post war beispielsweise nicht auszuschließen, dass personenbezogene Daten in unzulässiger Weise elektronisch verarbeitet werden. Erschwerend kam hinzu, dass nicht mehr erforderliche, elektronisch gespeicherte Dokumente nicht vollständig gelöscht werden konnten. Darüber hinaus mangelte es an dem ordnungsgemäßen Umgang mit Protokolldaten, sodass keine vorschriftsmäßige Revision möglich war. Zum Zeitpunkt der Präsentation lagen weder ein aktuelles Sicherheitskonzept noch eine formelle Freigabe zum Betrieb des Verfahrens vor.

In der Folge hat die Verfassungsschutzbehörde das Sicherheitskonzept mehrfach überarbeitet. Die datenschutzrechtlichen Anforderungen erfüllt das Konzept jedoch noch immer nicht in ausreichendem Maße. Inzwischen hat die Behörde angekündigt, angesichts neuer IT-Verfahren wie der Anti-Terror-Datei ein umfassendes IT-Sicherheits- und Datenschutzkonzept zu erstellen.

Es bleibt festzustellen, dass die Verfassungsschutzbehörde das Verfahren zur elektronischen Vorgangsbearbeitung nach wie vor ohne Rechtsgrundlage betreibt. Mit Blick auf die besondere Eingriffstiefe beim Umgang mit personenbezogenen Daten ist dies ein unhaltbarer Zustand. Ich erinnere daran, dass das Bundesverfassungsgericht in mehreren Entscheidungen ausdrücklich den Schutz des Kernbereichs der persönlichen Lebensgestaltung betont. Ein solcher Kernbereichsschutz ist nach dem derzeitigen Verfahrenstand nicht zu gewährleisten.

5. Ich empfehle dem Landtag erneut, für die elektronische Vorgangsbearbeitung bei der Verfassungsschutzbehörde eine gesetzliche Grundlage zu schaffen, und der Landesregierung, ein umfassendes Sicherheitskonzept für das Verfahren zu erstellen und vollständig umzusetzen.

2.4 Einwohnerwesen/Kommunales

2.4.1 E-Government-Zweckverband

Bereits Ende 2005 haben einige - in der Regel kleinere - Kommunen erwogen, künftig bei E-Government-Projekten zusammenzuarbeiten. Zu diesem Zweck wurde im Frühjahr 2006 der E-Government-Zweckverband Mecklenburg-Vorpommern gegründet. Gemäß seiner Satzung soll sich der Zweckverband der Erschließung und Nutzbarmachung von E-Government-Technologien und -Lösungen für die Städte, Ämter, Gemeinden und Landkreise widmen.

Die angesprochenen E-Government-Projekte werden einen erheblichen Einfluss auf die Verarbeitung personenbezogener Daten in den Verwaltungen der Städte und Gemeinden haben. Ich habe dem Zweckverband deshalb schon frühzeitig die Zusammenarbeit angeboten und auf bereits vorliegende Veröffentlichungen der Datenschutzbeauftragten des Bundes und der Länder zu diesem Thema hingewiesen (siehe 6. Tätigkeitsbericht, Punkt 2.16.2 und 7. Tätigkeitsbericht, Punkt A.II.1.12).

Wie groß der Beratungsbedarf zu Datenschutzfragen tatsächlich ist, wurde insbesondere bei der Umsetzung des novellierten Landesmeldegesetzes deutlich (siehe auch Punkt 2.4.3). Der Zweckverband plante daher, als Dienstleistung für seine Mitglieder einen gemeinsamen Datenschutzbeauftragten zu bestellen, und hat mich um Beratung und Unterstützung bei diesem Vorhaben gebeten.

Ein behördlicher Datenschutzbeauftragter soll Beschäftigter der datenverarbeitenden Stelle sein. Das Landesdatenschutzgesetz lässt aber auch zu, dass mehrere datenverarbeitende Stellen denselben behördlichen Datenschutzbeauftragten als externen Datenschutzbeauftragten bestellen. Insbesondere in kleinen Behörden ist es tatsächlich oft schwierig, Mitarbeiter zu finden, die als Datenschutzbeauftragte eingesetzt werden können, ohne einem Interessenkonflikt zu unterliegen. Deshalb halte ich das Angebot des Zweckverbandes für einen geeigneten Weg, auch in kleinen Kommunen ein angemessenes Datenschutzniveau zu erreichen.

Aus gegebenem Anlass habe ich jedoch darauf hingewiesen, dass die Bestellung eines externen Datenschutzbeauftragten nicht zum vollständigen Verlust der eigenen Datenschutzkompetenz führen darf. Für die Einhaltung der Vorschriften über den Datenschutz bleibt in jedem Fall die datenverarbeitende Stelle verantwortlich. Daher ist auch nach der Bestellung eines externen Datenschutzbeauftragten ein kompetenter Ansprechpartner vor Ort erforderlich, der in die alltäglichen Abläufe der Behörde eingebunden ist. Ich habe deshalb gefordert, dass neben dem externen Datenschutzbeauftragten ein kompetenter Mitarbeiter der Behörde als Stellvertreter des behördlichen Datenschutzbeauftragten (§ 20 Abs. 1 Satz 1 DSG M-V) zu bestellen und mit einem angemessenen Zeitbudget auszustatten ist.

Der Zweckverband ist meiner Empfehlung gefolgt. Im April 2007 wurde eine Juristin als gemeinsame Datenschutzbeauftragte beim Zweckverband eingestellt. Die Behörden, die sich für die gemeinsame Datenschutzbeauftragte als externe Datenschutzbeauftragte entschieden haben, bestellen als Stellvertreter immer einen eigenen Mitarbeiter.

Im Laufe des Jahres 2007 haben schon mehr als zehn Behörden die gemeinsame Datenschutzbeauftragte bestellt. Damit dürfte die Leistungsgrenze dieser Person erreicht sein. Um für weitere Behörden dauerhaft eine kompetente Beratung und ein angemessenes Datenschutzniveau garantieren zu können, wären im Zweckverband weitere Stellen erforderlich.

2.4.2 Protokollierung von E-Mails in einer Stadtverwaltung

Der Finanzausschuss der Bürgerschaft einer Stadt wollte in nichtöffentlicher Sitzung über die Strategie in einem Strafverfahren beraten. Umso mehr waren die Mitglieder erstaunt, dass Teile der vertraulichen Beschlussvorlage noch vor der Sitzung in den Medien zitiert wurden. Schnell kam die Vermutung auf, dass ein Mitarbeiter die Vorlage per E-Mail an eine Zeitungsredaktion gesendet haben könnte. Der Oberbürgermeister ordnete daraufhin an, die Protokolldaten des E-Mail-Verkehrs der Stadtverwaltung an drei Redaktionen lokaler Medien in der fraglichen Woche sicherzustellen und auszudrucken. Die Mitarbeiterinnen und Mitarbeiter der Pressestelle der Stadtverwaltung wurden über dieses Vorgehen informiert, andere Bedienstete offenbar nicht. Daraufhin hat mich ein Mitarbeiter gebeten zu prüfen, ob die Auswertung der E-Mail-Protokolldaten zulässig war.

Eine Kontrolle der Auswertung der Protokolldaten, des E-Mail-Systems sowie des Ratsinformationssystems, mit dem die Vorlagen für die Bürgerschaft, deren Ausschüsse und die Ortsbeiräte bearbeitet werden, ergab folgende Mängel:

Das Ratsinformationssystem wird sowohl von der Stadtverwaltung als auch von der Bürgerschaft genutzt. Beide sind jedoch eigenständige Organe der Gemeinde (§ 21 KV M-V), die Fraktionen zumindest Organteile, mithin aus datenschutzrechtlicher Sicht jede für sich öffentliche Stelle (§ 2 Abs. 1 DSG M-V). Zum gemeinsamen Betrieb des Ratsinformationssystems ist daher eine datenschutzrechtliche Freigabe sowohl durch den Oberbürgermeister als auch durch die Präsidentin der Bürgerschaft erforderlich. Die Präsidentin hatte das Verfahren jedoch nicht freigegeben. Der Oberbürgermeister hatte die Freigabeerklärung zwar unterschrieben, hätte jedoch nicht zustimmen dürfen, weil es weder eine Vorabkontrolle durch den behördlichen Datenschutzbeauftragten noch ein Sicherheitskonzept gab.

Im Ratsinformationssystem werden die Erstellung von Dokumenten und der weitere Umgang damit protokolliert. Dies ist grundsätzlich zulässig, weil dies für die Erfüllung der Aufgaben des Sitzungsdienstes erforderlich ist und weil nur so die Revisionsfähigkeit des Verfahrens sichergestellt werden kann. Die Protokollierung kann zur Überwachung der Beschäftigten und der Mitglieder und Mitarbeiter der Bürgerschaft genutzt werden. Deshalb hätte der Oberbürgermeister sowohl den Personalrat der Stadtverwaltung als auch die Präsidentin der Bürgerschaft umfassend über die Administration und die Protokollierung des Systems informieren müssen. Dem gesamten Protokollierungsverfahren hätten der Personalrat im Rahmen der Mitbestimmung und die Präsidentin durch Unterzeichnung einer Nutzungsvereinbarung ausdrücklich zustimmen müssen. Beides ist nicht geschehen.

Ähnliches wurde auch beim E-Mail-System festgestellt. Auch hier fehlten die erforderlichen Regelungen. Da der Oberbürgermeister den Bürgerschaftsmitgliedern und deren Mitarbeitern mit dem E-Mail-System einen Telekommunikationsdienst anbietet, hat er nach dem Telekommunikationsgesetz Vorkehrungen zu treffen, um das Fernmeldegeheimnis zu wahren. Diese Vorkehrungen können beispielsweise in einer Nutzungsvereinbarung mit der Präsidentin der Bürgerschaft geregelt werden. Eine solche Nutzungsvereinbarung existierte jedoch nicht. Aber auch für die Mitarbeiter der Stadtverwaltung war die E-Mail-Nutzung unklar. Den bestehenden Dienstanweisungen und -vereinbarungen war nicht zweifelsfrei zu entnehmen, ob das E-Mail-System nur zu dienstlichen Zwecken oder auch privat genutzt werden darf. Private Korrespondenz war somit nicht sicher auszuschließen. Kontrollen in diesem Bereich sind daher für den Dienstherrn unzulässig, da hier ebenfalls das Fernmeldegeheimnis gilt.

Somit greift die Kontrolle der E-Mail-Protokolle unzulässig in die Rechte der Betroffenen ein. Unter diesen Umständen durfte der Oberbürgermeister die E-Mail-Protokolle nicht speichern und nicht auswerten.

Ich habe daher empfohlen, die E-Mail-Protokolle der Staatsanwaltschaft im Rahmen eines Ermittlungsverfahrens gegen Unbekannt wegen Geheimnisverrats zu übergeben und alle in der Verwaltung vorhandenen Kopien zu löschen. Darüber hinaus sollte dieser Fall zum Anlass genommen werden, die Dienstanweisungen und -vereinbarungen zu präzisieren. Sie müssen ganz klar regeln, wie mit Protokolldaten verfahren wird und ob die private Nutzung des E-Mail-Systems zulässig ist. Gegebenenfalls ist mit jedem Bediensteten, der das E-Mail-System privat nutzen möchte, eine Vereinbarung abzuschließen, in der er sich mit Kontrollmaßnahmen einverstanden erklärt. In Nutzungsvereinbarungen mit der Präsidentin der Bürgerschaft ist insbesondere festzulegen, wie mit Protokolldaten verfahren wird und wie die Systeme administriert werden. Außerdem sind für das Ratsinformationssystem und das E-Mail-System Datenschutz- und IT-Sicherheitskonzepte zu erstellen. Die Vorabkontrolle ist nachzuholen.

Der Oberbürgermeister hat die Protokolle gelöscht und zugesagt, meine Empfehlungen umzusetzen. Mir ist mittlerweile ein umfassendes Sicherheitskonzept vorgelegt worden. Außerdem ist geplant, einen IT-Sicherheitsbeauftragten zu bestellen.

6. Ich empfehle der Landesregierung, im Rahmen der Kommunalaufsicht verstärkt auf die Einhaltung von Datenschutzvorschriften aus dem Telekommunikations- und Medienrecht zu dringen. Dabei sollte die 2007 überarbeitete Orientierungshilfe „Datenschutzgerechte Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz“ der Datenschutzbeauftragten des Bundes und der Länder beachtet werden. Besondere Aufmerksamkeit ist geboten, wenn kommunale Vertretungen die technische Infrastruktur der Stadt- und Gemeindeverwaltungen mit nutzen.

2.4.3 Melderegister: Elektronisches Auskunftsverfahren und zentrales Informationsregister

In meinem 7. Tätigkeitsbericht hatte ich bereits ausführlich über die geplante Modernisierung des Meldewesens berichtet (siehe dort Punkt A.II.1.4).

Von besonderer datenschutzrechtlicher Relevanz ist das zentrale Informationsregister (ZIR), das vom Land gemäß § 3 a Landesmeldegesetz (LMG M-V) für Datenübermittlungen im automatisierten Verfahren einzurichten ist. Das Innenministerium unseres Landes hat die Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH (DVZ M-V GmbH) mit der Entwicklung und dem Betrieb des ZIR beauftragt. Behörden und öffentliche Stellen können dort jederzeit Meldedaten nach den Vorgaben des LMG M-V abrufen. Auch Private mit einem Internetzugang erhalten über das Dienstleistungsportal des Landes Meldedaten aus dem ZIR auf elektronischem Wege, natürlich nur im Umfang einer einfachen Melderegisterauskunft.

Um die Vertraulichkeit und die Integrität der Meldedaten im gesamten Verfahren zu gewährleisten, waren zahlreiche technische und organisatorische Maßnahmen zu treffen. So war sicherzustellen, dass die Meldedaten im ZIR jederzeit richtig und aktuell sind, also immer ein genaues Spiegelbild der in den Meldebehörden gespeicherten Daten darstellen. Zu diesem Zweck muss ein regelmäßiger Datenabgleich stattfinden.

Die Datenschutzbeauftragten des Bundes und der Länder hatten schon in ihrer Entschließung vom 15. Dezember 2005 gefordert, für derartige E-Government-Projekte den OSCI-Standard (Online Services Computer Interface) zu nutzen (siehe 7. Tätigkeitbericht, Anlage 23). Dieser Empfehlung ist das Innenministerium gefolgt und hat mit der sogenannten Kommunikationsbox eine IT-Komponente entwickeln lassen, mit der eine OSCI-konforme Datenübermittlung von den Meldebehörden an das ZIR ermöglicht wird. Auf diese Weise werden die Anforderungen der 1. und der 2. Bundesmeldedatenübermittlungsverordnung bezüglich Signatur und Verschlüsselung vollständig umgesetzt.

OSCI-XMeld ist die von der Bundesvereinigung der kommunalen Spitzenverbände herausgegebene Beschreibung des Datensatzes für die Datenübermittlung im Bereich des Meldewesens. OSCI-Transport ist der vom Kooperationsausschuss ADV Bund/Länder/Gemeinden herausgegebene Standard für ein Datenübermittlungsprotokoll.

Aber auch in den Meldebehörden des Landes waren erhebliche Anstrengungen nötig, um ein ausreichendes IT-Sicherheits- und Datenschutzniveau zu gewährleisten. Um möglichst einheitlich hohe Standards umzusetzen, hat die DVZ M-V GmbH gemeinsam mit mir umfassende Checklisten für die Meldebehörden entwickelt. Diese Checklisten enthalten Empfehlungen zur Herstellung bzw. Aufrechterhaltung und zur Prüfung von IT-Sicherheit und Datenschutz. Sie orientieren sich an den Grundschutzkatalogen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und werden in Anlehnung an die BSI-Standards 100-1 und 100-2 abgearbeitet. Ich habe bereits angekündigt, in Meldebehörden stichprobenartig zu prüfen, ob die in den Checklisten beschriebenen Maßnahmen umgesetzt wurden.

Mit den Checklisten wird der Forderung des Landesdatenschutzgesetzes nach einem Sicherheitskonzept für die Meldebehörden weitgehend Rechnung getragen. Selbstverständlich wurde auch für die zentralen Komponenten des Verfahrens ein umfassendes Sicherheitskonzept erstellt und umgesetzt.

Vor der Inbetriebnahme habe ich alle Meldebehörden daran erinnert, dass sie das neue Verfahren für den eigenen Verantwortungsbereich formell nach den Vorschriften des § 19 Abs. 1 DSG M-V freigeben müssen.

§ 19 Abs. 1 DSG M-V: Freigabe

Die Einrichtung oder die wesentliche Änderung eines automatisierten Verfahrens zur Verarbeitung personenbezogener Daten bedarf der Freigabe durch den Leiter der datenverarbeitenden Stelle oder einen dafür beauftragten Vertreter. Die Freigabe hat schriftlich zu erfolgen.

Problematisch war die Tatsache, dass die Sicherheit und Datenschutzkonformität der zentralen Teile des Verfahrens von den Meldebehörden nur schwer zu beurteilen war, die Verantwortung für die Meldedaten dennoch bei den Meldebehörden liegt. Vor diesem Hintergrund habe ich folgendes Verfahren vorgeschlagen:

Das Innenministerium erstellt gemeinsam mit der DVZ M-V GmbH die Verfahrensbeschreibungen für die zentralen Verfahrensabschnitte wie ZIR und Auskunftsverfahren, gibt diese separat zur Nutzung frei und führt die Vorabkontrolle für das gesamte Verfahren durch.

§ 19 Abs. 2 DSG M-V: Vorabkontrolle

Vor der Einrichtung oder wesentlichen Änderung eines Verfahrens nach Absatz 1,
1. auf das § 17 Abs. 1 Anwendung findet oder
2. in dem Daten im Sinne von § 7 Abs. 2 verarbeitet werden,

ist dem behördlichen Datenschutzbeauftragten Gelegenheit zur Prüfung innerhalb einer angemessenen Frist zu geben, ob die Datenverarbeitung zulässig ist und die vorgesehenen Maßnahmen nach den §§ 21 und 22 ausreichend sind. Satz 1 gilt nicht für den Abruf aus Datenbeständen, die jedermann ohne oder nach besonderer Zulassung zur Benutzung offen stehen oder deren Veröffentlichung zulässig wäre.

Alle Dokumente werden den Meldebehörden zur Verfügung gestellt, damit diese in der Lage sind, das komplette Verfahren aus datenschutzrechtlicher und sicherheitstechnischer Sicht zu beurteilen. Die Meldebehörden erstellen Verfahrensbeschreibungen für ihre lokal eingesetzten Softwarekomponenten. Nach Vorlage aller Unterlagen bei den Meldebehörden sind diese dann in der Lage, die Freigabe für das Verfahren zu erteilen.

Ende Dezember 2006 habe ich einen Workshop durchgeführt, in dem ich den zahlreich erschienenen Mitarbeitern der Meldebehörden das gesamte Prozedere nochmals detailliert erläutern konnte. Mein Vorschlag wurde von allen Beteiligten akzeptiert und meine Empfehlungen vollständig umgesetzt.

Im Ergebnis der gemeinsamen Anstrengungen konnten die neuen automatisierten Verfahren des Meldewesens pünktlich zum Jahresbeginn 2007 in Betrieb genommen werden. Eine intensive datenschutzrechtliche Begleitung wird aber auch weiterhin erforderlich sein. So ist beispielsweise die Integration des Bezahlsystems (E-Payment) noch nicht vollständig abgeschlossen und zahlreiche Details der Melderegisterauskünfte an Behörden sind noch umzusetzen.

2.4.4 Veröffentlichung der Meldedaten aller Einwohner in einer Gemeindechronik

Eine Gemeinde gab eine Ortschronik heraus, die unter anderem personenbezogene Daten aller Einwohner enthielt. Die betreffenden Angaben entstammten dem Melderegister der Meldebehörde und wurden dem Bürgermeister der Gemeinde beziehungsweise den Ortschronisten übermittelt.

Nach § 31 Abs. 8 Landesmeldegesetz (LMG) können Daten aus dem Melderegister unter anderem einem Bürgermeister übermittelt werden, wenn dies zur Aufgabenerfüllung erforderlich ist. Die Erarbeitung einer Ortschronik gehört zu den freiwilligen Selbstverwaltungsaufgaben nach § 2 der Kommunalverfassung des Landes Mecklenburg-Vorpommern (KV M-V). Die Erarbeitung der Chronik liegt unbestritten im Interesse des Gemeinwohls, da durch sie eine geschichtliche Aufarbeitung der bisherigen Gemeindeentwicklung erfolgt. Dieses Interesse reicht jedoch nicht aus, um alle Namen der in der Gemeinde lebenden Personen zu veröffentlichen. Nur wenn das öffentliche Interesse gegenüber dem Grundrecht auf informationelle Selbstbestimmung und damit dem Recht des Einzelnen auf seine personenbezogenen Daten überwiegt, wäre die Übermittlung der Melderegisterdaten zum Zweck der Veröffentlichung in der Chronik zulässig.

Analog verhält es sich bei der Melderegisterauskunft an Ortschronisten. Nach § 34 Abs. 3 LMG kann die Meldebehörde diesen Auskunft über eine Vielzahl nicht namentlich bezeichneter Einwohner (Gruppenauskunft) geben, soweit dies im öffentlichen Interesse liegt. Das öffentliche Interesse erstreckt sich jedoch nicht auf die namentliche Nennung aller Einwohner in der Chronik, da hier der Persönlichkeitsschutz und damit das Recht auf informationelle Selbstbestimmung der Betroffenen überwiegt. Eine Veröffentlichung der personenbezogenen Daten war daher unzulässig.

Der Bürgermeister hat zugesagt, die Einwohnerliste aus der Chronik zu entfernen.

2.4.5 Herausgabe von Meldedaten zur Begrüßung von Neugeborenen

Eine von Müttern gegründete Initiative hat sich zum Ziel gesetzt, alle Neugeborenen einer Stadt zu begrüßen. Zu diesem Anlass sollte jedem Kind ein kleines Geschenk überreicht werden. Außerdem wollten die Mütter im Bedarfsfall Informationen über und Kontakte zu einer öffentlich geförderten Beratungsstelle vermitteln (siehe auch Punkt 2.8.4). Um dieses durchführen zu können, wurde die Stadtverwaltung um Informationen über jedes neu geborene Kind gebeten.

Es war zu prüfen, inwieweit eine Auskunft über eine Vielzahl nicht namentlich bezeichneter Einwohner (Gruppenauskunft) ohne vorherige Einholung einer Einwilligung gegeben werden darf. Eine Gruppenauskunft darf nach § 34 Abs. 3 Landesmeldegesetz (LMG) nur erteilt werden, wenn ein öffentliches Interesse an der Weitergabe dieser personenbezogenen Daten besteht. Ein öffentliches Interesse in diesem Sinne liegt dann vor, wenn die Datenübermittlungen Belange der Allgemeinheit betreffen und nicht nur im Interesse eines Einzelnen liegen. Ein öffentliches Interesse ist regelmäßig bei Datenübermittlungen für Zwecke der wissenschaftlichen Forschung oder die Tätigkeit caritativer Einrichtungen anzunehmen.

Um dem Anliegen dennoch gerecht zu werden, ersucht die Stadtverwaltung die betroffenen Eltern schriftlich um die Einwilligung zur Übermittlung ihrer personenbezogenen Daten. So können die Eltern selbst entscheiden, ob ihre personenbezogenen Daten zweckgebunden an die Initiative übermittelt werden. Ich habe diese Vorgehensweise aus datenschutzrechtlicher Sicht begrüßt.

2.4.6 Verwaltungsabkommen zur Mitnutzung der zentralen Erstaufnahmeeinrichtung durch die Hansestadt Hamburg

Für die Erstunterbringung von Asylbegehrenden nutzt die Freie und Hansestadt Hamburg (FHH) seit Ende 2006 die Einrichtung des Amtes für Migration und Flüchtlingsangelegenheiten (AMF) in Nostorf-Horst als Wohnaußenstelle. Unterzubringenden Ausländern wird dabei nach kurzer Erstaufnahme in Hamburg für einen bestimmten Zeitraum eine Wohneinrichtung beim AMF zur Verfügung gestellt (sogenannter Hotelbetrieb). Die FHH und das Land Mecklenburg-Vorpommern haben hierzu eine Verwaltungsvereinbarung geschlossen.

Für die ausländerbehördlichen Angelegenheiten der hamburgischen Asylbegehrenden und für die Durchführung des Asylbewerberleistungsgesetzes bleibt die Behörde für Inneres der FHH verantwortlich. Sie führt deshalb beim AMF regelmäßige Sprechzeiten durch. Zu prüfen war vor diesem Hintergrund, ob die einzelnen Mitarbeiter nur auf die für sie jeweils erforderlichen Daten zugreifen konnten.

Das AMF verarbeitet mit einer Datenbankanwendung die personenbezogenen Daten, die für die Unterbringung, Versorgung und Betreuung der Asylbegehrenden erforderlich sind. Die technische Realisierung des gesamten Verfahrens entspricht den datenschutzrechtlichen Anforderungen bereits sehr weitgehend. Während meines im Dezember 2006 durchgeführten Kontroll- und Informationsbesuches konnte ich feststellen, dass die Mitarbeiter des AMF und die der Behörde für Inneres tatsächlich nur auf die Datenbestände zugreifen können, die für die Erfüllung der jeweiligen Fachaufgaben erforderlich sind. Der Datenbankserver ist zudem im Hochsicherheitsbereich der DVZ M-V GmbH untergebracht. Es kann weitgehend sichergestellt werden, dass die in § 21 Abs. 2 Nr. 1 DSG M-V geforderte Vertraulichkeit personenbezogener Daten gewährleistet wird.

Solange mit dem AMF und der Behörde für Inneres lediglich zwei Nutzer auf den zentralen Datenbestand zugreifen und eine länderspezifische Differenzierung nur zwischen Hamburg und Mecklenburg-Vorpommern erforderlich ist, kann der differenzierte Zugriff durch Vergabe entsprechender Zugriffsrechte mit vertretbarem Aufwand realisiert werden. Da jedoch geplant ist, den sogenannten Hotelbetrieb auch anderen Bundesländern anzubieten, wird diese Lösung auf Dauer nicht ausreichend sein. Künftig sollte eine mandantenfähige Datenbank verwendet werden, bei der jeder Vertragspartner (d. h. jedes Bundesland) einen Mandanten zugewiesen bekommt.

Nach § 1 Ausländerdateienverordnung (AuslDatV) führt das AMF zwei Dateien unter der Bezeichnung „Ausländerdatei A“ und „Ausländerdatei B“. Daten aus der Ausländerdatei A dürfen nach § 5 AuslDatV in die Ausländerdatei B übernommen werden, wenn der Ausländer gestorben oder aus dem Bezirk der Ausländerbehörde fortgezogen ist. Die Gründe hierfür sind in der Datei entsprechend zu vermerken. Während meines Besuchs beim AMF stellte ich fest, dass nicht sichergestellt war, dass der Grund, der zu dem Datensatzwechsel führte, eingegeben und revisionssicher festgehalten wird. Meine hierauf ausgesprochene Empfehlung hat das AMF inzwischen umgesetzt. Danach kann ein Datensatzwechsel jetzt nur dann erfolgen, wenn eine Begründung für diesen Wechsel durch den zuständigen Bearbeiter eingegeben wird. Der Vorgang wird revisionssicher protokolliert.

Das AMF verarbeitet zusätzliche personenbezogene Daten, die für die Aufgabenerfüllung erforderlich sind, aber nicht in der AuslDatV mit aufgeführt sind. Hierzu gehören unter anderem auch Gesundheitsdaten und Angaben zur Volkszugehörigkeit. Diese Daten gelten als besonders sensibel und dürfen nach § 7 Abs. 2 DSG M-V nur dann verarbeitet werden, wenn eine Rechtsvorschrift dieses ausdrücklich erlaubt. Die AuslDatV sieht diese Datenverarbeitung indes nicht vor. Nach § 7 Abs. 3 Nr. 1 DSG M-V dürfen solche sensiblen Daten aber auch dann verarbeitet werden, wenn der Betroffene ausdrücklich eingewilligt hat. Aus diesem Grund gibt das AMF nunmehr an die Betroffenen in der jeweiligen Landessprache eine schriftliche Information aus, in der über die erbetene Einwilligung aufgeklärt wird. Sofern ein Asylbegehrender die Zustimmung zur Datenverarbeitung verweigert, dürfen die betreffenden Daten nicht verarbeitet werden.

2.4.7 Mängel beim elektronischen Reisepass

Elektronische Reisepässe mit biometrischen Merkmalen werden in Deutschland seit November 2005 ausgegeben. Zunächst wurden auf dem elektronischen Speicherchip des Reisepasses - einem sogenannten RFID-Chip (siehe dazu auch Punkt 2.15.4) - neben dem Namen, dem Geburtstag und dem Geschlecht auch biometrische Merkmale des Gesichts des Passinhabers gespeichert. Über die eher fragwürdige Leistungsfähigkeit der biometrischen Verfahren habe ich in meinem Siebten Tätigkeitsbericht unter Punkt A.1.II.3.3 berichtet.

Seit dem 1. November 2007 werden in den Chips der elektronischen Reisepässe zusätzlich die Daten zweier Fingerabdrücke des Betroffenen gespeichert. Dem Start des produktiven Betriebs in den Passbehörden gingen zwischen dem 1. März und dem 30. Juni 2007 bundesweit zahlreiche Tests und Feldversuche in ausgewählten Passbehörden voraus. Das Erprobungsverfahren war im Passgesetz geregelt. Mit dem Terrorismusbekämpfungsergänzungsgesetz war für den Zeitraum der Tests hierfür der § 23 a Passgesetz eingefügt worden.

§ 23 a Passgesetz

Zum Zwecke der Erprobung der zur Speicherung zweier Fingerabdrücke im Pass erforderlichen Verfahren sind Testmaßnahmen durchzuführen. Diese dienen der Überprüfung der Funktionalität, Interoperabilität, Stabilität und Sicherheit der einzelnen Bestandteile des Systems sowie ihres funktionalen und technischen Zusammenwirkens. Gleichfalls sind die Auswirkungen der Neuerungen auf die Abläufe des Verfahrens festzustellen.

Auf meine Anfrage teilte mir unser Innenministerium im Februar 2007 mit, dass auch eine Stadt in Mecklenburg-Vorpommern an den Tests teilnimmt. Bereits während der Testphase habe ich daraufhin den Bürgermeister der Stadt zu den datenschutzrechtlichen Rahmenbedingungen beraten. Ich habe darauf hingewiesen, dass für das Passantragsverfahren ein Sicherheitskonzept gemäß § 22 Abs. 5 DSG M-V zu erstellen ist, die Verfahrensbeschreibung nach § 18 DSG M-V erforderlich ist, eine Vorabkontrolle gemäß § 19 Abs. 2 DSG M-V durchzuführen und das gesamte Verfahren förmlich freizugeben ist (§ 19 Abs. 1 DSG M-V). Kurz vor dem Start des Produktivbetriebs war der Presse zu entnehmen, dass die Erprobungsphase in der betreffenden Passbehörde „super gelaufen“ wäre. Etwa 200 Personen hätten sich an den Tests beteiligt, ohne dass technische Probleme aufgetaucht wären.

Mit einem Kontroll- und Informationsbesuch in der Passbehörde der Stadt wollte ich mich Anfang November 2007 davon überzeugen, dass das gesamte Verfahren der Passbeantragung den gesetzlichen Vorgaben entsprechend umgesetzt wurde. In der Passbehörde habe ich geprüft, ob die technischen und organisatorischen Maßnahmen den Anforderungen entsprechen, die beispielsweise in der Passdatenerfassungs- und Übermittlungsverordnung (PassDEÜV) und in den vom Bundesamt für Sicherheit in der Informationstechnik (BSI) ausgearbeiteten technischen Sicherheitsrichtlinien vorgegeben sind.

Das Ergebnis war besorgniserregend. Keines der bereits während der Testphase angemahnten Dokumente (z. B. Sicherheitskonzept, Verfahrensbeschreibung, Freigabeerklärung) war vorhanden. Weder die Mitarbeiter der Passbehörde noch das Administrationspersonal konnten darüber Auskunft geben, ob das bereits im Wirkbetrieb befindliche Verfahren den Anforderungen der PassDEÜV und der BSI-Richtlinien genügt. Die Kontrolle offenbarte zudem massive Sicherheitsmängel beim Umgang mit den bereits erfassten Passantragsdaten. Vertraulichkeit und Integrität der Daten waren weder bei der vorübergehenden Speicherung auf den Servern der Passbehörde noch bei der Übertragung der Daten an den Passhersteller (die Bundesdruckerei) gewährleistet. Im Ergebnis konnte nicht mit Sicherheit ausgeschlossen werden, dass der Bundesdruckerei unrichtige oder gar vorsätzlich gefälschte Passantragsdaten übermittelt werden können. Dem Bürgermeister der Stadt sprach ich daraufhin eine förmliche Beanstandung aus und empfahl, dass Verfahren auszusetzen. Ich forderte ihn auf, die Mängel unverzüglich zu beheben und informierte den Innenminister als oberste Fachaufsichtsbehörde über die Beanstandung.

In der Hoffnung, dass es sich bei den Mängeln in der kontrollierten Passbehörde um eine Ausnahme handelt, forderte ich einige stichprobenhaft ausgewählte Passbehörden auf, mir die notwendigen Verfahrensunterlagen zur Prüfung zuzusenden. Aber auch diese Passbehörden konnten keine oder nur unvollständige Unterlagen zur Verfügung stellen. Ich musste deshalb davon ausgehen, dass in keiner Passbehörde des Landes der Datenschutz im Passantragsverfahren in angemessener Weise sichergestellt ist.

Sehr verwundert hat mich dann jedoch die Reaktion des Innenministers, insbesondere mit Blick auf seine Rolle als oberste Fachaufsichtsbehörde (§ 86 Kommunalverfassung M-V). Er teilte mir mit, dass in seinem Hause die Einzelheiten des Verfahrens nicht bekannt wären, da allein die Kommune für das eingesetzte Verfahren verantwortlich wäre. Aufgrund der fehlenden Detailkenntnis könne er nicht feststellen, ob es sich bei der Aufnahme biometrischer Daten um eine wesentliche Änderung des Verfahrens im Sinne des Landesdatenschutzgesetzes handelt. Die von mir empfohlene vorübergehende Einstellung des Passantragsverfahrens bis zur Behebung der Mängel lehnte er ab.

Im Ergebnis weiterer Gespräche zwischen meiner Behörde und dem Innenministerium wurde dann jedoch vereinbart, die Passbehörden bei der Beseitigung der festgestellten Mängel gemeinsam zu unterstützen. Alle Passbehörden erhielten vom Innenminister zunächst ein mit mir abgestimmtes Schreiben mit detaillierten Hinweisen zu den von ihnen zu treffenden technischen und organisatorischen Maßnahmen. Darüber hinaus wurde eine Kommune ausgewählt, in der mit meiner Unterstützung möglichst kurzfristig versucht werden soll, alle erforderlichen technischen und organisatorischen Maßnahmen so umzusetzen, dass das Verfahren den Vorgaben entsprechend betrieben wird. Die dabei entstandenen Unterlagen sollen dann als Musterdokumente für alle anderen Passbehörden dienen.

Schon lange vor der Einführung elektronischer Reisepässe mit biometrischen Merkmalen wurde über Sicherheitsfragen diskutiert. Forscher des durch die Universität Frankfurt koordinierten Forschungsnetzwerks FIDIS (Future of Identity in the Information Society, www.fidis.net) hatten im November 2006 in ihrer Budapest-Erklärung (abzurufen unter http://www.fidis.net/fileadmin/fidis/press/budapest_declaration_on_MRTD.de.pdf) auf Schwächen des europäischen Reisepasses hingewiesen und das Fehlen einer angemessenen Sicherheitsarchitektur beklagt. Sie kommen dabei anders als die Bundesregierung zu dem Schluss, dass die Implementierung des europäischen Passes Techniken und Standards enthält, die für den Verwendungszweck ungeeignet seien. In der Folge hat die Presse berichtet, dass das Kopieren des RFID-Chips gelungen sei und dass sich Angreifer Zugang zu den Passdaten verschafft hätten.

7. Ich empfehle der Landesregierung, künftig die Kommunen bei der Einführung zentraler E-Government-Verfahren frühzeitig bei der Umsetzung datenschutzrechtlicher Anforderungen und die Passbehörden des Landes bei der Umsetzung der datenschutzrechtlichen und der sicherheitstechnischen Vorgaben beim Betrieb des Passantragsverfahrens zu unterstützen.

2.5 Finanzwesen

2.5.1 Einführung einer bundeseinheitlichen Steueridentifikationsnummer

Am 1. Juli 2007 sind auf Bundesebene Verordnungen in Kraft getreten, welche die Einführung der Steueridentifikationsnummer (Steuer-ID) regeln. Gesetzliche Grundlage ist § 39 b Abgabenordnung. Mit der Einführung einer persönlichen Steuer-ID soll der Steuerbetrug deutlich erschwert werden und vor allem auch ein Steuerabgleich möglich sein. Die Identifikationsnummer ersetzt die bisherige Steuernummer. Sie gilt für alle Personen, einschließlich der Neugeborenen und aller Kinder, die noch gar nicht steuerpflichtig sind. Sie kann bis zu zwanzig Jahre über den Tod hinaus von den Finanzbehörden gespeichert werden. Das Bundeszentralamt für Steuern prüft und verwaltet die Steueridentifikationsnummern.

Vor Vergabe dieser Nummer haben die Meldebehörden dem Bundeszentralamt für Steuern von jedem im Melderegister registrierten Einwohner Daten wie Name, Anschrift, Geschlecht, Geburtstag und -ort zu übermitteln. Zweck der Übermittlung ist ein bundesweiter Abgleich der Meldedaten, das heißt, nach Übermittlung der Daten werden diese zusammengeführt und bereinigt. Anschließend - geplant war bis zum 1. Januar 2008, nach neueren Presseberichten jedoch erst im Frühjahr 2008 - vergibt das Bundeszentralamt für Steuern für jede gemeldete natürliche Person eine Identifikationsnummer und teilt sie der zuständigen Meldebehörde und dem Steuerpflichtigen unverzüglich mit. Die Steuerpflichtigen werden auch über die übrigen beim Bundeszentralamt für Steuern zu ihrer Person gespeicherten Daten unterrichtet.

Bis zu diesem Zeitpunkt werden also Datenbestände der rund 82 Millionen in Deutschland gemeldeten Personen aus rund 5.300 Meldestellen erstmals in einer zentralen Bevölkerungsdatei zusammengeführt. Dies ist aus datenschutzrechtlicher Sicht in mehrfacher Hinsicht sehr bedenklich. Es besteht die große Gefahr, dass das Grundrecht auf informationelle Selbstbestimmung nicht mehr gewährleistet werden kann, da durch die neue Datenbank Begehrlichkeiten, auch anderer Behörden, entstehen können. Die Verwendung der Steuernummer wird möglicherweise nicht auf den Zweck der Steueridentifikation beschränkt bleiben. So eröffnen sich Möglichkeiten, den Datenpool zu vergrößern und Personendaten miteinander zu verknüpfen.

Datenschutzrechtlich bedenklich ist jedoch auch der bundesweite Abgleich der von den Meldebehörden an das Bundeszentralamt für Steuern zu übermittelnden Meldedaten. Treten Unstimmigkeiten auf, haben die Meldebehörden diese zu klären. Dass die Steuer-ID später als geplant vergeben wird, wird auch darauf zurückzuführen sein, dass der Umfang solcher Fälle nicht absehbar ist und die Meldebehörden in dieser Hinsicht aufgrund der dezentralen Organisation auch keine Erfahrungen haben. Die entsprechende Rechtsvorschrift lässt offen, wie die Datenverarbeitung erfolgen soll bzw. welche Kriterien überhaupt erfüllt sein müssen, um einen Datensatz zu bereinigen, und wie die Daten abgeglichen werden sollen.

Die Einführung der Steueridentifikationsnummer birgt die Gefahr, dass Datenbestände stetig erweitert und zusammengeführt werden und dass auch andere öffentliche oder nichtöffentliche Stellen diese Datenbestände nutzen. Auf Bundesebene sind Maßnahmen erforderlich, um dies zu verhindern.

2.5.2 Kontenabrufverfahren

Entscheidung des Bundesverfassungsgerichtes

In meinem letzten Tätigkeitsbericht (Siebter Tätigkeitsbericht, Punkt A.1.II.2.6 und Punkt A.1.IV.5) hatte ich darüber berichtet, dass neue Regelungen in der Abgabenordnung (AO) in Kraft getreten sind, die den Finanzbehörden einen automatisierten Abruf von Konteninformationen über das Bundeszentralamt für Steuern ermöglichen. Die Entscheidung des Bundesverfassungsgerichts zu den Verfassungsbeschwerden, die sich im Wesentlichen gegen diese Regelungen (§ 93 Absatz 7 und § 93 Absatz 8 AO) gerichtet hatten, ist am 13. Juni 2007 ergangen. Erfolgreich war die Verfassungsbeschwerde gegen § 93 Absatz 8 AO, der die Erhebung von Kontostammdaten für Behörden oder Gerichte regelt.

Nach dem damaligen Gesetzestext ist der Anwendungsbereich dieser Norm eröffnet, wenn eine Behörde oder ein Gericht ein Gesetz anwendet, das an Begriffe des Einkommensteuergesetzes anknüpft.

Das Bundesverfassungsgericht hat festgestellt, dass § 93 Absatz 8 AO den Kreis der Behörden, die ein Ersuchen zum Abruf von Kontostammdaten stellen können, und die Aufgaben, denen solche Ersuchen dienen sollen, nicht hinreichend bestimmt festlegt. Das Gericht bestätigt den datenschutzrechtlichen Grundsatz, dass Regelungen, die zu Eingriffen in das Recht auf informationelle Selbstbestimmung ermächtigen, Anlass, Zweck und Grenzen präzise festlegen müssen. Damit stellt die Entscheidung des Gerichts auf das Gebot der Zweckbindung der erhobenen Daten ab und stärkt diesen Grundsatz.

Dies bedeutet, dass der Gesetzgeber in Zukunft den Verwendungszweck der Daten hinreichend präzise umgrenzen muss. Dies wird nach Aussage des Gerichts dann sichergestellt, wenn klar bezeichnet wird, welche staatliche Stelle zur Erfüllung welcher Aufgaben zur Informationserhebung berechtigt sein soll. Außerdem hält das Gericht im Hinblick auf das Instrument der Kontenabfrage die Verwendung unbestimmter Rechtsbegriffe für nicht verfassungsgemäß. Aufgrund der alten Formulierung kommt ein Kontenabruf für eine unübersehbare Vielzahl von Gesetzeszwecken infrage, denn an spezifisch einkommensteuerrechtliche Begriffe können Gesetze aus den unterschiedlichsten Regelungsgebieten anknüpfen.

Da mit dieser Norm insbesondere der Missbrauch von Sozialleistungen und die Nichtabführung von Sozialabgaben bekämpft werden sollen, ist nach Aussage des Gerichts die Norm dann verfassungsrechtlich nicht zu beanstanden, wenn der Anwendungsbereich in verfassungsmäßiger Weise auf die Sicherung der Erhebung von Sozialabgaben und die Bekämpfung des Missbrauchs von Sozialleistungen begrenzt wird.

Bis zur Neuregelung ist dem Gesetzgeber eine Frist bis zum 31. Mai 2008 auferlegt worden. Bis dahin ist die Regelung für die Erfüllung dieses genannten Zwecks für anwendbar erklärt worden. Allerdings hat der Bundesgesetzgeber bereits im August 2007 eine geänderte Fassung dieser Norm in Kraft gesetzt, die regelt, welche Sozialbehörden beim Vollzug welcher Vorschriften Kontendaten abrufen dürfen (zu den Auswirkungen der Regelungen zum Kontenabruf auf Hartz-IV-Empfänger siehe Punkt 2.8.8).

Datenschutzgerechtere Vordrucke für das Kontenabrufverfahren

Nachdem neben mir auch andere Landesbeauftragte für den Datenschutz das Kontenabrufverfahren geprüft haben, sind die Prüfungsergebnisse mit dem Bundesbeauftragten und den Landesbeauftragten für den Datenschutz im Arbeitskreis Steuern erörtert worden. Insbesondere wurde die oft mangelhafte Dokumentation der Ermessenserwägungen in Zusammenhang mit dem Kontenabruf kritisiert. Die Datenschutzbeauftragten haben auf der Grundlage der vorhandenen Vordrucke und der im Rahmen der Prüfungen gewonnenen Erfahrungen ein Formular entwickelt und dem Bundesministerium der Finanzen mit der Bitte vorgelegt, auf eine bundeseinheitliche Verwendung hinzuwirken.

Unser Finanzministerium hat mir das gegenwärtig eingesetzte Formular zur Kenntnis gegeben. Bei der Gestaltung sind die Anregungen der Datenschutzbeauftragten im Wesentlichen berücksichtigt worden. So wird zum Beispiel die Forderung nach einer gesonderten Dokumentation der zu § 93 AO erforderlichen besonderen Güterabwägung eines Kontenabrufs im Besteuerungsverfahren eines Berufsgeheimnisträgers im Sinne des § 112 Abgabenordnung berücksichtigt. Zu begrüßen ist, dass der Vordruck um einen Vermerk nach erfolgter Abfrage ergänzt worden ist. So soll die Erfassung der Ergebnisse eines Kontenabrufs erleichtert und die Information der Betroffenen über die Abfrage dokumentiert werden.

Aktuelle Zahlen aus Mecklenburg-Vorpommern

Die Zahl der Kontenabrufverfahren hat sich in diesem Berichtszeitraum erheblich erhöht. Dies betrifft vor allem Kontenabfragen gemäß § 93 Abs. 7 AO. Diese Norm regelt, dass die Finanzbehörde über das Bundesamt für Finanzen bei Kreditinstituten einzelne Daten aus den nach § 93 b Abs. 1 zu führenden Dateien abrufen darf, wenn dies zur Festsetzung oder Erhebung von Steuern erforderlich ist und ein Auskunftsersuchen an den Steuerpflichtigen nicht zum Ziele geführt hat oder keinen Erfolg verspricht. Aus der Landtagsdrucksache 5/1250 vom 18. Februar 2008 ergibt sich, dass die Finanzämter in Mecklenburg-Vorpommern seit Inkrafttreten der Vorschriften zum Kontenabrufverfahren 599 Abrufe nach § 93 Abs. 7 AO und acht Abrufe nach § 93 Abs. 8 AO beim Bundeszentralamt für Steuern durchgeführt haben. Nach Aussage des Finanzministeriums Mecklenburg-Vorpommerns wurden bis September 2007 durch 201 Kontenabrufe bisher unbekannte Konten und Depots festgestellt. (Zur Entwicklung der Anzahl von Kontenabrufen siehe auch Siebter Tätigkeitsbericht A.1.IV.5.)

2.5.3 Zweitwohnungssteuer: Datenübermittlung von der Uni an die Stadt

Im Rahmen eines Petitionsverfahrens zweier Studenten vor dem Petitionsausschuss des Landtages Mecklenburg-Vorpommern gegen die nachträgliche Forderung von Zweitwohnungssteuern durch eine Stadt bin ich vom Petitionsausschuss unter anderem gebeten worden, aus datenschutzrechtlicher Sicht zu der im Jahr 2005 erfolgten Datenübermittlung von der Universität an die Stadt Stellung zu nehmen. Dieser Datenübermittlung lag folgender Sachverhalt zugrunde:

Im Jahr 2004 hatte das Stadtkassen- und Steueramt der Stadt die Universität aufgefordert, die Anschriften aller an der Universität Studierenden zu übermitteln. Die Stadt hatte ihr Auskunftsersuchen mit der Erhebung der Zweitwohnungssteuer begründet. Hintergrund hierfür war das Ergebnis einer Befragung des Studentenwerks als Wohnungsgeber der Stadt, wonach 40 % aller dort eingemieteten Studenten ihren Meldepflichten gemäß Landesmeldegesetz nicht nachgekommen sind. Von der Zweitwohnungssteuerpflicht konnten jedoch nur Personen erfasst werden, die sich mit einem Zweitwohnsitz in der Stadt gemeldet haben. Aufgrund dieser Tatsache ist die Stadt davon ausgegangen, dass eine gleichmäßige Besteuerung hinsichtlich der Zweitwohnungssteuer nicht gegeben sei. Ihr Auskunftsersuchen hat die Stadt auf § 12 Kommunalabgabengesetz Mecklenburg-Vorpommern (KAG M-V) i. V. m. §§ 93, 111 Abgabenordnung (AO) gestützt.

Bei einem Kontroll- und Informationsbesuch habe ich festgestellt, dass die übermittelten Daten an das Meldeamt weitergereicht und dort zur Bereinigung des Meldedatenbestandes genutzt worden sind. Zur Erhebung der Zweitwohnungssteuer sollte also nicht an melderechtliche Verhältnisse angeknüpft werden, sondern es ging darum, durch den Datenabgleich überhaupt erst herauszufinden, welche der Studenten ihrer Meldepflicht nicht nachgekommen sind.

Für diese Datenübermittlung besteht keine melderechtliche Ermächtigungsgrundlage. Im Landesmeldegesetz Mecklenburg-Vorpommern ist abschließend geregelt, dass die Meldebehörde lediglich berechtigt ist, Auskunft vom Wohnungsgeber zu verlangen. Somit war allein die Datenübermittlung vom Studentenwerk an die Stadt zulässig.

Die Datenübermittlung stellte auch einen Verstoß gegen das Landeshochschulgesetz Mecklenburg-Vorpommern dar. Das Landeshochschulgesetz erlaubt nach § 7 ausschließlich die Verarbeitung „zur Aufgabenerfüllung der für die Hochschule erforderlichen personenbezogenen Daten über Hochschulzugang, Studium, Studienverlauf und Prüfungen. Das Nähere über die Verarbeitung der Daten der in Satz 1 genannten Personen regelt die Hochschule in einer Satzung auf Grundlage des Gesetzes zur Änderung datenschutzrechtlicher Vorschriften vom 28. März 2002.“ Die Satzung der Universität enthält keine entsprechende Zweckbestimmung der Nutzung von Anmeldedaten Studierender zur Zweitwohnungssteuererhebung, was auch gegen das Landesdatenschutzgesetz Mecklenburg-Vorpommern verstoßen würde.

Die Vorschriften des KAG M-V und der AO können ebenfalls nicht als Rechtsgrundlage für die erfolgte Datenerhebung bzw. -übermittlung herangezogen werden, denn mit der Datenübermittlung ist nicht der Zweck verfolgt worden, einen für die Besteuerung erheblichen Sachverhalt festzustellen.

Im Vorfeld der Datenübermittlung, über die die Studenten informiert worden sind, sind etliche Studenten ihrer Meldepflicht nachgekommen bzw. weitere Studenten taten dies, nachdem sie von der Meldebehörde dazu aufgefordert worden sind. Schon dies sei nach Aussage des Steueramtes als ein ausreichender Erfolg dieser Maßnahme angesehen worden. Das Steueramt hat aufgrund des Datenabgleichs auch keine gesonderten Steuerfestsetzungen vorgenommen, sondern ist lediglich aufgrund der regelmäßigen, monatlichen Mitteilungen der Meldebehörde tätig geworden.

Die Daten wurden also ohne Rechtsgrundlage übermittelt. Deshalb habe ich der Stadt gemäß § 32 Abs. 1 Landesdatenschutzgesetz Mecklenburg-Vorpommern eine Beanstandung ausgesprochen.

2.5.4 Zweitwohnungssteuer bei Gartenlauben

Ich bin darüber informiert worden, dass ein Amt Eigentümer von Gartenlauben zur Zweitwohnungssteuer heranzieht. Hierbei vollzieht das Amt die Satzungen über die Erhebung der Zweitwohnungsteuer der jeweiligen Gemeinden. Diese Satzungen regeln, dass der Inhaber einer im Gemeindegebiet liegenden Zweitwohnung steuerpflichtig ist. Zweitwohnung im Sinne der Satzungen ist jede Wohnung, die jemand neben seiner Hauptwohnung im melderechtlichen Sinne für seinen persönlichen Lebensbedarf oder den seiner Familienmitglieder innehat.

Zur Durchsetzung der Steuerpflicht wurden Personen angeschrieben, die laut Melderegister mit einer Zweitwohnung gemeldet sind, Personen, die bereits steuerlich veranlagt sind, und Personen, die jahreskurabgabepflichtig sind. Darüber hinaus sollen vom Amt auch Personen ermittelt werden, die noch nicht in den Datenbeständen erfasst sind, aber Zweitwohnungen innehaben sollen, zum Beispiel Dauermieter von Ferienwohnungen und Pächter von Wochenend- und Feriengrundstücken. Da diese Personen dem Amt unbekannt sind, werden Auskünfte von den Verpächtern, Vermietern und auch von Kleingartenvereinen eingeholt.

Das Amt rechtfertigt diese Datenerhebung mit dem Argument, dass Kontrollen durchzuführen seien, soweit Anhaltspunkte bestehen, die im Zuge des Veranlagungsverfahrens die gleichheitswidrige Nichtheranziehung von Steuerpflichtigen in erheblichen Umfang vermuten lassen. Als Rechtsgrundlage für die Datenerhebung stützt sich das Amt auf § 12 Kommunalabgabengesetz Mecklenburg-Vorpommern (KAG M-V) in Verbindung mit § 93 Abgabenordnung (AO).

Ich vertrete die Auffassung, dass § 12 KAG in Verbindung mit § 93 AO nicht anwendbar und es daher nicht zulässig ist, Verpächter, Vermieter und Vereine aufgrund dieser Vorschriften zur Feststellung eines für die Besteuerung erheblichen Sachverhaltes zur Auskunft zu verpflichten. Dies ergibt sich zum Beispiel auch daraus, dass § 93 AO vom Wortlaut her die Auskunftspflicht von Dritten über die steuerlichen Verhältnisse einer betroffenen, aber bekannten Person regelt. Hier geht es jedoch um die Ermittlung unbekannter Steuerpflichtiger.

Außerdem fordert das Landesdatenschutzgesetz Mecklenburg-Vorpommern, dass für Daten, die an eine öffentliche Stelle übermittelt werden sollen, eine Rechtsvorschrift vorhanden sein muss, die eine Datenübermittlung genau zu diesem Zweck, hier zum Zweck der Erhebung der Zweitwohnungssteuer, vorsieht. Eine solche Rechtsvorschrift existiert jedoch nicht.

Unserem Innenministerium habe ich meine Rechtsauffassung mitgeteilt und gleichzeitig darauf verwiesen, dass das Meldeamt gemäß § 21 Abs. 1 Landesmeldegesetz Mecklenburg-Vorpommern (LMG M-V) die Pflicht hat, die Richtigkeit des Melderegisters sicherzustellen und dass es daher bei konkreten Anhaltspunkten darauf, dass Pächter der Zweitwohnungssteuerpflicht unterliegen, jedoch keine Zweitwohnung angemeldet haben, berechtigt ist, hinsichtlich eines konkreten Gebietes vom Verpächter Auskunft gemäß § 20 LMG M-V zu verlangen.

Das Innenministerium hält § 12 KAG in Verbindung mit § 93 AO für eine zulässige Ermächtigung der Gemeinden, um einen Kleingartenverein zur Auskunft über die einzelnen Kleingärtner zu verpflichten, die der Gemeinde nicht bekannt sind und der Zweitwohnungssteuerpflicht unterfallen. Es stimmt hingegen meiner Auffassung zu, dass § 20 LMG M-V eine hinreichende Ermächtigung für das Auskunftsersuchen an die Verpächter einer Kleingartenanlage darstellt.

Hinsichtlich der konträren Rechtsauffassungen zur Auslegung des § 12 KAG in Verbindung mit § 93 AO und vor dem Hintergrund, dass es sich bei dieser Rechtsfrage um eine grundsätzliche Auslegungsfrage handelt, die in vielerlei Bezügen immer wieder auftreten wird, habe ich dem Innenministerium vorgeschlagen, einen Gutachter zu beauftragen. Das Ministerium sieht hier jedoch keine Notwendigkeit.

8. Ich empfehle dem Landtag, im Kommunalabgabengesetz eine Klarstellung dahingehend aufzunehmen, dass die Ermittlung von Steuerpflichtigen nicht im Wege einer Auskunftspflicht Dritter erfolgen darf.

2.5.5 Bearbeitung der Steuerfälle von Finanzamtsmitarbeitern bei Einleitung eines Steuerstrafverfahrens

Die Bearbeitung von Steuerfällen von Mitarbeitern des Finanzamtes birgt ein besonderes Risiko der unzulässigen Verwertung von Mitarbeiterdaten in sich. Deshalb habe ich Kontroll- und Informationsbesuche in einem Finanzamt sowie in der Buß- und Strafsachenstelle eines weiteren Finanzamtes durchgeführt und auch Einsicht in Verfahrensakten bei einer Staatsanwaltschaft genommen. In der Bußgeld- und Strafsachenstelle des Finanzamtes ist mir erläutert worden, wie Steuerfälle von Finanzamtsangehörigen bei Einleitung eines Steuerstrafverfahrens bearbeitet werden und wie die einzelnen Verfahrensschritte hierbei ablaufen. In dem anderen Finanzamt habe ich die einzelnen Verfahrenschritte in einem konkreten Steuerstrafverfahren eines Finanzamtsangehörigen geprüft.

Nach dieser Prüfung hat sich der Sachverhalt so dargestellt, dass der „Arbeitgeber Finanzamt“ im Besteuerungsverfahren seines „Arbeitnehmers“ hinsichtlich der Schlüssigkeitsprüfung der Steuererklärung Personalaktendaten (Vergleich Arbeitstage mit Urlaubs- und Krankentagen) verwendet hat. Diese Daten befanden sich auf Ausdrucken des Programms AKUSTIG, auf das nur wenige Mitarbeiter Zugriff haben. Diese elektronischen Personalaktenauszüge habe ich in der Disziplinarakte des Finanzamtsmitarbeiters, gegen den ein Steuerstrafverfahren eingeleitet worden ist, vorgefunden. Sie sind erstellt worden, bevor die Finanzamtsvorsteherin in einem Aktenvermerk dargelegt hat, dass der Verdacht bestehe, dass auf der Steuererklärung unrichtige Angaben gemacht worden seien. Anhand der Akten war jedenfalls nicht ersichtlich, dass zum Zeitpunkt der Erstellung der AKUSTIG-Ausdrucke schon der Verdacht der Steuerhinterziehung bestanden hat. Auf den Ausdrucken hat ein Vorgesetzter handschriftliche Notizen zu auf der Steuerklärung abgefragten Daten vorgenommen und diese mit den Personaldaten abgeglichen.

Aus datenschutzrechtlicher Sicht ist im Vorfeld der Einleitung des Steuerstrafverfahrens gegen wesentliche Grundsätze des Datenschutzrechts sowie auch gegen die Vorschriften des Landesbeamtengesetzes verstoßen worden.

Im Datenschutz gilt der Grundsatz des Trennungsgebotes. Danach sind zu unterschiedlichen Zwecken erhobene Daten auch getrennt zu verarbeiten. Mit diesem Grundsatz geht für Personalaktendaten der Grundsatz der Zweckbindung der Verwendung von Personalaktendaten einher. So dürfen gemäß § 100 Abs. 3 Satz 3 Landesbeamtengesetz M-V Personalakten nur für Zwecke der Personalverwaltung oder Personalwirtschaft verwendet werden, es sei denn, der Beamte willigt in eine anderweitige Verwendung ein.

Ein weiterer datenschutzrechtlich relevanter Grundsatz ist der Grundsatz der vertraulichen Behandlung von Personalakten, der ebenfalls im Landesbeamtengesetz (§ 100 Abs. 1 Satz 1, § 103 Abs. 1) verankert ist. Er ist eine Ausprägung des in Artikel 2 Abs. 2 in Verbindung mit Artikel 1 Abs. 1 Grundgesetz verankerten allgemeinen Persönlichkeitsrechts, das zugleich Grundlage des Rechts auf informationelle Selbstbestimmung ist. Dieser Grundsatz wird verletzt, wenn dem Trennungsgebot und dem Zweckbindungsgrundsatz nicht Rechnung getragen wird.

Nach diesen Vorschriften ist es also nicht zulässig, dass der Arbeitgeber, wenn er Kenntnis von Tatsachen oder Daten hat, die aufgrund personalrechtlicher Vorschriften erhoben worden sind, diese Daten für nicht personalrechtliche Zwecke verwendet. Somit dürfen beispielsweise anhand dieser Daten keine Tatsachen festgestellt werden, die in das Besteuerungsverfahren mit einfließen. Die Übermittlung dieser Daten an die Bußgeld- und Strafsachenstelle zum Zwecke steuerstrafrechtlicher Ermittlungen war damit ebenfalls unzulässig.

Die Aktenlage hat keinen Aufschluss darüber gegeben, wie die dem Steuerpflichtigen vorgeworfenen Unrichtigkeiten und Differenzen festgestellt worden sind und wie sich diese genau darstellen. Daher war für mich nicht nachvollziehbar, ob die Unrichtigkeiten auch ohne die rechtswidrige Verwendung der Personaldaten festgestellt worden wären oder ob der Verdacht der Steuerhinterziehung erst durch die Hinzuziehung der Personaldaten entstanden ist. Aus diesem Grunde war auch die Aktenführung im geprüften Finanzamt zu bemängeln, die weder vollständig noch nachvollziehbar war.

Das Finanzministerium als verantwortliche Stelle hat im Verfahrensverzeichnis den Zweck und die Rechtsgrundlage der Datenverarbeitung für das Verfahren AKUSTIG entsprechend den datenschutzrechtlichen Anforderungen festgelegt. Damit hat es die gemäß § 18 Landesdatenschutzgesetz M-V (DSG M-V) erforderlichen Vorkehrungen dafür getroffen, dass sich die Mitarbeiter der datenverarbeitenden Stelle einen Überblick über die für sie zutreffenden Arbeitsabläufe und Verfahren verschaffen können und in diesem Rahmen von der strengen Zweckbindung Kenntnis haben. Aus diesem Grund habe ich von einer Beanstandung gemäß § 32 DSG M-V abgesehen.

9. Ich empfehle der Landesregierung, in geeigneter Weise sicherzustellen, dass die Grundsätze des Trennungsgebotes und der Zweckbindung der Verwendung von Personalaktendaten eingehalten werden. Dabei sollte gesetzlich geregelt werden, dass Mitarbeiter von Finanzämtern generell in einem anderen Finanzamt veranlagt werden, um so der Gefahr einer unzulässigen Verwendung von Beschäftigtendaten im Rahmen von Steuerstrafverfahren strukturell begegnen zu können.

2.5.6 LUNA ohne ausreichende Rechtsgrundlage

Das Verfahren Länderumfassende Namensabfrage (LUNA) ist zur effektiveren Bekämpfung des Umsatzsteuerbetruges entwickelt worden. Durch eine bundesweite Nutzung soll erreicht werden, dass Umsatzsteuerhinterziehungen durch mehrfache umsatzsteuerliche Registrierungen in verschiedenen Bundesländern vermieden werden.

Die Version 2.0 dieses Verfahrens ist am 30. Juni 2007 bundesweit eingeführt worden. Mit dieser Version sind zusätzlich zum bisherigen Datenkatalog erheblich umfangreichere Datenbereiche des Grundinformationsdienstes und des Umsatzsteuer-Voranmeldeverfahrens bereitgestellt worden. Damit soll die Beschränkung der Verwendung von LUNA ausschließlich für die Umsatzsteuermissbrauchsbekämpfung aufgehoben werden. Es erfolgt also eine Ausweitung der Zugriffe auf Fahndungsbereiche anderer Steuerarten. Damit verbunden ist eine erhebliche Zunahme der Zahl der nutzungsberechtigten Personen.

Im Vorfeld der Einführung des Verfahrens in Mecklenburg-Vorpommern habe ich zu den rechtlichen und technisch-organisatorischen Aspekten des Einsatzes des Verfahrens LUNA 2.0 einen Kontroll- und Informationsbesuch bei der IT-Leitstelle des Finanzministeriums durchgeführt. Gegen die Einführung von LUNA 2.0 habe ich erhebliche rechtliche Bedenken geäußert, da für dieses Verfahren keine Rechtsgrundlage vorhanden ist. Gerade beim Verfahren LUNA ist eine spezifische Rechtsgrundlage unerlässlich. Einerseits ist die Datenbasis, auf die zugegriffen werden kann, erheblich erweitert worden, andererseits soll auch eine Erweiterung des Nutzerkreises erfolgen. §§ 85 und 88 a Abgabenordnung (AO) werden entgegen der Auffassung des Finanzministeriums den Anforderungen an eine spezifische Rechtsgrundlage nicht gerecht.

§ 85 AO verankert den Grundsatz der gleichmäßigen Besteuerung. In § 88 a AO heißt es: „Soweit es zur Sicherstellung einer gleichmäßigen Festsetzung und Erhebung der Steuern erforderlich ist, dürfen die Finanzbehörden nach § 30 geschützte Daten auch für Zwecke künftiger Verfahren ..., in Dateien oder Akten sammeln und verwenden."

Diese Normen sind zu unspezifisch und allgemein und genügen in keiner Weise den verfassungsrechtlichen Anforderungen, wie sie das Bundesverfassungsgericht in seinem Volkszählungsurteil formuliert. Sie können daher nicht als Grundlage für die Verwendung von Daten dienen, die dem Steuergeheimnis unterliegen. Eine entsprechende Rechtsgrundlage muss dem Gebot der Normenklarheit und dem Verhältnismäßigkeitsgrundsatz entsprechen. § 85 AO ist dagegen lediglich eine Aufgabennorm, § 88 a AO ist zu unspezifisch. Es ist nicht geregelt, wer welche Daten von wem zu welchen Zwecken verwenden beziehungsweise an andere Stellen übermitteln darf und welche Daten dem Zugriff anderer Stellen unterliegen. Die erforderliche Rechtssicherheit und die Gewährleistung einer entsprechenden Rechtmäßigkeitskontrolle ist somit nicht möglich.

Trotz meiner Empfehlung, von der Inbetriebnahme des Verfahrens LUNA 2.0 Abstand zu nehmen, ist die Freigabe für das Land Mecklenburg-Vorpommern am 26. Juni 2007 erfolgt.

Das Finanzministerium hat meine datenschutzrechtlichen Bedenken an das Bundesministerium der Finanzen (BMF) und die Steuerverwaltungen der Länder zur Prüfung, insbesondere im Gremium der AO-Referatsleiter, weitergeleitet. Da das Verfahren vorrangig in Hessen entwickelt wurde, hat sich das Bundesministerium an das Hessische Finanzministerium gewandt und um Darlegung der Auffassung des Arbeitskreises Steuerverwaltung des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz gebeten. In einem Schreiben hat der Hessische Datenschutzbeauftragte nochmals betont, dass die bereits in der Koordinierungsrunde zur Version 1.0 im Jahr 2004 gegenüber dem BMF vorgetragenen Bedenken nach wie vor aktuell seien. Insbesondere würden klare Vorgaben zum Kreis der Betroffenen, zur Speicherdauer, Zweckänderung, Übermittlung und Kontrolle sowie zur Verarbeitung der Daten mittels elektronischer Verfahren (Datenabgleiche) und der Dateiführung fehlen. Hinsichtlich der Forderung nach einer normenklaren Gesetzesgrundlage ist deutlich gemacht worden, dass der Arbeitskreis sich auch durch die Entscheidung des Bundesverfassungsgerichts zur Kontenabfrage (siehe Punkt 2.5.2) bestätigt sehe.

10. Ich empfehle der Landesregierung, sich umgehend um die Schaffung einer verfassungsgemäßen Rechtsgrundlage zu bemühen und bis dahin das Verfahren LUNA 2.0 einzustellen.

2.5.7 Jahressteuergesetz 2007 und Änderung der Steuerdaten-Übermittlungsverordnung

Für die Kommunikation mit der Finanzverwaltung ist wegen der besonderen Sensibilität der Steuerdaten in vielen Fällen die Schriftform erforderlich. Die Abgabenordnung (AO) lässt in § 87 a Abs. 3 jedoch zu, dass die für Anträge, Erklärungen oder Mitteilungen an die Finanzbehörden angeordnete Schriftform in bestimmten Fällen durch die elektronische Form ersetzt werden kann. In diesen Fällen ist das elektronische Dokument mit einer qualifizierten elektronischen Signatur zu versehen. Die Übermittlungsvorschriften der AO werden unter anderem in der Steuerdaten-Übermittlungsverordnung (StDÜV) konkretisiert. Bereits in meinem Sechsten Tätigkeitsbericht hatte ich Übergangsregelungen kritisiert, die ein wesentlich geringeres Sicherheitsniveau zulassen (siehe dort Punkt 2.16.3).

Mit dem Jahressteuergesetz 2007 wurden die sicherheitstechnischen Anforderungen in § 87 a AO erneut gesenkt. Neben der qualifizierten elektronischen Signatur kann das Bundesministerium der Finanzen demnach auch „ein anderes sicheres Verfahren zulassen, das die Authentizität und die Integrität des übermittelten elektronischen Dokuments sicherstellt“. Die neue StDÜV untersetzt dies weiter. Diese Regelung läuft jedoch leer, da es ein anderes Verfahren mit den Eigenschaften der qualifizierten elektronischen Signatur nicht gibt. Insbesondere entsprechen sogenannte fortgeschrittene elektronische Signaturen nicht diesem Niveau. Offenbar ist mit der Neuregelung des § 87 a AO beabsichtigt, die im ElsterOnline-Portal verwendeten Verfahren nachträglich auf eine Rechtsgrundlage zu stellen. Die Finanzverwaltung akzeptiert hier auch fortgeschrittene elektronische Signaturen und beabsichtigt dies auch weiterhin (siehe auch Punkt 2.15.2).

Risiken bei der Kommunikation mit der Finanzverwaltung können zudem aus der nicht sachgemäßen Nutzung verschiedener kryptographischer Schlüssel resultieren. So dürfen Authentisierungsschlüssel auf keinen Fall für Signaturen genutzt werden, weil sich daraus weit reichende Manipulationsmöglichkeiten ergeben würden.

Manipulationsmöglichkeiten bei Nutzung von Authentisierungsschlüsseln zur Signatur

Werden für Authentisierung und Signatur die gleichen Schlüssel benutzt, so kann der Prüfende statt einer Zufallszahl den Hashwert eines gültigen Dokuments übergeben. Der Nutzer kann dies nicht erkennen, weil Hashwerte und Zufallszahlen nicht voneinander unterschieden werden können. Arglos verschlüsselt er diesen Wert und muss feststellen, dass der Prüfende ihm ein Dokument mit seiner Signatur präsentiert. Der Nutzer könnte dann praktisch nie den Gegenbeweis führen, zu dem ihn die Entwurfsfassung des § 87 a AO gezwungen hätte. Zu der beschriebenen Manipulation wäre jeder Betreiber eines Authentisierungsverfahrens auf der Basis der gleichen Schlüssel in der Lage, also könnte beispielsweise der Betreiber eines Klubs mit elektronischer Zugangskontrolle auf diese Weise Steuererklärung für seine Besucher einreichen. Hätte der Prüfende diesen Trick versucht, obwohl für Signatur und Authentisierung verschiedene Schlüssel verwendet werden, so wäre dies aufgefallen.

Genau diese Nutzungsmöglichkeiten von Authentisierungsschlüsseln hätte aber ein vorheriger Entwurf des § 87 a AO erlaubt. Mit einer Entschließung haben die Datenschutzbeauftragten des Bundes und der Länder im Oktober 2006 deshalb ausdrücklich die Aufrechterhaltung der unterschiedlichen Funktionalität und Verbindlichkeit von Signatur und Authentisierung gefordert (siehe Anlage 1.5).

Technischer Ablauf bei Signatur und Authentisierung

Eine Signatur wird zu einem Dokument geleistet. Ein Dokument liegt in Form einer Datei mit einem bestimmten Inhalt (zum Beispiel Vertrag, Antrag oder Erklärung) und in einem bestimmten Format (zum Beispiel einem Text- oder Grafik-Format) vor. Bei der Signatur wird aus einem Dokument zunächst eine kurze Zeichenfolge, ein Hashwert, gebildet. Aus dem Hashwert kann das Dokument nicht ermittelt werden. Dieser Hashwert wird mit dem privaten Schlüssel der signierenden Person verschlüsselt. Dokument und verschlüsselter Hashwert werden übertragen oder zur späteren Verwendung gespeichert. Wer die Signatur prüfen will, berechnet aus dem Dokument den Hashwert und entschlüsselt den verschlüsselten Hashwert nunmehr mit dem öffentlichen Schlüssel. Passen berechneter und entschlüsselter Hashwert zusammen, ist das Dokument von dem Inhaber des privaten Schlüssels signiert worden.

Bei der Authentisierung erhält derjenige, der sich ausweisen soll, eine Zufallszahl. Diese verschlüsselt er mit seinem privaten Schlüssel und gibt das Ergebnis dem Prüfenden. Der Prüfende entschlüsselt die verschlüsselte Zufallszahl. Stimmen ursprüngliche und entschlüsselte Werte überein, hat der Prüfende tatsächlich den Besitzer des privaten Schlüssels vor sich.

Insbesondere weisen sie auf Folgendes hin: Elektronische Signaturen werden Dokumenten beigegeben. Wie bei handschriftlich unterschriebenen Dokumenten kann der Empfänger anhand der elektronischen Signatur prüfen, wer das Dokument ausgestellt hat und ob es verfälscht wurde. Die qualifizierte elektronische Signatur ist häufig der eigenhändigen Unterschrift gleichgestellt. Authentisierungsverfahren hingegen bestätigen lediglich die Identität einer Person oder Systemkomponente. Damit sind sie zur Anmeldung an einem IT-System oder als elektronisches Türschloss geeignet. Authentisierungsverfahren liefern also andere Aussagen und haben andere Rechtsfolgen als Signaturen, obwohl sie oft auf denselben asymmetrischen Kryptoverfahren beruhen. Benutzt man die gleichen Schlüssel zur Signatur und zur Authentisierung, so kann der Betreiber eines Authentisierungssystems dem Nutzer ein Dokument unterschieben und behaupten, der Nutzer hätte es signiert. Der Nutzer müsste dann die Rechtsfolgen tragen.

Überdies sollten die nicht existierenden „anderen sicheren Verfahren“ sogar denselben Beweiswert erhalten wie qualifizierte elektronische Signaturen. Hiervon hat der Bundesgesetzgeber jedoch nach Intervention der Datenschutzbeauftragten aus Bund und Ländern in letzter Minute Abstand genommen. In diesem Zusammenhang wurde die gesamte Ausnahmebestimmung bis Ende 2011 befristet und ist zu evaluieren.

11. Ich empfehle der Landesregierung, bei ihren Planungen für neue E-Government-Verfahren und der Weiterentwicklung bestehender Verfahren den Unterschied zwischen Signatur und Authentisierung genau zu beachten und nicht aus Kostengründen auf ungeeignete oder weniger sichere Verfahren auszuweichen. Die Landesregierung sollte insbesondere ihren Einfluss auf die Entwicklung der Software in der Finanzverwaltung in diesem Sinne nutzen. Darüber hinaus sollte sie sich dafür einsetzen, die Ausnahmebestimmung in § 87 a AO nicht weiter zu verlängern.

2.5.8 Outsourcing im Bereich der Zwangsvollstreckung

Eine Kommune hatte im Jahr 2006 erwogen, ihre gesamte städtische Vollstreckungstätigkeit für privat- und öffentlich-rechtliche Forderungen einer Inkasso-GmbH zu übertragen. Die Stadt hat sich an mich gewandt und um datenschutzrechtliche Stellungnahme zum Konzept der Inkasso-GmbH „Einziehung von Forderungen der öffentlichen Hand durch Private“ gebeten.

Mit der Auslagerung von Forderungen sollte die Inkasso-GmbH eigene Entscheidungskompetenzen erhalten. So war beispielsweise ein aktives Forderungsmanagement geplant, unter anderem das selbstständige Aushandeln von Ratenzahlungen.

Vollstreckungen nach dem Landesverwaltungsverfahrensgesetz unseres Bundeslandes gehören zum Kernbereich hoheitlicher Verwaltung. Öffentlich-rechtliche Geldforderungen sind nach den Bestimmungen des Verwaltungs-Vollstreckungsgesetzes im Verwaltungswege zu vollstrecken. Außerdem liegen den öffentlich-rechtlichen und privatrechtlichen Forderungen im Zusammenhang mit Vollstreckungen zum größten Teil besonders sensible Daten zugrunde, die zum Beispiel dem Steuer- und Sozialgeheimnis unterfallen. Gegen solche besonderen Geheimhaltungsvorschriften würde jedoch bei Auslagerung von Forderungen verstoßen werden. Darüber hinaus haben Beteiligte an einem Verwaltungsverfahren, soweit kommunale Forderungen nicht unter besondere Geheimhaltungsvorschriften fallen, gemäß § 30 Landesverwaltungsverfahrensgesetz Anspruch darauf, dass ihre Geheimnisse, insbesondere die zum persönlichen Lebensbereich gehörenden, von der Behörde nicht unbefugt offenbart werden. Unter Berücksichtigung dieser Gesichtspunkte ist eine Aufgabenausgliederung von sämtlichen öffentlich-rechtlichen Forderungen im Bereich der Zwangsvollstreckung aus datenschutzrechtlicher Sicht unzulässig.

Im November 2007 haben Vertreter der Kommune und der Inkasso-GmbH das Thema nochmals aufgegriffen und um ein Gespräch gebeten. Die Inkasso-GmbH und insbesondere die Kommune machten deutlich, dass sie meine Bedenken nachvollziehen können. Beide Seiten verfolgen nun das Ziel, einzelne Aufgaben des Forderungseinzuges im Wege der Auftragsdatenverarbeitung zu übertragen. Die Stadt bleibt so als „Herr der Daten“ verantwortliche Stelle. Die Inkasso-GmbH hat betont, dass sie den Forderungseinzug im Rahmen der Weisungen der Stadt lediglich begleiten würde.

Das Vorhaben soll also derart gestaltet werden, dass es den Anforderungen des Landesdatenschutzgesetzes Mecklenburg-Vorpommern (DSG M-V) zur Auftragsdatenverarbeitung gemäß § 4 DSG M-V entspricht.

§ 4 DSG M-V schließt grundsätzlich nicht aus, dass Daten, die einem besonderen Amts- oder Berufsgeheimnis unterliegen, im Wege der Auftragsdatenverarbeitung auch durch private Auftragnehmer verarbeitet werden. Die private Stelle muss jedoch in der Lage sein, die Anforderungen tatsächlich zu erfüllen, die an die Verarbeitung solcher Daten zu stellen sind. So sind zum Beispiel auch klare Regelungen darüber zu treffen, welcher Kenntnisse, Tätigkeiten oder Mittel sich die GmbH als privater Dritter bedienen darf. Die eigentlichen Kompetenzen der Stadt dürfen hierbei nicht überschritten werden. Anderenfalls würde sich die Stadt haftbar machen.

Kommune und Inkasso-GmbH werden mich über weitere konzeptionelle Schritte und Zwischenergebnisse informieren und lassen sich weiterhin datenschutzrechtlich beraten.

2.5.9 Data Center Steuern

Ende Dezember 2005 trat das Gesetz zum Dataport-Staatsvertrag in Kraft. Der Staatsvertrag regelt die gemeinsame Steuerdatenverarbeitung der vier Bundesländer Bremen, Hamburg, Schleswig-Holstein und Mecklenburg-Vorpommern (siehe Siebter Tätigkeitsbericht Punkt A.1.IV.1). Das gemeinsame Rechenzentrum für die Steuerverwaltung, welches jetzt Data Center Steuern (DCS) heißt, wird vom bisherigen zentralen IT-Dienstleister der Verwaltungen Hamburgs und Schleswig-Holsteins „Dataport“ betrieben. Während Dataport als Anstalt öffentlichen Rechts künftig auch für Bremen arbeiten wird, behält Mecklenburg-Vorpommern die DVZ M-V GmbH als zentralen IT-Dienstleister. Das DCS mit Standorten in Rostock und Schwerin wird aber die Steuerverwaltung aller vier Bundesländer mit Rechenzentrumsleistungen versorgen. Lediglich der zentrale Druck von Steuerbescheiden und anderen Unterlagen wird künftig bei Dataport in Kiel-Altenholz stattfinden.

Im August 2006 unterzeichneten die Landesdatenschutzbeauftragten der vier beteiligten Bundesländer eine Vereinbarung, mit der eine abgestimmte Verfahrensweise für eine effektive Datenschutzkontrolle von Dataport geregelt wird. Dort ist beispielsweise festgelegt, dass Prüfungen vor Ort durch den jeweils ortsnahen Datenschutzbeauftragten erfolgen und bei Bedarf auch eine gegenseitige Beauftragung möglich ist.

Die Zusammenarbeit sowohl mit Dataport als auch zwischen den Datenschutzbeauftragten hat sich bewährt. Es finden regelmäßig Arbeitstreffen statt, auf denen Dataport über den Stand der verschiedenen Projekte informiert und sich den Fragen der Datenschutzbeauftragten stellt. Während des ersten Treffens im März 2006 stellte Dataport unter anderem erste Planungen zum DCS-Datenschutzkonzept vor. Die Datenschutzbeauftragten konnten sich davon überzeugen, dass Dataport ein wirkungsvolles IT-Sicherheits- und Datenschutzmanagement auf der Grundlage der Grundschutzmethodik des Bundesamtes für Sicherheit in der Informationstechnik (BSI) konzipiert hat (siehe auch Punkt 2.15.5). Beim zweiten Arbeitstreffen im März 2007 wurden unter anderem der Stufenplan zur Erstellung des Sicherheitskonzeptes und das Managementsystem für Informationssicherheit vorgestellt. Im Oktober 2007 fand die dritte Beratung statt, während der Dataport umfassend zum Sachstand des Sicherheitskonzeptes berichtete.

Um einen Überblick über die Umsetzung der einzelnen Maßnahmen des Sicherheitskonzeptes zu erhalten, vereinbarten die Datenschutzbeauftragten eine gemeinsame Begehung der DCS-Rechenzentren in Kiel-Altenholz, Hamburg, Rostock und Schwerin. Im Rahmen eines sogenannten Basis-Sicherheitschecks nach der BSI-Grundschutzmethodik sollte das vorhandene IT-Sicherheitsniveau bewertet werden. Das Ergebnis des Checks war ein umfassender Bericht mit dem Umsetzungsstatus aller erforderlichen Maßnahmen.

Der Bericht hat den Eindruck bestätigt, dass Dataport recht erfolgreich Anstrengungen unternimmt, um den hohen Anforderungen an Sicherheit und Datenschutz bei der Verarbeitung sensibler Steuerdaten gerecht zu werden. Erfreulicherweise konnte festgestellt werden, dass in den DCS-Standorten Rostock und Schwerin bereits sehr viele Maßnahmen vollständig umgesetzt waren, beispielsweise die Infrastrukturmaßnahmen im Bereich der Rechenzentren. Umsetzungsdefizite gab es unter anderem im Bereich der UNIX-Server oder der Windows-Clients. Hier waren beispielsweise die umgesetzten Maßnahmen nicht vollständig dokumentiert, sicherheitsrelevante Patches und Updates nicht immer eingespielt und die Protokollierung nicht völlig revisionssicher ausgestaltet.

Schon während der gemeinsamen Auswertung der Prüfergebnisse im Anschluss an die Begehung hat Dataport zugesagt, die Defizite unverzüglich zu beseitigen und die Datenschutzbeauftragten der beteiligten Bundesländer auch weiterhin regelmäßig zu informieren.

2.6 Telekommunikation und Medien

2.6.1 Das neue Telemediengesetz

Am 1. März 2007 ist das neue Telemediengesetz (TMG) zusammen mit den Änderungen des Rundfunkstaatsvertrages in Kraft getreten. Gleichzeitig wurden das Teledienstegesetz, das Teledienstedatenschutzgesetz und der Mediendienstestaatsvertag aufgehoben.

Mit dem Telemediengesetz wird die bisherige Unterscheidung zwischen Tele- und Mediendiensten aufgehoben. Beide Dienste werden nun unter dem gemeinsamen Begriff der „Telemedien“ zusammengefasst. In der Bestimmung des Anwendungsbereichs des Gesetzes ist lediglich geregelt, dass „Telemedien“ alle Informations- und Kommunikationsdienste sind, die nicht unter Telekommunikation oder Rundfunk fallen. Aufgrund dieser Negativdefinition ist also zunächst immer zu prüfen, ob ein angebotener Dienst in den Anwendungsbereich des Staatsvertrags für Rundfunk und Telemedien oder des Telekommunikationsgesetzes fällt.

Eindeutige Telemediendienste sind nach der Gesetzesbegründung zum Beispiel Online-Angebote von Waren- und Dienstleistungen mit unmittelbarer Bestellmöglichkeit, elektronische Presse, News-Clubs, Chatrooms, Suchdienste und die kommerzielle Verbreitung von Informationen über das Angebot von Waren- und Dienstleistungen mit elektronischer Post (z. B. Werbe-Mails).

Es gibt jedoch auch die sogenannten doppelfunktionalen Dienste. Das heißt, neben der Übertragungsdienstleistung nach dem Telekommunikationsgesetz wird auch eine inhaltliche Dienstleistung angeboten, für die das Telemediengesetz gilt. Hier werden in der Gesetzesbegründung der Internetzugang und die E-Mail-Übertragung genannt. Für Teledienste können also das Telemediengesetz, das Telekommunikationsgesetz und auch der Staatsvertrag für Rundfunk und Telemedien nebeneinander zur Anwendung kommen.

Das Telemediengesetz gilt für alle Anbieter einschließlich der öffentlichen Stellen, unabhängig davon, ob für die Nutzung ein Entgelt erhoben wird. Inhaltlich sind die meisten Regelungen des Telemediengesetzes von den abgelösten Gesetzen übernommen worden. Eine Änderung zum Beispiel betrifft die Informationspflichten der Anbieter. Diese sind durch den Gesetzgeber dahingehend präzisiert worden, dass sie jetzt nur noch für Anbieter von Telemedien gelten, die diese geschäftsmäßig, in der Regel gegen Entgelt anbieten. Das bedeutet, dass die im Telemediengesetz verankerten Informationspflichten nur von den Anbietern zu leisten sind, deren Dienste in der Regel nur gegen eine wirtschaftliche Gegenleistung erbracht werden.

In § 6 Abs. 2 TMG ist eine neue Vorschrift aufgenommen worden, die eine Spam-Abwehr erleichtern soll. Zwar ist das Versenden von Spam-Mails nach dem Gesetz gegen den unlauteren Wettbewerb unzulässig. Die neue Vorschrift soll jedoch verhindern, dass der Absender oder der kommerzielle Charakter einer Nachricht verschleiert beziehungsweise verheimlicht wird. Denn wenn Spam-Filter auf diese Weise umgangen werden, liegt eine Ordnungswidrigkeit vor, die mit einem Bußgeld bis zu fünfzigtausend Euro geahndet werden kann.

Die bisher geltenden datenschutzrechtlichen Bestimmungen sind kaum verändert aus den alten gesetzlichen Regelungen übernommen worden. Neu ist jedoch die Ausweitung des Auskunftsrechts des Anbieters von Telemediendiensten gegenüber bestimmten Stellen. Nach den alten Regelungen durfte der Diensteanbieter lediglich an Strafverfolgungsbehörden und Gerichte zum Zwecke der Strafverfolgung Auskunft geben. Nun gilt dieses Auskunftsrecht außerdem zur Gefahrenabwehr durch die Polizeibehörden der Länder, zur Erfüllung der gesetzlichen Aufgaben durch die Verfassungsschutzbehörden, des Bundesnachrichtendienstes oder des militärischen Abschirmdienstes oder zur Durchsetzung der Rechte am geistigen Eigentum. Hinzu kommt, dass das Auskunftsrecht nicht nur für Bestandsdaten, sondern auch für Nutzungs- und Abrechnungsdaten gilt. Besonders kritikwürdig ist, dass sich neben das Auskunftsrecht der staatlichen Stellen auch ein Auskunftsrecht von privaten Stellen zur Durchsetzung des geistigen Eigentums reiht. Mit dieser Regelung soll zum Beispiel bezweckt werden, dass Anbietende und Nutzende illegal kopierter Musik- oder Videodateien oder Software leichter ermittelt werden können. Es ist zu befürchten, dass ähnliche Begehrlichkeiten anderer privater Interessengruppen geweckt werden.

2.6.2 Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz

Der Arbeitskreis Medien der Datenschutzbeauftragten des Bundes und der Länder hat seine Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz überarbeitet und aktualisiert.

In den Unternehmen und den öffentlichen Stellen des Landes besteht oftmals die Möglichkeit, das Internet auch am Arbeitsplatz zu nutzen. Gerade aber bei der privaten Nutzung dieser Dienste am Arbeitsplatz hat der Arbeitgeber bestimmte datenschutzrechtliche Anforderungen zu beachten. Vor allem auch im Hinblick darauf, dass E-Mail und andere Internetdienste geeignet sind, das Verhalten und die Leistung der Beschäftigten zu überwachen, stellt die Orientierungshilfe die bei der Nutzung dieser Dienste geltenden Anforderungen dar.

Ein wichtiger Aspekt bei der privaten Nutzung dieser Dienste ist der, dass der Arbeitgeber gegenüber den Beschäftigten Telekommunikations- bzw. Telemediendienstanbieter ist und somit zur Einhaltung des Fernmeldegeheimnisses verpflichtet ist. Dennoch muss es ihm grundsätzlich möglich sein, eine angemessene Art der Kontrolle der Internetnutzung durchzuführen. Der Umfang der privaten Nutzung, ihre Bedingungen sowie Art und Umfang der Kontrolle, ob diese Bedingungen eingehalten werden, müssen - am sinnvollsten durch Dienstvereinbarung oder -anweisung - unter Beteiligung des Personalrates eindeutig geregelt werden. Beschäftigte, die diese Einschränkungen bei der privaten Nutzung nicht hinnehmen wollen, können ihre Einwilligung hierzu ohne jeden dienstlichen Nachteil verweigern. Einer Einwilligung bedarf es jedoch nicht, wenn eine Kontrolle beziehungsweise Protokollierung zu Zwecken der Datenschutzkontrolle, der Datensicherung, zur Sicherung des ordnungsgemäßen Betriebs der Verfahren oder zu Abrechnungszwecken erforderlich ist.

Auch private E-Mails unterfallen dem Fernmeldegeheimnis und sind wie private Post zu behandeln. Der Umgang mit privaten E-Mails ist für alle Beschäftigten transparent zu gestalten. Wie bei der dienstlichen Nutzung dürfen aus Gründen der Datensicherheit auch eingegangene private E-Mails oder deren Anhänge unterdrückt werden, wenn sie ein Format aufweisen, das zu Sicherheitsrisiken führen kann. Die diesbezügliche Verfahrensweise ist transparent zu regeln. Im konkreten Fall ist der Beschäftigte dann darüber zu unterrichten und bei der Kenntnisnahme des Inhalts zu beteiligen.

Aus Gründen der Datensicherheit ist es heutzutage erforderlich, dass sowohl öffentliche als auch private Stellen geeignete Maßnahmen gegen Viren und Spam ergreifen. Hierzu wird in der Orientierungshilfe darauf hingewiesen, dass eine zentrale Spam-Filterung, bei der automatisch auf den Header oder Inhalte zugegriffen wird, nur mit Einwilligung des Empfängers erfolgen darf, da die Reichweite des Fernmeldegeheimnisses erst endet, wenn die E-Mail in seine vollständige Verfügungsgewalt gelangt ist. Die Beschäftigten sind über die Art und Weise der Spam-Filterung, insbesondere über die dabei stattfindende Verarbeitung personenbezogener Daten, zu informieren.

Eine darüber hinausgehende inhaltliche Kontrolle ist nicht zulässig.

12. Ich empfehle daher der Landesregierung, die öffentlichen Stellen des Landes für die datenschutzrechtlichen Aspekte bei der privaten Nutzung von Internetdiensten zu sensibilisieren. Dies betrifft vor allem auch die Notwendigkeit, die entsprechenden Bedingungen (Kontrollmöglichkeiten, Protokollierungen) für eine solche Nutzung für alle Mitarbeiter transparent zu regeln.

2.7 Statistik

2.7.1 Entwurf eines Zensusvorbereitungsgesetzes

Nachdem das Bundeskabinett im März 2007 dem Entwurf eines Zensusvorbereitungsgesetzes 2011 zugestimmt und sich damit an dem von der Europäischen Union für das Jahr 2011 geplanten gemeinschaftsweiten Zensus beteiligt hat, ist das Zensusvorbereitungsgesetz am 13. Dezember 2007 in Kraft getreten.

In der Bundesrepublik ist diese Volkszählung erstmals als „registergestützter Zensus“ geplant. Mit dem Zensusvorbereitungsgesetz und dem folgenden Zensusdurchführungsgesetz soll die Grundlage dafür geschaffen werden, dass nicht wie bei den bisherigen Volkszählungen alle Einwohner befragt, sondern dass hauptsächlich die Melderegister, die Register der Bundesagentur für Arbeit und andere Verwaltungsregister ausgewertet werden. Befragungen sollen das Verfahren lediglich ergänzen.

Auf der einen Seite mag die Notwendigkeit eines neuen Zensus in Deutschland zwar bestehen, denn die aktuellen Bevölkerungs- und Wohnungszahlen basieren auf Fortschreibungen der letzten Volkzählungen, die im früheren Bundesgebiet im Jahre 1987 und in der ehemaligen DDR im Jahre 1981 stattfanden. Auf der anderen Seite besteht allerdings die verfassungsrechtliche Frage, ob für Planungsaufgaben des Staates tatsächlich alle zu erhebenden Daten im Rahmen der gesetzlichen beziehungsweise statistikrechtlichen Anforderungen erhoben werden.

Die Gewinnung der Daten soll in erster Linie anhand vorhandener Dateien erfolgen. Wenn den statistischen Ämtern der Länder Anhaltspunkte auf unvollständige oder fehlerhafte Daten vorliegen, dürfen sie den Meldebehörden die betreffenden Anschriftenbereiche zur Klärung von Differenzen übermitteln. Die Einhaltung des im Volkszählungsurteils verankerten Gebots der strikten Trennung von Statistik und Verwaltungsvollzug wird durch die jetzige Gesetzesformulierung nicht gewährleistet, denn es besteht die Möglichkeit, dass durch die Weiterleitung der Daten von den Statistischen Ämtern an die Meldebehörden zwei unterschiedliche Zwecke mit unterschiedlichen Anforderungen verknüpft werden. Es ist nicht ausgeschlossen, dass die Meldebehörden Rückmeldungen für die Bereinigung des Melderegisters nutzen, ja sogar gemäß § 21 Landesmeldegesetz (Amtsermittlungsgrundsatz) nutzen müssen. Gerade aber bei einer Zusammenführung von Daten aus verschiedenen Verwaltungsbereichen muss die Verwendung der ursprünglich zu anderen Zwecken gespeicherten personenbezogenen Daten im Hinblick auf das Persönlichkeitsrecht Betroffener überschaubar bleiben.

Bei der öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages am 17. September 2007 zum Entwurf des Zensusvorbereitungsgesetzes 2011 habe ich daher als Sachverständiger darauf hingewiesen, dass die Zweckbestimmung der für statistikrechtliche Zwecke erhobenen Daten im Gesetzestext klar formuliert werden muss, sodass deutlich wird, dass die Daten an die Meldebehörden ausschließlich zur statistischen Erfassung übermittelt werden und Einzelprüfungen bzw. ergänzende Erhebungen der Meldebehörden in diesem Zusammenhang nicht zulässig sind. (Die Stellungnahme ist auf meiner Website unter http://www.datenschutz-mv.de/dschutz/presse/stellungnahme-zensus.pdf veröffentlicht.)

In meiner Stellungnahme vor dem Innenausschuss habe ich auch darauf verwiesen, dass die geplante Georeferenzierung der Gebäudeadressen dazu führt, dass die Koordinatenwerte aufgrund der kleinräumigen Darstellung durchaus personenbeziehbar sein können. Da der Gesetzesentwurf keine entsprechenden Regelungen zur Anonymisierung beinhaltet, sondern lediglich auf noch zu schaffende Anonymisierungsmethoden hinweist, genügt er nicht den verfassungsmäßigen Anforderungen. Daher stellt die im Gesetzesentwurf verankerte Georeferenzierung einen Eingriff in das allgemeine Persönlichkeitsrecht dar.

Trotz der von mir und dem Bundesbeauftragten für den Datenschutz geäußerten Kritik vor dem Innenausschuss des Deutschen Bundestages hat dieser am 19. September 2007 dem Gesetzesentwurf zugestimmt und damit den Weg für die Durchführung des registergestützten Zensus im Jahr 2011 freigemacht. Im Hinblick auf das dem Zensusvorbereitungsgesetz folgende Zensusanordnungsgesetz ist es daher von großer Bedeutung, dass die datenschutzrechtlichen Kritikpunkte erneut vor dem Hintergrund der in der Verfassung verankerten Grundsätze verdeutlicht werden.

2.7.2 Umstellung der Schulstatistik auf Individualdaten mit bundeseinheitlichem Kerndatensatz

Die Kultusministerkonferenz arbeitet seit einigen Jahren an der Einführung eines bundesweit einheitlichen Schulstatistiksystems, in dem über das bisherige Maß hinaus Daten aus dem Schulbereich verarbeitet werden sollen. Die Kultusministerkonferenz ist zwar inzwischen von der Schaffung einer bundeseinheitlichen Schüler-ID abgerückt und bestrebt, mit der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ein Einvernehmen herzustellen. Die zweite Besprechung der AG Kerndatensatz/Datengewinnung der Kommission für Statistik mit Vertretern der Datenschutzkonferenz hat jedoch gezeigt, dass aus datenschutzrechtlicher Sicht noch zahlreiche Fragen offen und die grundlegenden datenschutzrechtlichen Forderungen noch nicht erfüllt sind.

Auf eine zentrale Datenhaltung soll nunmehr verzichtet werden. In den Ländern sind jedoch ein einheitlicher Kerndatensatz und länderübergreifende Auswertungen zu Bildungsverläufen in Einzelfällen vorgesehen.

Unter datenschutz- und statistikrechtlichen Gesichtpunkten ist es auch in diesem Verfahren erforderlich, die rechtlichen Voraussetzungen der amtlichen Statistik einzuhalten. Hierzu gehört die Festlegung von Erhebungs- und Hilfsmerkmalen, die Regelung der Auskunftspflicht und die Festlegung der technischen und organisatorischen Maßnahmen zur frühestmöglichen Pseudonymisierung/Anonymisierung.

In Mecklenburg-Vorpommern sind anhand der Daten, die statistisch gewonnen werden, zurzeit keine Schülerverläufe darstellbar. Nach Auskunft des Ministeriums für Bildung, Wissenschaft und Kultur ist eine solche Erweiterung auch nicht geplant.

2.8 Soziales

2.8.1 ELENA (ehemals JobCard-Verfahren)

Mit dem JobCard-Verfahren, das aus sprachlichen Gründen in ELENA-Verfahren (**El**ektronischer **E**inkommens**na**chweis) umbenannt wurde, könnte eine der größten Sammlungen personenbezogener Daten Deutschlands entstehen. In einer zentralen Datenbank sollen Einkommensnachweise von rund 40 Millionen abhängig Beschäftigten in elektronischer Form gespeichert werden. Es ist vorgesehen, diese Daten für verschiedene sozialrechtliche Verfahren sowie für Prozesskostenhilfeverfahren und für Zwecke des Versorgungsausgleichs zum Abruf bereitzustellen. Ein wesentliches Ziel des Vorhabens ist die Entlastung von Unternehmen, die bisher jährlich etwa 60 Millionen Einkommensbescheinigungen in Papierform ausstellen. In meinem 7. Tätigkeitsbericht habe ich bereits ausführlich über datenschutzrechtliche Aspekte des Vorhabens berichtet (siehe dort unter Punkt A.VIII.2).

Im Februar 2007 hat das Bundesministerium für Wirtschaft und Technologie (BMWi) den Entwurf eines „Gesetzes über die Einrichtung des Verfahrens des elektronischen Einkommensnachweises“ vorgelegt. Diesem Gesetzentwurf gingen drei JobCard-Projekte voraus, mit denen die Machbarkeit des gesamten Verfahrens getestet werden sollte:

JobCard I: testete den Abruf von Arbeitsbescheinigung aus einer Datenbank mit Hilfe eines Signaturkartenverfahrens (Projektende 2004),

JobCard II: übertrug die Ergebnisse des Projektes JobCard I auf Einkommensbescheinigungen aus dem gesamten Sozialrecht sowie dem Zivilprozessrecht (Projektende 2005),

JobCard III: testete die Einbeziehung von Entgeltersatzleistungen wie Arbeitslosengeld oder Kindergeld (Projektende 2007).

Die Landesbeauftragten für den Datenschutz wurden im Laufe des Projektes JobCard II beteiligt. Während der Begleitung des Projektes zeigten sich erhebliche datenschutzrechtliche Defizite. Von vornherein war klar, dass ein großer Teil der erhobenen Daten nie gebraucht wird, da viele Betroffene nie eine der fraglichen Sozialleistungen beantragen würden. Damit werden Daten in unzulässiger Weise auf Vorrat gespeichert. Ob damit das gesamte Verfahren dem verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit entspricht, ist nach wie vor ungeklärt.

Angesichts der Sensibilität und der Menge der gespeicherten Daten sind besonders hohe Anforderungen an die technischen und organisatorischen Datensicherheitsmaßnahmen zu stellen. Das Teilprojekt JobCard II kam daher einerseits zu dem Ergebnis, dass der Abruf von Daten aus der zentralen Datenbank nur unter Mitwirkung der betroffenen Person erfolgen darf. Dafür ist eine Signaturkarte mit einem qualifizierten elektronischen Zertifikat erforderlich, die beim ELENA-Verfahren angemeldet werden muss. Ein Datenabruf soll nur möglich sein, wenn sowohl Antragsteller als auch der Mitarbeiter der Sozialbehörde, bei der die Sozialleistung beantragt wird, den Abruf mit Vorlage der Signaturkarte autorisieren. Dieses sogenannte Zwei-Karten-Prinzip soll sicherstellen, dass Daten nur von einer berechtigten Stelle und nur mit Einwilligung der betroffenen Person abgerufen werden können.

Andererseits forderte das Teilprojekt JobCard II, dass die Daten nur in verschlüsselter Form in der zentralen Datenbank gespeichert werden dürfen. Ein Gutachten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) kam zu dem Ergebnis, dass die sogenannte asymmetrische Verschlüsselung mit einem Schlüssel, der ausschließlich auf der Signaturkarte der Betroffenen gespeichert ist, nicht praktikabel wäre. Die damit erreichbare Ende-zu-Ende-Verschlüsselung würde im Falle des Verlustes der Signaturkarte nach Ansicht des BSI zu erheblichen Problemen führen. Daher beschloss das BMWi, ein symmetrisches Verschlüsselungsverfahren einzusetzen, bei dem alle Daten mit demselben Schlüssel verschlüsselt werden. Damit ist es aber prinzipiell möglich, unter Umgehung der verfahrensspezifischen Sicherheitsvorkehrungen (etwa des Zwei-Karten-Prinzips) auf Daten der zentralen Datenbank ohne die Beteiligung Betroffener zuzugreifen. Der Abschlussbericht des Projektes fordert deshalb, das Verfahren und insbesondere den Umgang mit den kryptographischen Schlüsseln von einer unabhängigen Stelle verwalten zu lassen.

Der vom BMWi vorgelegte Gesetzentwurf erfüllt die oben beschriebenen datenschutzrechtlichen und technischen Anforderungen bisher nicht in ausreichendem Maße. Im März 2007 äußerte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder deshalb erhebliche Zweifel daran, dass die wesentlichen verfassungsrechtlichen Voraussetzungen für die Einrichtung des Registers tatsächlich gegeben sind. In einer Entschließung (siehe Anlage 1.14) forderte die Konferenz den Nachweis der Erforderlichkeit und der Verhältnismäßigkeit des Verfahrens und sah in den folgenden Punkten Klärungsbedarf:

- Es muss gesetzlich festgelegt werden, dass die Daten aus der Datenbank nur mit Mitwirkung der Teilnehmerinnen und Teilnehmer des Verfahrens entschlüsselbar sind.
- Das Verfahren muss so ausgestaltet werden, dass die Ver- und Entschlüsselung der Daten ohne Vorliegen der Signaturkarte des Betroffenen nur in klar definierten Ausnahmefällen durch eine unabhängige Treuhänderstelle möglich ist.
- Sämtliche im Rahmen des Verfahrens verarbeiteten Daten müssen einem gesetzlichen Beschlagnahmeschutz unterworfen sein.
- Die technischen Komponenten müssen auf der Basis einer unabhängigen Prüfung zertifiziert werden.

13. Ich empfehle der Landesregierung erneut, dem ELENA-Verfahrensgesetz im Bundesrat nur dann zuzustimmen, wenn die Verfassungsmäßigkeit des Verfahrens nachgewiesen, die Sicherheit der Daten garantiert und eine Kontrolle durch unabhängige Stellen gewährleistet ist.

2.8.2 Arbeitslosengeld II/Sozialgeld - Eine unendliche (Datenschutz-)Geschichte?

Innerhalb des Bereiches „Soziales“ waren Datenschutzfragen zum Arbeitslosengeld II/ Sozialgeld ein Arbeitsschwerpunkt. In einer erheblichen Anzahl von Petitionen schilderten Bürgerinnen und Bürger ihre Erfahrungen mit den Arbeitsgemeinschaften nach dem Sozialgesetzbuch Zweites Buch (ARGE nach SGB II) oder der Sozialagentur und fragten, ob eine bestimmte Datenverarbeitung zulässig sei. Es würde den Rahmen dieses Berichtes sprengen, wenn alle Einzelfragen hier behandelt würden. Die folgende Auswahl soll vielmehr vermitteln, in welchen Bereichen sich Anfragen häuften, und aufzeigen, durch welche Maßnahmen datenschutzrechtliche Verbesserungen erreicht werden können.

Auf vielfache Kritik bei den Bürgerinnen und Bürgern stießen die baulichen und auch organisatorischen Gegebenheiten in den Arbeitsagenturen. Es wurde mir mehrfach berichtet, dass Dritte im Empfangsbereich der ARGEn sowie in den einzelnen Arbeitsbereichen Gespräche mithören können, weil der Diskretionsabstand dies nicht verhindert oder beispielsweise die individuellen Beratungen in Großraumbüros stattfinden. Die ARGEn begründen Großraumbüros wiederum damit, dass sie für ihre Kunden transparent sein möchten. Transparenz für die Wartenden kann jedoch einen Eingriff in das Recht auf informationelle Selbstbestimmung der Person, die gerade beraten wird, nicht rechtfertigen. Im Übrigen trifft dies nicht nur auf Gesprächsinhalte zu, die eventuell durch entsprechende akustische Gestaltungen vor fremden Ohren geschützt werden können, sondern auch auf die nonverbale Kommunikation, die unter solchen Bedingungen nicht geschützt werden kann. Abhilfe ist hier möglich, wenn Betroffene auf Wunsch auch in einem separaten Raum beraten werden können. Darauf sollte die ARGE alle Besucher im Eingangsbereich hinweisen. Die ARGEn haben zugesichert, die Empfehlung umzusetzen.

Ein Bürger beschwerte sich darüber, dass der Briefkasten der ARGE vor allem an den Wochenenden so überfüllt sei, dass die dort eingeworfenen Briefe von außen leicht wieder herausgenommen werden können. Er befürchtete, dass unberechtigte Dritte seine Sozialdaten ohne große Mühe zur Kenntnis nehmen könnten. Ich habe die ARGE darauf hingewiesen, dass sie gesetzlich verpflichtet sei, das Sozialgeheimnis zu wahren, § 35 Sozialgesetzbuch Erstes Buch (SGB I). Dies bedeute auch, dass sie einen gesicherten Postzugang zu ermöglichen habe. Die ARGE hat diesen Hinweis so umgesetzt, dass sie für die Kunden einen zweiten Briefkasten aufstellen ließ.

Viele Beschwerden und Anfragen betrafen die Datenerhebung bei Dritten. So haben ARGEn Daten statt bei den Betroffenen bei Vermietern, Versorgungsunternehmen, Finanzbehörden oder Arbeitgebern erhoben. Häufig ist dabei gegen den Grundsatz der Datenerhebung bei der betroffenen Person verstoßen worden (§ 67a Abs. 2 Satz 1 SGB X), und es waren auch nicht die Ausnahmetatbestände für eine Erhebung bei anderen Stellen oder Personen erfüllt (§ 67a Abs. 2 Satz 2 SGB X). ARGEn haben Daten häufig dann bei Dritten erhoben, wenn die betroffene Person die Daten nicht zur Verfügung stellen wollte. Meist sind die Betroffenen vor der Datenerhebung nicht über die Folgen einer Verweigerung von Angaben aufgeklärt worden. Die ARGEn haben ihr Vorgehen in der Regel mit dem Untersuchungsgrundsatz (§ 20 SGB X) und damit begründet, dass sich die Behörde der Beweismittel bedient, die sie nach pflichtgemäßem Ermessen zur Ermittlung des Sachverhaltes für erforderlich hält (§ 21 SGB X). Die ARGEn übersehen hierbei allerdings, dass eine Erhebung, Verarbeitung und Nutzung von Sozialdaten nur unter den Voraussetzungen der Vorschriften zum Schutz von Sozialdaten im 2. Kapitel des SGB X zulässig ist, § 35 Abs. 2 SGB X.

Außerdem bestimmt § 37 Satz 3 SGB X, dass der Schutz von Sozialdaten dem Verwaltungsverfahren vorgeht, soweit sich die Ermittlung des Sachverhaltes auf Sozialdaten erstreckt. Dies bedeutet, dass die Datenerhebung den Vorgaben des § 67 a SGB X entsprechen muss. Unter bestimmten Voraussetzungen kann danach von dem Grundsatz der Datenerhebung bei der betroffenen Person abgewichen werden, beispielsweise wenn ein Sozialleistungsträger zur Übermittlung an die erhebende Stelle befugt ist, wenn eine Rechtsvorschrift die Erhebung bei der anderen Stelle zulässt oder die Übermittlung an die erhebende Stelle ausdrücklich vorschreibt, § 67 a Abs. 2 Satz 2 SGB X. Es gibt innerhalb der Bücher des Sozialgesetzbuches eine Reihe bereichsspezifischer Auskunfts- und Übermittlungsvorschriften, die derartige Erhebungen bei anderen Personen oder Stellen oder Übermittlungen von anderen Stellen erlauben. Im Umkehrschluss bedeutet dies aber auch, dass Datenerhebungen bei anderen Personen oder Stellen ohne eine Rechtsgrundlage nicht zulässig sind. Sie können dann auch nicht mit Normen des Verwaltungsverfahrens, beispielsweise mit den §§ 20 und 21 SGB X begründet werden.

Bei den Datenerhebungen spielt ein weiterer Aspekt eine Rolle, der in der Praxis von den ARGEn vielfach nicht beachtet wird. So sind die Betroffenen darauf hinzuweisen, ob die Daten aufgrund einer Rechtsvorschrift erhoben werden, die zur Auskunft verpflichtet, ob die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen ist oder ob die Daten auf freiwilliger Basis anzugeben sind. Außerdem sind die Betroffenen über die Folgen einer Verweigerung von Angaben zu informieren, § 67 a Abs. 3 Satz 3 SGB X. Werden also Daten zur Erfüllung einer Aufgabe benötigt, sind die Betroffenen entsprechend aufzuklären. Sofern keine Datenerhebung bei Dritten zulässig ist, muss ihnen insbesondere erklärt werden, welche Folgen eine Verweigerung der Angaben hat. Neben entsprechenden Auskunftspflichten kann die Angabe von Daten und die Vorlage von Unterlagen im Einzelfall durchaus eine Obliegenheitspflicht des Betroffenen sein, § 60 SGB I. Folge einer Verletzung dieser Pflicht kann wiederum sein, dass die Leistung bis zur Nachholung der Mitwirkung ganz oder teilweise versagt oder entzogen wird. Darauf ist der Betroffene hinzuweisen. Folgender Fall soll dies weiter illustrieren:

Eine Petentin informierte mich darüber, dass die ARGE Daten über sie bei ihrem Vermieter, einer Wohnungsgesellschaft, erhoben hatte. Es ging um eine Betriebskostenabrechnung. Bei einem Minderverbrauch an Heizkosten könnte ein entsprechendes Guthaben auf die Kosten der Unterkunft angerechnet werden. Der Geschäftsführer der ARGE war der Auffassung, dass er verpflichtet sei, den Sachverhalt von Amts wegen zu ermitteln. Rechtlich begründete er die Datenerhebung mit den §§ 20 und 21 SGB X (siehe oben). Dabei hatte er übersehen, dass nach § 35 Abs. 2 SGB I eine Erhebung, Verarbeitung oder Nutzung von Sozialdaten nur unter den Voraussetzungen der Normen zum Schutz von Sozialdaten (2. Kapitel des SGB X) zulässig ist. Eine Erhebung der Daten über die Betriebskostenabrechnung hätte deswegen bei der Betroffenen mit Hinweis auf die Folgen einer Verweigerung der Angaben erfolgen müssen (siehe oben). Eine Erhebung der Daten beim Vermieter ohne Einwilligung der Betroffenen halte ich für unzulässig, weil die Erhebung bei der Betroffenen keinen unverhältnismäßigen Aufwand erfordern würde und außerdem überwiegend schutzwürdige Interessen der Betroffenen beeinträchtigt würden, § 67 a Abs. 2 Satz 2 SGB X. Der Vermieter würde durch diese Datenerhebung darüber informiert, dass die Betroffene Leistungen nach dem SGB II erhält. Diese Information fällt jedoch unter das Sozialgeheimnis nach § 35 Abs. 1 SGB I. Dies habe ich dem Geschäftsführer mitgeteilt und ihn aufgefordert, künftig die datenschutzrechtlichen Bestimmungen einzuhalten, was er zusagte.

Häufig wurde ich auch gefragt, ob Empfänger von Leistungen nach dem SGB II verpflichtet seien, der ARGE Kontoauszüge über einen größeren Zeitraum vorzulegen. Wer Sozialleistungen beantragt oder erhält, ist verpflichtet, seine Hilfsbedürftigkeit nachzuweisen. Hierzu gehört auch, dass die hierfür erforderlichen Nachweise und Belege vorgelegt werden. Eine ARGE darf daher bei der erstmaligen bzw. erneuten Beantragung von Leistungen, zur Klärung einzelner Angaben oder auch bei Verdacht auf Leistungsmissbrauch in der Regel Kontoauszüge der letzten drei Monate verlangen. Datenschutzrechtlich bedenklich ist es jedoch, wenn beispielsweise ohne nähere Begründung alle Kontoauszüge des letzten Jahres verlangt werden. Hinweise zur datenschutzgerechten Ausgestaltung von Kontoauszügen bei der Beantragung von Sozialleistungen habe ich auch auf meiner Internetseite www.datenschutz-mv.de veröffentlicht.

Beim Arbeitslosengeld II/Sozialgeld hat es inzwischen erfreuliche datenschutzrechtliche Entwicklungen gegeben. So ist beispielsweise ein bundesweiter Zugriff auf die Daten der im Softwaresystem bei der Bundesagentur für Arbeit gespeicherten Daten nicht mehr möglich. Mitarbeiterinnen und Mitarbeiter der ARGEn können jetzt nur noch auf die Daten zugreifen, die für ihre Sachbearbeitung jeweils erforderlich sind.

2.8.3 Akteneinsicht im Sozialleistungsbereich

Immer wieder wenden sich Bürgerinnen und Bürger an mich, denen von einem Sozialleistungsträger ihr Recht auf Auskunft bzw. Einsicht in ihre Unterlagen verwehrt wurde. Die Ablehnung der Auskunftsersuchen wird häufig damit begründet, dass dies aus datenschutzrechtlicher Sicht nicht möglich sei.

Die kostenfreie Auskunft ist ein datenschutzrechtlicher Grundsatz, der durch verschiedene Vorschriften näher ausgeformt wird. Dieses Recht ist in vielen Fällen die Grundlage, um weitergehende Rechte wie Ansprüche auf Schadensersatz oder Berichtigung, Sperrung und Löschung von Daten überhaupt erst geltend zu machen. Fehlt es an einer spezialgesetzlichen Regelung wie beispielsweise im Sozialgesetzbuch Achtes Buch (SGB VIII), ist der Auskunftsanspruch im Sozialleistungsbereich nach § 83 Sozialgesetzbuch Zehntes Buch (SGB X) zu beurteilen. Danach ist dem Betroffenen auf Antrag Auskunft über die zu seiner Person gespeicherten Sozialdaten zu erteilen. Darüber hinaus ist er zu informieren, an welche Personen oder Stellen die Daten übermittelt worden sind. In welcher Form dem Auskunftsanspruch entsprochen wird, das heißt, ob aus den Unterlagen vorgetragen wird oder ob man es ermöglicht, sie einzusehen oder Kopien zu erhalten, entscheidet die verantwortliche Stelle nach pflichtgemäßem Ermessen. Die Auskunftsverpflichtung nach § 83 SGB X besteht für alle in § 35 Sozialgesetzbuch Erstes Buch (SGB I) genannten Stellen wie Jugendamt, Sozialamt, Wohngeldstelle oder Arbeitsagentur.

Sollte dem Wunsch auf Auskunft oder Einsichtnahme nicht entsprochen werden, kann sich jeder an mich wenden. Ich werde mich dann dafür einsetzen, dass die betroffenen Personen ihr Recht wahrnehmen können.

2.8.4 Kindeswohlgefährdung

In den Medien wurde in der vergangenen Zeit häufig darüber berichtet, dass Kinder tot oder verwahrlost aufgefunden wurden. Den Berichten konnte man immer wieder entnehmen, dass der Datenschutz ein frühzeitiges wirksames Eingreifen der Jugendämter behindert habe. Allerdings waren datenschutzrechtliche Regelungen in den bekannt gewordenen Fällen nicht das Problem gewesen. Gesetzliche Möglichkeiten waren meist vorhanden und hätten nur genutzt werden müssen. Diese Ereignisse wurden nun zum Anlass genommen, um ein Frühwarnsystem zu erarbeiten, in dem der Austausch zwischen den Ämtern, Ärzten, Kindergärten und der Justiz besser verzahnt werden soll.

Auch in Mecklenburg-Vorpommern hat das Ministerium für Soziales und Gesundheit mit dem Entwurf eines Dritten Gesetzes zur Änderung des Gesetzes über den Öffentlichen Gesundheitsdienst (Gesetz zur Förderung der Kindergesundheit und des Kindeswohl) eine entsprechende Gesetzesinitiative auf den Weg gebracht. Die Notwendigkeit einer gesetzlichen Regelung wurde damit begründet, dass wissenschaftliche Studien und Berichte darauf hindeuten, dass es einer zunehmenden Zahl von Eltern nicht gelingt, die für die Entwicklung ihrer Kinder erforderlichen Rahmenbedingungen zu gewährleisten. Mit gesetzgeberischen Maßnahmen soll nun die Teilnahmequote an den Früherkennungsuntersuchungen erhöht werden, da ein starker Indikator für einen gesteigerten Hilfebedarf die Nichtteilnahme von Kindern an den sogenannten U-Untersuchungen sei. Über einen Abgleich zwischen den Daten des Einwohnermelderegisters und den von Ärzten gemeldeten Teilnehmern an einer Untersuchung der jeweiligen Altersstufe könnten die Eltern und Kinder festgestellt werden, die eine Untersuchung versäumt haben. Sie würden dann von einer sogenannten Servicestelle darauf hingewiesen, an den Folgeuntersuchungen teilzunehmen oder die Untersuchung nachzuholen. Geschieht dies nicht, übermittelt die Servicestelle die Daten des Kindes und seiner Eltern an das zuständige Gesundheitsamt, das die Eltern dann weiter beraten soll.

Unzweifelhaft ist dem Schutz der Kinder und Jugendlichen hohe Bedeutung zuzumessen, schließlich ist dies der Auftrag der Verfassung - Art. 14 Verfassung des Landes Mecklenburg-Vorpommern (Verf M-V). Jedoch berühren die neuen Regelungen des Gesetzentwurfes auch das verfassungsrechtlich garantierte Recht auf informationelle Selbstbestimmung nach Art. 6 Abs. 1 Verf M-V. Dieses Recht besteht nicht schrankenlos und kann im überwiegenden Interesse der Allgemeinheit eingeschränkt werden. Ob die mit dieser Gesetzesänderung angestrebte Regelung jedoch geeignet, erforderlich und angemessen ist, um den Schutz der Kinder und Jugendlichen zu gewährleisten, ist nach meiner Auffassung im Entwurf nicht hinreichend begründet. Zumal bei den bisher in den Medien berichteten Gefährdungen des Kindeswohls kein Zusammenhang zu versäumten Vorsorgeuntersuchungen bekannt wurde. Vielmehr hatten die staatlichen Behörden und anderen Stellen überwiegend Kenntnis von den Gefährdungen, denen die Kinder ausgesetzt waren. Exemplarisch hierfür sei der tragische Fall „Lea-Sophie“ aus Schwerin genannt. Hier gab es entsprechende Informationen an das Jugendamt. Dem Kind hätte daher mit einer Erinnerung des Sorgeberechtigten, an der Früherkennungsuntersuchung teilzunehmen, vermutlich nicht geholfen werden können. Dass es selbst dann, wenn alle Kinder an den Untersuchungen teilnehmen, für Ärzte schwierig ist, Misshandlungen zu erkennen, zeigt auch der Fall des Kindes Lea-Marie aus Teterow, über den die Medien Ende des Jahres 2006 berichteten. Dem Kind wurden von seiner Mutter ätzende Chemikalien eingeflößt und es wurde mit kochendem Wasser überbrüht.

Das Kind ist nach den Medienberichten 31 Mal stationär behandelt worden, bevor seine Tortur entdeckt wurde. Die Qual dieses Kindes hätte daher vermutlich auch mit einer Erinnerung, an einer Untersuchung teilzunehmen, nicht verhindert werden können. Die bisher öffentlich gewordenen Fälle belegen vielmehr Defizite in anderen Bereichen und nicht in fehlenden oder behindernden Datenverarbeitungsvorschriften bei freiwilligen Vorsorgeuntersuchungen.

Nach meiner Auffassung sollte in dem Gesetzentwurf erkennbar sein, welche Argumente nach einer entsprechenden Gewichtung schließlich dazu geführt haben, dass hier konkret der Schutz der Kinder und Jugendlichen höher zu bewerten ist als ihr Recht und das ihrer Eltern auf informationelle Selbstbestimmung. Ziel und Zweck der Früherkennungsuntersuchung bei Kindern ist es primär, Gesundheitsstörungen jeder Art zu erkennen. Deshalb müsste auch belegt werden, dass durch das Erreichen der Kinder, die bisher den Untersuchungen fernblieben, die gesundheitliche und allgemeine Situation dieser Kinder wesentlich verbessert werden kann. Ich habe daher empfohlen, die gesetzlichen Regelungen nach einer bestimmten Zeit zu evaluieren, um auf dieser Basis zu entscheiden, ob sie sich bewährt haben, geändert werden müssen oder künftig entfallen können.

Zur weiteren datenschutzrechtlichen Beratung, insbesondere zum Verfahren des Datenabgleichs, bin ich gern bereit.

2.8.5 Aktenführung in der Versorgungsverwaltung

Eine Petentin machte mich darauf aufmerksam, dass in den Versorgungsämtern medizinische Gutachten und Verwaltungsangelegenheiten in einer gemeinsamen Sachakte aufbewahrt werden. Insbesondere bei psychologischen Gutachten könnten die Sachbearbeiter jederzeit auch Kenntnis über sehr sensible Angelegenheiten einer Familie erhalten, da die Familienanamnese Bestandteil dieser Gutachten ist. Auch ein Arzt wollte wissen, ob er verpflichtet sei, einem Sachbearbeiter des Versorgungsamtes ärztliche Gutachten zu übersenden, da die Sachbearbeiter in der Regel nicht über die entsprechenden medizinischen Kenntnisse verfügten.

Diese meines Erachtens berechtigten Bedenken habe ich dem Landesamt für Gesundheit und Soziales (LaGuS) mitgeteilt und auch darauf hingewiesen, dass ich mit einer vergleichbaren Frage bereits in der Rentenversicherung befasst war. Damals habe ich empfohlen, medizinische Unterlagen von den Verwaltungsunterlagen zu trennen, sodass auf die medizinischen Unterlagen nur Ärzte zugreifen können. Da die Rentenversicherung Nord diese Empfehlung inzwischen realisiert hat, habe ich dem LaGuS vorgeschlagen zu prüfen, ob dort ebenso verfahren werden könnte.

Das LaGuS teilte mir mit, dass eine Änderung der Verfahrensweise nicht möglich sei, da der Sachbearbeiter ständig „Herr des Verfahrens“ sei und letztlich auch über den Antrag entscheide. Er kontrolliere auch, ob der Gutachter alle für die Entscheidung erheblichen Angaben berücksichtigt hat (z. B. ob alle Krankenhausaufenthalte, Vorerkrankungen etc. in die Bewertung einbezogen wurden oder die Vollständigkeit), und prüfe darüber hinaus die Kausalität (Antrag, Tatbestand, Gesundheitsschädigung). Dazu müsse der Verwaltungsmitarbeiter Zugang zu den medizinischen Unterlagen haben.

Im Ergebnis wurde vereinbart, dass die Versorgungsverwaltung prüft, ob eine getrennte Aufbewahrung der sensiblen medizinischen Unterlagen möglich wäre, wenn der Bescheid des Versorgungsamtes bestandskräftig ist. Eine Antwort steht noch aus.

2.8.6 Fragen der Antragsteller zum Erhebungsbogen „Wohngeld“

Im Berichtszeitraum wurde ich mehrfach zum Umfang der Datenerhebung im Zusammenhang mit einem Wohngeldantrag befragt. So hatte eine Wohngeldstelle beispielsweise eine Petentin aufgefordert, neben dem Antrag auch einen Zusatzfragebogen auszufüllen. Hier sollte sie angeben, wie viel Geld sie für das tägliche Leben (Frühstück, Mittag und Abendessen u. a.) ausgibt und wie hoch ihre Versicherungskosten sind. Darüber hinaus sollte sie ihr Vermögen nachweisen.

Die Wohngeldstelle begründete ihr Vorgehen damit, dass sie verpflichtet sei, alle für die Entscheidung erheblichen Tatsachen zu ermitteln. Hierzu sei sie nach §§ 20, 21 Sozialgesetzbuch Zehntes Buch (SGB X) verpflichtet. Außerdem habe man aus den Angaben der Petentin nicht erkennen können, aus welchen Mitteln sie ihren Lebensunterhalt bestritt.

Im Wohngeldgesetz ist konkret geregelt, welche Daten zur Entscheidung eines Wohngeldantrages erhoben werden dürfen. Der Nachweis täglicher oder monatlicher Ausgaben gehört keinesfalls dazu. Wer Wohngeld beantragt, hat im Rahmen des Wohngeldgesetzes und der §§ 60 bis 65 Sozialgesetzbuch Erstes Buch (SGB I) zwar Mitwirkungspflichten. Danach sind der zuständigen Wohngeldstelle alle Tatsachen anzugeben, die für die zu gewährende Leistung erheblich sind. Entscheidend jedoch für die Berechnung des Wohngeldes ist die Höhe des Einkommens und nicht die Höhe der monatlichen Ausgaben. Daher kann die Wohngeldstelle von den betroffenen Personen auch nur Auskunft und Nachweise über die Einnahmen verlangen. Bei der Auswahl der geforderten Nachweise hat die Wohngeldstelle dann den Grundsatz der Verhältnismäßigkeit, insbesondere das in § 67 a Abs. 1 SGB X verankerte Gebot der Erforderlichkeit, zu beachten. Dies bedeutet, dass nur die Sozialdaten erhoben und demzufolge verarbeitet werden dürfen, die für die konkrete Aufgabe erforderlich sind.

Sofern der Antragsteller kein regelmäßiges Einkommen hat und seinen Lebensunterhalt aus vorhandenem Vermögen bestreitet, kann im Rahmen der Mitwirkung nur verlangt werden, die Höhe des Vermögens zu belegen. Zwar ist auch das Vermögen kein Datum, welches bei der Antragstellung abgefragt werden darf. Wenn jedoch der Lebensunterhalt davon bestritten wird, ist es im Einzelfall möglich, entsprechende Unterlagen wie Sparbücher vorlegen zu lassen. Anhand dieser Unterlagen kann die Wohngeldstelle dann prüfen, ob tatsächlich regelmäßig Geld für die Lebensführung abgehoben wird.

Vor diesem Hintergrund war es nicht zulässig, von der Antragstellerin Informationen zu verlangen, die weder Einnahmen noch für das Wohngeld maßgebende Umstände betrafen. Bereits in meinem 7. Tätigkeitsbericht habe ich in Abschnitt VIII Punkt 1 auf die Unsicherheiten hingewiesen, die bei den Wohngeldstellen im Zusammenhang mit dem Umfang der Datenerhebung bestehen.

2.8.7 Kompetenzagenturen unterstützen beim Start ins Berufsleben

Im April 2007 übersandte mir ein Coach der Kompetenzagentur Mecklenburg-Vorpommern den Fragebogen der Kompetenzagenturen zur Unterstützung der beruflichen und sozialen Integration arbeitsloser Jugendlicher. Er bat mich um datenschutzrechtliche Beratung.

Das Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ) hat im Jahr 2002 das Modellkonzept Kompetenzagenturen (www.kompetenzagenturen.de) eingerichtet, um die Arbeitslosigkeit unter Jugendlichen abzubauen. Bundesweit arbeiten im Modellprogramm 15 Agenturen daran, besonders benachteiligte junge Menschen durch das Spektrum der Hilfs- und Förderangebote zu lotsen, um ihre soziale und berufliche Integration passgenau zu unterstützen. Ziel des Vorhabens ist es auch, Schwachstellen und Lücken in den lokalen Förderangeboten aufzudecken und in Zusammenarbeit mit den entsprechenden Institutionen neue Angebote anzustoßen.

Über die hilfesuchenden Jugendlichen sollte eine elektronische Fallakte angelegt und zentral gespeichert werden. Die hierfür erforderlichen Daten sollten mit Einwilligung der betroffenen Jugendlichen erhoben werden. Es wurden auch sehr sensible Daten erfragt, deren Erforderlichkeit zu bezweifeln war, zum Beispiel Mitgliedschaft in einer fundamentalistischen Vereinigung, gesundheitsgefährdende Verhaltensweisen wie Drogenmissbrauch oder Familieneinkommen.

Eine Datenverarbeitung auf Basis der Einwilligung ist unter den Voraussetzungen des § 4 a Bundesdatenschutzgesetz (BDSG) zulässig. Dies erfordert eine realistische Wahlmöglichkeit. Für den Fall, dass die Leistungen für die Jugendlichen nur erbracht werden können, wenn die Daten in der elektronischen Fallakte gespeichert werden, habe ich vorgeschlagen, bei der Datenerhebung auf die Freiwilligkeit der Teilnahme hinzuweisen und das gesamte Verfahren transparent darzustellen. Unter Berücksichtigung des § 4 a BDSG sollten die bereits erarbeiteten Einwilligungs- und Schweigepflichtentbindungserklärungen überarbeitet werden. Unklar war auch, ob und welche technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit umgesetzt waren. Ich habe der Kompetenzagentur daher empfohlen, von den Entwicklern der elektronischen Fallakte ein Datenschutz- und Datensicherheitskonzept zu verlangen. Es sollte auch darauf gedrungen werden, die Daten kryptographisch zu verschlüsseln, um die Vertraulichkeit zu sichern.

Meine Hinweise wurden dankend aufgenommen und zum Teil bereits umgesetzt. Beispielsweise wurde auf die Fragen nach der fundamentalistischen Ausrichtung, der Sucht- und Drogenproblematik und dem Familieneinkommen verzichtet. Darüber hinaus wurde ich darüber informiert, dass von den Providern ein Datenschutz- und Datensicherheitskonzept erarbeitet und die Datenübermittlung in jedem Fall verschlüsselt erfolgen wird. Auch die Einwilligungserklärungen wurden bereits überarbeitet.

2.8.8 Gesetzliche Regelungen zum Kontenabruf neu - Auswirkungen auf Hartz IV

Das Bundesverfassungsgericht (BVerfG) hat in seiner Entscheidung vom 13. Juni 2007 (1 BvR 1550/03) festgestellt, dass die damalige Rechtsvorschrift (§ 93 Abs. 8 Abgabenordnung - AO), nach der die Abrufe durchgeführt worden sind, nicht hinreichend bestimmt ist. Die Vorschrift verstößt gegen das Gebot der Normenklarheit, da der Kreis der Behörden, die ein Ersuchen zum Abruf von Kontostammdaten stellen können, und die Aufgaben, denen solche Ersuchen dienen sollen, nicht hinreichend bestimmt festgelegt sind.

Das BVerfG hat aber auch ausgeführt, dass die Verfassungswidrigkeit der oben genannten Rechtsvorschrift nicht zu ihrer Nichtigkeit führt. Ausnahmsweise sind verfassungswidrige Vorschriften weiter anzuwenden, wenn gewichtige rechtliche Belange es rechtfertigen, die Norm als Regelung für eine Übergangszeit fortbestehen zu lassen.

Der Gesetzgeber hat nach diesem Urteil des BVerfG den Kontenabruf neu geregelt. In § 90 Abs. 8 AO ist jetzt festgelegt, dass neben den Finanzbehörden auch die Träger der Grundsicherung für Arbeitssuchende (Arbeitsgemeinschaften - ARGEn) beim Bundeszentralamt für Steuern Kontoinformationen abrufen dürfen, wenn ein vorheriges Auskunftsersuchen an den Betroffenen nicht zum Ziel geführt hat oder keinen Erfolg verspricht. Folgende Daten dürfen abgerufen werden: Kontonummer, Tag der Errichtung und gegebenenfalls Tag der Auflösung, Name und Geburtstag des Kontoinhabers. In § 90 Abs. 9 AO ist jetzt außerdem geregelt, dass der Betroffene auf die Möglichkeit des Kontoabrufes hinzuweisen und nach dem Abruf über die Durchführung zu benachrichtigen ist.

Die Bundesagentur für Arbeit hat hierzu eine Geschäftsanweisung erlassen, um ein einheitliches Vorgehen bei den Trägern der Grundsicherung zu erreichen. Hier sind sowohl Regelungen der Bundesagentur zur Frage, wann ein Kontenabruf erfolgen soll, als auch eine Beschreibung des mit dem Bundeszentralamt für Steuern abgestimmten Verfahrens festgeschrieben. Es wird nunmehr darauf ankommen, ob und in welchem Umfang die Arbeitsgemeinschaften von dem neuen Mittel Gebrauch machen. Dabei liegt die Prüfung der Praxis bei den ARGEn in der Zuständigkeit des Landesbeauftragten für den Datenschutz, während die Kontrolle des Verfahrens beim Bundeszentralamt für Steuern dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit obliegt.

2.8.9 Adressierung ermöglichte Kenntnisnahme durch Dritte - Postzustellung und Datenschutz

Ein Petent schilderte mir, dass er seinen Briefkastenschlüssel für die Urlaubszeit an den Nachbarn gegeben hatte. Als dieser ihm nach dem Urlaub die Post brachte, stellte der Petent fest, dass im Adressfeld eines Schreibens des Sozialgerichts neben seinem Namen der Zusatz „als Vertreter der Bedarfsgemeinschaft im Sinne von § 38 SGB II“ vermerkt war. Er fragte mich, ob dies mit den datenschutzrechtlichen Bestimmungen vereinbar sei.

Vom Sozialgericht habe ich dazu die Auskunft erhalten, dass ein solcher Hinweis weder rechtlich geboten noch in sonstiger Weise zweckdienlich sei. Der Direktor des Sozialgerichtes räumte auch ein, dass der Hinweis im Adressfeld auf die Vertretung einer Bedarfsgemeinschaft als diskriminierend empfunden werden kann, da Dritte daraus Rückschlüsse auf einen Leistungsbezug und damit auch auf die persönlichen und wirtschaftlichen Verhältnisse des Empfängers ziehen könnten. Er hat daher diesen Vorfall mit den Mitarbeitern ausgewertet, sodass solche Adressierungen künftig ausgeschlossen werden können.

2.8.10 Entsorgen von Datenträgern und Schriftgut

Immer wieder werde ich gefragt, wie man Datenträger und Schriftgut datenschutzgerecht entsorgt. So wandte sich im Berichtszeitraum die Kassenärztliche Vereinigung Mecklenburg-Vorpommern an mich, weil sie für ihre Mitglieder, niedergelassene Ärzte und Psychotherapeuten, praktikable Lösungen suchte. Ich gebe hier wesentliche Empfehlungen wieder, weil sie sich auf viele andere Bereiche übertragen lassen.

Wer personenbezogene Daten verarbeitet, hat sie gegen unbefugte Kenntnisnahme zu sichern. Dies verlangen bereichsspezifische Vorschriften wie § 78 a Sozialgesetzbuch Zehntes Buch (SGB X) oder allgemeines Datenschutzrecht wie § 21 Abs. 2 Nr. 1 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V). Ausgesonderte Akten und Datenträger sind demnach bis zum Abschluss der Vernichtung vor unbefugtem Lesen und Kopieren zu schützen. Wird eine andere Stelle mit der Vernichtung beauftragt, so bleibt der Auftraggeber dennoch für die ordnungsgemäße Löschung der Daten verantwortlich. So regeln es beispielsweise § 80 SGB X oder § 4 DSG M-V. Der Auftraggeber muss sich vor der Auftragserteilung davon überzeugen, dass der Auftragnehmer die datenschutzrechtlichen Vorschriften einhält. Auch während der Vertragslaufzeit muss der Auftraggeber dies kontrollieren können.

Um die Leistungsfähigkeit potenzieller Auftragnehmer beurteilen zu können, ist es empfehlenswert, sich an Bewertungen unabhängiger Dritter zu orientieren. § 5 Abs. 2 DSG M-V sieht mit dem Datenschutzaudit eine solche Zertifizierung vor. Dieses Zertifikat könnte sogar als Entscheidungskriterium bei der Auswahl eines Dienstleisters herangezogen werden. Allerdings ist die Landesregierung nach wie vor der Auffassung, dass in Mecklenburg-Vorpommern kein Bedarf für solch ein Gütesiegel besteht, und hat bisher die dazu erforderliche Rechtsverordnung nicht erlassen. Somit sind Produktaudits auf dieser Basis noch immer nicht möglich (siehe auch Punkt 2.15.1).

Als Anhaltspunkt kann deshalb ein Gütesiegel des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein herangezogen werden, ebenso ein Zertifikat des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Manche Betriebe lassen von unabhängigen Prüfstellen wie dem TÜV untersuchen, ob sie die Bestimmungen des § 9 Bundesdatenschutzgesetz (BDSG) einhalten. Die Zertifizierung nach der Entsorgungsfachbetriebeverordnung sagt hingegen nichts über die Datenschutzkonformität aus. Dies gilt zwar grundsätzlich auch für die Qualitätsmanagement-Normen ISO 9001/9002. Jedoch ist ein funktionierendes Qualitätsmanagement für die Einhaltung des Datenschutzes in einem Entsorgungsunternehmen zumindest förderlich.

Die technischen Anforderungen an den Vernichtungsprozess sollten anhand der Norm DIN 32757 Teil 1 festgelegt werden. Für personenbezogene Daten ist mindestens Sicherheitsstufe 3 erforderlich. Besonders sensible Daten sollten nach den Sicherheitsstufen 4 oder 5 vernichtet werden.

Die datenschutzgerechte Entsorgung geringer Mengen an Datenträgern und Schriftgut ist oft sehr teuer. Passende Sammelcontainer oder das Vernichten vor Ort lohnen oft nur für größere Einrichtungen wie Krankenhäuser. Daher sollten Organisationen wie die Kassenärztliche Vereinigung prüfen, ob sie Datenträger und Schriftgut nicht zentral sammeln, sicher zwischenlagern und dann datenschutzgerecht mit einer mobilen Entsorgungsanlage vernichten lassen.

2.9 Gesundheitswesen

2.9.1 Aufbewahrung von Patientenakten geregelt - Änderung des Heilberufsgesetzes

In meinem Sechsten Tätigkeitsbericht habe ich im Abschnitt 2.12.8 darüber berichtet, dass vor allem in den neuen Bundesländern vermehrt Arztpraxen geschlossen werden, ohne dass es einen Praxisnachfolger gibt. Für die Ärzte stellt sich mit der Praxisauflösung auch die Frage, wohin mit den Patientenunterlagen.

Nach der Berufsordnung für die Ärztinnen und Ärzte Mecklenburg-Vorpommern ist der Arzt verpflichtet, die Patientenunterlagen zehn Jahre nach Abschluss der Behandlung aufzubewahren. Er hat auch dafür zu sorgen, dass Patienten nach Schließung der Praxis ihre Krankenunterlagen innerhalb dieser gesetzlichen Aufbewahrungsfristen einsehen und Kopien erhalten können.

Bisher war es so, dass der Arzt eine Lösung zur Aufbewahrung seiner Unterlagen finden musste. Da dies von den Ärzten häufig nicht zu leisten war, hatte ich seinerzeit das Ministerium für Soziales und Gesundheit unseres Landes gebeten, sich für eine einheitliche Regelung einzusetzen. Ein Handlungsbedarf wurde zum damaligen Zeitpunkt jedoch nicht gesehen.

Mit dem Entwurf eines „Zweiten Gesetzes zur Änderung des Heilberufsgesetzes“ wurde dieses Problem nun gelöst. Danach sind die Kammern verpflichtet, Patientenunterlagen ihrer Mitglieder für die Dauer der Aufbewahrungspflicht in Obhut zu nehmen und den Patienten Einsicht zu gestatten, sofern Aufbewahrung und Einsichtnahme nicht durch die niedergelassenen Kammermitglieder oder auf andere Weise gewährleistet ist. Die Kammern können ein Kammermitglied mit der Erfüllung dieser Aufgabe betrauen.

Diese klarstellende Regelung gewährleistet, dass Patientenunterlagen sicher verwahrt werden und Patientinnen und Patienten ihre Rechte wahrnehmen können.

2.9.2 Wechselnde Zuständigkeiten im Schlichtungsverfahren

Im Januar 2006 erhielt ich Kenntnis davon, dass eine Frau aus Niedersachsen ein Schlichtungsverfahren wegen eines vermuteten Behandlungsfehlers an ihrer Mutter in einer Klinik beantragt hat. Dazu hatte sie einen Fragebogen ausgefüllt und diesen mit umfangreichen behandlungsbezogenen Unterlagen an die Schlichtungsstelle gesandt. Die Schlichtungsstelle gab diese Unterlagen direkt an den Beschwerdegegner und dessen Haftpflichtversicherer weiter.

Es entwickelte sich hierzu ein längerer Schriftwechsel, da nach der Verfahrensordnung der Schlichtungsstelle neun Ärztekammern, darunter auch die Ärztekammer Mecklenburg-Vorpommern, eine Arbeitsgemeinschaft gebildet haben. Deren Aufgabe ist es, in Arzthaftpflichtfragen zu schlichten. Die Schlichtungsstelle schließt ein Verfahren mit einem Schlichtungsvorschlag ab (§ 5 Verfahrensordnung). Wegen der jährlich wechselnden Außenvertretung wurde der Vorgang mit der Jahreswende auf die Ärztekammer Mecklenburg-Vorpommern übertragen. Damit war die dritte Ärztekammer und mit meiner Dienststelle auch der dritte Landesbeauftragte für den Datenschutz mit derselben Sache befasst.

Die Schlichtungsstelle hat die Übermittlung der Behandlungsunterlagen an den Beschwerdegegner (Klinik) damit begründet, dass die Patientin mit ihrem Anliegen, den Sachverhalt zu prüfen, und mit der Zusendung der Unterlagen ihre Zustimmung gegeben hätte.

Aus datenschutzrechtlicher Sicht war die Übermittlung der Behandlungsunterlagen nicht zulässig, da noch nicht feststand, ob beide Seiten mit einem Schlichtungsverfahren einverstanden sind. Ich habe die Schlichtungsstelle daher darauf hingewiesen, dass sie in einem ersten Schritt zunächst hätte feststellen müssen, ob beide Parteien mit einem Schlichtungsverfahren einverstanden sind. Erst wenn dies feststeht, können die hierfür erforderlichen Unterlagen weitergegeben werden. Dieses Vorgehen entsprach im Übrigen auch den im Internet veröffentlichten Verfahrensbestimmungen der Schlichtungsstelle. Im Interesse der Petentin sowie künftiger Antragsteller habe ich auch vorgeschlagen, entsprechende Beschwerden ausschließlich durch eine Schlichtungsstelle bearbeiten zu lassen.

Eine abschließende Antwort liegt mir bis heute nicht vor. Die Ärztekammer Mecklenburg-Vorpommern hat mir mitgeteilt, dass meine Empfehlung im Gremium der Gesellschafter der Schlichtungsstelle beraten wird. Sobald sich die Gesellschafterversammlung mit dieser Frage befasst hat, werde ich über ihren Standpunkt informiert.

2.9.3 Notrufaufzeichnungen: Wer hört mit?

Ich wurde darüber informiert, dass im Zusammenhang mit einer Disziplinarmaßnahme die Aufzeichnung eines Notrufes mehreren Personen vorgespielt wurde, die mit dieser Angelegenheit zum Teil nicht befasst waren.

Vom dienstlichen Vorgesetzten erhielt ich die Auskunft, dass ein Disziplinarverfahren eingeleitet wurde, da nach einem Notruf die hilfebedürftige Person verstorben sei, weil der Mitarbeiter der Rettungsleitstelle nicht angemessen reagiert habe. In diesem Zusammenhang wurde der Mitschnitt neben den Fachvorgesetzten auch auf den privaten Laptop des leitenden Notarztes überspielt, der zu diesem Vorfall eine fachliche Stellungnahme abgeben sollte. Der leitende Notarzt hatte die Aufzeichnung dann einem Familienangehörigen vorgespielt.

Die Übermittlung der Tonbandaufzeichnung an Fachvorgesetzte, die Fachaufsicht und dem Mitarbeiter der Personalverwaltung ist aus datenschutzrechtlicher Sicht nicht zu beanstanden, denn nach den Bestimmungen des Landesdatenschutzgesetzes (§ 7 Abs. 1 Nr. 1 DSG M-V) dürfen personenbezogene Daten verarbeitet werden, wenn unter anderem die Vorschriften des DSG M-V es zulassen. Danach dürfen personbezogene Daten, die für andere Zwecke erhoben oder erstmals gespeichert worden sind, unter anderem zu Zwecken der Ausübung von Aufsichts- und Kontrollbefugnissen oder auch für Ausbildungszwecke in dem dafür erforderlichen Umfang genutzt werden, § 14 Abs. 1 i. V. m. § 10 Abs. 4 DSG M-V. Diese Vorschrift erlaubt somit eine Nutzung personenbezogener Daten durch Vorgesetzte bzw. eine Weitergabe an diese. Unter den Begriff Aufsicht fallen sowohl die Fach- und Rechtsaufsicht als auch die Dienstaufsicht.

Für das Überspielen des Notrufes auf den privaten Laptop war jedoch keine rechtliche Grundlage vorhanden, sodass dies nicht zulässig war. Ich habe daher gefordert, den Mitschnitt umgehend zu löschen. Des Weiteren sollten die Mitarbeiter darauf hingewiesen werden, dass für die Verarbeitung von personenbezogenen Daten für dienstliche Zwecke keine privaten Rechner genutzt werden dürfen, weil hier, wie der Vorfall zeigt, das Datengeheimnis nicht immer gewahrt bleibt. Ich habe auch vorgeschlagen, in ähnlichen Fällen zunächst zu prüfen, ob der Zweck auch mit anonymisierten oder pseudonymisierten Daten erfüllt werden kann. Beispielsweise könnte anstelle der Tonbandaufzeichnung ein Gesprächsprotokoll ohne personenbezogene Daten genutzt werden. Nur wenn die nonverbalen emotionalen Informationen eines Notrufes zur Prüfung erforderlich sind, kann eine Tonbandaufzeichnung genutzt werden; in diesem Fall allerdings mit anonymisierten Daten.

Meine Empfehlungen wurden umgehend umgesetzt. Um Rechtssicherheit für alle Mitarbeiter zu gewährleisten, empfiehlt es sich, technische und organisatorische Maßnahmen zum Umgang mit personenbezogenen Daten in einer Dienstanweisung zu regeln.

2.9.4 Datenschutzrechtliche Fragen beim Mammographiescreening

In Mecklenburg-Vorpommern haben inzwischen alle Screening-Einheiten ihren Betrieb aufgenommen, sodass nach und nach alle Frauen zwischen 50 und 69 Jahren zum Mammographie-Screening eingeladen werden. Der Medizinische Dienst der Krankenversicherung (MDK) verschickt in seiner Funktion der „Zentralen Stelle für das Einladungswesen Mammographie-Screening“ die Einladungen und überwacht die Teilnahme. Um beurteilen zu können, ob den Anforderungen des Datenschutzes Rechnung getragen wird, habe ich mir im Berichtszeitraum das Verfahren beim MDK und bei einer Screening-Einheit angesehen.

Zur Pseudonymisierung der Identitätsdaten aller Frauen ist die Bildung einer Screening-Identitätsnummer (Screening-ID) vorgeschrieben. Die Qualität dieser Nummer entsprach jedoch nicht den Vorgaben der Krebsfrüherkennungsrichtlinie vom 15. Dezember 2003. Dies hat zur Folge, dass die in den Einladungslisten gespeicherten personenbezogenen Daten nicht durch das nach den Richtlinien zu verwendende Pseudonym, die Screening-ID, ersetzt werden können. Außerdem müssen dadurch Widersprüche von Frauen gegen das Mammographie-Screening personenbezogen für die Dauer der Anspruchsberechtigung gespeichert werden, wenn keine den Vorgaben entsprechende Nummer gebildet wird.

Um Lösungen für ein datenschutzkonformes Screening zu finden, wurden die offenen Fragen mit den beteiligten Stellen beraten. Im Ergebnis wurde eine richtlinienkonforme Bildung der Screening-ID zugesagt. Sobald eine solche Screening-ID durch die geänderte Software gebildet werden kann, würde auch das Datenmanagement richtlinienkonform gestaltet werden können. Es werden dann nur noch die Screening-ID und die Teilnahmeinformation pseudonymisiert gespeichert.

Ferner verlangt die Krebsfrüherkennungsrichtlinie, dass die beim Screening erhobenen Daten getrennt von den im Rahmen von Heilbehandlungen anfallenden Daten verarbeitet werden. Diese Regelung wird bisher in der von mir kontrollierten Screening-Einheit missachtet.

Bei den Beratungen musste ich außerdem feststellen, dass zentrale IT-Sicherheitsfragen bisher unzureichend gelöst sind. Die Software zur Unterstützung des Mammographie-Screenings, Mammasoft, wird von der Kassenärztlichen Vereinigung Bayern (KVB) entwickelt und betrieben. Der MDK tritt zwar gegenüber der KVB als Auftraggeber auf, konnte dieser Verantwortung aber bisher nicht in vollem Umfang gerecht werden. So wurden Berechtigungen für Mitarbeiterinnen und Mitarbeiter der einladenden Stelle „auf Zuruf“ eingerichtet. Die Dokumentation und Freigabe von Verfahrensänderungen war ebenfalls verbesserungswürdig. Ein IT-Sicherheitskonzept existiert zwar, ist aber kein Vertragsbestandteil und somit unverbindlich. Die Programmverantwortlichen Ärztinnen und Ärzte sowie die Screeningeinheiten waren über die Sicherheitseigenschaften von Mammasoft nur unzureichend informiert, sodass sie zum Teil nicht wissen, wie sie Mammasoft sicher in ihre bereits vorhandene Technik integrieren können. Mir wurde zugesagt, dass diese Probleme bis spätestens Frühjahr 2008 gelöst werden.

Darüber hinaus gibt es noch Mängel beim Betrieb des zentralen Zugangs für die Screening-Einheiten des Landes zum KV-Safenet. Das KV-Safenet ist ein kryptographisch gesichertes Virtuelles Privates Netz, welches der Übertragung medizinischer Daten dient. Zum Betrieb von Mammasoft ist ein Zugang zum KV-Safenet unabdingbar. Nach wie vor existiert keine Vereinbarung zwischen der Universität, die den Netzknoten betreut, und dem Unternehmen, das KV-Safenet betreibt, welche den Anforderungen an die Datenverarbeitung im Auftrag genügen würde. Dieser Zustand ist unhaltbar und muss beendet werden. Ich werde weiter darauf dringen, dass die vorgegebenen und datenschutzrechtlich erforderlichen Regelungen umgesetzt werden.

2.9.5 Datenschutz im Krankenhaus

Im Krankenhaus werden wie in kaum einer anderen sozialen Institution sensible persönliche Daten verarbeitet (erhoben, übermittelt und gespeichert). Im Berichtszeitraum habe ich daher die Einhaltung der datenschutzrechtlichen Bestimmungen in verschiedenen Krankenhäusern in Mecklenburg-Vorpommern geprüft.

Rechtsgrundlage für den Umgang mit Patientendaten sind insbesondere die datenschutzrechtlichen Regelungen im Landeskrankenhausgesetz für das Land Mecklenburg-Vorpommern (LKHG M-V) sowie die in § 203 Strafgesetzbuch normierte ärztliche Schweigepflicht. Im Ergebnis meiner Besuche habe ich festgestellt, dass die Bestimmungen des LKHG M-V nicht immer vollständig umgesetzt waren. Hier einige Beispiele:

Wird ein Patient aus dem Krankenhaus entlassen und ist das Behandlungsentgelt von der Krankenkasse oder dem Patienten bezahlt worden, gilt eine Behandlung als abgeschlossen. Damit sind die Daten gemäß § 19 LKHG M-V zu sperren und spätestens nach Ablauf von 30 Jahren zu löschen. Werden die Daten gesperrt, so sind diese nach den Vorschriften im LKHG M-V gesondert zu speichern. Dies bedeutet auch, dass die Daten für die regelmäßige Verarbeitung im Krankenhausinformationssystem nicht mehr zur Verfügung stehen. Diese Rechtsvorschrift war in den Krankenhäusern nicht umgesetzt. Ich habe daher empfohlen, eine den gesetzlichen Vorgaben entsprechende Sperrfunktion ins Krankenhausinformationssystem aufzunehmen.

Die Archivierung von Patientenakten entspricht nicht immer den datenschutzrechtlichen Anforderungen. Nach dem LKHG M-V sind Patientenakten im Krankenhaus so zu archivieren, dass es anderen Mitarbeitern nicht ohne Weiteres möglich ist, die Akten allein mit Kenntnis von Namen, Vornamen und Geburtsdatum zu erschließen. Jedoch wurden beispielsweise in einem Krankenhaus die Patientenakten genau nach diesen Ordnungsmerkmalen, das heißt nach dem Geburtsdatum und bei gleichem Geburtsdatum alphabetisch nach Namen, archiviert. Wie die Bestimmungen des LKHG M-V adäquat umgesetzt werden können, habe ich dann in einem anderen Krankenhaus gesehen. Hier wurde die Verbindung zu einem Behandlungsfall über eine aktenbezogene Identifikationsnummer (ID) hergestellt. Diese ID wird bei Akteneingang ins Archiv vergeben. Die Zuordnung zwischen dem Namen des Patienten und der Archiv ID ist nur dem Archivpersonal und eingeschränkt der Abteilung Notaufnahme/Rettungsstelle mit Hilfe eines entsprechenden Anwendungsprogrammes möglich.

Patientendaten, die im Krankenhaus verarbeitet werden, sind umfassend gegen zweckentfremdete und unzulässige Nutzung geschützt. So können diese Daten zum Beispiel nicht beschlagnahmt werden, § 97 Abs. 2 Strafprozessordnung. Sollte es im Einzelfall dennoch erforderlich sein, die Daten durch eine Stelle außerhalb des Krankenhauses verarbeiten zu lassen, bleibt das Krankenhaus dafür verantwortlich, dass die Verarbeitung entsprechend den gesetzlichen Bestimmungen gemäß § 21 LKHG M-V erfolgt und die datenschutzrechtlichen Bestimmungen eingehalten werden. Ansprüche der Patienten, die sich aus der Verarbeitung ihrer personenbezogenen Daten ergeben, beispielsweise Berichtigung, Löschung und Sperrung der Daten, sind gegen das Krankenhaus zu richten. Das Krankenhaus hat daher bei der Auswahl eines geeigneten Auftragnehmers darauf zu achten, dass dieser in der Lage ist, die hohen Anforderungen, die an die Verarbeitung von Patientendaten gestellt werden, zu erfüllen. Das Krankenhaus hat den Auftrag schriftlich zu erteilen. In dem Vertrag sind die Verantwortungsbereiche von Auftragnehmer und Auftraggeber abzugrenzen, Art, Umfang und Dauer der Verarbeitung sind zu regeln und die vom Auftragnehmer zu treffenden allgemeinen und speziellen Sicherungsmaßnahmen nach §§ 21 und 22 DSG M-V sind hier ebenfalls festzulegen. Der Auftragnehmer darf die ihm überlassenen Patientendaten nur im Rahmen des Auftrages und der Weisung des Krankenhauses verarbeiten. Geht der Auftragnehmer über die vertraglichen Weisungen hinaus, handelt er unbefugt, was Schadensersatzansprüche oder die Beendigung des Vertrages zur Folge haben kann.

Bei meinen Kontrollen habe ich festgestellt, dass einige Verträge mit Dienstleistern nicht vollständig den Vorschriften zur Datenverarbeitung im Auftrag entsprachen und daher zu überarbeiten waren. Einen „Mustervertrag zur Verarbeitung personenbezogener Daten im Auftrag“ habe ich auch in meinem Internetangebot www.datenschutz-mv.de veröffentlicht.

2.9.6 Unfallkasse erhebt Daten bei Krankenkasse ohne Kenntnis der Betroffenen

Eine Anwältin schilderte mir, dass ihre Mandantin im Gebäude ihres Arbeitgebers von der Treppe gestürzt sei und um Anerkennung dieses Unfalls als Arbeitsunfall mit der Unfallkasse Mecklenburg-Vorpommern streite. Die Anwältin hatte in diesem Zusammenhang bei der Unfallkasse Einsicht in die Unterlagen ihrer Mandantin genommen. Dabei ist ihr ein an die Unfallkasse gerichtetes Schreiben der Krankenkasse ihrer Mandantin zur Kenntnis gelangt, in dem ein Auszug aus dem Leistungsverzeichnis über alle Erkrankungen für die gesamte Zeit ihrer Mitgliedschaft enthalten war. Die Anwältin hat mich gebeten, den Sachverhalt datenschutzrechtlich zu prüfen.

Ich habe mich bei der Unfallkasse erkundigt, warum die Anfrage an die Krankenkasse nicht auf solche Erkrankungen beschränkt worden sei, die mit dem Versicherungsfall in einem ursächlichen Zusammenhang stehen, § 188 Satz 2 Sozialgesetzbuch Siebtes Buch (SGB VII).

Die Unfallkasse hat dazu mitgeteilt, dass dies im Regelfall so gehandhabt werde. Jedoch handele es sich um eine „Soll-Vorschrift“, von der im Ausnahmefall abgewichen werden könne. Im vorliegenden Fall sei dies erfolgt, da das Krankheitsbild der Betroffenen eine solche Einschränkung nicht zuließ. Es ging gerade darum, auf der Basis des Vorerkrankungsverzeichnisses ein Zusammenhangsgutachten erstellen zu lassen. Zu diesem Zweck benötige ein begutachtender Arzt die Angaben.

Diese Argumentation war für mich nachvollziehbar. Allerdings hätte die Unfallkasse die betroffene Person auch darüber informieren müssen, dass ihr gegen eine solche Datenübermittlung ein Widerspruchsrecht zusteht. Dies wurde hier versäumt, was die Unfallkasse bedauerte. Um solche Versäumnisse künftig auszuschließen, wurde der Sachverhalt mit allen Mitarbeitern ausgewertet.

Über das Ergebnis habe ich die Anwältin informiert und mich für ihren Hinweis bedankt, der dazu beigetragen hat, dass die Unfallkasse Mecklenburg-Vorpommern künftig die Hinweispflichten beachten wird.

2.9.7 Krankenkasse will Daten ihres Versicherten bei einer Universität erheben

Ich wurde darüber informiert, dass eine Krankenkasse bei einer Universität die Zahl des Fachsemesters eines Studenten erheben will, der bei ihr versichert ist. Sie hatte nach ihrer Darstellung bereits mehrfach erfolglos versucht, die erforderlichen Daten beim Betroffenen zu erheben. Die Krankenkasse stützte ihr Auskunftsersuchen auf § 67 a Abs. 2 Satz 2 Nr. 2 baa) Sozialgesetzbuch Zehntes Buch (SGB X). Der Datenschutzbeauftragte der Universität wollte nun von mir wissen, ob die Universität zur Auskunft verpflichtet sei.

Die von der Krankenkasse angeführte Rechtsvorschrift erlaubt die Datenerhebung bei anderen Personen und Stellen ohne Mitwirkung des Betroffenen, wenn die Aufgaben nach dem Sozialgesetzbuch ihrer Art nach diese Erhebung erforderlich machen und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Diese Voraussetzungen waren hier jedoch nicht erfüllt. Die Krankenkasse wollte prüfen, ob die Voraussetzungen für die Studentenkrankenversicherung fortbestehen. Dies war aus meiner Sicht keine Aufgabe, die ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich macht.

Die Krankenkasse ist hinsichtlich der Prüfung, ob die Studentenkrankenversicherung fortbestehen kann, vielmehr an die Mitwirkung des Betroffenen gebunden. Die Mitwirkungspflichten sind in den §§ 60 bis 62 und 65 Sozialgesetzbuch Erstes Buch (SGB I) normiert. Danach ist derjenige, der Sozialleistungen beantragt oder erhält, verpflichtet, alle Tatsachen anzugeben, die für die Leistung erheblich sind. Kommt der Betroffene dieser Pflicht nicht nach, hat der Sozialleistungsträger darüber hinaus die Möglichkeit, die Leistung ganz oder teilweise zu versagen, § 66 SGB I. Allerdings dürfen die Leistungen erst entzogen oder versagt werden, wenn der Betroffene schriftlich auf seine Mitwirkungspflichten hingewiesen worden ist und sie nicht erfüllt hat. Die von der Krankenkasse angeführte Norm ist jedenfalls keine Rechtsgrundlage, nach der eine Erhebung bei der Universität zulässig wäre.

Meine rechtliche Bewertung habe ich dem Datenschutzbeauftragten der Universität mitgeteilt und empfohlen, die erbetenen Daten nicht an die Krankenkasse zu übermitteln.

2.9.8 AGnES

Der demographische Wandel wirkt sich auch auf das Gesundheitswesen aus. So zeichnet sich in Mecklenburg-Vorpommern ab, dass viele ältere Ärzte ihre Praxis aufgeben, ohne dass ein Nachfolger die medizinische Versorgung der Patienten übernimmt. Gerade in Gebieten mit einer geringen Bevölkerungsdichte müssen deshalb neue Wege in der ärztlichen Betreuung gegangen werden. Einen sehr wesentlichen Baustein dazu hat das Institut für Community Medicine der Ernst-Moritz-Arndt-Universität Greifswald entwickelt. Das Projekt trägt die Bezeichnung AGnES und wird gegenwärtig erprobt. AGnES steht für **A**rztentlastende **G**emeinde**n**ahe **E**-Health gestützte **S**ystemische Intervention.

Das Institut für Community Medicine hat mich frühzeitig in die Entwicklung des Projektes einbezogen und das Datenschutz- und Datensicherheitskonzept zur Begutachtung zugesandt. Ziel des Projektes ist die Entlastung des Hausarztes durch eine Telegesundheitsschwester, die die Patienten zu Hause aufsucht und Leistungen für den Arzt erbringt. Der Versorgungsradius des Hausarztes soll dadurch vergrößert werden. Die Telegesundheitsschwester handelt dabei auf Anweisung des Hausarztes. Patienten können bei bestimmten Krankheitsbildern, die eine intensive medizinische Betreuung erfordern, auf freiwilliger Basis an dieser Versorgungsform teilnehmen und jederzeit ihre Teilnahmebereitschaft widerrufen. Bei den teilnehmenden Patienten werden sogenannte Telecaregeräte installiert, mit denen sie ihre gesundheitlichen Parameter selbstständig messen und an die Hausarztpraxis übermitteln können. Damit ist der Hausarzt in der Lage, den Gesundheitszustand seiner Patienten kontinuierlich zu überwachen und rechtzeitig geeignete therapeutische Maßnahmen zu veranlassen, wenn sich der Zustand verschlechtert. Der Arzt kann somit trotz großer Entfernung zwischen Praxis und Wohnort eine große Zahl von Patienten betreuen, wobei die Telegesundheitsschwester regelmäßig die Patienten besucht und sie auch bei der Handhabung der Telecaregeräte berät und unterstützt. Die Telecaregeräte bestehen im Wesentlichen aus 12-Kanal-EKG-Geräten, Waagen und Blutdruckmessgeräten sowie aus Geräten zur Blutzucker- und Augeninnendruckmessung. Damit können vor allem Patienten mit Herzrhythmusstörungen, Herzinsuffizienz und Diabetes mellitus betreut werden.

Die wesentliche datenschutzrechtliche Grundlage für die Verarbeitung der Daten innerhalb des Projektes AGnES ist die freiwillige Teilnahme der Hausärzte sowie weiterer Angehöriger von Heilberufen, wie Apotheker und Krankenschwestern, sowie die freiwillige Teilnahme der Patienten einschließlich ihrer umfassenden Aufklärung, auch über die begleitende Forschung. Im Mittelpunkt meiner datenschutzrechtlichen Beratung standen daher technische Maßnahmen zur Gewährleistung der Datensicherheit, insbesondere bei der Übertragung der Daten aus der Häuslichkeit des Patienten an den Arzt und an den Forschungsbereich. Für Forschungszwecke werden pseudonymisierte Daten der Teilnehmer verarbeitet. Die Datenübertragung ist sowohl per Tabletpersonalcomputer (Tablet-PC) der Telegesundheitsschwester, die die Daten beim Patienten erfasst beziehungsweise von ihm übernimmt und sie anschließend in der Arztpraxis auf das dortige Computersystem überspielt, als auch per Internet über eine Virtual-Private-Network-Verbindung (VPN-Verbindung) vorgesehen. Auch bei der Übermittlung der Daten per Tablet-PC habe ich empfohlen, sie zu verschlüsseln, um bei einem Verlust des Computers zu verhindern, dass die Gesundheitsdaten der Patienten von Dritten zur Kenntnis genommen werden können. Bei einer Datenübermittlung über das Internet ist eine Verschlüsselung selbstverständlich. Außerdem kann durch eine Verschlüsselung mit einer entsprechenden Schlüsselverwaltung die Integrität und Authentizität der Daten gesichert werden. Die Schlüsselverwaltung umfasst dabei die Erzeugung, Beglaubigung, Verteilung, Gültigkeitsprüfung, Speicherung und gegebenenfalls Vernichtung von kryptographischem Material. An den jeweiligen Schnittstellen der Praxisinformationssysteme müssen darüber hinaus Vorkehrungen getroffen sein, um Manipulationsversuche wirksam zu unterbinden (z. B. Firewall). Meine Empfehlungen sind berücksichtigt worden.

Inzwischen ist über AGnES auch in den überregionalen Medien sehr positiv berichtet worden. AGnEs soll auch in anderen Bundesländern eingesetzt werden.

2.10 Personalwesen

2.10.1 Travel-Management-System

Die Landesregierung möchte künftig vielen Bediensteten ermöglichen, Dienstreisen auf elektronischem Wege am eigenen Arbeitsplatz zu organisieren und zu beantragen. In die Planungen des dafür erforderlichen Travel-Management-Systems des Landes (TMS M-V) bin ich seit 2004 einbezogen. Ich erhielt beispielsweise die Entwürfe von Dienstvereinbarungen, Sicherheitskonzepten und Verträgen zur Auftragsdatenverarbeitung, sodass ich frühzeitig Empfehlungen zur datenschutzgerechten Ausgestaltung des Verfahrens geben konnte.

Mit einer Änderung des Landesreisekostengesetzes (LRKG M-V) sollte im Dezember 2006 nun auch der rechtliche Rahmen für die Einführung des TMS M-V geschaffen werden. Insbesondere sollen künftig Genehmigungen auch elektronisch erteilt werden können. Da eine Genehmigung bisher der Schriftform bedurfte, ist somit für die elektronische Variante der Einsatz der qualifizierten elektronischen Signatur erforderlich (siehe auch Punkt 2.15.2). Auf die besondere datenschutzrechtliche Relevanz dieser Signatur als Ersatz der handschriftlichen Unterschrift habe ich bereits in meinem Sechsten Tätigkeitsbericht hingewiesen (siehe dort Punkt 2.16.3).

In den gemeinsamen Beratungen mit dem Finanzministerium zur Einführung des TMS M-V habe ich folgerichtig den Einsatz qualifizierter Signaturen gefordert. Das Ministerium sah zunächst jedoch keine Möglichkeit, alle PC-Arbeitsplätze der künftigen Antragsteller mit der hierfür notwenigen Infrastruktur (z. B. Kartenleser, Signaturkarten) auszustatten, und schlug stattdessen vor, mit einer entsprechenden Ergänzung des LRKG M-V die Vorschrift des Landesverwaltungsverfahrensgesetzes, die die qualifizierte Signatur fordert, für nicht anwendbar zu erklären.

Der Verzicht auf die qualifizierte elektronische Signatur hätte jedoch zur Folge, dass Antragsteller im Zweifelsfall die Echtheit einer Dienstreisegenehmigung nicht beweisen könnten. Es liegt auf der Hand, dass dies für die Betroffenen im Einzelfall erhebliche Nachteile haben kann. Zudem widerspricht das weniger sichere Verfahren auch klar den Modernisierungsbestrebungen, welche die Landesregierung in ihrem E-Government-Masterplan formuliert hat (siehe Sechster Tätigkeitsbericht, Punkt 2.16.4). Eine zentrale Forderung dort ist die Einführung und Nutzung der Basiskomponente Signatur/Verschlüsselung.

Das Finanzministerium konnte meine Bedenken nachvollziehen. Da es das elektronische Antragsverfahren datenschutzgerecht ausgestalten wollte, wurde im Ergebnis der folgende Kompromissvorschlag unterbreitet:

Auf die qualifizierte Signatur der zur Unterschrift berechtigten oder verpflichteten Personen wird zunächst verzichtet. Stattdessen soll die Integrität und Authentizität der betreffenden Dokumente durch eine Kombination aus Nutzerkennung/Passwort dieser Personen und einer Stapelsignatur durch die zuständige Landesbehörde sichergestellt werden. Die Stapelsignatur ist eine besondere Form der qualifizierten elektronischen Signatur, bei der automatisch eine Vielzahl von Dokumenten mit einer einzigen Signaturkarte signiert wird. Auf diese Weise können die rechtlichen Voraussetzungen geschaffen werden, die der qualifizierten elektronischen Signatur durch die genannten Personen sehr nahe kommen, und die spätere Migration zu einem Verfahren mit persönlichen qualifizierten Signaturen wird ermöglicht.

Ich habe diesem Kompromiss, mit dem meine Empfehlungen zumindest teilweise umgesetzt werden können, mit der Maßgabe zugestimmt, dass auch weiterhin die flächendeckende Verfügbarkeit von Kartenlesern und Signaturkarten angestrebt wird. Das oben beschriebene und nunmehr auch in der Begründung zum LRKG M-V skizzierte Verfahren kann nur als Übergangslösung angesehen werden.

14. Ich empfehle der Landesregierung, die flächendeckende Verfügbarkeit von Kartenlesern und Signaturkarten für die qualifizierte elektronische Signatur voranzutreiben und somit die Basiskomponente Signatur/Verschlüsselung des E-Government-Masterplans umzusetzen.

2.10.2 Datenschutzrechtliche Fragen im Rahmen des betrieblichen Eingliederungsmanagements

Aufgrund einer Anfrage eines öffentlich-rechtlichen Arbeitgebers habe ich mich im Berichtszeitraum mit dem im Gesetz zur Förderung der Ausbildung und Beschäftigung schwerbehinderter Menschen in § 84 Sozialgesetzbuch Neuntes Buch (SGB IX) eingeführten betrieblichen Eingliederungsmanagement (BEM) befasst. Arbeitgeber haben das BEM jedem Beschäftigten, der innerhalb eines Jahres länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig war, anzubieten. Ziel ist es, durch geeignete Gesundheitsprävention das Arbeitsverhältnis möglichst dauerhaft zu sichern und eine Entlassung zu vermeiden. Der Personalrat ist nach § 84 Abs. 2 Satz 7 SGB IX verpflichtet, darauf zu achten, dass der Arbeitgeber dieser gesetzlichen Pflicht nachkommt. In diesem Zusammenhang gab es unterschiedliche Auffassungen, welche personenbezogenen Daten der Beschäftigten dem Personalrat zu übermitteln sind.

Nach dem Urteil des Verwaltungsgerichtes Hamburg vom 10. November 2006, 23 FB 17/06, und einem Gespräch mit dem Personalrat habe ich die Übermittlung der Namen der für das BEM infrage kommenden Beschäftigten auch ohne Einwilligung als zulässig bewertet. Als Rechtsgrundlage kommt nach meiner Auffassung § 35 Abs. 1 Landesdatenschutzgesetz (DSG M-V) in Verbindung mit § 84 Abs. 2 SGB IX in Betracht. Nach § 35 DSG M-V dürfen öffentliche Stellen Daten ihrer Beschäftigten nur verarbeiten, wenn dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung innerdienstlicher organisatorischer, sozialer und personeller Maßnahmen erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung es vorsieht.

Dem Arbeitgeber habe ich vorgeschlagen, in Stufen vorzugehen. In der ersten Stufe sollte der Arbeitgeber dem Personalrat/der Schwerbehindertenvertretung mitteilen, wie vielen Beschäftigten das BEM hätte angeboten werden müssen, wie vielen es angeboten worden ist und wie viele das Angebot angenommen haben. Wenn sich aus diesen Zahlen individueller Beratungsbedarf der Beschäftigten ergibt, sollten den Personalvertretungen auf der oben genannten Rechtsgrundlage in der zweiten Stufe die Namen der Beschäftigten, denen das BEM angeboten werden müsste, mitgeteilt werden.

Arbeitgeber und Personalvertretung müssen die Beschäftigten auf die Freiwilligkeit des BEM hinweisen. Das BEM kommt nur infrage, wenn eine Erkrankung eines Beschäftigten mit der Arbeitssphäre zusammenhängt. Erklärt ein Beschäftigter, dass die Krankheit mit dem Arbeitsplatz nicht zusammenhängt, kommt meines Erachtens kein BEM infrage.

Ich habe empfohlen, das Verfahren in einer Dienstanweisung zu regeln.

2.10.3 Behördeninterne Veröffentlichung von Personaldaten

Immer wieder erreichen mich Eingaben und Anfragen aus der Verwaltung, ob es zulässig sei, in den Personalnachrichten über Ernennungen, Höhergruppierungen, Versetzungen, Abordnungen oder Dienstjubiläen zu informieren.

Personaldaten sind grundsätzlich vertraulich zu behandeln und vor Einsicht unbefugter Personen zu schützen. Die Besonderheiten der Datenverarbeitung bei Beschäftigungsverhältnissen im Bereich der öffentlichen Verwaltung des Landes Mecklenburg-Vorpommern sind für Arbeiter und Angestellte in § 35 Landesdatenschutzgesetz (DSG M-V) und für Landesbeamte in § 100 Abs. 4 Landesbeamtengesetz (LBG M-V) geregelt. Danach dürfen öffentliche Stellen mit Daten ihrer Beschäftigten nur umgehen, wenn es zur Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung innerdienstlicher Maßnahmen erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung es vorsieht.

Informationen über Abordnungen, Versetzungen, Ausscheiden aus dem Dienstverhältnis oder bei Personalwechsel sind für die Durchführung des Dienstverkehrs erforderlich und damit nach § 35 DSG M-V bzw. § 100 LBG M-V zulässig. Die Beförderung oder Zuweisung eines neuen Amtes bei Beamten ist regelmäßig mit einer Änderung der Amtsbezeichnung verbunden, und es ist daher datenschutzrechtlich nicht zu beanstanden, wenn darüber informiert wird. Das heißt, wenn die Bekanntgabe zur Durchführung des Dienstbetriebes oder für sogenannte Organisations- und Funktionsaufgaben wie Name und Funktionsbezeichnung am Dienstzimmer notwendig ist, bestehen gegen die Veröffentlichung von Mitarbeiterdaten keine datenschutzrechtlichen Bedenken.

Bei Dienstjubiläen jedoch oder bei Geburtstagslisten, die häufig in Dienststellen verbreitet werden, sollte das Persönlichkeitsrecht der Mitarbeiter angemessen berücksichtigt werden, indem vor der Veröffentlichung eine Einwilligung der Betroffenen eingeholt wird.

Bei Veröffentlichungen von Mitarbeiterdaten in Hausmitteilungen oder im Intranet sind das Personalaktengeheimnis und der Mitarbeiterdatenschutz zu beachten.

2.10.4 Interne Veröffentlichung von Vertriebsleistungen der Mitarbeiter

Eine Sparkasse informierte mich über ihre Absicht, Leistungskennziffern von Mitarbeitern innerhalb ihres Teams zu veröffentlichen, und bat mich um datenschutzrechtliche Beratung.

Eine innerbetriebliche Veröffentlichung von Arbeitsergebnissen in sogenannten „Bestenlisten“ kann unter einer der folgenden rechtlichen Voraussetzungen zulässig sein:

- der Arbeitsvertrag sieht dies vor, § 28 Abs. 1 Satz 1 Nr. 1 Bundesdatenschutzgesetz (BDSG) oder
- die betroffenen Personen haben in die Veröffentlichung eingewilligt oder
- die Voraussetzungen des § 28 Abs. 1 Satz 1 Nr. 2 BDSG liegen vor, das heißt, der Arbeitgeber hat ein berechtigtes Interesse an der Veröffentlichung, beispielsweise um die Leistungsbereitschaft der Mitarbeiter zu fördern, und es besteht kein Grund zur Annahme, dass schutzwürdige Interessen der Betroffenen überwiegen.

Eine Veröffentlichung auf Basis der Einwilligung setzt voraus, dass sie tatsächlich freiwillig ist. Ob in einem Abhängigkeitsverhältnis von einer Freiwilligkeit ausgegangen werden kann, ist nach meiner Auffassung zweifelhaft. Daher habe ich empfohlen, die Leistungsdaten nicht auf dieser Basis zu veröffentlichen.

Aus meiner Sicht kam für beabsichtigte innerbetriebliche Veröffentlichungen die dritte Alternative in Betracht. Zur Stärkung der Leistungsbereitschaft kann es zulässig sein, Leistungsdaten zu veröffentlichen, sofern schutzwürdige Interessen der betroffenen Personen nicht entgegenstehen. Bei sehr guten und guten Leistungsdaten werden die betroffenen Mitarbeiter in der Regel kein schutzwürdiges Interesse gegen die Veröffentlichung innerhalb des Teams geltend machen. Im Einzelfall jedoch kann es einem Mitarbeiter dieser Leistungsgruppe unangenehm sein, wenn seine Ergebnisse bekannt gegeben werden. Daher habe ich empfohlen, vor der öffentlichen Leistungsauswertung jeden Mitarbeiter persönlich über sein Ergebnis zu informieren und ihm Gelegenheit zu geben, Einwände geltend zu machen. Im Falle eines Einwandes sollte das Ergebnis des Mitarbeiters nicht dem Team mitgeteilt werden.

2.11 Bildung, Kultur, Wissenschaft und Forschung

2.11.1 Videoüberwachung an Schulen

Zahlreiche Schulen in Mecklenburg-Vorpommern gehen dazu über, Videoüberwachungsanlagen zu installieren. In der Regel soll damit der Schutz gegen strafbare Handlungen, insbesondere Diebstähle und Sachbeschädigung, verbessert werden. Die datenschutzrechtlichen Bestimmungen, die beim Einsatz von Videoüberwachungsanlagen zu beachten sind, sind den Schulen häufig nicht bekannt.

Eine Videoüberwachung ist nur unter bestimmten rechtlichen Voraussetzungen erlaubt, § 37 Landesdatenschutzgesetz (DSG M-V). Danach ist sie nur zulässig, wenn sie zur Wahrnehmung des Hausrechtes erforderlich ist und keine Anhaltspunkte für überwiegend schutzwürdige Interessen der von der Videoüberwachung betroffenen Personen vorliegen. Erforderlich ist eine Videoüberwachung nur, wenn der Zweck durch andere, weniger eingreifende Maßnahmen, beispielsweise eine Hofaufsicht durch Lehrer, nicht erreicht werden kann. Kostengesichtspunkte können allenfalls in extremen Ausnahmefällen in die Bewertung mit einfließen. Dies dürfte sich mithin auf die Zeiten außerhalb des regulären Unterrichts beschränken.

Darüber hinaus verlangt das DSG M-V, dass die Überwachung durch geeignete Maßnahmen, in der Regel Hinweisschilder/Piktogramme, erkennbar zu machen ist, damit jeder frei entscheiden kann, ob er die videoüberwachte Zone betreten möchte oder nicht. Sollen auch Bilder aufgezeichnet werden, sind weitere Bestimmungen zu beachten, § 37 Abs. 2 DSG M-V. Danach darf das Bildmaterial gespeichert werden, wenn dies zur Abwendung einer konkreten Gefahr oder zu Zwecken der Beweissicherung erforderlich ist. Auch auf die Tatsache der Aufzeichnung muss durch Hinweisschilder aufmerksam gemacht werden. Die Aufzeichnungen sind spätestens nach sieben Tagen zu löschen, es sei denn, die weitere Speicherung ist zur Aufklärung oder Verfolgung der dokumentierten Vorkommnisse erforderlich. Es empfiehlt sich, dass die verantwortliche Stelle die angefallenen Aufnahmen unverzüglich einer Bedarfsprüfung unterzieht.

In den Fällen, in denen die Aufnahmen nicht mehr für die Erreichung des dokumentierten Aufnahmezwecks benötigt werden, sind sie unverzüglich zu löschen. Um Rechtssicherheit zu gewährleisten sollte daher ein Konzept zur Datensicherheit erarbeitet werden, in dem Zugriffsregelungen, Speicherdauer und Verwendungszweck geregelt sind (§ 21 DSG M-V). Auch sollten alle mit dem System betrauten Personen zum Einsatz der Videotechnik geschult werden, damit sie Schülern und Lehrern auf Nachfrage sachgerecht Auskunft geben können.

15. Ich empfehle der Landesregierung, dafür Sorge zu tragen, dass ich über jede Planung einer schulischen Videoüberwachung analog zu § 32 Abs. 3 Satz 6 DSG M-V frühzeitig unterrichtet werde.

2.11.2 Forschungsvorhaben im Bildungsbereich/Normierungsstudie VERA

Innerhalb des Berichtszeitraumes habe ich zu verschiedenen Forschungsvorhaben Stellung genommen. Bei den Beratungen ging es in erster Linie darum, eine anonyme oder pseudonyme Datenverarbeitung sicherzustellen sowie Aufklärungs- und Einwilligungstexte zu formulieren. Ich möchte dies am Beispiel des Projektes „Vergleichsarbeiten in der Grundschule (VERA)“ darstellen.

Die Schüler der 4. Klassen sollten bei diesem Projekt zum einen Aufgaben in den Fächern Mathematik und Deutsch lösen und zum anderen Fragen zur familiären Situation beantworten. Hier ist zu unterscheiden, ob schulisches Wissen abgefragt wird oder ob es sich um Angaben handelt, die der Privatsphäre zuzurechnen sind. Für die Teilnahme der Schüler an dem Mathematik- und Deutschtest ist § 39 a Abs. 5 Schulgesetz für das Land Mecklenburg-Vorpommern (SchulG M-V) die gesetzliche Grundlage. Nach dieser Vorschrift sind Schüler, Lehrer sowie schulische Mitarbeiter verpflichtet, an Tests, Befragungen, Erhebungen und Unterrichtsbeobachtungen teilzunehmen. Die Teilnahme der Schüler an diesem Teil der Befragung war somit unstrittig.

Die Schülerbefragung erhielt jedoch nicht nur Elemente mit schulischem Bezug, sondern es wurden auch Angaben erhoben, die der Privatsphäre zuzurechnen waren. Rechtsgrundlage für diesen Teil der Befragung sind die Bestimmungen in § 71 SchulG M-V in Verbindung mit § 34 Landesdatenschutzgesetz (DSG M-V). Danach soll die Verarbeitung personenbezogener Daten zu wissenschaftlichen Zwecken grundsätzlich in anonymisierter Form erfolgen. Ist dies nicht möglich, können die Daten auch in pseudonymisierter Form verarbeitet werden. Personenbezogene Daten dürfen für ein Forschungsvorhaben nur unter den engen Voraussetzungen des § 34 Abs. 2 DSG M-V verarbeitet werden.

In den Projektunterlagen wurde davon ausgegangen, dass die Daten anonymisiert verarbeitet werden. Dies entsprach dann jedoch nicht dem dargestellten Ablauf, da auf den Erhebungsbogen zum Beispiel neben einer Schülernummer auch die Klasse und die Schule anzugeben waren. Mit diesen Angaben war zumindest den Lehrern, die die Fragebögen entgegennehmen sollten, ein Personenbezug möglich. Die Daten wären jedoch erst dann anonym, wenn Schülernummer, Klasse und Schule aus dem Datensatz nicht mehr erkennbar sind. Daher habe ich vorgeschlagen, den Schülern entweder ein Kuvert mitzugeben, in das sie den Fragebogen stecken und verschlossen bei der Lehrkraft abgeben können, oder die Eltern darüber zu informieren, dass aus Gründen des Verfahrens zwar die Lehrkraft die Antworten zur Kenntnis nehmen kann, die Auswertung der Antworten durch das Forschungsinstitut jedoch anonym bzw. pseudonym erfolgt.

Darüber hinaus war vorgesehen, die Eltern auf die Freiwilligkeit der Angaben hinzuweisen. Sie sollten hier auch erklären, ob sie mit der Teilnahme ihres Kindes an der Befragung einverstanden sind oder nicht. Diese Form habe ich für ausreichend gehalten. Allerdings habe ich empfohlen, ein negatives Votum der Eltern nicht zu erfassen, sondern lediglich eine positive Meinungsäußerung festzuhalten.

Aufgrund meiner Hinweise wurden die Projektunterlagen überarbeitet, sodass nun alle Schritte der Datenverarbeitung pseudonymisiert erfolgen. Den beteiligten Schulen, Kindern und Lehrkräften werden Codenummern zugeordnet, die es ermöglichen, die verschiedenen Datenbereiche (z. B. Leistungen eines Schülers in Deutsch und in Mathematik) einander zuzuordnen, jedoch keinen Rückschluss auf die Identität der Kinder oder Lehrkräfte erlauben. Alle Unterlagen sind mit der Codenummer versehen und enthalten weder Namens- noch Ortsangaben. Für die Fragen zum persönlichen/familiären Hintergrund wird das schriftliche Einverständnis der Eltern eingeholt. Die Eltern werden auch darüber informiert, dass sie die Möglichkeit haben, die Projektunterlagen (Fragebogen) im Schulsekretariat einzusehen. Sie werden auch darüber aufgeklärt, dass die Teilnahme freiwillig ist und dass Kinder, die an der Befragung nicht teilnehmen, keine negativen Konsequenzen zu befürchten haben. So konnte durch meine rechtzeitige Beteiligung eine datenschutzrechtliche Verbesserung erreicht werden, ohne dass das Forschungsvorhaben beeinträchtigt wurde.

2.11.3 Nachweis krankheitsbedingter Prüfungsunfähigkeit durch ärztliches Attest

Ein Student machte mich auf ein Formular aufmerksam, welches Studierende beim Zentralen Prüfungsamt vorzulegen haben, wenn sie aus gesundheitlichen Gründen nicht an einer Prüfung teilnehmen, sie abbrechen oder nach Beendigung von ihr zurücktreten wollen. Der Petent hat mich gefragt, ob dieses Verlangen der Universität rechtmäßig ist.

Rechtsgrundlage für diese Datenerhebung ist die Prüfungsordnung der Universität. Wenn ein Student nicht zur Prüfung erscheint oder diese abbricht, hat er dem Zentralen Prüfungsamt die Erkrankung glaubhaft zu machen. Der Arzt muss dann zum Beispiel auf dem Formular angeben, welche körperlichen beziehungsweise psychischen Auswirkungen durch die Krankheit hervorgerufen wurden, die letztlich zu einer Prüfungsunfähigkeit geführt haben. Die Entscheidung, ob die nachgewiesene gesundheitliche Beeinträchtigung den Abbruch der Prüfung oder den Rücktritt von der Prüfung rechtfertigen, ist keine Aufgabe des Arztes, dies hat die Prüfungsbehörde in eigener Verantwortung zu entscheiden. Eine allgemeine ärztliche Bescheinigung „Prüfungsunfähigkeit liegt vor“ würde hier nicht genügen.

Das Formular selbst entsprach allerdings nicht vollständig den datenschutzrechtlichen Bestimmungen. Werden personenbezogene Daten bei den Betroffenen erhoben, so sind diese nach § 9 Abs. 3 Landesdatenschutzgesetz in geeigneter Weise über den Zweck der Erhebung sowie über die Art und den Umfang der Verarbeitung aufzuklären. Diese Aufklärung fehlte in dem Formular. Ich habe daher vorgeschlagen, den Vordruck entsprechend zu ergänzen.

In den Erläuterungen für den Arzt wurde darauf hingewiesen, dass der behandelnde Arzt erforderlichenfalls von der Schweigepflicht zu entbinden sei. Dies würde bedeuten, dass das Prüfungsamt die Daten direkt beim Arzt erheben kann. Bei diesem Verfahren ist nach meiner Auffassung nicht auszuschließen, dass das Prüfungsamt auch Informationen erhält, die für seine Entscheidung nicht erforderlich sind. Meines Erachtens sollte die Regel sein, dass der Arzt dem Studenten die ärztliche Bescheinigung übergibt und dieser dann selbst entscheidet, ob er sie dem Prüfungsamt vorlegt oder nicht.

Des Weiteren wird der Arzt in den Erläuterungen darüber informiert, dass die Diagnose selbst nicht bekannt gegeben werden muss. Deshalb habe ich empfohlen, auf diese Frage zu verzichten.

Schließlich sollte der Arzt auch angegeben, ob die Gesundheitsstörung dauerhaft oder vorübergehend ist. Da ein Antrag auf Rücktritt von der Prüfung jedoch nur Erfolg hat, wenn die Gesundheitsstörung vorübergehend ist, habe ich vorgeschlagen, die betroffenen Studenten darüber zu informieren.

Die Universität hat das Formular entsprechend meiner Hinweise überarbeitet.

2.11.4 Archivorganisation

In allen Bereichen der öffentlichen Verwaltung ist seit einiger Zeit ein Trend zur Privatisierung kommunaler Aufgaben zu verzeichnen. Im Berichtszeitraum wurde ich zum Beispiel gefragt, ob es mit den datenschutzrechtlichen Bestimmungen zu vereinbaren ist, ein Kommunalarchiv in eine Gesellschaft mit beschränkter Haftung umzuwandeln. Vor dem Hintergrund der gegenwärtigen Rechtslage bewerte ich dies folgendermaßen:
Eine Überführung der kommunalen Archive in juristische Personen des Privatrechts ist mit den Bestimmungen des Landesarchivgesetzes (LArchivG M-V) in der derzeitigen Fassung nicht zu vereinbaren. Das LArchivG M-V selbst regelt zwar nicht ausdrücklich, in welcher Rechtsform kommunale Archive zu führen sind, weist jedoch ausdrücklich darauf hin, dass es sich um öffentliche Archive und öffentliches Archivgut handelt. Auch die in § 12 LArchivG M-V getroffenen Regelungen unterstützen diese Argumentation. Hier bestimmt der Gesetzgeber, dass die kommunalen Körperschaften ihre archivrechtliche Aufgabe durch die Errichtung und Unterhaltung „eigener Archive“ zu erfüllen haben. Das mit „öffentlich“ nur „öffentlich-rechtliche“ Archive gemeint sind, geht auch aus der Gesetzesbegründung zum LArchivG M-V hervor. Hier wurde darauf hingewiesen, dass eine bereichsspezifische gesetzliche Regelung des Landesarchivwesens erforderlich geworden ist, um die Befugnis des Einzelnen zu gewährleisten, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Mit dem LArchivG M-V sollte somit das Spannungsverhältnis zwischen Informations- und Wissensfreiheit einerseits und das Persönlichkeitsrecht andererseits berücksichtigt werden.

Zu bedenken ist in diesem Zusammenhang auch, dass alle in den Unterlagen erfassten personenbezogenen Daten ursprünglich zum Zweck der Erfüllung bestimmter öffentlicher Aufgaben der Kommunen und zumeist aufgrund gesetzlicher Eingriffsbefugnisse erhoben, gespeichert und genutzt wurden. Hierzu gehören zum Beispiel Sozial-, Gesundheits-, Personal- oder Steuerdaten. Wenn diese Daten für die zu erfüllende Aufgabe nicht mehr erforderlich und die Aufbewahrungsfristen abgelaufen sind, müssen sie aus Gründen des Datenschutzes gelöscht werden. Hiervon kann nur abgesehen werden, wenn der Löschung gesetzliche Aufbewahrungsfristen, zum Beispiel im Landesarchivgesetz, entgegenstehen. Die staatlichen Archive haben dann dafür zu sorgen, dass personenbezogene Daten oder solche Unterlagen, die einem besonderen gesetzlichen Geheimnisschutz unterliegen, nur unter den Bedingungen des Landesarchivgesetzes genutzt werden. Darüber hinaus bedeutet jede Erlaubnis einer Einsichtnahme in personenbezogene Unterlagen einerseits einen Eingriff in teilweise von besonderen Schweigepflichten geschützte persönliche Bereiche von Personen und andererseits ihre Ablehnung eine Beschränkung der Informationsrechte der Anfragenden. Die Archive müssen somit Entscheidungen treffen, die in Grundrechte eingreifen können. Daher müssen alle Entscheidungen stets rechtlich nachprüfbar sein. Das Führen der kommunalen Archive mit personenbezogenem Archivgut ist damit ein Bereich der Verwaltung, dessen Kernaufgabe mit Grundrechtseingriffen einhergeht und in dem die Verwaltung hoheitlich tätig wird.
Verfassungsrechtliche Gründe sprächen meines Erachtens jedoch nicht grundsätzlich gegen ein solches Vorhaben. Allerdings müsste eine gesetzliche Neuregelung den oben ausgeführten Ansprüchen genügen.
Das Landesarchivgesetz Mecklenburg-Vorpommern vom 7. Juli 1997 wurde durch das Gesetz zur Reform der Landesverwaltung im Geschäftsbereich des Ministeriums für Bildung, Wissenschaft und Kultur vom 28. November 2005 novelliert. Es wurde das Landesamt für Kultur und Denkmalpflege errichtet, in dem nun die Archive gemeinsam mit der Landesbibliothek Schwerin, dem Landesamt für Denkmalpflege und dem Landesamt für Bodendenkmalpflege zusammengefasst worden sind. Der Fachbereich Landesarchiv im Landesamt für Kultur und Denkmalpflege besteht aus den Archiven Schwerin und Greifswald. Ich habe aus den oben genanten Gründen empfohlen, die organisatorische, räumliche und personelle Trennung des Fachbereiches Landesarchiv von den Aufgaben des Landesamtes für Kultur und Denkmalpflege in einer Dienstanweisung klar abzugrenzen.
Das Ministerium für Bildung, Wissenschaft und Kultur hat mich darüber informiert, dass eine entsprechende Dienstanweisung erarbeitet wird.

2.12 Wirtschaft und Gewerbe

2.12.1 Gästebefragung einer Fachhochschule

Mir ist mitgeteilt worden, dass eine Fachhochschule Hotelgäste von der Insel Rügen befragt und dazu die Adressen der Gäste nutzt. Das Anschreiben an die Gäste ließ vermuten, dass die Anschriften von den Hotels übermittelt beziehungsweise von der Fachhochschule dort erhoben wurden.

Entscheidend für die datenschutzrechtliche Bewertung des Sachverhaltes war, ob die Fachhochschule die Gästebefragung als eigenes Projekt oder im Auftrag der Hotels oder Hotelorganisationen durchgeführt hat. Soweit es sich um ein eigenes Forschungsprojekt handelt, beurteilt sich der Sachverhalt nach den Vorschriften des Landesdatenschutzgesetzes, da die Fachhochschule eine öffentliche Stelle des Landes Mecklenburg-Vorpommern ist. Haben allerdings Hotels oder Hotelorganisationen die Fachhochschule mit der Gästebefragung zum Zweck der Markt- und Meinungsforschung beauftragt, ergibt sich eine andere Rechtslage. Hotels und Hotelorganisationen sind im datenschutzrechtlichen Sinne nichtöffentliche Stellen und unterliegen damit den Bestimmungen des Bundesdatenschutzgesetzes (BDSG).

Der Projektleiter teilte mir auf Nachfrage mit, dass verschiedene Hotels und Apartmenthäuser der Insel Rügen ihn mit der Auswertung der Gästebefragung beauftragt hatten. Die Hotels senden die Fragebögen selbst an ihre Gäste. Der ausgefüllte Fragebogen soll dann direkt an die Fachhochschule gesendet werden. Dieses Vorgehen entspricht den datenschutzrechtlichen Vorschriften, weil die Hotels keine personenbezogenen Daten (Adressen) an Dritte weitergeben, die Teilnahme freiwillig ist und der Datenempfänger (die Fachhochschule) aus den einzelnen Fragen keine Person bestimmen konnte. Die Befragung war damit hinreichend anonym.

Da die Gäste jedoch dieses Vorgehen nicht aus dem Anschreiben entnehmen konnten, hatte ich empfohlen, sie kurz über das Vorhaben zu informieren. Insbesondere darüber, dass sie den Fragebogen direkt von ihrem Hotel erhalten und ihre Adresse nicht an Dritte weitergegeben wurde. Auch ein Hinweis auf die Freiwilligkeit der Angaben sollte erfolgen.

Die Fachhochschule hat sich für meine Hinweise bedankt und sie unverzüglich umgesetzt.

2.12.2 Datenübermittlung aus der Lehrlingsrolle an eine Versicherung

Eine Staatsanwaltschaft informierte mich darüber, dass sie ein Ermittlungsverfahren gegen Unbekannt wegen des Verstoßes gegen das Landesdatenschutzgesetz führt. Einer Handwerkskammer wurde vorgeworfen, personenbezogene Daten aus der Lehrlingsrolle an eine Versicherung übermittelt zu haben. Die Staatsanwaltschaft wollte nun wissen, ob ich ebenfalls einen Strafantrag stellen werde. Vor einer Entscheidung wollte ich jedoch die Handwerkskammer um eine Stellungnahme bitten, womit sich die Staatsanwaltschaft einverstanden erklärte.

Nicht die Handwerkskammer, sondern eine Kreishandwerkerschaft aus ihrem Kammerbezirk hatte die personenbezogenen Daten von Auszubildenden an eine Versicherung weitergegeben. Die Kreishandwerkerschaft begründete die Übermittlung damit, dass sie ein Versorgungswerk gegründet habe (§ 87 Nr. 3 Handwerksordnung - HandwO), über das Kollektivversicherungsverträge abgeschlossen werden können. Mitglied dieses Versorgungswerkes sei auch die Versicherung.

Die Kreishandwerkerschaft hatte Näheres in einer Satzung über das Versorgungswerk beschlossen. Die Satzung enthielt allerdings keine Regelungen zur Verarbeitung personenbezogener Daten. Zur Gewinnung der Auszubildenden für die mit der Versicherung vereinbarten Leistungen des Versorgungswerkes war es üblich, nach der Registrierung der Berufsausbildungsverträge die volljährigen bzw. die Eltern der minderjährigen Auszubildenden anzuschreiben und zu informieren. Sofern die Angeschriebenen nicht innerhalb von zwei Wochen gegen die Weitergabe ihres Namens, ihrer Anschrift, ihres Geburtsdatums und ihrer Ausbildungsrichtung widersprochen haben, wurden diese Daten an das Versorgungswerk übermittelt und gelangten damit auch an die Versicherung.

Die Leistungen des Versorgungswerkes unterliegen der Freiwilligkeit und können von Interessenten beantragt werden. Kein Auszubildender oder in einem Handwerksbetrieb Beschäftigter ist verpflichtet, dem Versorgungswerk beizutreten. Darüber hinaus ist in der Satzung die Verarbeitung personenbezogener Daten nicht geregelt. Somit sind für die Verarbeitung der personenbezogenen Daten der Auszubildenden die Regelungen des Landesdatenschutzgesetzes (DSG M-V) maßgebend. Das Landesdatenschutzgesetz enthält aber keine Regelung zur Übermittlung von Daten, wenn die betroffenen Personen nicht vorher ihr Interesse an solchen Angeboten geäußert haben. Folglich darf die Kreishandwerkerschaft die Daten der Auszubildenden an das Versorgungswerk und damit an die Versicherung nur übermitteln, wenn die Betroffenen eingewilligt haben. Für die Einwilligung sind die Bestimmungen des § 8 DSG M-V maßgeblich.

Der Geschäftsführer der Kreishandwerkerschaft hat zugesagt, dass Daten von Auszubildenden künftig nur mit ihrer Einwilligung an das Versorgungswerk übermittelt werden.

Von einem zusätzlichen Strafantrag habe ich in diesem Fall abgesehen, weil die Kreishandwerkerschaft die erforderlichen Maßnahmen eingeleitet hat. Die Auszubildenden konnten der weiteren Verarbeitung ihrer Daten widersprechen, sodass die Rechtsverletzung meines Erachtens ohne negative Folgen für die betroffenen Personen geheilt werden konnte.

2.12.3 Auskunft über alle in der Stadt angemeldeten Gewerbe an einen Verlag

Ein Bürgermeister beabsichtigte zusammen mit einem Städteverlag, den Stadtplan neu aufzulegen. Die Finanzierung des Drucks sollte über Gewerbeanzeigen der ortsansässigen Firmen erfolgen. Um Firmen für dieses Projekt zu gewinnen, beauftragte er einen Mitarbeiter seiner Stadtverwaltung, eine Übersicht aller ortsansässigen Firmen zu erstellen und diese dem Verlag zu senden. In dieser Liste sollten Name, Vorname, Wohnanschrift, Betriebsanschrift, Art des Gewerbes, Beginn und Ende der Tätigkeit sowie das Meldedatum aufgenommen werden. Der Mitarbeiter hatte Zweifel, ob dies rechtlich zulässig sei, und bat mich, den Sachverhalt zu prüfen.

Rechtlich war der Sachverhalt nach den Bestimmungen der Gewerbeordnung (GewO) zu beurteilen. Danach dürfen Daten der Gewerbetreibenden aus dem Gewerberegister an nicht öffentliche Stellen übermittelt werden, wenn der Auskunftsbegehrende ein berechtigtes Interesse glaubhaft macht, § 14 Abs. 8 GewO. Von einem berechtigten Interesse ist auszugehen, wenn es sich aus vernünftigen Überlegungen ergibt und der Zweck und die damit verbundene Datenverarbeitung im Einklang mit der Rechtsordnung stehen. Dies sind in der Regel geschäftliche oder wirtschaftliche Beweggründe. Das Interesse des Bürgermeisters, den Druck des Stadtplaners über Gewerbeanzeigen zu finanzieren, konnte daher als berechtigtes Interesse anerkannt werden. Allerdings dürfen für diesen Zweck nur die in § 14 Abs. 8 Satz 1 genannten Daten (Name, betriebliche Anschrift und angezeigte Tätigkeit des Gewerbetreibenden) übermittelt werden. Diese Daten dürften auch genügen, um Kontakt mit den Gewerbetreibenden aufzunehmen. Die Übermittlung der weiteren Daten (Wohnanschrift, wann die Gewerbeanmeldung erfolgt und wann mit dem Gewerbe begonnen wurde) hätten an den Verlag nur übermittelt werden dürfen, wenn der Auskunftsbegehrende ein rechtliches Interesse hat, das heißt, wenn er Rechtsansprüche geltend macht und kein Grund zur Annahme besteht, dass das schutzwürdige Interesse des Gewerbetreibenden überwiegt. Diese Voraussetzungen waren hier nicht erfüllt, sodass es nicht zulässig war, diese Daten zu übermitteln.

Über meine Rechtsauffassung habe ich den Bürgermeister informiert und empfohlen, seine Mitarbeiter sowie den Verlag auf die gesetzlichen Bestimmungen der Gewerbeordnung hinzuweisen. Darüber hinaus sollte er den Verlag auffordern, die unzulässig übermittelten Daten zu löschen.

So geht es aber nicht!

Für den Mitarbeiter der Verwaltung hatte das Ergebnis meiner datenschutzrechtlichen Prüfung jedoch Folgen. Der Bürgermeister leitete dienstrechtliche Maßnahmen gegen ihn ein, weil er durch seine Anfrage bei mir die Stadtverwaltung und damit den Bürgermeister in Misskredit gebracht hätte.

Dies ist so nicht hinzunehmen. Der Mitarbeiter hatte sich an mich gewandt, da er Zweifel an der Auslegung der GewO hatte. Es muss das Interesse jeder datenverarbeitenden Stelle sein, dass ihre Daten rechtmäßig verarbeitet werden. Ein Beschäftigter, der sich mit Fragen an mich wendet, verfolgt dieses Interesse. Es war daher völlig abwegig, einem Beschäftigten zu unterstellen, er habe dem Ansehen seiner Beschäftigungsbehörde oder des Behördenleiters dadurch geschadet. Die Beratung der öffentlichen Stellen ist eine wichtige Aufgabe meiner Behörde, die nur funktionieren kann, wenn jeder sich mit Fragen an mich wenden kann.

Auf meine Kritik erwiderte der Bürgermeister, dass der Beschäftigte absolut richtig gehandelt habe, indem er mit mir Kontakt aufnahm. Die dienstrechtlichen Maßnahmen seien eingeleitet worden, weil eine Liste mit Daten übermittelt wurde, die nicht mit den gesetzlichen Bestimmungen vereinbar war.

16. Ich empfehle dem Landtag klarzustellen, dass keinem Mitarbeiter wegen der Anrufung des Landesbeauftragten für den Datenschutz oder des behördlichen Datenschutzbeauftragten Nachteile entstehen dürfen.

2.13 Land-, Forst- und Wasserwirtschaft und Umweltschutz

2.13.1 Weitergabe von Daten an Dritte - Zugriff auf zentrale Datei

Eine Petentin schilderte mir, dass ihre nach EU-Recht zugeteilten Zahlungsansprüche in einer zentralen Datei gespeichert sind. Auf diese Datenbank können nur die betroffenen Landwirte und das Amt für Landwirtschaft über eine zugeteilte Nummer zugreifen. Diese Zugriffsnummer war nach ihrer Schilderung an einen Rechtsanwalt weitergegeben worden. Sie bat mich, den Sachverhalt zu prüfen.

Ich habe beim zuständigen Amt für Landwirtschaft angefragt, ob von dort aus die Nummer an den Rechtsanwalt weitergegeben worden ist und welche Maßnahmen (z. B. Protokollierung lesender Zugriffe) getroffen wurden, um einen unberechtigten Zugriff auf die zentrale Datenbank auszuschließen.

Dem Amt lagen keine Erkenntnisse vor, dass die Nummer der Zahlungsansprüche von einem Mitarbeiter an einen Rechtsanwalt oder an Dritte weitergegeben wurde. Der lesende Zugriff der Mitarbeiter wird im Amt für Landwirtschaft allerdings auch nicht protokolliert. Damit konnte auch nicht nachgewiesen werden, welcher Mitarbeiter wann die Daten der Petentin zur Kenntnis genommen hat. Sofern beim Amt für Landwirtschaft Anfragen über Zahlungsansprüche von Dritten eingehen, werden diese vom Justitiar geprüft und beantwortet. Diese Anfragen werden dann auch dokumentiert. Bisher hätten dem Amt nur zwei Anfragen nach dem Informationsfreiheitsgesetz Mecklenburg-Vorpommern (IFG M-V) vorgelegen, diese betrafen allerdings nicht die Petentin. Im Übrigen stehe es den Empfängern von Zahlungsansprüchen auch frei, diese zu verkaufen, sodass die Zugriffsnummer möglicherweise über diesen Weg an den Rechtsanwalt gelangt sein könnte.

Da der lesende Zugriff durch die Mitarbeiter des Amtes für Landwirtschaft nicht protokolliert wurde, konnte der Sachverhalt mit datenschutzrechtlichen Mitteln nicht weiter aufgeklärt werden. Dieses Ergebnis ist aus datenschutzrechtlicher Sicht nicht zufriedenstellend und zeigt einmal mehr, wie wichtig es ist, auch den lesenden Zugriff zu protokollieren.

2.13.2 Nutzung der Adressdaten von Fischereischeininhabern zu Forschungszwecken

Die Landesforschungsanstalt für Landwirtschaft und Fischerei hat mich darüber informiert, dass sie beabsichtigt, die Einflüsse der Angelscheininhaber auf die Aalbestände zu untersuchen. Zu diesem Zweck sollten die Adressdaten der Fischereischeininhaber, die in den kommunalen Ordnungsämtern vorliegen, genutzt werden. Ich wurde gefragt, welche datenschutzrechtlichen Bestimmungen bei diesem Vorhaben zu beachten wären.

Ausgehend von den Bestimmungen des Landesdatenschutzgesetzes Mecklenburg-Vorpommern (DSG M-V) ist die Verarbeitung personenbezogener Daten für Forschungszwecke unter den in § 34 DSG M-V genannten Voraussetzungen zulässig. Die Vorschrift betont, dass Daten für wissenschaftliche Zwecke anonym verarbeitet werden sollten, da es überwiegend nicht auf die einzelne Person ankommt. In meiner ersten datenschutzrechtlichen Bewertung hatte ich daher vorgeschlagen, zunächst zu prüfen, ob das Vorhaben mit anonymisierten Daten durchgeführt werden kann. Ist dies nicht möglich, hatte ich empfohlen, dass sogenannte Adressmittlungsverfahren zu nutzen.

Hierbei werden Fragebögen sowie Schreiben, in denen das Vorhaben erläutert wird, über die Stelle, welche die personenbezogenen Daten speichert (Ordnungsbehörde), an die Betroffenen gesandt. Der Vorteil ist, dass keine personenbezogenen Daten zur Realisierung des Projektes übermittelt werden müssen. Personenbezogene Daten dürfen für Forschungszwecke nur genutzt werden, wenn die Voraussetzungen des § 34 Abs. 2 DSG M-V erfüllt sind. Dies bedeutet, dass die für die Ordnungsämter zuständige Kommunalaufsichtsbehörde prüfen und feststellen muss, dass das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange der Betroffenen erheblich überwiegt und der Zweck der Forschung nicht auf andere Weise erreicht werden kann.

Einige Zeit später übersandte mir ein behördlicher Datenschutzbeauftragter ein Schreiben des Ministeriums für Ernährung, Landwirtschaft, Forsten und Fischerei zur Kenntnis. Als für Fischereiangelegenheiten zuständige Stelle forderte das Ministerium die Ordnungsbehörden auf, der Landesforschungsanstalt die Anschriften der Fischereischeininhaber zu übermitteln. In diesem Schreiben wurde auch ausgeführt, dass das Verfahren zur Erhebung von Adressdaten durch mich geprüft und für unbedenklich erklärt worden wäre. Diese Aussage hatte ich in meiner Stellungnahme nicht getroffen, sodass es hierzu weiteren Gesprächsbedarf gab.

Es stellte sich heraus, dass das Landwirtschaftsministerium nach § 34 Abs. 2 DSG M-V das Vorhaben genehmigt hatte, sodass die Ordnungsbehörden auf dieser Grundlage die Anschriften der Fischereischeininhaber übermitteln konnten.

Darüber hinaus war geplant, die Angelscheininhaber telefonisch zu befragen. Die Befragung sollte einem Markt- und Meinungsforschungsinstitut übertragen werden.

Es ist durchaus zulässig, dass die Landesforschungsanstalt eine andere Stelle mit der Befragung beauftragt. Bei der Auftragsdatenverarbeitung bleibt die auftraggebende Stelle aber dafür verantwortlich, dass die übertragenen Aufgaben den gesetzlichen Bestimmungen entsprechend erledigt werden und das Datenschutzrecht eingehalten wird. Der Auftraggeber hat daher mit dem Auftragnehmer einen Vertrag zur Datenverarbeitung im Auftrag zu schließen, in dem die technischen und organisatorischen Maßnahmen vorzugeben sind, welche die Einhaltung datenschutzrechtlicher Bestimmungen sicherstellen, § 4 DSG M-V.

Da die Betroffenen bei einer telefonischen Befragung nicht erkennen können, ob der Anrufer derjenige ist, für den er sich ausgibt, hatte ich ein zweistufiges Vorgehen vorgeschlagen. Zunächst sollten die Betroffenen in einem Anschreiben über den Zweck des Forschungsvorhabens, über die freiwillige Teilnahme und darüber, woher das Institut die Anschriften erhalten hat, aufgeklärt werden. Darüber hinaus sollte ihnen hier bereits mitgeteilt werden, dass sie in den nächsten Tagen von einem Mitarbeiter eines Markt- und Meinungsforschungsinstitutes angerufen werden.

Meine datenschutzrechtlichen Forderungen wurden umgesetzt.

2.14 Eigenbetriebe

2.14.1 Umgang mit Kundendaten bei einer Sparkasse

Ein Petent beschwerte sich bei mir über den Umgang mit Kundendaten in einer Sparkasse. Er hatte die Filiale aufgesucht, um eine Bareinzahlung vorzunehmen. Im Verlauf des Gespräches hatte sich die Mitarbeiterin der Sparkasse laut über sein privates Insolvenzverfahren geäußert, sodass andere Kunden dies mithören konnten. Wegen dieses höchst indiskreten Kundengespräches hatte er sich bereits an das Beschwerdemanagement gewandt, aber nur eine sehr allgemeine Antwort erhalten, die aus seiner Sicht nicht zufriedenstellend war. Er bat mich, ihn in dieser Angelegenheit zu unterstützen.

Ich habe dem Vorstand der Sparkasse diesen Sachverhalt geschildert und um Stellungnahme dazu gebeten.

Im Ergebnis wurde der Petent zu einem Gespräch eingeladen, an dem auch die zuständige Teilmarktleiterin und der Abteilungsleiter Unternehmenskommunikation teilnahmen. In diesem Gespräch wurde der Vorfall umfassend mit dem Kunden besprochen. Die Mitarbeiter der Sparkasse haben sich dann in aller Form beim Petenten für den Vorfall entschuldigt.

Intern wurde der Vorfall zum Anlass genommen, um noch einmal alle Mitarbeiter auf die Einhaltung der Diskretion hinzuweisen. Die Mitarbeiter wurden auch aufgefordert, für Gespräche mit sensiblen Inhalten die vorhandenen abgeschlossenen Beratungsbereiche zu nutzen.

2.14.2 Zugriffsregelungen einer Sparkasse auf Mitarbeiterdaten

In einer Sparkasse sollten die Zugriffsrechte der Mitarbeiter auf Kundendaten neu geregelt werden. Bisher war der Zugriff auf die Daten der Mitarbeiter und Organmitglieder, die auch Kunden der Sparkasse sind, auf einzelne Personen beschränkt, während die anderen Kundendaten für alle Mitarbeiter zugänglich waren. Nun war beabsichtigt, die bestehenden, nach Funktion unterschiedlichen Zugriffsrechte auf Mitarbeiterdaten den Zugriffsrechten auf andere Kundendaten gleichzusetzen. Die Mitarbeiter befürchteten nun, dass Arbeitgeber oder Kollegen die Zugriffsrechte missbrauchen könnten. Zum Beispiel könnten Kollegen die Höhe ihres Gehaltes zur Kenntnis nehmen, oder der Arbeitgeber könnte Erkenntnisse aus der Datenauswertung für Personalentscheidungen nutzen. Ein Petent bat mich daher zu prüfen, ob die geplante Erweiterung der Zugriffsrechte datenschutzrechtlich zulässig sei.

Die Frage war im Wesentlichen nach den Vorgaben unter Nummer 3 der Anlage zu § 9 Satz 1 Bundesdatenschutzgesetz (BDSG) zu beantworten. Danach sind öffentliche und nichtöffentliche Stellen verpflichtet, technische und organisatorische Maßnahmen zu treffen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle).

Nach meiner Auffassung ist diese Vorgabe so auszulegen, dass Mitarbeiter der Sparkasse, außer vielleicht auf Stammdaten, nicht auf alle Daten der Kunden zugreifen können dürfen. Die Zugriffsrechte müssen nach der zu erfüllenden Aufgabe des Mitarbeiters ausgerichtet sein. Hierzu eignen sich entsprechende Rollenkonzepte. Wenn auch lesende Zugriffe ausreichend protokolliert werden und jeder weiß, dass er sich für den Lesezugriff gegebenenfalls rechtfertigen muss, müsste meines Erachtens nicht weiter zwischen Zugriffsrechten auf Kundendaten der Mitarbeiter und denen der anderen Kunden differenziert werden. Voraussetzung wäre dann allerdings auch, dass die Protokolldaten regelmäßig ausgewertet werden und bei Auffälligkeiten die Nutzung der Rechte überprüft wird.

Eine spezielle Beschränkung von Zugriffen auf Daten ist mir aus den Regelungen zum Sozialgeheimnis bekannt. In § 35 Absatz 1 Satz 3 Sozialgesetzbuch Erstes Buch (SGB I) heißt es: „Sozialdaten der Beschäftigten und ihrer Angehörigen dürfen Personen, die Personalentscheidungen treffen oder daran mitwirken können, weder zugänglich sein noch von Zugriffsberechtigten weitergegeben werden."

Ich hatte der Sparkasse empfohlen, eine ähnliche Regelung innerhalb der Sparkasse für Kundendaten der Mitarbeiter einzuführen. Nach meiner Auffassung darf ein Vorgesetzter keine Kenntnis darüber erlangen können, wofür ein Mitarbeiter sein Geld ausgibt oder in welchen Geschäften er mit seiner EC-Karte bezahlt oder wohin er sein Geld überweist.

2.15 Technik und Organisation

2.15.1 Gütesiegel

Die Novellierung unseres Landesdatenschutzgesetzes (DSG M-V) im Jahr 2002 eröffnete mit den Regelungen zum Datenschutzaudit die Möglichkeit, informationstechnische Produkte (Hardware, Software, Verfahren) auf ihre Datenschutzfreundlichkeit prüfen zu lassen. Ergibt die Prüfung, dass ein Produkt mit den Vorschriften über den Datenschutz und die Datensicherheit vereinbar ist, kann es ein Gütesiegel erhalten. Die Details des gesamten Audit-Verfahrens müssen jedoch durch eine Rechtsverordnung geregelt werden.

§ 5 Abs. 2 DSG M- V

Informationstechnische Produkte, deren Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit in einem Prüfverfahren festgestellt wurde, sollen vorrangig eingesetzt werden. Die Landesregierung regelt durch Rechtsverordnung Inhalt, Ausgestaltung und die Berechtigung zur Durchführung des Verfahrens.

Die Vorteile dieses Audit-Verfahrens für die Wirtschaft und die Verwaltung unseres Landes habe ich bereits ausführlich erläutert (siehe Sechster Tätigkeitsbericht, Punkt 2.18.1 und Siebter Tätigkeitsbericht, Punkt A.I.4.1.3). Auch die von mir jährlich durchgeführte Datenschutzfachtagung, die im Jahr 2006 unter dem Motto „Datenschutz durch Technik - Chancen für Unternehmen und öffentliche Verwaltung" stand, unterstrich den Nutzen des Gütesiegels für die Wirtschaft und die Verwaltung eindrucksvoll (siehe auch Anlage 4).

Obwohl mich regelmäßig Anfragen zur Prüfung von Produkten erreichen, ist die Landesregierung - gestützt auf ein ablehnendes Votum der Industrie- und Handelskammern - noch immer der Auffassung, dass in Mecklenburg-Vorpommern kein Bedarf für ein Gütesiegel besteht, und hat die Verordnung nach wie vor nicht erlassen. Diese Auffassung verwundert umso mehr, als dass der Nutzen eines solchen Gütesiegels selbst auf internationaler Ebene erkannt wurde. So hat beispielsweise die Firma Microsoft als einer der bedeutendsten Softwarehersteller der Welt im Februar 2007 die Produkte „Microsoft Update Service 6.0“ und „Windows Server Update Service 2.0“ vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD S-H) prüfen lassen und im Ergebnis das Datenschutz-Gütesiegel erhalten. Im September 2007 erhielt Microsoft für das Produkt „Microsoft Windows Genuine Advantage (WGA)“ ein weiteres Gütesiegel.

Auch auf europäischer Ebene wird das Datenschutz-Gütesiegel an Bedeutung gewinnen. Die EU-Kommission hat ein Konsortium aus acht europäischen Organisationen und Unternehmen beauftragt, die Anforderungen für ein europäisches Datenschutz-Gütesiegel zu erarbeiten und zu erproben. Das Projekt „European Privacy Seal“ (EuroPriSe) wurde im Juni 2007 unter Federführung des ULD S-H gestartet. Das europäische Gütesiegel soll künftig bescheinigen, dass informationstechnische Angebote mit dem europäischen Recht, insbesondere mit der seit 1998 geltenden Datenschutzrichtlinie, im Einklang stehen.

Auch auf Bundesebene wurde jetzt offensichtlich die Bedeutung des Datenschutzes als Wettbewerbsfaktor erkannt. Endlich sollen die Vorgaben des Bundesgesetzgebers aus dem Jahr 2001 umgesetzt und die Anforderungen an das Datenschutzaudit-Verfahren des Bundes geregelt werden. Im September 2007 hat das Bundesministerium des Innern einen Referentenentwurf für ein Bundesdatenschutzauditgesetz vorgelegt. In meiner Stellungnahme habe ich das Vorhaben ausdrücklich begrüßt, musste jedoch noch erhebliche Mängel des Entwurfs feststellen. So halte ich es entgegen den Vorstellungen des BMI für unabdingbar, im Rahmen der Prüfung informationstechnischer Produkte auch die Sicherheit dieser Produkte zu prüfen. Eine Datenschutzauditierung ohne Prüfung der technischen und organisatorischen Sicherheitsmaßnahmen wäre aussage- und damit sinnlos, weil eine grundlegende Anforderung des Datenschutzrechts ignoriert würde. Ich habe weiterhin vorgeschlagen, die Akkreditierung von Sachverständigen nicht regional zu beschränken, da kein Grund erkennbar ist, warum die Tätigkeit von Sachverständigen örtlich gebunden sein muss. Schließlich habe ich eine wirkungsvolle Qualitätssicherung des Zertifikats empfohlen. Nicht der Sachverständige selbst, sondern eine unabhängige, fachlich anerkannte und öffentlicher Kritik zugängliche Stelle sollte das Zertifikat vergeben. Dieses Verfahren hat sich seit vielen Jahren bei der Vergabe des Gütesiegels in Schleswig-Holstein bewährt.

Unsere Landesregierung verweigert auch sechs Jahre nach Inkrafttreten der Regelung den Erlass einer Verordnung, obwohl der Bedarf der Unternehmen und die datenschutzpolitische Notwendigkeit stetig zunehmen.

17. Ich empfehle dem Landtag, durch eine Änderung des § 5 Abs. 2 Landesdatenschutzgesetz (DSG M-V) die erforderliche gesetzliche Grundlage für die Durchführung eines Auditierungsverfahrens zu schaffen.

2.15.2 Digitale Signatur auf dem Rückzug?

Seit 1997 hat Deutschland ein Signaturgesetz. Es regelt die technischen Rahmenbedingungen für die Anwendung elektronischer Signaturen und soll in Verbindung mit weiteren fachspezifischen Gesetzen zu mehr Rechtssicherheit bei der elektronischen Kommunikation im Geschäftsleben und bei E-Government-Verfahren führen. Das Signaturgesetz stellt technische und organisatorische Anforderungen an Produkte (etwa Signaturkarten und Kartenleser) und Anbieter von Dienstleistungen in diesem Umfeld. Da elektronische Signaturen sehr gut geeignet sind, die Übertragung und Speicherung personenbezogener Daten zu sichern und die Verbindlichkeit der Verarbeitung personenbezogener Daten zu verbessern, habe ich bereits mehrfach deren Nutzung auch in der öffentlichen Verwaltung gefordert, zuletzt im Sechsten Tätigkeitsbericht, Punkt 2.16.3.

Elektronische Signaturen werden mehr als zehn Jahre nach Inkafttreten des ersten Signaturgesetzes immer noch sehr selten verwendet. Potenzielle Anwender weisen häufig auf hohe Kosten bei der Einführung und auf die geringe Verbreitung der hierfür nötigen Ausstattung hin. Hier zeigt sich ein Teufelskreis: Die Technik ist nicht verbreitet, weil sie relativ teuer ist, und die Technik ist teuer, weil sie nicht in hohen Stückzahlen nachgefragt wird. Dies gilt insbesondere für die sogenannten qualifizierten Zertifikate, die Voraussetzung für qualifizierte Signaturen sind. Nur diese Signaturen bieten ein so hohes Maß an Integrität und Verbindlichkeit, dass sie als elektronischer Ersatz für die handschriftliche Unterschrift dienen können.

Zwei Entwicklungen beobachte ich in diesem Zusammenhang mit Sorge:

Einerseits verzichtet der Gesetzgeber in zunehmendem Maße auf Signaturen auf der Basis qualifizierter Zertifikate, obwohl nur so die erforderliche Sicherheit gewährleistet werden kann. Dies gilt beispielsweise für das Jahressteuergesetz 2007 und die geänderte Steuerdatenübermittlungsverordnung (siehe Punkt 2.5.7) sowie für das Justizkommunikationsgesetz. Andererseits lassen Bundes- und Landesregierung viele Möglichkeiten, die Verbreitung qualifizierter Signaturen zu fördern, bisher ungenutzt verstreichen. Weder der neue Bundespersonalausweis im Chipkartenformat noch die elektronische Gesundheitskarte sollen standardmäßig mit qualifizierten Signaturzertifikaten ausgestattet werden. Auch beim Verfahren zum elektronischen Einkommensnachweis ELENA (siehe Punkt 2.8.1) ist eine flächendeckende Ausstattung mit diesen Zertifikaten nicht vorgesehen. Auch von der Landesregierung gehen keine positiven Impulse aus. In E-Government-Verfahren des Landes und der Kommunen Mecklenburg-Vorpommerns spielt die qualifizierte elektronische Signatur praktisch keine Rolle. Im E-Government-Masterplan des Landes sind zwar Verschlüsselung und Signatur als Basiskomponenten für viele Projekte vorgesehen, aber eine Public-KeyInfrastruktur (PKI), die zur Verwaltung der Schlüssel für Verschlüsselung und Signatur erforderlich ist, gibt es immer noch nicht.

Die flächendeckende Ausstattung von Bürgerinnen und Bürgern mit qualifizierten Signaturzertifikaten kostet Geld. Wenn Bundes- und Landesregierung dieses Geld jedoch nicht ausgeben wollen, wird es auch in den nächsten zehn Jahren keine nennenswerten Anwendungen in Wirtschaft und Verwaltung geben. Das Ausweichen auf unsichere Ersatzverfahren kann jedoch erhebliche Schäden verursachen, welche die ursprüngliche Ersparnis mehr als aufwiegen.

18. Ich empfehle der Landesregierung, ihre Beschlüsse zur Basiskomponente Signatur entschlossen umzusetzen. Sie sollte sich darüber hinaus für eine stärkere Verbreitung der qualifizierten elektronischen Signatur einsetzen und ihren Einfluss im Bundesrat in diesem Sinne ausüben. In Mecklenburg-Vorpommern sollte sie Anwendungen der qualifizierten elektronischen Signatur sowohl in der Verwaltung als auch in der Wirtschaft fördern.

2.15.3 IP-Telefonie in der Landesverwaltung

Die Landesregierung führt zurzeit Internet-Telefonie in den obersten Landesbehörden Mecklenburg-Vorpommerns ein und löst damit die herkömmlichen Telefonanlagen ab. Die Planungen dafür begannen bereits 2004 (siehe Siebter Tätigkeitsbericht, Punkt A.II.1.10). Es war vorgesehen, im April 2007 3.000 Anschlüsse einzurichten und bis Ende Juni im Pilotbetrieb laufen zu lassen. Der Projektablauf verzögerte sich jedoch, sodass die Pilotphase erst Anfang Dezember 2007 begonnen werden konnte. Es ist vorgesehen, in den nächsten Jahren alle Landesbehörden und damit etwa 25.000 Fernsprechteilnehmer mit IP-Telefonie zu versorgen.

Rechtzeitig vor dem Start des Pilotbetriebs handelten das Innenministerium und der Hauptpersonalrat beim Innenministerium eine Dienstvereinbarung zur IP-Telefonie aus. Dabei habe ich sie beraten, insbesondere zur Verarbeitung der Verkehrsdaten von IP-Telefonverbindungen. Zwei Regelungen in der Dienstvereinbarung halte ich für besonders datenschutzgerecht. Erstens dürfen Privatgespräche nur unter Verwendung sogenannter Calling Cards geführt werden. Bedienstete wählen ihren Calling-Card-Anbieter über eine kostenlose 0800-Nummer an und können ihr Gespräch nach Eingabe einer PIN auf eigene Rechnung führen. Auf diese Weise werden ihre privaten Gespräche niemals in der zentralen Gebührenerfassung gespeichert. (Zur Erfassung der Kosten werden von allen kostenpflichtigen Telefonaten, welche das Landesnetz verlassen, Verkehrsdaten gespeichert. Dies betrifft nicht nur Verbindungen zu Teilnehmern außerhalb der Landesverwaltung, sondern auch solche Gespräche, die über konventionelle Leitungen geschaltet werden, falls das Landesnetz überlastet oder gestört sein sollte.) Zweitens dürfen Verkehrsdaten nur unter Beteiligung des jeweiligen Personalrates personenbezogen ausgewertet werden.

Verkehrsdaten sind Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden (§ 3 Nr. 30 Telekommunikationsgesetz). Dies sind Daten wie:

Beginn und Ende der Verbindung

Nummer oder andere Kennung der verbundenen Anschlüsse

bei Mobiltelefonen: Standort

übertragene Datenmengen

Im März 2007 legte der Landesdienstleister DVZ M-V GmbH, welcher als Generalauftragnehmer für das Projekt fungiert, ein IT-Sicherheitskonzept vor. Demnach sind Inhalte und Verkehrsdaten innerhalb des Landesnetzes zu verschlüsseln. Dazu werden insbesondere die Protokolle SRTP, TLS und IPSEC eingesetzt.

Außerdem sollen die Konfigurationsdaten und die Firmware der Telefone vor Manipulationen geschützt und Sprache und Daten in den Dienststellennetzen getrennt voneinander übertragen werden. Den Realisierungsstand dieser und anderer Datensicherheitsmaßnahmen werde ich nach Abschluss der Pilotphase prüfen.

Auch meine Behörde erwägt eine Teilnahme am IP-Telefonie-System des Landes. Dies setzt allerdings voraus, dass deren Verkehrsdaten strikt getrennt von denen der sonstigen Landesverwaltung verarbeitet werden. Auch dies werde ich zu gegebener Zeit untersuchen.

2.15.4 RFID

In der sogenannten Hannoverschen Erklärung erläutert das Bundesministerium für Wirtschaft und Technologie (BMWi) die Ergebnisse des Zweiten Nationalen IT-Gipfels 2007. Unter anderem wurde beschlossen, RFID als Kerntechnologie zu fördern.

RFID (Radio Frequency Identification) ist die englische Bezeichnung für Funk-Identifizierung. Daten werden auf einem kleinen Chip (Transponder) berührungslos und in der Regel ohne Sichtkontakt geschrieben und gelesen. Diese Transponder werden an Gegenständen (auch unsichtbar) befestigt, die dann mittels spezieller Lesegeräte kontaktlos über Entfernungen bis zu zehn Metern automatisch identifiziert werden können. So könnten beispielsweise alle Waren eines Supermarkts mit solchen Transpondern ausgestattet und die Preise an der Kasse automatisch ausgelesen werden.

Die Datenschutzbeauftragten des Bundes und der Länder befassen sich schon seit vielen Jahren mit den Datenschutzaspekten dieser Technologie. So besuchte der Arbeitskreis Technik (siehe auch Punkt 5) bereits im Jahr 2005 das RFID Technology Center der Firmen Siemens und Intel (siehe Siebter Tätigkeitsbericht Punkt A.0). Die 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder verabschiedete im Oktober 2006 eine Entschließung (siehe Anlage 1.9), in der sie auf die folgenden Risiken der Technik für das Recht auf informationelle Selbstbestimmung hinwies: Die RFID-Kennungen verschiedenster Gegenstände können sowohl miteinander als auch mit weiteren personenbezogenen Daten der Nutzenden - in der Regel ohne deren Wissen und Wollen - zusammengeführt werden. Auf diese Weise werden detaillierte Verhaltens-, Nutzungs- und Bewegungsprofile von Betroffenen ermöglicht. Deshalb fordert die Konferenz, jedenfalls auf heimliche Profilbildungen zu verzichten, Gegenstände mit RFID-Chips zu kennzeichnen und die Verfahren zur Nutzung dieser Chips transparent auszugestalten. Zudem muss das unbefugte Auslesen der gespeicherten Daten beispielsweise durch Verschlüsselung bei ihrer Speicherung und Übertragung unterbunden werden. Schließlich müssen Kunden im Handels- und Dienstleistungssektor die Möglichkeit haben, RFID-Tags dauerhaft zu deaktivieren beziehungsweise die darauf enthaltenen Daten zu löschen, wenn sie nicht mehr erforderlich sind.

Die Datenschutzbeauftragten forderten den Gesetzgeber auf zu prüfen, ob für alle Risiken adäquate und rechtliche Schutzmechanismen vorhanden sind, und insbesondere für den Fall tätig zu werden, dass die Hersteller und Anwender keine verbindlichen Selbstverpflichtungserklärungen abgeben.

Die Entschließung führte zu kontroversen Diskussionen zwischen Datenschützern und verschiedenen Interessenvertretungen von Industrie und Handel. Insbesondere wurde der Personenbezug von auf RFID-Chips gespeicherten Daten und damit der Geltungsbereich der Datenschutzgesetze von Bund und Ländern angezweifelt. Jedenfalls sahen die RFID-Protagonisten keinen Bedarf für ein Eingreifen des Gesetzgebers.

Um die charakteristischen Datenschutzrisiken der RFID-Technologie noch besser zu verdeutlichen und Anwender weiter zu sensibilisieren, veröffentlichte der Arbeitskreis Technik im Dezember 2006 eine Orientierungshilfe zum datenschutzgerechten Einsatz von RFID (abrufbar aus meinem Internetangebot unter http://www.datenschutz-mv.de/dschutz/informat/rfid/ohrfid.pdf). Das Dokument richtet sich auch an die Hersteller von RFID-Komponenten. Sie sollen motiviert werden, schon während der Entwicklung und der Produktion von RFID-Systemen datenschutzrechtliche Grundsätze zu beachten. Nicht zuletzt richtet sich die Orientierungshilfe an Kunden und Verbraucher. Sie können sich über die Datenschutz-Risiken moderner RFID-Systeme informieren und erhalten somit die Möglichkeit, die Risiken für das Recht auf informationelle Selbstbestimmung durch RFID-Systeme in der Praxis besser einzuschätzen, um ihr Verhalten diesen Risiken anpassen zu können.

In einer gemeinsamen Stellungnahme haben die Datenschutzbeauftragten des Bundes und der Länder nochmals ausdrücklich ihre Bereitschaft zum konstruktiven Dialog und zur Begleitung einzelner RFID-Projekte erklärt. Ich erwarte, dass die Selbstverpflichtungserklärungen von Herstellern und Anwendern der RFID-Technik zu einer datenschutzfreundlichen Technikgestaltung und zu einer offensiven Informationspolitik führen. Datenschutzaspekte müssen auch dann schon berücksichtigt werden, wenn eine Bedrohung erst durch nachträgliche Herstellung des Personenbezugs etwa über Kundenkarten oder elektronische Bezahlsysteme entsteht.

19. Ich empfehle dem Landtag, die technische Entwicklung von RFID-Systemen aufmerksam zu beobachten und sofort gesetzgeberisch aktiv zu werden, wenn die rechtlichen Schutzmechanismen den neuen Risiken nicht mehr gerecht werden.

2.15.5 IT-Sicherheits- und Datenschutzmanagement

Werden personenbezogene Daten verarbeitet, müssen technische und organisatorische Maßnahmen getroffen werden, um deren Sicherheit zu gewährleisten. § 21 des Landesdatenschutzgesetzes (DSG M-V) fordert, dass diese Maßnahmen nach dem Stand der Technik und nach der Schutzbedürftigkeit der zu verarbeitenden Daten erforderlich und angemessen sein müssen. In einem Sicherheitskonzept nach § 22 Abs. 5 DSG M-V ist für jedes automatisierte Verfahren festzulegen, in welcher Form die Anforderungen des § 21 DSG M-V umgesetzt worden sind.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt seit vielen Jahren Hilfsmittel zur Verfügung, mit denen die Erstellung von Sicherheitskonzepten erheblich vereinfacht wird. Dazu gehören beispielsweise die Grundschutzkataloge und die Grundschutz-Standards des BSI (ehemals Grundschutzhandbuch). Für Sicherheitsfragen Verantwortliche werden damit bei der Schutzbedarfsfeststellung und bei der Auswahl geeigneter Sicherheitsmaßnahmen wirkungsvoll unterstützt.

Mit dem Grundschutz-Tool bietet das BSI zudem ein Softwareprodukt an, mit dem Sicherheitskonzepte teilautomatisiert erstellt werden können, was eine erhebliche Zeitersparnis bewirkt.

Datenschutzaspekte haben in den Grundschutzmaterialien des BSI jedoch lange Zeit nur eine untergeordnete Rolle gespielt. Die Kataloge haben vorwiegend Sicherheits-Maßnahmen auf der Infrastrukturebene geliefert, etwa für ein Rechenzentrum, einen bestimmten Servertyp, einen Arbeitsplatz-PC oder die Hausverkabelung. Die vom Datenschutzgesetz geforderten verfahrensbezogenen Sicherheitskonzepte haben immer zusätzlichen Aufwand erfordert. Dennoch haben die Datenschutzbeauftragten von Bund und Ländern schon frühzeitig empfohlen, Sicherheitskonzepte nach der Grundschutzmethodik zu erstellen (siehe Zweiter Tätigkeitsbericht, Punkt 2.16.5).

Um die beschriebenen Defizite zu beseitigen, haben die Datenschutzbeauftragten dem BSI angeboten, einen zusätzlichen Baustein zum Thema Datenschutz zu erarbeiten (siehe Dritter Tätigkeitsbericht, Punkt 3.18.10). Den Text hat eine Arbeitsgruppe des Arbeitskreises Technik (siehe Punkt 5) erarbeitet und im Laufe des Jahres 2007 als separaten Baustein fertiggestellt. Seit September 2007 ist der neue Baustein „B 1.5 Datenschutz“ als Teil der Grundschutzkataloge aus dem Internetangebot des BSI abrufbar (http://www.bsi.de/gshb/deutsch/baust/b01005.htm).

Bei der Planung eines Sicherheitskonzeptes nach der Grundschutzmethodik können nun auch rechtliche Datenschutzfragen berücksichtigt werden. Neben den Aspekten der Informationssicherheit werden auch die Gefährdungen aus der Sicht des Datenschutzes in die Sicherheitsbetrachtungen einbezogen. Das betrifft beispielsweise die datenschutzrechtliche Zulässigkeit der Datenverarbeitung, die Einhaltung der Zweckbindung einmal erhobener personenbezogener Daten, die Umsetzung von Vorschriften zur Datensparsamkeit oder die mögliche Gefährdung der Rechte Betroffener. Im Datenschutzkapitel werden Maßnahmen vorgeschlagen, die das Risiko der Verletzung datenschutzrechtlicher Anforderungen minimieren. So wird beispielsweise die Regelung der Verantwortlichkeiten im Bereich Datenschutz oder die Vorabkontrolle für bestimmte Verfahren gefordert. Auch wird daran erinnert, Mitarbeiter auf das Datengeheimnis zu verpflichten, die Verfahrensverzeichnisse ordnungsgemäß zu führen und Verfahren zur Nutzung formell freizugeben.

Von besonderer Bedeutung sind die Empfehlungen zur Etablierung eines Datenschutz-Managements (Maßnahme 7.1). Der enge Zusammenhang zwischen Datenschutz und Informationssicherheit kommt hier besonders zum Tragen. Mit Datenschutzmanagement werden die Prozesse bezeichnet, die notwendig sind, um die gesetzlichen Anforderungen des Datenschutzes bei der Planung, Einrichtung, dem Betrieb und nach Außerbetriebnahme von Verfahren zur Informationsverarbeitung sicherzustellen. Sicherheits-Management hingegen umfasst die Prozesse, die der Gewährleistung der Informationssicherheit dienen.

Mit der Neustrukturierung der Grundschutzmaterialien hat das BSI den Prozesscharakter der Informationssicherheit unterstrichen. Der BSI-Standard 100-1 befasst sich beispielsweise ausschließlich mit Managementsystemen für Informationssicherheit und der BSI-Standard 100-2 beschreibt die Grundschutz-Vorgehensweise.

Der in der Maßnahme 7.1 beschriebene Datenschutzprozess orientiert sich genau an diesen BSI-Standards und ist als integrativer Bestandteil des IT-Sicherheitsprozesses nach IT-Grundschutz anzusehen. Die nachfolgende Abbildung zeigt den engen Zusammenhang der beiden Prozesse und lässt erkennen, dass bei der gemeinsamen Bearbeitung von Datenschutz- und Informationssicherheit erhebliche Synergieeffekte zu erzielen sind.

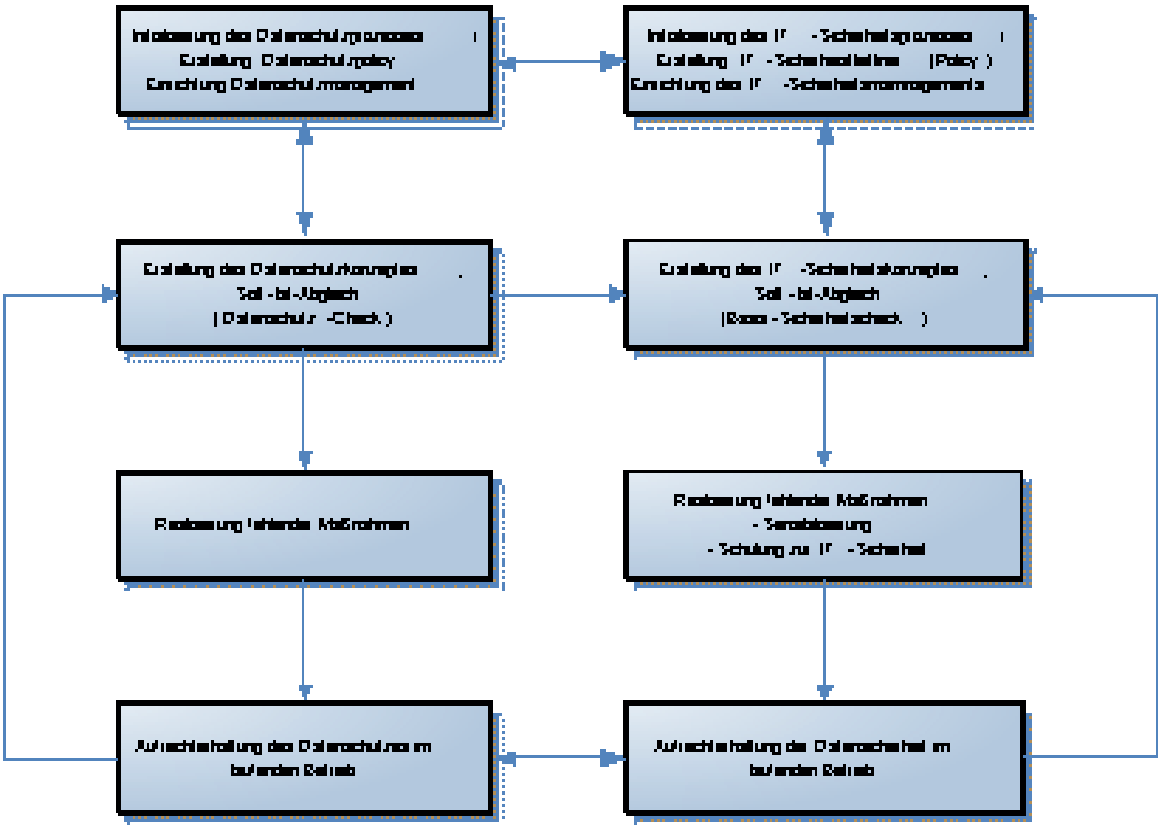


Abbildung: Datenschutzprozess

Ich begrüße sehr, dass die Landesverwaltung die Hilfsmittel des BSI bereits seit geraumer Zeit nutzt. Sicherheitskonzepte werden grundsätzlich mit dem Grundschutz-Tool nach der Grundschutzmethode erstellt. Der Datenschutzbaustein wurde frühzeitig in das gesamte System eingebunden. Alle auf diese Weise erstellten Sicherheitskonzepte werden im zentralen GSTOOL-Server abgelegt. Ein detailliertes Zugriffsrechte-Konzept ermöglicht jedem Eigentümer eines Sicherheitskonzeptes festzulegen, wer in welcher Weise auf die Daten zugreifen kann. Diese zentrale Datenhaltung hat beispielsweise den Vorteil, dass bereits erstellte Einzelmodule eines Konzeptes bei Bedarf sehr einfach in andere Sicherheitskonzepte eingebunden werden können.

Aber auch für meine Beratungs- und Kontrolltätigkeit wird der GSTOOL-Server in Zukunft ein sehr effektives Hilfsmittel werden. Nach der Erteilung der erforderlichen Leserechte werde ich Sicherheitskonzepte jederzeit einsehen und den Umsetzungsgrad der einzelnen Maßnahmen kontrollieren können.

20. Ich empfehle der Landesregierung, Informationssicherheits- und Datenschutzfragen künftig in engem Zusammenhang zu bearbeiten und die vom BSI beschriebenen Managementprozesse bei der Planung, der Einrichtung, dem Betrieb und nach der Außerbetriebnahme von IT-Verfahren vollständig umzusetzen.

3. Erster Bericht zum Informationsfreiheitsgesetz Mecklenburg-Vorpommern

3.1 Das neue Informationsfreiheitsgesetz in der Praxis

Das Gesetz zur Regelung des Zugangs zu Informationen für das Land Mecklenburg-Vorpommern (Informationsfreiheitsgesetz - IFG M-V) ist seit etwas über einem Jahr in Kraft. Es sind innerhalb dieses Zeitraumes 40 Petitionen beim Landesbeauftragten für Informationsfreiheit M-V eingegangen und bearbeitet worden. In diesen Fällen war der Landesbeauftragte für Informationsfreiheit vermittelnd zwischen den Antragstellern und den Behörden tätig.

Insgesamt dürfte bei den Behörden des Landes jedoch eine Vielzahl von weiteren Anträgen eingegangen sein, die positiv oder negativ beschieden worden sind. Belastbare Zahlen hierzu liegen mir jedoch nicht vor, da das Gesetz keine Statistikpflicht eingeführt hat und auf freiwilliger Basis nur wenige Rückmeldungen erfolgten.

In meiner Dienststelle gingen zahlreiche Anfragen von Behörden sowohl schriftlich als auch telefonisch ein. Dies ist sicher darauf zurückzuführen, dass im Fall eines ganz oder teilweise ablehnenden Bescheides neben dem Hinweis auf das förmliche Verwaltungsverfahren auch der Hinweis auf die Anrufung des Landesbeauftragten für Informationsfreiheit zu erfolgen hat (§ 12 Abs. 1 Satz 2 IFG M-V). Diese Form der „vorbeugenden Beratung“ der Behörden ist sicher die effektivste Form, können doch Streitfälle auf diesem Weg vermieden werden.

Mit Hilfe der Kommunalen Studieninstitute und im Rahmen der Veranstaltungsreihe „Datenschutz vor Ort“ war es möglich, durch zahlreiche Schulungen im gesamten Land 1.600 Mitarbeiterinnen und Mitarbeiter unterschiedlicher Verwaltungen mit dem Gesetz vertraut zu machen. Hierfür erarbeitete meine Behörde Schemata, Einführungshinweise, Kurzinformationen für die Mitarbeiter bis hin zu einem umfangreichen Aufsatz über das IFG M-V, der in Kurzfassung auch in der Fachzeitschrift Landes- und Kommunalverwaltung (LKV) Nummer 1-2007 erschienen ist.

Mit Hilfe der Presse und aufgrund eigener Aktivitäten wurden die Informationen über dieses neue Gesetz schnell im Land verbreitet. Beispielsweise ist das Informationsblatt „Welche Akte darf ich lesen?“ inzwischen in der zweiten Auflage mit 9.000 Stück im Land verteilt und auch im Internet unter http://www.informationsfreiheit-mv.de sind umfassende Informationen zu finden.

Die Laufzeit des IFG M-V ist zunächst bis zum 30. Juni 2011 begrenzt worden. Die Landesregierung ist verpflichtet, den Landtag zwei Jahre vor Außerkrafttreten über die Anwendung des Gesetzes zu unterrichten. Um eine Gesetzesevaluierung durchführen zu können, wurden in den durch unser Innenministerium herausgegebenen Durchführungshinweisen (siehe Amtsblatt für Mecklenburg-Vorpommern Nr. 41, S. 486 - 510) Statistikbögen an die Behörden des Landes herausgegeben.

3.2 Einsichtnahme in Rechnungen zum Bush-Besuch 2006 in Stralsund

Ein Antragsteller begehrte den Informationszugang beim Innenministerium zu den Rechnungen zum Bush-Besuch im Juli 2006 in Stralsund. Er hatte in der Sache beim Verwaltungsgericht Schwerin Untätigkeitsklage erhoben, weil ihm das Innenministerium weder innerhalb der 1-Monatsfrist des § 11 Abs. 1 IFG M-V geantwortet noch ihn unter Hinweis auf Umfang oder Komplexität der begehrten Informationen schriftlich über eine Fristverlängerung benachrichtigt hatte. Das Verwaltungsgericht hat durch Beschluss vom 5. Januar 2007 entschieden. Der Rechtsstreit war in der Hauptsache für erledigt erklärt worden. Das Gericht hatte aber dem Innenministerium als Beklagtem die Kosten des Verfahrens auferlegt und inhaltlich darauf verwiesen, dass die Untätigkeitsklage bereits vor Ablauf der in § 75 S. 2 Verwaltungsgerichtsordnung (VwGO) normierten 3-Monats-Frist zulässig war, da die in § 11 Abs. 1 IFG M-V formulierte 1-Monats-Frist als ein „besonderer Umstand“ im Sinne des § 75 S. 2 VwGO anzusehen sei.

Im vorliegenden Fall hatte das Innenministerium den Informationszugang zunächst weitgehend mit der Begründung abgelehnt, aus dem Inhalt der Rechnungen (Aufschlüsselung der Rechnungen der Innenministerien der anderen Bundesländer zu den auf ihr Land entfallenen Kosten für den Polizeieinsatz) könnten im Hinblick auf den im Juni 2007 stattgefundenen G8-Gipfel in Heiligendamm Schlussfolgerungen gezogen werden, in welchem Bundesland - durch Abzug von Polizisten - Defizite hinsichtlich der inneren Sicherheit (vergleiche § 5 Nr. 1 IFG M-V) bestehen.

Erst auf unsere Empfehlung hin wurde dann die sogenannte Drittbeteiligung gemäß § 5 Nr. 3 IFG M-V durchgeführt. Allerdings wurde in dem betreffenden Schreiben sehr tendenziös und nicht neutral, wie es im Lichte des Informationsfreiheitsgesetzes erforderlich gewesen wäre, angefragt. Des Weiteren wurde es unterlassen abzufragen, ob die Länderinnenministerien - wenn schon nicht mit einer Vollauskunft zu den Rechnungen - wenigstens in die Gewährung einer Teilauskunft - siehe § 11 Abs. 3 IFG M-V - einwilligen würden. Trotz allem hatten immerhin drei Bundesländer (Schleswig-Holstein, Nordrhein-Westfalen und Berlin) schriftlich mitgeteilt, dass sie keine Bedenken in Bezug auf die Bekanntgabe der auf ihr Land angefallenen Gesamtkosten hätten, wie wir durch eine Kontrolle der Unterlagen feststellen konnten. Wenigstens diese Teilinformation hätte dem Antragsteller zur Verfügung gestellt werden können. Dies ist jedoch weder in dem Ursprungsbescheid noch in dem Widerspruchsbescheid des Innenministeriums an den Antragsteller erfolgt. Der Rechtsstreit ist noch vor dem Verwaltungsgericht Schwerin anhängig.

Ein weiterer Antragsteller hatte in der gleichen Angelegenheit beim Innenministerium einen Informationszugangsantrag gestellt. Auch dieser Anspruch wurde durch Widerspruchsbescheid abgelehnt. Zusätzlich erhielt der Betroffene eine Kostenentscheidung, die aus meiner Sicht fehlerhaft war. Der Antragsteller sollte 53 € für fiktiv entstandene Gebühren zahlen, obwohl er keine Informationen erhalten hat. Dies stützte das Ministerium auf § 80 Abs. 1 S. 3 Verwaltungsverfahrensgesetz Mecklenburg-Vorpommern (VwVfG M-V), wonach die notwendigen Aufwendungen der Rechtsverteidigung der Ausgangsbehörde - fiktiv ermittelt - anrechenbar sein sollen. Eine solche Auslegung widerspricht jedoch sowohl den Regelungen des Verwaltungsverfahrensgesetzes als auch denen der Informationskostenverordnung. Darauf habe ich das Innenministerium hingewiesen und um Beachtung in künftigen Fällen gebeten.

3.3 Das Informationsfreiheitsgesetz im Besteuerungsverfahren

Das Finanzministerium unseres Landes hatte mir mit Datum vom 31. August 2006 einen Erlass über die „Nichtanwendung des Informationsfreiheitsgesetzes Mecklenburg-Vorpommern (IFG M-V) im Besteuerungsverfahren“ übersandt. Im Wesentlichen bezog man sich darauf, dass der Bundesgesetzgeber bei Verabschiedung der Abgabenordnung absichtlich ein Akteneinsichtsrecht für Betroffene nicht geregelt habe. Darin liege nach ständiger Rechtsprechung des Bundesfinanzhofs ein erkennbarer, absichtsvoller Regelungsverzicht des Bundesgesetzgebers, der als eine Ausnutzung der ihm eingeräumten Regelungskompetenz zur Schaffung abschließender Regelungen für Auskunfts- und Akteneinsichtsrechte im Bereich der Abgabenordnung (AO) anzusehen sei.

Ich habe in der sich anschließenden Korrespondenz unser Finanzministerium darauf hingewiesen, dass diese Begründung nach Inkrafttreten des IFG M-V nicht mehr greift. Nach § 1 Abs. 1 S. 1 hat jede natürliche und juristische Person des Privatrechts Anspruch auf Zugang zu den bei einer Behörde vorhandenen Informationen. Nach Abs. 3 S. 1 dieser Vorschrift bleiben besondere Rechtsvorschriften über den Zugang zu amtlichen Informationen, die Auskunftserteilung oder die Gewährung von Akteneinsicht unberührt. Es handelt sich somit um konkurrierende Ansprüche. Konkurrenzfragen nach dieser Vorschrift sind in jedem Einzelfall durch systematische, am Sinn und Zweck des Gesetzes orientierten Auslegung der jeweiligen Informationszugangsrechte zu klären. Eine Vorrangigkeit im Sinne einer Ausschließlichkeit ist nur dort anzunehmen, wo die jeweiligen Rechte die gleichen Anliegen verfolgen. Wenn spezialgesetzliche Regelungen für einen gesonderten Sachbereich einen begrenzten Informationsanspruch - nach der Abgabenordnung lediglich Entscheidung nach Ermessen - vorsehen, ist hier im konkreten Einzelfall zu untersuchen, ob diese Grenzen auch für den Anspruch aus § 1 Abs. 3 S. 1 IFG M-V bindend sind. Es war Intention des Landesgesetzgebers, mit der Einführung des Informationsfreiheitsgesetzes mehr Transparenz und Zugang zu Informationen der öffentlichen Verwaltung zu schaffen. Davon sind die Finanzverwaltungen grundsätzlich nicht ausgeschlossen. Etwaige Beschränkungen lassen sich daher allein aus den Versagungstatbeständen der §§ 5 bis 8 IFG M-V herleiten. Danach darf Akteneinsicht grundsätzlich nur unter Wahrung der Belange Dritter gewährt werden. Personenbezogene Daten Dritter dürfen auch nach dem IFG M-V nicht herausgegeben werden, sodass das Steuergeheimnis Dritter nicht gefährdet ist. Es ist jedoch zu prüfen, ob ein Anspruch auf Zugang zu den übrigen Informationen besteht. Die Finanzbehörden sind daher nach meiner Auffassung unter Umständen verpflichtet, personenbezogene Informationen zu anonymisieren beziehungsweise abzutrennen.

Das Finanzministerium ist meiner Argumentation nicht gefolgt. Eine Entschließung der Datenschutzbeauftragten und der Informationsfreiheitsbeauftragten des Bundes und der Länder zu dieser Thematik ist in Arbeit.

3.4 Windparkprojektierer wünscht Zugang zu Informationen bei Regionalen Planungsverbänden

Ein Windparkprojektierer begehrte bei allen vier Regionalen Planungsverbänden in Mecklenburg-Vorpommern Informationen zu Vorrang- und Eignungsgebieten für Windenergieanlagen auf Basis der Entwürfe der Regionalplanungen.

Die Anträge wurden durch alle Planungsverbände mit einer gleichlautenden Begründung, die sich auf eine Empfehlung der obersten Landesplanungsbehörde stützte, abgelehnt.

Im Ergebnis meiner Recherche teilten mir die Planungsverbände mit, dass es sich bei den Eignungsgebietskulissen für Windenergieanlagen um eine interne Arbeitsgrundlage handelt. Würde deren Inhalt bekannt werden, käme es sofort zu Protesten Betroffener, sodass es nicht mehr gelänge, eine brauchbare und allen Interessen gerecht werdende Entscheidung für einen Entwurf, der für eine Öffentlichkeitsbeteiligung und eine Auslegung geeignet ist, zu treffen. Es würde somit frühzeitig versucht werden, nach nicht objektiven Gesichtspunkten Einfluss auf den Entscheidungsprozess zu nehmen.

Diese Bewertung hielt ich im Ergebnis für nachvollziehbar, wies aber darauf hin, dass nach § 6 Abs. 1 IFG M-V ein Antrag auf Zugang zu Informationen für Entwürfe zu Entscheidungen sowie die Arbeiten und Beschlüsse zu ihrer unmittelbaren Vorbereitung nur dann abzulehnen sind, soweit und solange die vorzeitige Bekanntgabe der Informationen den Erfolg der Entscheidung vereiteln würde. Nach Abschluss des Verfahrens, im vorliegenden Fall also nach Beschlussfassung des jeweiligen Regionalen Raumentwicklungsprogramms, muss der Informationszugang erfolgen. Dieser Bewertung schlossen sich die Regionalen Planungsverbände an, sodass dem Windparkprojektierer nach vorliegender Beschlussfassung ein Informationszugang zugesichert wurde.

Das Verwaltungsgericht Greifswald hat einen Antrag des Windparkprojektierers auf Erlass einer einstweiligen Anordnung mit dem Ziel, einen Planungsverband zum begehrten Informationszugang zu verpflichten, abgelehnt. Diesen Beschluss hat das Oberverwaltungsgericht Mecklenburg-Vorpommern (Beschluss vom 27. August 2007, 1M81/07) inzwischen bestätigt.

3.5 Einsichtnahme in sogenannte Fortführungsrisse beim Katasteramt

Ein Landkreis schilderte mir einen Fall, bei dem ein Eigentümer unter anderem Akteneinsicht in sogenannte Fortführungsrisse seines Grundstückes haben wollte. Hierbei handelt es sich um Vermessungsrisse, die den exakten geometrischen Nachweis über alle Vermessungen der Grenzen und Gebäude sowie Lage von Grenzpunkten und Grenzzeichen enthalten und als Grundlage für die Herstellung und Fortführung der Liegenschaftskarte dienen. Die Fortführungsrisse sind Bestandteil des Katasters.

Nach § 12 Abs. 3 des Gesetzes über die Landesvermessung und das Liegenschaftskataster des Landes Mecklenburg-Vorpommern (VermKatG) dürfen unter anderem Eigentümern Grenzlängen und Grenzabstände von Gebäuden sowie weitere für einen bestimmten Verwendungszweck geeignete Angaben aus dem Katasterzahlenwerk mitgeteilt werden, wenn die Maße geprüft sind. In den Fortführungsrissen werden maßgeblich ungeprüfte Maße angegeben. Nach § 12 Abs. 3 VermKatG besteht für den Grundstückseigentümer somit kein Anspruch auf Einsicht in diese Risse.

Demgegenüber kann ein Informationszugang nach dem IFG M-V gewährt werden, wenn keine Ausnahmetatbestände nach §§ 5 - 8 IFG M-V vorliegen. Solche waren hier nicht ersichtlich. Insbesondere handelt es sich bei den Fortführungsrissen nicht um Entwürfe oder Notizen, sondern um eigenständige, in sich abgeschlossene Datensammlungen. Der in § 12 Abs. 3 VermKatG zum Ausdruck gekommenen Wertung, wonach für die „richtige“ Auswertung und Verwendung der Fortführungsrisse eine vermessungstechnische Vorbildung erforderlich sei, ist im Rahmen des § 1 Abs. 2 in Verbindung mit § 10 Abs. 3 S. 1 IFG M-V Rechnung zu tragen. Danach besteht grundsätzlich ein Zugangsrecht zu den bei einer Behörde vorhandenen Informationen, wobei die betreffende Behörde nicht verpflichtet ist, die inhaltliche Richtigkeit der Informationen zu prüfen. Ich habe dem Landkreis in diesem Fall empfohlen, bei der Gewährung des Informationszugangs auf die Ungenauigkeit der Angaben im Fortführungsriss hinzuweisen.

3.6 Einsichtnahme in Verträge einer Gemeinde mit Dritten

Der Antragsteller begehrte Einsicht in Erschließungsverträge für ein Baugebiet, welche die Gemeinde mit dem Investor im Hinblick auf die Zufahrtsstraßen geschlossen hatte. Die Gemeinde argumentierte, es handele sich um privatrechtliche Verträge, die sie mit Dritten geschlossen habe. Deshalb sei das Informationsfreiheitsgesetz nicht anwendbar. Ich habe die Gemeinde darauf hingewiesen, dass es nach dem Informationsfreiheitsgesetz nicht darauf ankommt, ob die Verträge öffentlich-rechtlicher oder privatrechtlicher Natur sind, sondern allein darauf, dass es sich um Unterlagen handelt, die bei der Gemeinde - als Behörde - verfügbar sind.

Des Weiteren berief sich die Gemeinde auf das Vorliegen von Betriebs- und Geschäftsgeheimnissen mit der Begründung, in dem Vertrag seien sensible Daten enthalten, die nur dem Vertragspartner und bestimmten Mitarbeitern in der Gemeindeverwaltung bekannt seien. Ich habe den Leitenden Verwaltungsbeamten darauf hingewiesen, dass selbst, wenn Anhaltspunkte für ein Betriebs- oder Geschäftsgeheimnis vorliegen, die sogenannte „Drittbeteiligung“ durchzuführen ist. Nach § 9 Abs. 1 IFG M-V ist einem Dritten, dessen Belange durch den Antrag auf Informationszugang berührt sind, schriftlich Gelegenheit zur Stellungnahme innerhalb eines Monats zu geben, sofern Anhaltspunkte dafür vorliegen, dass er ein schutzwürdiges Interesse am Ausschluss des Informationszugangs haben kann. Die Gemeinde hat auf meine Empfehlung hin den Vertragspartner nachträglich beteiligt.

3.7 Einsichtnahme in eine Bauakte - Schutz personenbezogener Daten

Bei einer Landkreisverwaltung wurde der Antrag auf Einsicht in eine Bauakte gestellt. Diese Akte enthielt unter anderem personenbezogene Daten des Bauherrn. Es lagen Anhaltspunkte vor, dass der Bauherr diesbezüglich ein schutzwürdiges Interesse am Ausschluss des Informationszugangs haben kann. Im Ergebnis der Beteiligung des Bauherrn nach § 9 IFG M-V lehnte dieser den Informationszugang ab. In seiner Stellungnahme zweifelte der Bauherr insbesondere an, ob die betreffende Bauakte Informationen nach § 2 IFG M-V beinhaltet. Seiner Auffassung nach erfasst das IFG M-V nicht Schriftwechsel, Ersuchen und zum persönlichen Lebensbereich gehörende Daten.

Die Bauakte enthielt zweifelsohne Informationen im Sinne des IFG M-V, da hierzu alle Informationen zählen, die bei der Erfüllung amtlicher Tätigkeit gewonnen und verarbeitet werden. Hierzu zählen auch solche, die die Behörde unbeabsichtigt erhält und die einem amtlichen Zweck dienen.

Die in der Bauakte enthaltenen personenbezogenen Daten konnten in diesem Fall geschwärzt werden, da der Antragsteller lediglich Informationen zum Zeitpunkt der Erteilung einer Baugenehmigung und zu Gestaltungsfragen begehrte.

3.8 Einsichtnahme in Gaspreiskalkulation

Ein Petent begehrte die Einsichtnahme in Unterlagen bei einem Energieversorger (Stadtwerke), aus denen sich die Kalkulation des Gaspreises ergibt. Da die Stadt mit einer Mehrheit der Anteile oder Stimmen an diesen Stadtwerken beteiligt ist, musste der Antrag auf Informationszugang nach § 3 Abs. 3 in Verbindung mit § 10 Abs. 1 S. 3 IFG M-V direkt an den Oberbürgermeister dieser Stadt als zuständige Behörde gerichtet werden, was vorliegend auch geschah. Die Behörde versäumte es, den Antrag nach § 11 Abs. 1 IFG M-V unverzüglich (spätestens jedoch nach Ablauf einer Frist von einem Monat nach Stellung des ordnungsgemäßen Antrags) zu bescheiden. Nach meinem Hinweis wurde der Antrag zwar beschieden, der Informationszugang unter Hinweis auf vorliegende Betriebs- oder Geschäftsgeheimnisse aber größtenteils abgelehnt.

Meine Prüfung bezog sich mithin auf die Frage des Vorliegens von Betriebs- und Geschäftsgeheimnissen. Gemäß § 8 IFG M-V ist ein Antrag auf Zugang zu Informationen unter anderem dann abzulehnen, soweit durch die Übermittlung von Informationen ein Betriebs- oder Geschäftsgeheimnis offenbart wird und der Betroffene nicht eingewilligt hat.

Nach der Rechtsprechung des Bundesgerichtshofs sind Betriebs- oder Geschäftsgeheimnisse
- im Zusammenhang mit einem Geschäftsbetrieb stehende Tatsachen,
- die nicht offenkundig, also nur einem begrenzten Personenkreis bekannt sind,
- nach dem erkennbaren Willen des Inhabers geheim gehalten werden sollen und
- an deren Geheimhaltung der Geheimnisträger ein berechtigtes Interesse hat.

Meine Recherche ergab, dass sich der Gaspreis vorliegend aus verschiedenen Komponenten (Gaseinkauf, Vertriebskosten, Netznutzung, Konzessionsabgabe und Erdgas- und Umsatzsteuer) zusammensetzt. Lediglich die Informationen zum Gaseinkauf könnten ein Betriebs- oder Geschäftsgeheimnis und damit einen Ablehnungsgrund nach § 8 IFG M-V darstellen.

Das Gas wird bei einem Unternehmen eingekauft, die hierzu erforderlichen Bezugskonditionen werden jeweils ausgehandelt. Nach Auskunft der Stadtwerke ist hinsichtlich des Vertragsinhalts zwischen beiden Vertragspartnern Verschwiegenheit vereinbart worden. Sollte der Bezugspreis offenbart werden, hätten andere Energieversorger gegebenenfalls einen nicht unerheblichen Wettbewerbsvorteil, der sich auf künftige Verhandlungen wettbewerbsrelevant auswirken würde. Ein Informationszugang würde dabei insbesondere einen Rückschluss auf die Wirtschafts- und Marktstrategie der Stadtwerke gegenüber diesem Unternehmen zulassen.

In Bezug auf die übrigen begehrten Informationen hatte die Stadt kein berechtigtes Geheimhaltungsinteresse beziehungsweise hatte diese im Zusammenhang mit anderen Publikationen (z. B. Geschäftsbericht) bereits veröffentlicht. Die Behörde hatte nach § 4 Abs. 4 IFG M-V teilweise auf die Veröffentlichung dieser Informationen hingewiesen.
Interessanterweise konnte ich feststellen, dass die Angaben zur Zusammensetzung des Gaspreises und damit dem Schwerpunkt der begehrten Informationen auf der Internetseite der Stadtwerke bereits veröffentlicht waren. Dem Antragsteller hätten also sehr schnell und unbürokratisch die gewünschten Informationen übermittelt werden können, was vorliegend jedoch erst im Ergebnis meiner Prüfung geschah.

3.9 Einsichtnahme in ministerielles Genehmigungsverfahren beim Ministerium für Bildung, Wissenschaft und Kultur

Ein Antragsteller beantragte die Einsichtnahme in Vorgänge unseres Ministeriums für Bildung, Wissenschaft und Kultur zum Genehmigungsverfahren einer Schule in privater Trägerschaft. Das Ministerium war der Auffassung, der Antragsteller müsse sein Begehren gemäß § 10 Abs. 2 IFG M-V konkretisieren. Nach dieser Vorschrift sind die begehrten Informationen zu umschreiben. Vorliegend war es jedoch ziemlich offensichtlich, dass der Antragsteller dies mangels Kenntnis vom Ablauf eines solchen Genehmigungsverfahrens nicht konnte. Ich hatte das Ministerium für Bildung, Wissenschaft und Kultur darauf hingewiesen, dass es seine Pflicht ist, in Fällen, in denen dem Antragsteller Angaben zur Umschreibung der begehrten Informationen fehlen, beratend tätig zu werden. Dies kann so aussehen, dass dem Antragsteller mitgeteilt wird, wie eine derartige Akte aufgebaut ist, ob diese beispielsweise aus mehreren Teilen besteht, ob und in welchem Umfang der Schutz personenbezogener Daten tangiert ist, sodass gegebenenfalls Dritte zu beteiligen sind.

Nach einigen Telefonaten und einer großen Presseresonanz wurde dem Informationsbegehren stattgegeben.

3.10 Einsichtnahme in Akte zu einem abgeschlossenen Ermittlungsverfahren durch einen Beschuldigten

Ein Petent begehrte Einsicht in einen bei einer Staatsanwaltschaft abgeschlossenen Vorgang, in dem er als Beschuldigter geführt wurde. Im vorliegenden Fall war zu prüfen, ob gegenüber der Staatsanwaltschaft überhaupt ein Informationszugangsanspruch nach dem IFG M-V besteht.

Nach § 3 Abs. 4 IFG M-V sind Behörden im Sinne dieses Gesetzes nicht Gerichte oder Strafverfolgungs- und Strafvollstreckungsbehörden, soweit sie als Organe der Rechtspflege oder aufgrund besonderer Rechtsvorschriften in richterlicher Unabhängigkeit tätig werden, sowie Disziplinarbehörden.

Sofern das Auskunftsersuchen in dem Bereich der Rechtspflegeaufgaben einzuordnen ist, findet das IFG M-V keine Anwendung (vergleichbar mit den datenschutzrechtlichen Bestimmungen in § 2 Abs. 4 DSG M-V). Demgegenüber werden aber Verwaltungsangelegenheiten vom IFG M-V mit erfasst.

Nicht in jedem Fall sind diese beiden Bereiche eindeutig voneinander zu trennen. Ein inzwischen allgemein anerkanntes Hilfsmittel zur Klassifizierung der bei einem Gericht und ebenso bei einer Staatsanwaltschaft anfallenden Tätigkeiten ist die sogenannte Hamburger Liste. Diese Liste hat der Hamburger Senat auf Ersuchen der Bürgerschaft im Frühjahr 1993 erstellt, um alle verfassungsrechtlichen Möglichkeiten einer Datenschutzkontrolle bei Gerichten sicherzustellen und Fragen der Kontrollbefugnis des Hamburgischen Datenschutzbeauftragten zu klären. Nach der Hamburger Liste zählt die Gewährung von Akteneinsicht nach Abschluss eines Verfahrens (unabhängig von etwaiger Beteiligtenstellung im abgeschlossenen Verfahren) zu den Verwaltungsangelegenheiten.

Da vorliegend das Verfahren bereits eingestellt und somit abgeschlossen war, unterlag das betreffende Informationsbegehren zumindest auch den Bestimmungen des IFG M-V.

Dem hielt der zuständige Leitende Oberstaatsanwalt entgegen, dass das IFG M-V nicht anwendbar sei, da der Antragsteller Auskunft aus einem strafrechtlichen Ermittlungsverfahren, mithin also aus einer Rechtssache, begehre. Maßgeblich für die Staatsanwaltschaft sei vielmehr gewesen, ob das Verfahren, aus dem Auskunft erteilt werden soll, eine Verwaltungssache oder eine Rechtssache ist (unabhängig von der Frage, ob das Verfahren bereits eingestellt ist). Dieser Auffassung konnte ich mich nicht anschließen.

Nach § 1 Abs. 3 IFG M-V bleiben besondere Rechtsvorschriften über den Zugang zu amtlichen Informationen, die Auskunftserteilung oder die Gewährung von Akteneinsicht unberührt. § 147 Abs. 7 Strafprozessordnung (StPO) räumt einem Beschuldigten ein weiteres gegebenenfalls über die Bestimmungen des IFG M-V hinausgehenden Akteneinsichtsrecht ein. Da dem Antragsteller im vorliegenden Fall eine umfassende Aktenauskunft nach dieser Vorschrift gewährt wurde, habe ich auf die Anwendbarkeit des IFG M-V nicht weiter gedrungen.

4. Nicht-öffentlicher Bereich

4.1 Einführung zum 3. Tätigkeitsbericht gemäß § 38 Absatz 1 Bundesdatenschutzgesetz (BDSG)

Gemäß § 33 a Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) in Verbindung mit § 38 Absatz 1 BDSG lege ich als zuständige Aufsichtsbehörde für den nicht-öffentlichen Bereich in Mecklenburg-Vorpommern dem Landtag und der Landesregierung den Bericht über die Tätigkeit der Aufsichtbehörde vor, der den Zeitraum vom 1. Januar 2006 bis zum 31. Dezember 2007 umfasst. Die Berichterstattung der Datenschutz-Kontrollstellen ist in der Richtlinie 95/46/EG des Europäischen Parlamentes und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Europäische Datenschutzrichtlinie) vorgesehen und wurde mit der Regelung in § 38 Absatz 1 Satz 6 BDSG in nationales Recht übernommen.

Der rechtliche Rahmen für meine Tätigkeit als Aufsichtsbehörde ist in § 38 BDSG festgelegt. Das BDSG ist gemäß § 1 Absatz 2 BDSG Grundlage für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch nicht-öffentliche Stellen (Unternehmen und Betriebe). Es regelt insbesondere die Zulässigkeit der Datenverarbeitung, die Rechte der Betroffenen und die Aufsicht über den Datenschutz im nicht-öffentlichen Bereich.

Die Aufsichtsbehörde kann im Rahmen ihrer Prüfungstätigkeit Auskünfte verlangen (§ 38 Abs. 3 BDSG), Geschäftsräume zu Prüfungen betreten und Einsicht in Unterlagen nehmen. Im Falle nicht ausreichender Datensicherungsmaßnahmen kann sie ferner anordnen, dass die Mängel beseitigt werden, oder - in schwerwiegenden Fällen - unter bestimmten Umständen ein Zwangsgeld festsetzen beziehungsweise den Einsatz einzelner Verfahren untersagen (§ 38 Abs. 5 BDSG). Die Aufsichtsbehörde hat ferner nach § 38 Absatz 5 Satz 3 BDSG die Möglichkeit, die Abberufung eines betrieblichen Datenschutzbeauftragten zu verlangen, wenn ihm Fachkunde und Zuverlässigkeit fehlen. Gegen solchen Bescheid der Aufsichtsbehörde gemäß § 38 Absatz 5 BDSG ist eine Klage vor dem Verwaltungsgericht möglich.

Ähnlich wie in einem vorgerichtlichen Verfahren klärt die Aufsichtsbehörde im Rahmen ihrer Möglichkeiten den Sachverhalt auf und nimmt eine rechtliche Bewertung vor. Sie spricht in Fragen der Zulässigkeit der einzelnen Datenverarbeitung zunächst Empfehlungen aus, die allerdings keinen Verwaltungsakt darstellen, weil nicht konkret regelnd eingegriffen wird.

Für den Petenten liegt mit der datenschutzrechtlichen Bewertung zugleich eine Grundlage vor, aufgrund derer das jeweilige Unternehmen als datenverarbeitende Stelle in der Mehrzahl der Fälle zu einem datenschutzrechtlich korrekten Verfahren zurückgeführt werden kann. Gleichzeitig kann die Stellungnahme der Aufsichtsbehörde gegebenenfalls auch in gerichtlichen Verfahren - ähnlich wie ein Gutachten - verwendet werden. Wenn nach meiner Ansicht eine unzulässige Datenverarbeitung vorliegt, habe ich ferner die Möglichkeit, ein Ordnungswidrigkeitsverfahren einzuleiten (§ 43 BDSG) beziehungsweise - in besonders schwerwiegenden Fällen - Strafantrag zu stellen (§ 44 Abs. 2 BDSG).

Gemäß § 38 Absatz 1 in Verbindung mit § 21 Absatz 1 Satz 1 BDSG hat jedermann die Möglichkeit, sich an die Aufsichtsbehörde zu wenden, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch nicht-öffentliche Stellen in seinen Rechten verletzt worden zu sein. Die entsprechenden Eingaben im Berichtszeitraum umfassten inhaltlich die gesamte Palette der datenschutzrechtlichen Fragen eines Unternehmens und - aus Arbeitnehmersicht - der Mitarbeiter von Unternehmen und Betrieben. Die Anfragen und Beschwerden betrafen häufig die Bereiche Auskunfteien, Werbung (per Post, E-Mail und Internet), Datenverarbeitung im Versandhandel, Einsatz von Videokameras bis hin zu Fällen unsachgemäß entsorgter beziehungsweise ungesichert gelagerter Personalakten. In zwei Fällen habe ich als Aufsichtsbehörde Strafantrag gestellt. Bußgeldverfahren, die Bußgelder von bis zu 25.000 Euro bei Verstößen gegen formale Vorschriften und bis zu 250.000 Euro bei materiellen datenschutzrechtlichen Verstößen nach sich ziehen können, musste ich während des Berichtszeitraums nicht einleiten.

Zu einem Aufgabenschwerpunkt meines Tätigkeitsbereichs als Aufsichtsbehörde zählt die Beratung, Schulung und Unterstützung betrieblicher Datenschutzbeauftragter. Nicht-öffentliche Stellen, die personenbezogene Daten automatisiert erheben, verarbeiten oder nutzen, haben grundsätzlich die Pflicht, einen betrieblichen Beauftragten für den Datenschutz zu bestellen (§ 4 f Abs. 1 BDSG). Dieser betriebliche Datenschutzbeauftragte hat insbesondere die Aufgabe, auf die Einhaltung der Datenschutzregelungen in seinem Betrieb hinzuwirken. Er ist der Geschäftsleitung unmittelbar unterstellt, in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei und muss die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzen. Im Rahmen der Fortbildung der betrieblichen Datenschutzbeauftragten beziehungsweise der Geschäftsleitungen von Unternehmen und Firmen im Lande haben Mitarbeiter meiner Behörde datenschutzrechtliche und datensicherheitstechnische Seminare und Schulungsveranstaltungen - unter anderem in Zusammenarbeit mit der Industrie- und Handelskammer zu Schwerin und politischen Stiftungen - durchgeführt. Zum Tagesgeschäft gehören Einzelberatungen von Betrieben und Unternehmen zum gesamten Spektrum der datenschutzrechtlichen Fragen in diesem Bereich. Darüber hinaus organisiert die Gesellschaft für Datenschutz und Datensicherung e. V. (GDD) die Einrichtung von regionalen Erfahrungsaustauschkreisen - sogenannten ERFA-Kreisen. Auch in Mecklenburg-Vorpommern treffen sich im ERFA-Kreis regelmäßig betriebliche Datenschutzbeauftragte aus Betrieben des Landes unter Beteiligung von Vertretern aus Behörden und anderen öffentlichen Stellen. Die Datenschutzaufsichtsbehörde ist jeweils zu den Sitzungen eingeladen und nimmt regelmäßig an diesen rund dreimal im Jahr stattfindenden Gesprächsrunden teil - ebenso wie an den jährlichen Datenschutzfachtagungen der GDD.

Ferner arbeiten die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich aller Bundesländer sowie der Bundesbeauftragte für den Datenschutz seit vielen Jahren im sogenannten Düsseldorfer Kreis zusammen, um eine möglichst einheitliche Anwendung des BDSG in Bund und Ländern zu gewährleisten. In den zweimal jährlich stattfindenden Sitzungen werden die wichtigsten Fachfragen der Datenschutzaufsicht im nicht-öffentlichen Bereich diskutiert und abgestimmte Lösungen entwickelt. Dies ist insbesondere dann von Bedeutung, wenn sich die Beratungs- und Kontrolltätigkeit der Aufsichtsbehörden auf länderübergreifende Wirtschaftsunternehmen bezieht.

Schwerpunkte innerhalb des Berichtszeitraumes waren unter anderem die Themenbereiche Kredit- und Versicherungswirtschaft, Auskunfteien, Scoring-Verfahren sowie SWIFT und RFID (siehe auch Punkte 2.15.4, 4.4.1 und 4.3.2). Als Aufsichtbehörde für Mecklenburg-Vorpommern bin ich zusätzlich beteiligt an der „Arbeitsgruppe SCHUFA/Handels- und Wirtschaftsauskunfteien“ des Düsseldorfer Kreises, die ebenfalls Bund-Länder-übergreifend zweimal jährlich zusammenkommt. Weitere Arbeitsgruppen des Düsseldorfer Kreises sind mit den Themenbereichen Internationaler Datenschutz, Versicherungswirtschaft, Kreditwirtschaft, Telekommunikation sowie Tele- und Mediendienste befasst.

Mit der Übernahme der Aufgabe wurde meine Dienststelle mit einem Mitarbeiter verstärkt. Diese Verstärkung erweist sich als völlig unzureichend. Aufgrund der Fülle und Breite der Problemstellungen bin ich trotz organisatorischer Anpassungen auch nach der Einarbeitungsphase noch immer nicht in der Lage, Petitionen und Anfragen in der erforderlichen Geschwindigkeit und Tiefe zu bearbeiten. Eine personelle Verstärkung ist dringend geboten, um den wachsenden Anforderungen gerecht werden zu können, ohne die Qualität und die Unabhängigkeit zu gefährden.

4.2 Grunddatenerhebung betrieblicher Datenschutz in Mecklenburg-Vorpommern

Im Zeitraum vom 15. Juni bis 14. Dezember 2007 habe ich das Projekt „Grunddatenerhebung betrieblicher Datenschutz in Mecklenburg-Vorpommern“ durchgeführt. Eine repräsentative Befragung von Unternehmen in Mecklenburg-Vorpommern sollte einen verlässlichen Überblick über den gegenwärtigen Stand der Umsetzung der Datenschutzvorschriften ermöglichen, um wichtige Informationen zur Umsetzung meines gesetzlichen Auftrages als Aufsichtsbehörde zu gewinnen.

Nicht-öffentliche Stellen sind gemäß § 2 Absatz 4 Bundesdatenschutzgesetz (BDSG) alle natürlichen und juristischen Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie keine öffentlichen Stellen sind. Darunter fallen vor allem private Einzel- und Gesellschaftsunternehmen aller Branchen, beispielsweise Handel, Versandhandel, Banken, Versicherungen, Auskunfteien, Markt- und Meinungsforschung, Werbung, Adress- und Telefonbuchverlage, Vermietung, Reisebüros, aber auch Angehörige der sogenannten freien Berufe wie Steuerberater, Rechtsanwälte, Ärzte oder Apotheker.

Die wichtigsten Ergebnisse der Umfrage vorweg:

Insgesamt sind von 1.002 versendeten Fragebögen 758 Antworten eingetroffen. Aus verschiedenen Gründen waren für das Projekt 716 Fragebögen verwertbar. Damit handelt es sich um die bisher größte repräsentative Befragung solcher Art in Deutschland.

Die aus dem ersten Fragenkomplex erzielten Ergebnisse zu den Angaben des befragten Unternehmens spiegeln die Unternehmensstruktur in Mecklenburg-Vorpommern wider. Der Hauptanteil der befragten Unternehmen - 61,87 % (443 Unternehmen) - haben einen bis neun Mitarbeiter beschäftigt. An zweiter Stelle - 12,01 % (86 Unternehmen) - stehen Firmen mit einer Beschäftigtenanzahl von 10 bis 19 Arbeitnehmern. Nur jeweils 10 Unternehmen, also 1,4 % der Teilnehmer, gaben an, 100 bis 249 bzw. 250 und mehr Mitarbeiter zu beschäftigen. Die Mehrzahl der befragten Unternehmen - 445, 62,2 % - gab an, dass eine bis neun Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.

Damit entfällt für diese Unternehmen grundsätzlich die Pflicht zur Bestellung eines Datenschutzbeauftragten. Somit haben 70 Unternehmen, die mehr als 9 Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen, einen Datenschutzbeauftragten zu bestellen.

In diesem Zusammenhang wird in Frage 18 ermittelt, wie viele der Unternehmen nun tatsächlich einen Datenschutzbeauftragten bestellt haben. Hier ergibt sich, dass insgesamt 122 Unternehmen einen betrieblichen bzw. externen Datenschutzbeauftragten bestellt haben.

324 Unternehmen (45 %) gaben an, dass eine Dienstanweisung bzw. eine Dienstvereinbarung zum Datenschutz existiert. 344 (48 %) Unternehmen verneinen dies.

Obwohl laut dem Ergebnis zu Frage 18 538 Unternehmen keinen Datenschutzbeauftragten bestellt haben, also die Geschäftsführung die Aufgaben des Datenschutzbeauftragten zu übernehmen hat, gaben lediglich 390 Geschäftsführungen an, sich persönlich verantwortlich zu fühlen. 170 Unternehmen bleiben nach eigenen Angaben entgegen den gesetzlichen Vorschriften ohne Kontrolle des Datenschutzes, gleichwohl in den Unternehmen eine entsprechende Verantwortungszuordnung (Datenschutzbeauftragter, Geschäftsführer) erfolgt ist, was eine formale Bestellung nahe legt.

Die Mehrzahl der Unternehmen (417; 58 %) nimmt das Datengeheimnis erklärtermaßen ernst und kann eine entsprechende Verpflichtung ihrer Mitarbeiter vorweisen. Nach dem Ergebnis zu Frage 2 verarbeiten in 515 Unternehmen Mitarbeiter personenbezogene Daten automatisiert. Somit haben 98 Unternehmen einen entsprechenden Nachholbedarf. Das Bundesdatenschutzgesetz schreibt die Schriftform nicht vor. Deshalb ist auch eine mündliche Verpflichtung auf das Datengeheimnis gesetzeskonform. Allerdings ist aus Nachweisgründen eine schriftliche Verpflichtung auf das Datengeheimnis dringend zu empfehlen.

Obwohl nach den Antworten zu Frage 2 mindestens 515 Unternehmen datenschutzrechtliche Schulungen ihrer Mitarbeiter durchführen müssten, haben dies insgesamt lediglich 290 Umfrageteilnehmer (41 %) angegeben. Davon schulten nach eigenen Angaben 118 Firmen (16,48 %) bei Bedarf, nur 103 regelmäßig (14,39 %) und 66 Unternehmen haben bislang ein Mal geschult. 332 Unternehmen (46,4 %) haben bisher nicht geschult. Hierin zeigt sich ein erheblicher Nachholbedarf, den sowohl die Kammern und Verbände als auch die Aufsichtsbehörde verstärkt abdecken müssen.

Für alle meldepflichtigen Verfahren automatisierter Verarbeitungen personenbezogener Daten ist ein (internes) Verfahrensverzeichnis gemäß § 4 e Bundesdatenschutzgesetz zu erstellen. Aus den Angaben des internen Verfahrensverzeichnisses, das dem Datenschutzbeauftragten zur Verfügung zu stellen ist, erstellt dieser das Verfahrensverzeichnis nach § 4 e S. 1 Nr. 1 - 8 Bundesdatenschutzgesetz, welches jedermann auf dessen Antrag hin verfügbar zu machen ist. Von den befragten 716 Unternehmen antworteten 511 (71,4 %) damit, dass sie kein Verfahrensverzeichnis erstellt und vorrätig haben.

Weitere Fragen befassten sich mit der Sicherheit verwendeter technischer Systeme. Aus der Statistik zur Existenz von Regelungen zum Passwortgebrauch ist zu entnehmen, dass der Zugang zu EDV-Systemen nicht einmal durch eine Authentisierung mittels Nutzerkennung und Passwort ausgeprägt ist. Die überwiegende Anzahl von Unternehmen nutzt somit schon nicht den Mindeststandard für einen Missbrauchsschutz.

Die Ergebnisse zur IT-Sicherheit im 4. Fragenkomplex sind besorgniserregend. Das zeigt der hohe Anteil (78 %) der Unternehmen, die ihre Unternehmensdaten nicht verschlüsseln. Die Sensibilität und das Sicherheitsbewusstsein zum Schutz von Unternehmensdaten, und dazu zählen auch personenbezogene Daten, hat sich trotz zunehmender Gefahren beim elektronischen Geschäftsverkehr und durch das Internet bisher offensichtlich nicht ausreichend entwickelt.

Ich sehe hier einen erhöhten Beratungsbedarf und eine hohe Verantwortung bei den Anbietern von Kommunikationssystemen, stärker auf die Gefahren unverschlüsselter Kommunikation hinzuweisen.

9 % der Unternehmen nutzten den datenschutzkonformen Umgang mit personenbezogenen Daten bereits als Marketinginstrument bzw. erkennen, dass Kunden dieses fordern und somit gute Voraussetzungen für die Geschäftsanbahnung und für die Kundenbindung gegeben sind.

Insgesamt bestätigte die Befragung einen höheren Datenschutzstandard, als es meine bisher dreijährige Erfahrung als Aufsichtsbehörde vermuten ließ. Die Bestellung betrieblicher Datenschutzbeauftragter und die Grundsensibilisierung für die Relevanz des Datenschutzes für das eigene Unternehmen sind eine gute Grundlage für eine verstärkte Aufklärungs- und Unterstützungsarbeit meiner Behörde.

Bemerkenswert hoch (32 %) ist die Aussage der Unternehmen, datenschutzrechtliche Vorgaben nach dem Bundesdatenschutzgesetz im Unternehmen nur deshalb umzusetzen, um Straf- und Bußgelder sowie Schadensersatzforderungen zu vermeiden. Gleiches gilt für Unternehmen (24 %), die keine Vorteile im datenschutzkonformen Umgang mit personenbezogenen Daten sehen. Diese Antworten zeigen, dass viele Regeln nur aus formalen Gründen eingehalten werden, was eine effektivere Arbeit des Datenschutzbeauftragten im Sinne des Unternehmens erschwert. Diese Datenschutzbeauftragten möchte ich durch einen weiteren Ausbau meiner Dienstleistungsangebote, soweit dies mit meinen Ressourcen möglich ist, unterstützen und baue hierfür auf die Unterstützung der Kammern, Verbände und des Landtages.

Die Umfrageergebnisse sind im Einzelnen auf meiner Website unter http://www.datenschutz-mv.de/navi/dschutz/grunddaten.html veröffentlicht.

In Mecklenburg-Vorpommern gibt es derzeit rund 150.000 Betriebe, worunter Gewerbebetriebe und auch Freiberufler gefasst sind[1]. 1.002 von diesen nicht-öffentlichen Stellen wurden im Rahmen des Projektes zur Einhaltung datenschutzrechtlicher Regelungen nach dem BDSG mit einem anonymisierten Fragebogen befragt.

Nach Abschluss der Planungsphase führte ich mit den berufsständischen Kammern und Vereinigungen Mecklenburg-Vorpommerns ein Kick-off-Seminar am 17. Juli 2007 durch. Während der Veranstaltung habe ich über die wesentlichen Eckpunkte des Vorhabens informiert.

[1] Nach einer Angabe des Finanzministeriums Mecklenburg-Vorpommern, Bereich Betriebsprüfung, Stand: 1. Januar 2007

Die Architekten-, Ingenieur-, Apotheker-, Steuerberaterkammer, die Industrie- und Handelskammern sowie die Handwerkskammern und die Kassenärztliche und Kassenzahnärztliche Vereinigung sollten ihren von der Befragung betroffenen Mitgliedern fundiert Auskunft bezüglich der Durchführung des Projektes geben können und das Projekt mittels einer Information an die Unternehmen in ihrer Verbandszeitschrift bekannt machen. Darüber hinaus wurden die Landtagsfraktionen sowie das Ministerium für Wirtschaft, Arbeit und Tourismus und die Neue Verbraucherzentrale Mecklenburg-Vorpommern in die Information einbezogen.

Ich habe die berufsständischen Kammern und Vereinigungen um die Übermittlung der Anschriften ihrer Mitglieder gebeten, um aus den unterschiedlichen Adresspools per Zufallsprinzip Umfrageteilnehmer auswählen zu können. Der Direktbezug der Adressen von der jeweiligen Kammer bzw. Vereinigung war nötig, um möglichst aktualisierte Betriebsanschriften zu gewinnen und somit die Anzahl der unzustellbaren Fragebögen gering zu halten. In diesem Zusammenhang habe ich gegenüber den berufsständischen Kammern und Vereinigungen die Anonymität und Vertraulichkeit der Auswertung zugesichert und die daraus resultierende Sanktionsfreiheit in Bezug auf festgestellte Datenschutzrechtsverstöße garantiert, um Nachteile für das einzelne Unternehmen von vornherein auszuschließen und den Aussagewert der Befragungsergebnisse zu erhöhen.

Mein Auskunftsbegehren stützte ich auf § 31 Absatz 1 Satz 1 Landesdatenschutzgesetz (DSG M-V).

Die gesetzlich geregelte Pflicht des Landesbeauftragten für den Datenschutz M-V zur Durchführung von Kontrollen bei nicht-öffentlichen Stellen (z. B. bei privaten Unternehmen) ergibt sich aus § 38 Absatz 1 BDSG in Verbindung mit § 33 a DSG M-V. § 38 Absatz 1 BDSG verlangt von der Aufsichtsbehörde, dass die „Ausführung“ des BDSG „sowie anderer Vorschriften über den Datenschutz“ kontrolliert wird.

Hinsichtlich der Entscheidung, ob, wie und welche Unternehmen kontrolliert werden sollen, steht dem Landesbeauftragten für den Datenschutz M-V das Opportunitätsprinzip zur Seite. Der Landesbeauftragte entscheidet unabhängig über Form und Umfang seiner Aufsichtstätigkeit. Dies ist Ausfluss und Kern der durch die europäische Datenschutzrichtlinie 95/46/EG vom 24. Oktober 1995 geforderten und durch das BDSG umgesetzten „völligen Unabhängigkeit“, Artikel 28 Absatz 1 Satz 2 RL 95/46/EG. Die stichprobenweise Befragung von rund 1.000 privaten Unternehmen in Mecklenburg-Vorpommern ist somit eine rechtlich zulässige Form der Kontrolltätigkeit des Landesbeauftragten für den Datenschutz M-V und entspricht seinem gesetzlichen Auftrag nach dem BDSG.

Die Apotheker-, Ingenieur- und Architektenkammer sowie die Kassenärztliche und Kassenzahnärztliche Vereinigung übermittelten die für die Durchführung des Projektes notwendigen Mitgliederanschriften.

Mit den Wirtschaftskammern konnte keine Einigkeit über die Zulässigkeit einer Übermittlung der Daten ihrer zugehörigen Unternehmen erzielt werden, weshalb ich eine auf dem Markt erhältliche CD-ROM für die Adressermittlung nutzte, die eine nach Branchen sortierte Auswahl an Unternehmen im Land enthielt. Hieraus ergaben sich zwar relativ viele unverwertbare Rückläufe (62 von insgesamt 676 versendeten Fragebögen) wegen Unzustellbarkeit, was jedoch die Repräsentativität wegen der entsprechend hohen Zahl der gezogenen Stichproben nicht negativ beeinflusste.

Während des Kick-off-Seminars wurde der Entwurf des Fragebogens diskutiert. Aufgrund von Schwierigkeiten im Verständnis von datenschutzrechtlichen Terminologien und Fachbegriffen wurde die Länge des Fragebogens von 82 auf 39 Fragen reduziert und jede einzelne Frage möglichst selbsterklärend oder mittels einer erläuternden Anmerkung am Ende formuliert. Zudem befindet sich seit dem Start des Projektes eine Informationsbroschüre zum Thema Datenschutz im Betrieb auf meiner Internetseite, auf die die befragten Unternehmen im Anschreiben hingewiesen wurden.

Ebenfalls habe ich für das Projekt eine für die Unternehmen kostenlose Telefonhotline von Montag bis Donnerstag von 08:00 bis 19:00 Uhr und am Freitag von 08:00 bis 17:00 Uhr einrichten lassen. Sie sollte dazu dienen, Fragen der Unternehmen zum Ausfüllen des Fragebogens sofort, unmittelbar und kompetent zu beantworten und somit die Teilnahme am Projekt erleichtern. Die Nutzung der Telefonhotline gestaltete sich moderat; insgesamt sind 93 Anrufe im Zeitraum vom 3. September bis 9. November 2007 eingegangen. Vorwiegend wurden Erklärungen bestimmter datenschutzrechtlicher Terminologien nachgefragt.

Im Vorfeld der Befragung habe ich mich von Herrn Dr. Schiffer, dbb Akademie Bonn, einem auf empirische Sozialforschung spezialisierten Fachmann, hinsichtlich statistischer Gesichtspunkte beraten lassen. Diese Beratung hat gewährleistet, dass die Befragung von rund 1.000 Unternehmen im Lande repräsentative Aussagen zum Datenschutzniveau zulässt. Bei der Ermittlung der zu befragenden Unternehmen handelte es sich um eine proportional geschichtete Zufallsstichprobenziehung. Proportional geschichtet deshalb, da der gesamte Adresspool aus einzelnen Adressbeständen der öffentlich-rechtlichen Kammern und Vereinigungen bzw. eines veröffentlichten Branchenbuchs besteht und die aus den einzelnen Adressbeständen gezogene Anzahl der Unternehmensadressen proportional abhängig von der Höhe des einzelnen Adressbestandes zur Anzahl 1.002 des gesamten Adresspools gewesen ist.

Die Umfrage wurde unter Wahrung der Anonymität und der Vertraulichkeit mittels eines Fragebogens durchgeführt. Um die Anonymität zu gewährleisten, war einem adressierten und frankierten Rückumschlag zusätzlich ein Blankoumschlag für die Rücksendung des ausgefüllten Fragebogens beigefügt. Dieser Blankoumschlag wurde in meiner Behörde von dem Umfrageteilnehmer-identifizierenden Rückumschlag getrennt und separat geöffnet. Datenschutzrechtsverstöße konnten somit - wie von mir zugesichert - nicht geahndet werden.

Der Fragebogen enthielt 39 Fragen, die in folgenden fünf Gruppen zusammengefasst waren:

- Angaben zum befragten Unternehmen,
- Allgemeine Fragen zur Einhaltung des Bundesdatenschutzgesetzes,
- Fragen an den betrieblichen oder externen Datenschutzbeauftragten,
- Fragen zur automatisierten Verarbeitung personenbezogener Daten,
- Freiwillige Meinungsäußerungen zu datenschutzrelevanten Themen.

Im Gegensatz zu konkreten Fragestellungen zur Einhaltung des Datenschutzes ab Frage 5 werden die allgemeinen Angaben zur Firma, die in den Fragen 1 bis 4 ermittelt werden, beinahe vollständig gemacht. Dies mag daran liegen, dass die allgemeinen Angaben zum Unternehmen leicht fallen. Werden dagegen speziell datenschutzrechtliche Terminologien - wie sie im Bundesdatenschutzgesetz zu finden sind - verwendet (so ab Frage 5), findet man häufiger, dass Fragen überhaupt nicht beantwortet, also keine Angaben gemacht werden. Letzteres liegt, wie sich auch aus persönlichen Gesprächen mit den Umfrageunternehmen ergab, in den meisten Fällen daran, dass die unbekannten Begrifflichkeiten im Bereich des Datenschutzrechts abschreckten und verunsicherten. Diese Unsicherheiten hätten durch eine intensivere Inanspruchnahme der projektbegleitenden Telefonhotline vermieden werden können.

Die Fragebögen wurden in zwei Durchgängen verschickt. Für das Ausfüllen hatten die Unternehmer je zweieinhalb Wochen Zeit. Im ersten Durchgang, in dem Apotheker, Architekten, Ärzte, Zahnärzte und Ingenieure angeschrieben wurden, antworteten 148 von 326 Befragten, also 45,4 %. Ebenfalls im ersten Durchgang erfolgte die Umfrage unter 676 Firmen im Land. Insgesamt reagierten 212 Unternehmen in der ersten Runde, also 31,4 % der angeschriebenen Unternehmen.

Im zweiten Durchgang erfolgte die wiederholte Befragung der im ersten Durchgang säumigen Unternehmen. Von insgesamt 635 Unternehmen antworteten nun 398, also 62,7 % der angeschriebenen Unternehmen.

Wie bereits erwähnt, sind von 1.002 versendeten Fragebögen 758 Antworten eingetroffen. Allerdings waren für das Projekt aus verschiedenen Gründen lediglich 716 Fragebögen verwertbar.

Die weiteren Ausführungen im Projektbericht sind im Wesentlichen darauf gerichtet, die Ergebnisse der Befragung vorwiegend deskriptiv darzustellen. Wo angezeigt und möglich, werden auch Zusammenhänge und beobachtete Tendenzen erläutert. Der vollständige Projektbericht ist auf meiner Website unter http://www.datenschutz-mv.de/navi/dschutz/grunddaten.html veröffentlicht.

4.3 Internationale Datenübermittlungen, EU-Angelegenheiten, Änderungen im Datenschutzrecht der Bundesrepublik Deutschland

4.3.1 Unabhängigkeit der Datenschutzaufsicht - Klageverfahren der Europäischen Kommission

Die Einhaltung datenschutzrechtlicher Vorschriften in den EU-Mitgliedsstaaten muss nach der Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EG-Datenschutzrichtlinie) von Stellen überwacht werden, die ihre Aufsichtsaufgaben in völliger Unabhängigkeit wahrnehmen. In einer Vielzahl der deutschen Bundesländer ist demgegenüber die Datenschutzaufsicht über die Privatwirtschaft (sog. nicht-öffentliche Stellen) in den Geschäftsbereichen der jeweiligen Innenministerien angesiedelt und damit in den hierarchischen ministeriellen Weisungsstrang eingebunden.

Diese Aufsichtsstruktur bei der Datenschutzkontrolle verstößt nach Feststellung der Europäischen Kommission gegen europäisches Recht und ist seit längerer Zeit Gegenstand eines Vertragsverletzungsverfahrens gegen die Bundesrepublik Deutschland.

Mangels Änderungen bei den genannten Aufsichtsstrukturen hatte die EU-Kommission am 18. Juli 2007 beschlossen, gegen die Bundesrepublik Deutschland Klage wegen fehlerhafter Umsetzung der EU-Datenschutzrichtlinie zu erheben. Sie ist der Auffassung, den Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich fehle die in der EU-Datenschutzrichtlinie vorgeschriebene völlige Unabhängigkeit. Die Bundesregierung hat dieser Auffassung in Abstimmung mit den für den Datenschutz zuständigen Ministerien der Länder widersprochen. Ein Gespräch mit der EU-Kommission über eine Kompromisslösung war ergebnislos geblieben. Die EU-Kommission hat daraufhin im November 2007 Klage gegen die Bundesrepublik Deutschland erhoben.

Die Funktion der Aufsichtsbehörde gemäß § 33 a Landesdatenschutzgesetz (DSG M-V) ist in Mecklenburg-Vorpommern dem Landesbeauftragten für den Datenschutz übertragen worden, der in Ausübung dieser Tätigkeit der Rechtsaufsicht der Landesregierung unterliegt.

In dem von der Europäischen Kommission eingeleiteten Vertragsverletzungsverfahren vertritt die Kommission auch zu dieser Regelung die Auffassung, dass die Unterstellung unter die Rechtsaufsicht der Landesregierung, ebenso wie die verschiedenen Formen von Fach-, Rechts- und Dienstaufsicht in den anderen Bundesländern, nicht mit Gemeinschaftsrecht vereinbar ist, da diese Organisationsformen nicht den Anforderungen der verlangten „völligen Unabhängigkeit“ im Sinne des Artikels 28 Abs. 1 Satz 2 der Europäischen Datenschutzrichtlinie entspricht.

Demgegenüber können die Datenschutzbeauftragten des Bundes und der Länder eine einheitliche Datenschutzkontrolle des öffentlichen und privaten Bereichs in völliger Unabhängigkeit sicherstellen. Dies habe ich bereits im Jahre 2005 gemeinsam mit meinen Kollegen in der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstrichen. Die Datenschutzaufsichtsbehörde sollte demgemäß sowohl beim Bund als auch in den Bundesländern als eigenständige oberste Bundes- beziehungsweise oberste Landesbehörde eingerichtet werden, die keinerlei Weisungen anderer administrativer Organe unterliegt.

4.3.2 Übermittlung von Bankverbindungsdaten an US-Sicherheitsbehörden

Im Sommer 2006 wurde bekannt, dass sich US-Behörden nach den Anschlägen vom 11. September 2001 ohne Information der Öffentlichkeit und unter Verstoß gegen europäische Datenschutzregelungen Zugang zu Daten des Zentralen Bankenkommunikationsnetzes SWIFT verschafft hatten.

Die „Society for Worldwide Interbank Financial Telekommunications“ (SWIFT) betreibt in Brüssel ein Telekommunikationsnetz für den standardisierten Zahlungsverkehr zwischen rund 7.800 Banken, Börsen und sonstigen Finanzinstituten in Europa und mehr als 200 Staaten weltweit. In der Bundesrepublik Deutschland werden, wie in ganz Europa, grenzüberschreitende Überweisungsgeschäfte ausschließlich über SWIFT abgewickelt.

Die Daten umfassen täglich bis zu zwölf Millionen Finanztransaktionen mit einem Gesamtumfang von mehreren Billionen Euro. Sämtliche Datenüberweisungen, die weltweit über die jeweiligen Kreditinstitute von SWIFT vorgenommen werden, führen zurzeit zu einer Datenspeicherung sowohl in Europa als auch in den USA.

SWIFT hatte Ende Juni 2006 Informationen bestätigt, man habe auf Anfragen des US-Finanzministeriums reagiert und sich den nach amerikanischem Gesetz bestehenden Pflichten zur Kooperation unterworfen. Infolgedessen wurden ab dem Jahr 2001 systematisch Finanzdaten von Privaten und Unternehmen über das SWIFT-Datenzentrum in Belgien an amerikanische (Sicherheits-)Behörden übermittelt. Bis 2003 wurde offenbar der gesamte Datenbestand an US-Behörden übermittelt - danach regelmäßig Teilmengen in unbekannter Größenordnung. Die Datenweiterleitung erfolgte bis Mitte 2006 offenbar ohne Wissen der meisten betroffenen einzelnen Banken.

Das EU-Parlament hat am 6. Juli 2006 eine Resolution verabschiedet, in der die Überwachung von SWIFT verurteilt worden ist. Die zur Verfügung gestellten Daten hätten es ermöglicht, „Informationen über die ökonomischen Aktivitäten von Individuen und Ländern zu erhalten“. Dies könne „umfangreichen Formen der Wirtschafts- und Industriespionage“ Vorschub leisten. In dem Beschluss wurden die EU-Kommission, der EU-Rat und die Europäische Zentralbank (EZB) zugleich aufgefordert, ihr Wissen und ihre Rolle in dem Fall aufzuklären. Der Präsident der Europäischen Zentralbank und die Leitung der Deutschen Bundesbank hatten inzwischen eingeräumt, bereits im Jahr 2002 von US-Seite auf vertraulicher Basis informiert worden zu sein.

Die zuständige belgische Datenschutzkommission hat in ihrem Bericht vom September 2006 festgestellt, dass das SWIFT-Verfahren gegen grundlegende EU-Datenschutzprinzipien verstößt. In Deutschland haben die Datenschutzaufsichtsbehörden der Länder über die Arbeitsgruppe Kreditwirtschaft des Düsseldorfer Kreises Gespräche und Verhandlungen mit Vertretern von SWIFT und dem Zentralen Kreditausschuss (ZKA) geführt, um die Vertragsgestaltung zwischen SWIFT und deutschen Kreditinstituten zu klären und für die Zukunft auf eine möglichst datenschutzgerechte Verfahrensweise hinzuwirken.

Ferner haben die Datenschutzaufsichtsbehörden des Bundes und der Länder am 8./9. November 2006 im Düsseldorfer Kreis in einem gemeinsamen Beschluss (siehe Anlage 2.2) festgestellt, dass die Spiegelung von Datensätzen im SWIFT-Rechenzentrum in den USA und die Herausgabe von dort gespeicherten Daten an US-amerikanische Behörden wegen fehlender Rechtsgrundlage sowohl nach deutschem als auch nach EG-Datenschutzrecht unzulässig ist. Gleichzeitig wurde die Verpflichtung der Banken unterstrichen, nach § 4 Abs. 3 BDSG ihre Kunden über die Weiterleitung von Daten an SWIFT/USA im Falle grenzüberschreitender Zahlungsaufträge zu informieren.

Es ist insgesamt davon auszugehen, dass der Datenaustausch von Finanzinstituten aller Bundesländer bei internationalen Finanztransaktionen (zumindest mittelbar) über die SWIFT Datenverarbeitungszentrale abgewickelt wird und daher betroffen ist. Damit besteht derzeit bei jeder Auslandsüberweisung die Gefahr der Verletzung der Vertraulichkeitspflicht des Finanzinstituts gegenüber dem einzelnen Kunden (Bankgeheimnis). Bereits bei der aus Datensicherheitsgründen erfolgenden „Spiegelung“ der Daten sind die durch die EU-Datenschutzrichtlinie definierten Garantien für einen Datentransfer in einen Drittstaat in wesentlichen Punkten nicht gewährleistet, weil die Datenübermittlung über den Server SWIFT/USA erfolgt und dort derzeit keine ausreichenden Regelungen zur Gewährleistung eines angemessenen Datenschutzniveaus bestehen.

Inzwischen hat SWIFT angekündigt, man wolle das System der Speicherung beziehungsweise Spiegelung der Überweisungsdaten umstrukturieren. Nach Abschluss der entsprechenden technischen Umsetzung im Jahr 2009 sollen dann künftig keine Daten zu innereuropäischen Transaktionen mehr in die USA gespiegelt werden. Bis zum Abschluss der Umstrukturierung hat sich SWIFT ferner den Regelungen des Safe-Harbour-Abkommens unterworfen.

Dies ist aus datenschutzrechtlicher Sicht allerdings sehr kritisch zu beurteilen, weil - unabhängig von der Frage der Anwendbarkeit des Abkommens auf Bank- und Telekommunikationsdaten - die Zertifizierung durch die US Federal Trade Commission den Zugriff von US-(Sicherheits-)Behörden auf die SWIFT-Daten nicht verhindert.

Darüber hinaus ist absehbar, dass die beabsichtigte Änderung der Serverstruktur allenfalls zu einem verbesserten Schutz von Bankdaten innerhalb des europäischen Wirtschaftsraumes und der Schweiz führen kann - nicht jedoch Banktransaktionsdaten schützt, die aus diesen Staaten heraus in die USA übermittelt werden.

Die insofern zwischen der EU-Kommission und den US-Behörden erzielte Einigung über den datenschutzrechtlichen Umgang mit den SWIFT-Daten ist deshalb meines Erachtens mit den bestehenden datenschutzrechtlichen Regelungen in Europa und Deutschland nicht vereinbar.

4.3.3 Änderung des Bundesdatenschutzgesetzes

Im Herbst 2006 wurde das Bundesdatenschutzgesetz (BDSG) durch das Erste Gesetz zum Abbau bürokratischer Hemmnisse insbesondere in der mittelständischen Wirtschaft vom 22. August 2006 (BGBl. I S. 1970) in mehreren Punkten geändert. Die Neuregelungen betreffen insbesondere eine Lockerung bei der Pflicht zur Bestellung betrieblicher Datenschutzbeauftragter durch Unternehmen und deren Meldepflicht gemäß §§ 4 d und 4 f BDSG. Während die gesetzliche Verpflichtung bisher bereits ab fünf Arbeitnehmern bestand, müssen Unternehmen nach der Neuregelung nun erst dann einen betrieblichen Datenschutzbeauftragten bestellen, wenn sie mehr als neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Gleiches gilt für die Meldepflicht.

Diese Neuregelung ist unter mehreren Gesichtspunkten kritisch zu bewerten. Bei der Mehrzahl der Betriebe und Unternehmen in Mecklenburg-Vorpommern handelt es sich um kleine Betriebsgrößen mit weniger als zehn Mitarbeitern. Sie unterliegen nach der Neuregelung des BDSG nun nicht mehr der Verpflichtung, einen betrieblichen Datenschutzbeauftragten zu bestellen. Die Lockerung dieser Pflicht befreit das jeweilige Unternehmen jedoch nicht von den inhaltlichen Anforderungen an den Datenschutz und den im BDSG und anderen datenschutzrechtlichen Normen festgelegten Verpflichtungen. Diese sind durch den Leiter der nicht-öffentlichen Stelle, also durch die Geschäftsleitung, unverändert sicherzustellen, was der Gesetzgeber in der ebenfalls neugefassten Regelung des § 4 g Absatz 2a BDSG ausdrücklich betont hat. Die durch die Bezeichnung des Gesetzes („Mittelstandsentlastungsgesetz“) suggerierte Entlastung der Geschäftsleitung tritt somit nicht ein. Vielmehr kann es unter Umständen zu einer faktischen Zusatzbelastung der Geschäftsleitung kommen, wenn sie nicht die (nach wie vor bestehende und auch empfehlenswerte) Möglichkeit nutzt, die Durchführung der Datenschutzaufgaben im eigenen Unternehmen auf einen spezialisierten betrieblichen Datenschutzbeauftragten zu delegieren. Parallel dazu kommt mit der Lockerung der Pflicht zur Bestellung von betrieblichen Datenschutzbeauftragten ein erhöhter datenschutzrechtlicher Beratungsaufwand für Unternehmen und Betriebe auf die Aufsichtsbehörden im nicht-öffentlichen Bereich zu.

Eine demgegenüber begrüßenswerte Neuregelung betrifft die Aufnahme eines Zeugnisverweigerungsrechtes für externe Datenschutzbeauftragte von Berufsgeheimnisträgern (z. B. Rechtsanwälten, Ärzten etc.). Durch die parallele Neuregelung in § 203 Abs. 2a Strafgesetzbuch (StGB) zählen diese im Gegenzug nunmehr zu den Berufsgruppen, die sich gegebenenfalls gemäß § 203 Abs. 1 StGB (Verletzung von Privatgeheimnissen) strafbar machen können.

4.4 Datenschutzrecht beim Einsatz neuer Technologien

4.4.1 Strichcode ade - RFID-Chips und Verbraucherrechte

Der Einsatz von RFID-Chips im Verbraucherbereich hat bereits begonnen. Mittel- und langfristig sollen die derzeit mit Strichcode versehenen Waren des täglichen Lebens flächendeckend durch RFID-Chips ersetzt werden. Mit RFID-Chips können Daten mit Hilfe von Funkwellen auf einem Chip berührungslos und ohne Sichtkontakt gelesen, gespeichert und gegebenenfalls verarbeitet werden (siehe auch Punkt 2.15.4). Auf diese Weise gekennzeichnete Gegenstände können mit einem Lesegerät innerhalb einer gewissen Reichweite identifiziert und lokalisiert werden. Der Einsatz dieser Technik kann im Handel und im Dienstleistungssektor gerade bei Logistik und Produktion zu erheblichen Kosteneinsparungen führen - er birgt jedoch auch erhebliche Risiken für das Persönlichkeitsrecht von Verbrauchern. Im Gegensatz zum bisher verwendeten Strichcode sind RFID-Chips ohne ausdrückliche Kennzeichnung wegen ihrer geringen Größe für den Verbraucher kaum oder nicht mehr erkennbar. Sie sind teilweise nur briefmarkengroß (oder kleiner) und können unter anderem auf der Rückseite von Waren-Etiketten aufgedruckt werden oder sich - nicht tastbar - in einem gekauften Kleidungsstück befinden. Der Kunde kann das Auslesen des Chips an der Kasse nicht mehr erkennen, weil eine Abtastung durch das Gerät der Kassiererin wie beim Strichcode künftig entfällt. Der Chip wird kontaktlos über ein Lesegerät ausgelesen, das sich - ohne Hinweis kaum erkennbar - beispielsweise im Bereich der Warteschlange vor der Kasse befindet. Sofern es sich um personenbeziehbare Daten handelt, wird die Wahrnehmung der im Bundesdatenschutzgesetz (BDSG) garantierten Auskunfts-, Berichtigungs- und Löschungsrechte (§§ 34 und 35 BDSG) auf diese Weise für Verbraucher künftig erheblich erschwert, wenn nicht gar verhindert. Die Wirtschaft versichert dagegen, dass auf den eingesetzten RFID-Chips lediglich produktbezogene Daten gespeichert werden.

Ein Kunde könnte allerdings keine Auskunft über Art und Inhalt von Daten einholen, wenn er nicht weiß, dass sie sich auf einem Chip in dem Kleidungsstück befinden, das er gerade gekauft hat. Er kann den Chip - ohne Hinweis und Kennzeichnung - nicht am gekauften Produkt erkennen und deshalb auch nicht entfernen. Er kann nicht überprüfen, ob der Chip noch aktiv ist und beim Betreten von Kaufhäusern oder anderen Gebäuden mit entsprechenden Lesegeräten ausgelesen wird, und er kann dieses Auslesen nur dann erkennen, wenn das Lesegerät gekennzeichnet ist.

Eine generelle rechtliche Regelung zur Kennzeichnungspflicht von RFID-Chips und Lesegeräten existiert bisher nicht. Handel und Dienstleistungssektor sowie deren Verbände haben seit ungefähr zwei Jahren zugesichert, verbindliche und nachprüfbare Selbstverpflichtungen für eine datenschutzfreundliche Ausgestaltung dieser Technologie abzugeben. Ein greifbares Ergebnis liegt bisher nicht vor. Dagegen forciert die Wirtschaft den Einsatz von RFID-Chips stark. Die Technik gilt als Zukunftstechnologie.

Angesichts des Gefährdungspotenzials der RFID-Technologie und des künftigen flächendeckenden Einsatzes bei Waren und Gegenständen des täglichen Lebens erscheint allerdings fraglich, ob die bestehenden gesetzlichen Regelungen ausreichen, den weiteren wirksamen Schutz der Persönlichkeitsrechte zu gewährleisten.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben in einem Beschluss am 8. und 9. November 2006 (siehe Anlage 2.1) die Erforderlichkeit betont, dass die RFID-Technologie datenschutzkonform entwickelt und eingesetzt wird und sowohl Hersteller als auch Anwender im Handel und im Dienstleistungssektor die Möglichkeiten der datenschutzgerechten Gestaltung dieser Technologie nutzen sollen. Ungeachtet der Vorteile dieser Technik sei zu befürchten, dass künftig massenhaft personenbezogene Daten verarbeitet werden, indem nahezu alle Gegenstände des täglichen Lebens (einschließlich Kleidung, Lebensmittel, Verpackungen, Medikamente usw.) über Hintergrundsysteme dauerhaft den Betroffenen zugeordnet werden können. Dies kann nach Auffassung der Datenschutzaufsichtsbehörden technisch zu einer unbemerkten Ausforschung der Lebensgewohnheiten und des Konsumverhaltens von Verbrauchern führen.

Auch Informationen, die zunächst lediglich ein Produkt kennzeichnen und keinen Personenbezug haben, können langfristig (je nach Lebensdauer des Chips) unter Umständen später einer konkreten Person zugeordnet werden. Damit würden aber rückwirkend alle gespeicherten Daten über einen Gegenstand, der mit einem RFID-Chip gekennzeichnet ist, zu personenbezogenen Daten werden. Nach dem Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich ist es deshalb unabdingbar, dass

- Verbraucher wegen des möglichen Personenbezugs der auf RFID-Chips gespeicherten Daten umfassend über den Einsatz-, Verarbeitungs- und Verwendungszweck und Inhalt von RFID-Chips informiert werden,
- die Betroffenen zu benachrichtigen sind, wenn durch den Einsatz von RFID-Chips personenbezogene Daten gespeichert werden,
- nicht nur die eingesetzten RFID-Chips, sondern auch die Kommunikationsvorgänge die durch sie und Lesegeräte beziehungsweise Hintergrundsysteme ausgelöst werden für Verbraucher transparent und leicht zu erkennen sein müssen (keine heimliche Anwendung),
- Verbraucher nach dem Kauf von Produkten mit RFID-Chips die Möglichkeit haben, die RFID-Chips dauerhaft zu deaktivieren oder die darauf enthaltenen Daten zu löschen,
- das Recht der Verbraucher auf Deaktivierung und Löschung der Daten auf RFID-Chips von gekauften Produkten nicht durch Gewährleistungsbeschränkungen in Allgemeinen Geschäftsbedingungen beeinträchtigt wird.

Falls sich die Festschreibung der genannten Verbraucherrechte weiter verzögert und die Verbreitung von RFID-Chips im Alltag einen gewissen Schwellenpunkt überschreitet, sehe ich die Gefahr einer technischen Eigendynamik, die durch gesetzliche Regelungen nur noch schwer einzufangen sein wird und geeignet ist, die informationellen Selbstbestimmungsrechte aller Bürger faktisch zu reduzieren.

Zum gegenwärtigen Zeitpunkt halte ich die Verwendung von RFID-Chips im Verbraucherbereich für rechtlich unzulässig, wenn die gespeicherten Daten personenbeziehbar sind und keine Einwilligung vorliegt, und werde gegebenenfalls aufsichtsbehördlich gegen die Verwendung in Mecklenburg-Vorpommern einschreiten.

4.4.2 Datenspeicherung in Kraftfahrzeugen

Aus modernen Kraftfahrzeugen sind Mikrocomputer kaum mehr wegzudenken. Sie steuern Motor, Anti-Blockier-System (ABS), Beleuchtung, Scheibenwischer, Klimatechnik und vieles mehr. Um Herstellern und Werkstätten die Fehlersuche in diesem komplexen System zu erleichtern, werden in vielen Bauteilen Daten über Fehler und besondere Betriebssituationen gespeichert. Einige dieser Daten lassen auch Schlüsse auf das Verhalten des Fahrers zu. So wird in der Bremssteuerung mitunter gespeichert, wie häufig gebremst wurde und wie oft dabei das ABS angesprochen hat. Dass solche Daten gespeichert werden, erfährt der Besitzer eines modernen Autos oft erst, wenn ein Unfall rekonstruiert werden soll oder wenn seine Werkstatt oder der Hersteller einem Defekt auf den Grund gehen muss.

Noch aussagekräftiger sind die Daten, die in Unfalldatenspeichern aufgezeichnet werden. Diese messen beispielsweise Beschleunigungswerte, Geschwindigkeiten, Schaltzustände der Beleuchtung und des Horns und zeichnen diese Werte auf, wenn sie einen Unfall feststellen. Solche Geräte werden häufig in beruflich genutzte Fahrzeuge eingebaut, so in Busse und Polizeiwagen. Es gibt jedoch Bestrebungen, diese „Black Boxes“ auch in Privatautos zur Pflicht zu machen. Die Europäische Kommision hat Untersuchungen auf diesem Gebiet unterstützt, an denen sich Versicherer, Straßenverkehrs- und Polizeibehörden, Gutachterorganisationen, Kraftfahrzeughersteller und Zulieferer sowie Forscher beteiligt haben. Eine Pflicht zum Einbau von Unfalldatenspeichern bedarf einer klaren gesetzlichen oder vertraglichen Grundlage.

Einige Versicherungen setzen bereits auf ähnliche Geräte. Sie bieten Tarife an, die sich an den gefahrenen Kilometern, den benutzten Straßen, der Uhrzeit, der Einhaltung von Geschwindigkeitsbegrenzungen und anderen Faktoren des Fahrverhaltens orientieren. Zu diesem Zweck muss der Kunde ein elektronisches Logbuch in seinem Auto installieren lassen, welches unter anderem mit dem Satellitennavigationssystem GPS den Standort bestimmt und anhand von speziellem Kartenmaterial die jeweils zulässige Geschwindigkeit ermittelt. Verletzt der Kunde die Versicherungsbedingungen, so meldet sich das Logbuch über Mobilfunk beim Versicherungsunternehmen.

Eine Arbeitsgruppe aus Mitgliedern der Aufsichtsbehörden des Bundes und der Länder für den nicht-öffentlichen Bereich (Düsseldorfer Kreis) und des Arbeitskreises Technische und organisatorische Datenschutzfragen der Datenschutzbeaufragten des Bundes und der Länder hat sich im Berichtszeitraum mit der Frage befasst, wann insbesondere Fehler- und Unfalldatenspeicher unzulässig in die Rechte der Fahrer und Besitzer von Kraftwagen eingreifen. Dabei entstand ein internes Papier, welches den Aufsichtsbehörden hilft, technische, organisatorische und einzelne rechtliche Aspekte der Datenspeicherung in Kraftfahrzeugen zu beurteilen. Die Arbeitsgruppe konnte jedoch noch keine gemeinsame Position zur Frage finden, wer für die Verarbeitung der Daten verantwortlich ist und in welchen Fällen die gespeicherten Daten personenbezogen sind. Der Düsseldorfer Kreis hat eine Ad-hoc-Arbeitsgruppe mit der Klärung dieser Fragen beauftragt.

4.5 Auskunfteien/Werbung per Post und E-Mail, Arbeitsweise von Auskunfteien und Datenschutzrechte betroffener Bürger

4.5.1 Neues Anfragemerkmal bei der SCHUFA - „Konditionenanfrage“

Vor Aufnahme eines Kredits ist es allgemein üblich, bei verschiedenen Kreditinstituten die Kredit- und Rückzahlungskonditionen einzuholen, um das individuell günstigste Angebot wählen zu können. In der Vergangenheit hatte dies in der Regel dazu geführt, dass sich der SCHUFA-Scorewert des Kunden mit jedem eingeholten Angebot verschlechterte, weil es keine Unterscheidung zwischen dem SCHUFA-Anfragemerkmal für einen tatsächlich beantragten Kredit einerseits und einer unverbindlichen Anfrage andererseits gab. In beiden Fällen wurde das Anfragemerkmal „Kreditanfrage“ benutzt. Die unverbindlichen Angebotserkundigungen von Verbrauchern waren daher innerhalb des SCHUFA-Scores quasi als nicht zustande gekommene beziehungsweise abgelehnte Kreditanträge gewertet worden.

Im September 2006 hat daraufhin die SCHUFA ein neues Merkmal „Konditionenanfrage“ eingeführt. Dieses Merkmal soll - im Gegensatz zum Merkmal „Kreditanfrage/Kreditantrag“ - nicht in den Scorewert einfließen. Dadurch wird vermieden, dass der allgemein übliche Vergleich von Kreditkonditionen vor Abschluss eines konkreten Kreditvertrags weiterhin zu negativen Scorewerten und damit auch zu schlechteren Kreditkonditionen führt.

Ein Bericht der Zeitschrift „Finanztest“ (Stiftung Warentest) vom Januar 2007 hat allerdings gezeigt, dass bei Anfragen von Testpersonen zu Kreditkonditionen im Zeitraum Oktober bis Dezember 2006 keines der getesteten Kreditinstitute bei entsprechenden Bonitätsanfragen das neue Merkmal an die SCHUFA gemeldet hatte. Nach Mitteilung des Zentralen Kreditausschusses der Banken waren diese Umsetzungsdefizite darauf zurückzuführen, dass der Test unmittelbar im Anschluss an die Einführung des neuen Merkmals stattgefunden habe.

Die korrekte Verwendung und Unterscheidung der beiden Anfragemerkmale durch die Banken ist auch datenschutzrechtlich von Bedeutung, weil das Merkmal „Kreditanfrage/Kreditantrag“ (nach konkreter Entscheidung für tatsächliche Aufnahme eines Kredits durch den Kunden) erst nach dessen unterschriebener oder einer sonstigen wirksam erteilten Einwilligung gemäß § 4 a Bundesdatenschutzgesetz (BDSG) an die SCHUFA übermittelt werden darf, worauf die Aufsichtbehörden für den nicht-öffentlichen Bereich die SCHUFA und den Zentralen Kreditausschuss hingewiesen haben.

In allen anderen Fällen, in denen die Kreditsuchenden zunächst keinen verbindlichen Kreditantrag stellen wollen, ist demgegenüber das Merkmal „Konditionenanfrage“ zu verwenden, das nicht in die Score-Berechnung einfließt und deshalb lediglich einer (auch mündlich zu erklärenden) Einwilligung des betroffenen Verbrauchers hinsichtlich der Befreiung vom Bankgeheimnis bedarf.

4.5.2 Unaufgeforderte Werbung

Auch in diesem Berichtszeitraum erhielt ich eine große Zahl von Anfragen zur Zulässigkeit von unaufgeforderter Werbung und zu den Schutzmöglichkeiten für betroffene Verbraucher.

Viele Firmen erhalten ihre Werbeadressen über Kundenbindungsprogramme und Rabattsysteme („Bonuspunkte“) oder über die Adressbestände anderer Unternehmen. Andere Unternehmen führen Preisausschreiben durch, um Anschriften für Werbezwecke zu erhalten. Hierbei warne ich insbesondere vor sogenannten „Gewinnmitteilungen“, die oft auch telefonisch erfolgen. Häufig ist eine Gewinnausschüttung von vornherein nicht vorgesehen, was kaum zu erkennen ist, weil nur in versteckter Form auf die Unverbindlichkeit der Gewinnmitteilung hingewiesen wird. Teilweise ist der „Gewinn“ auch an bestimmte Bedingungen geknüpft, die den Vorteil des Gewinns aufheben. Vielfach werden andere Firmen beauftragt, für das eigene Unternehmen zu werben, sodass bei dem werbenden Unternehmen selbst weder die Adresse des Betroffenen noch sonstige Informationen über ihn gespeichert sind.

Namen und Anschriften erhalten die Adresshandelsunternehmen oft aus allgemein zugänglichen Quellen (Adress- und Telefonbüchern, E-Mail-Verzeichnissen, Handels- und Vereinsregistern, Internetseiten etc.). Teilweise werden diese Informationen für den Werbeauftraggeber auf spezielle Zielgruppen zugeschnitten (z. B. nach Altersgruppen - Senioren etc.). Nach dem Bundesdatenschutzgesetz (BDSG) ist die Weitergabe und Nutzung der Adressen auch ohne die Einwilligung des Betroffenen nicht grundsätzlich unzulässig, weil bestimmte Kategorien personenbezogener Daten - insbesondere Name, Anschrift, Berufsbezeichnung und Geburtsjahr - nach § 28 Abs. 3 BDSG für Werbezwecke übermittelt werden dürfen, solange nicht Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung oder Nutzung hat.

Widerspricht der Betroffene dagegen der Nutzung seiner personenbezogenen Daten für diese Zwecke, so ist deren Übermittlung oder Nutzung für Werbezwecke gemäß § 28 Absatz 4 BDSG unzulässig. Ein solcher Widerspruch kann oft schon beim Abschluss von Verträgen eingelegt werden, indem etwa die in Kaufverträgen etc. fast überall verwendete Werbeklausel im „Kleingedruckten“ gestrichen oder durch einen Hinweis darauf ergänzt wird, dass keine Übermittlung oder Nutzung zu Werbezwecken erwünscht ist. Der Vertragspartner ist dann verpflichtet, dies als Widerspruch zu akzeptieren. Wenn ein Unternehmen die vom Verbraucher erhaltenen Daten auch für Werbezwecke nutzen möchte, muss es diesen bereits bei der Erhebung der Daten über diese Zwecke und über die möglichen Arten von Empfängern der Daten unterrichten (§ 4 Abs. 3 BDSG). Dies gilt auch bei Verlosungen und Preisausschreiben, mit denen Daten gewonnen werden, die später zu Werbezwecken genutzt werden sollen.

Der Betroffene muss ferner mit dem Werbeschreiben über die sogenannte verantwortliche Stelle (hier: das werbende Unternehmen) und über sein Widerspruchsrecht informiert werden. Wenn ein Betrieb ein anderes Unternehmen mit der Werbung beauftragt (und die Adress- und Namensdaten nur bei dem beauftragten Unternehmen gespeichert sind), so muss der Betrieb auch sicherstellen, dass der Betroffene über die Herkunft der Daten Kenntnis erhalten kann (§ 28 Abs. 4 BDSG). Gegenüber dem werbenden Unternehmen besteht gemäß § 34 Abs. 1 BDSG grundsätzlich ein Auskunftsrecht über die zur Person des Betroffenen gespeicherten Daten, ihre Herkunft, den Zweck der Speicherung bzw. über die Kategorien von Empfängern, an die die Daten gegebenenfalls weitergegeben werden.

Nur wenn das Unternehmen ein überwiegendes Interesse an der Wahrung eines Geschäftsgeheimnisses darlegt, kann es die Auskunft zu Herkunft und Empfänger der Daten verweigern.

Einen gewissen Schutz vor unadressierter Werbung bieten entsprechende Briefkastenaufkleber („Bitte keine Werbung“). Wird der Wunsch ignoriert, liegt ein Verstoß gegen das Gesetz gegen den unlauteren Wettbewerb vor. Bei persönlich adressierter Werbung kann ein Eintrag in die „Robinson-Liste“ helfen, die vom Deutschen Direkt-Marketing-Verband (DDV) organisiert wird. Lässt sich ein Verbraucher in diese Liste aufnehmen, so werden die Unternehmen, die dem DDV angeschlossen sind, darüber benachrichtigt, dass die jeweilige Person keine Werbung wünscht. Auf diese Weise können postalische Werbesendungen zumindest reduziert werden. Der Eintrag in die Liste ist kostenfrei und gilt für fünf Jahre. Das Formular für die Aufnahme in die Robinson-Liste ist erhältlich bei: DDV, Robinson-Liste, Postfach 14 01, 71243 Ditzingen, Telefonnummer 07156/951010 oder unter www.direktmarketing-info.de.

Gegen Werbung per SMS kann der Online-Eintrag der Telefonnummer in die vom Interessenverband Deutsches Internet e. V. (I. D. I.) geführte Schutzliste (www.robinsonliste.de) hilfreich sein (er schützt jedoch nicht gegen den zunehmend verbreiteten Einsatz von Zufallsgenerator-Programmen, mit denen große Mengen von Handynummern zunächst generiert und dann mit Blick auf eine vorher kalkulierte Wahrscheinlichkeits-Trefferquote – telefonisch „abgearbeitet“ werden).

4.5.3 Falscher Kandidat im Wahl-Werbeflyer

Ein Petent übersandte mir einen Wahl-Werbeflyer eines Direktkandidaten für die Wahl zum Deutschen Bundestag. Der Flyer enthielt unter anderem ein stilisiertes Muster eines Stimmzettels für die Wahl, bei dem unter der Rubrik „Erststimme“ Name, Vorname, Anschrift und Berufsbezeichnung des Petenten im Rahmen der Darstellung eines Direktkandidaten einer Bundestagspartei verwandt wurde. Der Petent hat weder als Kandidat dieser Partei noch als Direktkandidat der Liste einer anderen Partei für die Wahl kandidiert, sondern engagiert sich - unabhängig von seiner Nichtkandidatur zu der genannten Wahl - für eine andere politische Partei. Er teilte mir mit, er habe keine Kenntnis von der Verwendung seiner personenbezogenen Daten innerhalb des Wahlflyers gehabt.

Das Erheben und die Verarbeitung von Name und Anschrift des Petenten (auch für Zwecke der Werbung) war weder nach § 28 Absatz 1 beziehungsweise Absatz 3 Nummer 3 BDSG noch nach § 29 Absatz 1 und 2 BDSG zulässig, da das schutzwürdige Interesse des Petenten an dem Ausschluss der Verarbeitung seiner Daten offensichtlich überwog. Auch wenn Name und Adresse nach § 28 Absatz 1 Nummer 3 BDSG allgemein zugänglich gewesen sein dürften, war bei einer Verwendung dieser Daten im Muster eines Stimmzettels als Kandidaturbeispiel für den Vertreter einer anderen Partei davon auszugehen, dass das schutzwürdige Interesse des als Kandidat der „Konkurrenzpartei“ bezeichneten Petenten gegenüber dem Werbeinteresse des Flyer-Erstellers offensichtlich überwog - sofern diese Abwägung nicht von vornherein dadurch obsolet wird, dass das Interesse des Flyer-Erstellers nicht als „berechtigt“ gewertet werden konnte.

Auch nach § 29 Absatz 1 und 2 und § 28 Absatz 3 Nummer 3 BDSG („Zweck der Parteienwerbung“) hätte - unabhängig vom Vorliegen der sonstigen Tatbestandsvoraussetzungen - unter den gleichen Gesichtspunkten im Rahmen der Vorbereitung des Flyers Grund zu der Annahme bestanden, dass der Betroffene unter den genannten Gesichtspunkten ein schutzwürdiges Interesse am Ausschluss der Übermittlung/Nutzung seiner Daten hat.

Gleichzeitig waren durch die Verwendung der Namens- und Adressdaten für die Darstellung eines Direktkandidaten einer anderen politischen Partei Angaben des Petenten berührt, bei denen es sich um besondere personenbezogene Daten gemäß § 3 Absatz 9 BDSG - Angaben über politische Meinungen - handelt.

Der Ersteller des Flyers hat mitgeteilt, dass er persönlich (und nicht die Partei) für den Flyer verantwortlich zeichnete. Er habe bei der Korrektur eines von der Druckerei erstellten Musters für den Flyer die Angaben zu dem Petenten übersehen. Er räumte ein, bei der Korrektur nicht gründlich genug geprüft zu haben, bedauerte den Vorfall und hat versichert, künftig die erforderliche Sorgfalt hinsichtlich der Vorgaben des Bundesdatenschutzgesetzes walten zu lassen.

4.5.4 Datennutzung innerhalb eines Unternehmens mit Post- und Detekteisparte

Im Rahmen einer Petition erhielt ich Hinweise auf ein Unternehmen, in dem unter einem gemeinsamen Firmendach sowohl ein Postzustellungsunternehmen als auch eine Detektei sowie ein Inkassobüro betrieben werde. Nach Schilderung des Petenten führe das Unternehmen in seiner Post-Sparte unter anderem den Postversand für die Arbeitsgemeinschaften zur Grundsicherung für Arbeitssuchende der Landkreise (ARGE) in Mecklenburg-Vorpommern sowie Zustellungen für ein Energieversorgungsunternehmen durch. In diesem Zusammenhang wurde die Vermutung geäußert, dass die Postzustellungssparte des Unternehmens Daten an die Detekteisparte desselben Unternehmens (evtl. auch im Zusammenhang mit Inkasso-Aufträgen) übermitteln würde.

Dabei wurde exemplarisch der Fall eines ALG-II-Empfängers erwähnt, dessen Stromanbieter die Stundung einer Rechnung mit der Begründung abgelehnt habe, der Kunde sei „Hartz-IV-Empfänger“. Da die ARGEn entsprechende personenbezogene Informationen nicht an Dritte mitteilen würden, wurde im Zusammenhang mit der Information über eine Postzustellungsbefassung des Mehrspartenunternehmens sowohl für die ARGEn als auch für das Stromversorgungsunternehmen sowie der Kombination mit der Detekteisparte des Unternehmens die Vermutung geäußert, dass Daten aus der Sparte „Postzustellung“ der Firma an die Unternehmenssparten „Detektei“ beziehungsweise „Inkasso“ desselben Unternehmens weitergegeben worden seien.

Die Geschäftsführung des Mehrspartenunternehmens hat umgehend auf mein Stellungnahmeersuchen reagiert und umfassend Auskünfte über Struktur und Datenflüsse innerhalb der Sparten des Unternehmens erteilt.

Im Ergebnis der Sachverhaltsermittlung stellte sich heraus, dass die Detekteitätigkeit der Firma lediglich in sehr geringem Umfang erfolgte und sich dabei im Wesentlichen auf die Ermittlung von ladungsfähigen Postanschriften (etwa als Voraussetzung für die Einreichung von Klagen) beziehungsweise auf die Einholung von Angaben bei den Grundbuchämtern der Amtsgerichte zur Feststellung von Vermögensverhältnissen beschränkte. Inkasso-Aufträge wurden durch das Unternehmen nicht durchgeführt.

Durch die Postsparte des Unternehmens erfolgten im Bedarfsfall jeweils einzelne Adressnachforschungen durch direkte Abfragen bei der Deutschen Post AG beziehungsweise bei einem entsprechenden Internetsuchprogramm. Diese wurden jedoch nicht an die Detekteisparte übermittelt. Zudem hat die Bundesanstalt für Arbeit Nord bestätigt, dass das Unternehmen nicht mit Postzustellungen für die ARGEn in Mecklenburg-Vorpommern befasst war.

Insgesamt ergab sich, dass keine personenbezogenen Informationen, die im Zusammenhang mit der Sparte „Briefzustellungen“ verarbeitet wurden, in unzulässiger Weise an eine andere Unternehmenssparte weitergegeben worden waren, sodass sich die ursprüngliche Sachverhaltsinformation nicht erhärtet hat, sondern widerlegt wurde.

4.6 Banken, Scoring, Videoüberwachung und Internet

4.6.1 Unbefugte Übermittlung von Kunden-Kontodaten durch eine Bank

Von einer Journalistin erhielt ich den Hinweis, dass sie im Rahmen einer Recherche den Hinweis auf die unbefugte Übermittlung von Kontodaten durch eine Bank erhalten haben. Ein Kunde habe von der Bank ein Schreiben erhalten, auf dessen Rückseite sich der Abdruck von Kontoverbindungsdaten eines anderen Bankkunden befand, mit dem keinerlei finanzielle Verbindung bestanden habe. Nach Schilderung der Journalistin hatte die Bank Kontoauszüge eines Kunden als „Schmierpapier“ für eine Faxübermittlung an einen anderen Kunden der Bank benutzt. Ich habe die Bank im Rahmen meines Stellungnahmeersuchens vorab darauf hingewiesen, dass die nicht legitimierte Mitteilung von Kontodaten eines Kunden nicht nur einen Verstoß gegen das Bundesdatenschutzgesetz (BDSG), sondern auch eine Verletzung des Bankgeheimnisses darstellen würde, das über die Allgemeinen Geschäftsbedingungen der Banken Bestandteil des Vertrages zwischen der Bank und dem Drittkunden ist.

Die Bank hat sehr zeitnah reagiert und den Sachverhalt bestätigt. Hauptursache des fraglichen „Faxversehens“ sei das Verhalten einer Mitarbeiterin einer Filiale gewesen, die zunächst ein Fax abgesandt und sodann nach Ende des Faxvorganges den Obligo-Ausdruck mit der Rückseite nach oben in den Papierschacht des Faxgerätes gelegt habe, um eine zweite hausinterne Verwendung für ankommende Faxnachrichten zu ermöglichen.

Das folgende ankommende Fax habe die Kreditantragstellung eines Drittkunden betroffen. Dieses (nunmehr doppelt bedruckte) Fax habe danach eine weitere Sachbearbeiterin der Kreditabteilung erhalten und - ohne Kontrolle der Rückseite - an den Drittkunden versandt. Nach Mitteilung der Bank war der von der Datenschutzverletzung betroffene Kunde inzwischen informiert.

Wenn personenbezogene Daten ohne Rechtsgrundlage an Dritte übermittelt werden, soll die verantwortliche Stelle den Betroffenen entsprechend § 4 Absatz 3 und § 33 BDSG unterrichten, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat.

Man habe innerbetrieblich - zusätzlich zu den bestehenden Arbeitsanweisungen und Verpflichtungserklärungen - aus gegebenem Anlass eine Anweisung an die Mitarbeiter gegeben, die die Doppelverwendung von Papier mit Kundendaten nochmals ausdrücklich verbiete und auf die besondere Sorgfaltspflicht beim Postausgang hinweist. Die schon bestehende Arbeitsanweisung „Datenschutz“ werde überarbeitet.

Die Bank hat in ihrer innerbetrieblichen Organisation und deren Umsetzung in den täglichen Arbeitsabläufen sichergestellt, dass sich derartige Vorfälle nicht wiederholen werden und mir hierzu umfangreiche Unterlagen übersandt - insbesondere eine überarbeitete Datenschutzanweisung sowie Muster der Verpflichtungen der Mitarbeiter auf das Bankgeheimnis sowie das Datengeheimnis gemäß § 5 BDSG.

4.6.2 Scoring-Verfahren in der Kreditwirtschaft und datenschutzrechtliche Grenzen

Als Grundlage für Kreditentscheidungen haben sich bei Banken und Kreditinstituten sogenannte Scoring-Verfahren durchgesetzt. Hierbei werden auf mathematisch-statistischer Grundlage Risikoklassen gebildet, denen der Kreditsuchende zugeordnet wird und auf deren Grundlage er einen bestimmten Score-Wert erhält. Die Verfahren werden insbesondere von Banken, jedoch zunehmend auch von Versicherungen, Telekommunikationsunternehmen und dem Versandhandel eingesetzt. Ein Risiko des Kredit-Scoring liegt für den Kunden darin, dass er einer bestimmten statistischen Kategorie zugeordnet wird, die seinen individuellen Lebensumständen möglicherweise nicht gerecht wird. Ein weiteres Risiko besteht dann, wenn der betroffene Kunde keinen Einblick darin erhält, welche seiner Daten verarbeitet werden und nach welchen Maßstäben aus diesen Daten innerhalb der Verfahrenskategorien sein persönlicher Bewertungswert ermittelt worden ist.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) haben deshalb im April 2007 einen Beschluss über die Anforderungen und datenschutzrechtlichen Grenzen beim Einsatz von Scoring-Verfahren im Bereich der Kreditwirtschaft gefasst.

Danach dürfen als personenbezogene Merkmale nur Parameter genutzt werden, deren Bonitätsrelevanz in einem wissenschaftlich, mathematisch-statistischen Verfahren nachgewiesen wurden. Ferner dürfen gemäß § 28 Absatz 1 Satz 1 Nummer 1 BDSG nur Daten erhoben und gespeichert werden, soweit dies zur Zweckbestimmung eines Vertragsverhältnisses erforderlich ist. Banken dürfen daher nur Daten für das Scoring-Verfahren verwenden, die das Institut im Rahmen eines Kreditvertrages erheben darf (Erforderlichkeitsprinzip). Soweit Daten für andere Zwecke (etwa aufgrund von Vorgaben des Kreditwesengesetzes - KWG) erhoben und gespeichert wurden, dürfen diese Daten nur für Zwecke des KWG, nicht jedoch für Scoring-Verfahren verwendet werden. Sensitive Daten im Sinne des § 3 Absatz 9 BDSG dürfen nicht in die Score-Berechnung einfließen. Auch darf das Kreditinstitut nicht auf Daten mit Indiz-Charakter zurückgreifen, wenn es die Möglichkeit hat, konkrete, unmittelbar bonitätsrelevante Daten zu erheben.

Insbesondere ist bei jedem einzelnen Score-Merkmal zu prüfen, ob der Betroffene überwiegende schutzwürdige Interessen am Ausschluss der Datennutzung geltend machen kann. Die reine statistische Relevanz eines Kriteriums führt noch nicht zu dessen Zulässigkeit. Bei der Abwägung sind sowohl Wertungen des einfachen Rechts als auch des Grundgesetzes daraufhin zu prüfen, ob eine eventuelle Benachteiligung der Kunden aufgrund eines bestimmten Kriteriums unzumutbar sein kann. Da der Einsatz von Scoring-Verfahren zunehmend dazu führen wird, jeden Kredit entsprechend dem individuellen Risiko zu bezinsen, ist die Datennutzung für Scoring-Verfahren nur dann zulässig, wenn in einer Gesamtschau der Kriterien sichergestellt ist, dass diesem Anliegen Rechnung getragen wurde und keine überwiegenden schutzwürdigen Interessen der Betroffenen tangiert sind.

Die Aufsichtbehörden für den Datenschutz im nicht-öffentlichen Bereich haben ferner festgestellt, dass für Betroffene und Aufsichtsbehörden insbesondere nachvollziehbar sein muss,

- welche personenbezogenen Merkmale in die Berechnung des Score-Wertes einfließen,
- welche konkreten personenbezogenen Daten der kreditsuchenden Person dafür genutzt wurden und
- welches die maßgeblichen Merkmale sind, die den konkreten Score-Wert der betroffenen Person negativ beeinflusst haben. Diese maßgeblichen Merkmale sollen nach ihrer Bedeutung beziehungsweise dem Grad ihres Einflusses auf den konkreten Score-Wert aufgelistet werden, wobei sich die Auflistung auf die vier bedeutsamsten Merkmale beschränken soll.

Darüber hinaus sind bei der Anwendung von Scoring-Verfahren die datenschutzrechtlichen Vorgaben des § 6 a BDSG hinsichtlich automatisierter Einzelentscheidungen zu beachten.

4.6.3 Videoüberwachung eines Verkehrstunnels

Die Betreibergesellschaft eines mautpflichtigen Verkehrstunnels wollte diesen videoüberwachen und bat hierzu um eine datenschutzrechtliche Bewertung. Die Videoüberwachung soll dabei der Verkehrslenkung und -beobachtung, der Kontrolle der Mautstellen und der Verfolgung strafbarer Handlungen dienen.

Aufgrund einer Vorschrift muss der Verkehrsraum eines Tunnels, sofern dieser länger als 400 m ist, lückenlos videoüberwacht werden. Da dieses zum Zwecke der Verkehrslenkung und -beobachtung durchgeführt wird, ist die Erhebung personenbezogener Daten nicht erforderlich und außerdem durch die betreffende Vorschrift nicht vorgesehen.

Ein weiterer Zweck der Videoüberwachung ist indes die Kontrolle der Mautstellen und des dazugehörigen Zahlvorganges. Das Fernstraßenbauprivatfinanzierungsgesetz (FStrPrivFinG) sieht die Erhebung personenbezogener Daten zur Kontrolle der Mautzahlungen vor. Nach § 6 Absatz 3 FStrPrivFinG dürfen beispielsweise das Kennzeichen des Fahrzeugs und der Name der Person, die die Strecke benutzt, erhoben, verarbeitet und genutzt werden. Der Einsatz der Videoüberwachungsanlage für diesen Zweck ist aus datenschutzrechtlicher Sicht somit zulässig.

Mit Hilfe der Videoüberwachung sollen auch strafbare Handlungen an der Mautstelle (wie das Zerstören/Durchbrechen von Absperreinrichtungen) verfolgt werden. Die erhobenen personenbezogenen Daten (beispielsweise das Fahrzeugkennzeichen) sollen der Beweissicherung dienen. Die Videoüberwachung dient somit sowohl der Wahrnehmung des Hausrechts als auch der Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke und ist nach § 6 b Absatz 1 Bundesdatenschutzgesetz (BDSG) zulässig.

Nach § 6 Absatz 2 BDSG sind der Umstand der Videoüberwachung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen. Hierfür sollten entsprechende Hinweisschilder errichtet werden. Die Betreibergesellschaft informierte mich darüber, dass die Schilder in solchen Abschnitten der Tunnelzufahrten vorgesehen sind, die entweder ein rechtzeitiges Verlassen oder aber ein Nichtbenutzen der Zufahrten zulassen. Auf einen Schilderhinweis auf die für die Überwachung verantwortliche Stelle musste in diesem Fall allerdings verzichtet werden, da ein entsprechender Text im Vorbeifahren ohnehin kaum lesbar wäre und hierdurch etwaige Verkehrsgefährdungen entstehen könnten. Ich habe der Betreibergesellschaft empfohlen, die erforderlichen Hinweise stattdessen beispielsweise an der Mautstelle selbst anzubringen.

4.6.4 Videoüberwachung in Sauna und Umkleidekabine

Im Rahmen einer Petition erreichte mich der Hinweis auf eine Videokamerainstallation im Saunabereich eines Sportparks. Die Geschäftsleitung hatte dort zwei Videokameras installieren lassen, von denen eine auf den Sauna-Ruheraum und die andere auf den Übergangsbereich von der Sauna zum Ruhebereich gerichtet war, wobei die Saunatür erfasst wurde. Die Kameraüberwachung war weder direkt vor Ort noch im Eingangsbereich des Sportparks durch Hinweisschilder kenntlich gemacht worden.

Ich habe mich in dieser Angelegenheit mit dem betrieblichen Datenschutzbeauftragten des Unternehmens, zu dem auch der Sportpark gehört, in Verbindung gesetzt, der in erfreulich kurzer Zeit die Angelegenheit vor Ort überprüfte und mich über das Ergebnis informiert hat.

Danach seien von der Geschäftsleitung des Sportparks als Grund für die Installation der Kameras Vorfälle in der Vergangenheit angegeben worden, bei denen einige Besucher nach Verlassen der Sauna (wohl kreislaufbedingt) das Bewusstsein verloren hätten.

Die Sportparkbetreiber haben daher Vorsorge treffen wollen, dass in derartigen Notfällen ein schnelles (gegebenenfalls medizinisches) Eingreifen insbesondere in den Fällen gewährleistet sei, in denen sich nur eine einzelne Person in der Sauna aufhalte.

Im Hinblick auf die damit verbundene Beeinträchtigung des allgemeinen Persönlichkeitsrechts habe ich grundlegende Bedenken gegen die Zulässigkeit der Kamerainstallation in diesem Bereich geäußert und darum gebeten, die Kameras durch die Geschäftsleitung des Sportparks abschalten zu lassen. Gegebenenfalls sollten vorrangig andere geeignete Vorsorgemaßnahmen geprüft werden, die nicht gegen die Persönlichkeits- und Datenschutzrechte der betroffenen Besucher des Sportparks verstoßen.

In einem anderen Fall erhielt ich durch den Hinweis eines Bürgers die Information über eine Videoüberwachungsinstallation im Damenumkleidebereich der Filiale eines großen Kaufhauskonzerns. Danach seien in den Einzelkabinen des Damenumkleidebereichs an den Spiegeln Aufkleber angebracht, auf denen sich jeweils ein Piktogramm einer Videokamera mit dem Hinweis „Videoüberwacht“ befinde. Ich habe den Datenschutzbeauftragten des Konzerns im Rahmen meines Stellungnahmeersuchens darauf hingewiesen, dass eine Videoüberwachung in Damenumkleidekabinen in Abwägung mit den schutzwürdigen Interessen der Betroffenen zur Wahrnehmung des Hausrechts im Rahmen des § 6 b BDSG nicht gerechtfertigt ist (Eingriff in das allgemeine Persönlichkeitsrecht).

Auch in diesem Falle reagierte der betriebliche Datenschutzbeauftragte in erfreulich kurzer Zeit und teilte mit, dass in den Filialen grundsätzlich keine Videoüberwachung in den Kabinen stattfinde. Seine Überprüfung der betreffenden Filiale habe ergeben, dass es sich um eine durch die Konzernzentrale nicht genehmigte Einzelmaßnahme der Filialleitung gehandelt habe, die nach einer erhöhten Diebstahlsquote versucht habe, weiteren Vorfällen durch Videowarnschilder in den Kabinen entgegenzuwirken.

Tatsächlich seien auch in dieser Filiale - trotz der angebrachten Hinweisschilder - keine Kameras installiert. Der Konzerndatenschutzbeauftragte sagte zu, die Aufkleber innerhalb weniger Tage zu entfernen. Eine Prüfung vor Ort bestätigte diese Angaben. Die entsprechenden Schilder waren entfernt und durch einen allgemeinen Warnhinweis („Dieses Geschäft ist elektronisch gegen Ladendiebstahl gesichert.“) ersetzt worden.

4.6.5 Mieterdatenbank im Internet - „Schwarze Schafe“-Liste

Im Zusammenhang mit einer Petition erreichte mich der Hinweis auf eine Internet-Homepage, auf der unter der Bezeichnung „Vermietertraum“ eine Datenbank über sogenannte Schwarze Schafe geführt wurde. Unter dieser Bezeichnung sollte Vermietern von Wohnungen oder Häusern gegen ein Entgelt die Möglichkeit gegeben werden, beliebige Personen ohne nähere Begründung im Zusammenhang mit (behaupteten) Mietverhältnissen als „Schwarze Schafe“ sowohl eintragen als auch abfragen zu können. Für entsprechende Eingaben oder Abfragen von Vermietern waren unter der Bezeichnung „Ihr schwarzes Schaf“ die Rubriken Vorname, Name sowie Geburtsdatum als Datenfelder vorgesehen.

Ich habe den Betreiber der Homepage darauf hingewiesen, dass eine Datenverarbeitung dieser Art gemäß § 29 Bundesdatenschutzgesetz (BDSG) unzulässig ist, da die Betroffenen (hier die jeweiligen Mieter) unter verschiedenen Aspekten ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung und Übermittlung an Dritte haben.

Ein solches Interesse ergab sich im vorliegenden Fall bereits daraus, dass der Betreiber der Internetseite explizit dazu aufforderte, Name, Vorname und Geburtsdaten von Mietern ohne deren Kenntnis und ohne jegliche Begründung unter der diffamierenden Bezeichnung „Schwarze Schafe“ einzugeben und dann zum Abruf gegen Entgelt bereitzustellen.

Eine Rubrik für die Glaubhaftmachung des berechtigten Interesses eines Vermieters an der entsprechenden Datenabfrage beziehungsweise die Abwägung entgegenstehender berechtigter Interessen der Betroffenen am Ausschluss der Übermittlung (§ 29 Abs. 2 BDSG) war nicht vorgesehen.
Der Betreiber der Homepage hat auf meine Intervention hin die Internetseite deaktiviert.

4.6.6 Internetaufruf einer Partei zur Übersendung von Fotos von Gegendemonstranten

Einer Pressemeldung entnahm ich, dass auf der Internet-Homepage einer im Landtag vertretenen Partei dazu aufgerufen wurde, im Zusammenhang mit einer Demonstration dieser Partei Fotos von Gegendemonstranten an den Landesverband der Partei zu übersenden. Presseberichten zufolge soll die Partei erklärt haben, sie wolle „mit eigenen Mitteln Steinewerfer der Gegenseite enttarnen".

Ich habe den Landesverband der Partei um Stellungnahme dazu gebeten, zu welchem Verwendungszweck die genannten Personenfotos dienen sollten, inwieweit solche Fotos beim Landesvorstand der Partei eingegangen sind und dort gespeichert beziehungsweise an Dritte übermittelt wurden und habe insbesondere gebeten, mir die Rechtsgrundlage gemäß § 4 Absatz 1 BDSG für die angestrebte Datensammlung der Partei mitzuteilen.

Politische Parteien und Verbände zählen - unabhängig von der Verschiedenheit ihrer Zielsetzungen - zu den nicht-öffentlichen Stellen nach § 2 Absatz 4 BDSG.
Reine Privatfotos werden - als Datenverarbeitung für ausschließlich persönliche oder familiäre Tätigkeiten im Sinne des § 1 Absatz 2 Nummer 3 BDSG - grundsätzlich nicht vom Anwendungsbereich des Bundesdatenschutzgesetzes erfasst, wenn sie nicht - wie im vorliegenden Fall - zu weitergehenden Zwecken gespeichert oder (an Dritte) übermittelt werden.

Der Landesverband der Partei antwortete, der Aufruf zur Übersendung von Personenfotos von Gegendemonstranten per Internet diene der Auffindung von Beweismitteln für konkrete gegen die Partei gerichtete Straftaten, auch im Hinblick auf zivilrechtliche Schadensersatzforderungen/Schmerzensgeldansprüche. Übersandte Personenfotos würden nicht gespeichert, sondern an die zuständigen Behörden weitergeleitet.

Auf meine Frage, ob und gegebenenfalls wie viele Personenfotos an welche örtlichen Dienststellen der zuständigen Polizeibehörden beziehungsweise Staatsanwaltschaften weitergegeben worden sind und wie viele konkrete Schadensersatzforderungen und Schmerzensgeldansprüche der Weiterleitung von Fotos an Ermittlungsbehörden zugrunde gelegen haben, informierte der Landesverband, dass keinerlei Fotos an ihn eingesandt worden seien oder sich in seinem Besitz befänden. Demzufolge seien auch keine Fotos an die Behörden weitergegeben worden.

Der Aufruf zur Übersendung von Fotos von Gegendemonstranten war von der Homepage der Partei entfernt worden.

4.6.7 Handyverträge im Müllcontainer

Durch den telefonischen Hinweis eines Bürgers wurde ich über einen offenen Abfallcontainer im Bereich eines Einkaufs-Centers informiert, in dem eine Firma Papierbündel und Aktenordner mit personenbezogenen Kundendaten zwischengelagert hatte, die offensichtlich zusammen mit Sperrmüll entsorgt werden sollten. Hintergrund war offenbar die Insolvenz der Firma.

Es handelte sich um eine große Anzahl von Leitz-Ordnern mit Hunderten von Handyverträgen, auf denen - für jedermann zugänglich - nicht nur die Namen und Handynummern der jeweiligen Kunden, sondern auch beispielsweise deren Personalausweisnummern vermerkt waren.

Dank der schnellen Reaktion der Polizei konnten durch eine koordinierte Aktion der Beamten des Polizeireviers Schwerin und der Datenschutzaufsichtsbehörde innerhalb einer Stunde alle Unterlagen sichergestellt werden.

Im Hinblick auf die Menge der Kundendaten und deren Sensibilität habe ich Strafanzeige sowie einen Strafantrag gemäß § 44 Abs. 2 BDSG gestellt.

Strafantrag des Landesbeauftragten für den Datenschutz:

Bei vorsätzlich begangenen Verstößen gegen das Bundesdatenschutzgesetz, die nach § 43 Abs. 2 BDSG mit Bußgeld geahndet werden können, handelt es sich nach § 44 Abs. 1 BDSG dann um Straftatbestände, wenn die Tat gegen Entgelt beziehungsweise in Bereicherungs- oder Schädigungsabsicht begangen wird.

Solche Straftaten sind sogenannte Antragsdelikte. Die Tat wird durch die Staatsanwaltschaft daher nach § 44 Abs. 2 BDSG nur verfolgt, wenn ein Strafantrag gestellt wird. Antragsberechtigt sind der von der Straftat Betroffene und - nach § 44 Abs. 2 BDSG - auch die Aufsichtsbehörde, hier der Landesbeauftragte für den Datenschutz.

4.6.8 Personalaktenfund in verlassener Fabrik

Nur wenige Tage nach dem Fund und der Sicherstellung von Aktenordnern mit Kundendaten und Handyverträgen (siehe auch Punkt 4.6.7) erhielt ich den Hinweis eines Bürgers auf die Lagerung von Akten mit personenbezogenen Daten in einer verlassenen Fabrik.

In dem nur unzureichend gesicherten Gebäude eines ehemaligen Großunternehmens fanden sich unter anderem Hunderte von Akten - insbesondere Personalunterlagen mit personenbezogenen Daten sowie Lichtbildern.

Auch in diesem Fall konnten - trotz der großen Menge des Aktenmaterials - alle Unterlagen innerhalb kurzer Zeit durch die Beamten der Schweriner Polizei sichergestellt und damit vor dem unbefugten Zugriff Dritter geschützt werden.

Im Hinblick auf die große Menge der personenbezogenen Daten habe ich Strafanzeige gegen Unbekannt gestellt.

Der erneute Vorfall in kurzer Zeit beweist, dass gerade bei Unternehmensübernahmen der Schutz und die Absicherung von Mitarbeiterdaten oft in gefährlicher Weise vernachlässigt wird. Umgekehrt zeigen die beiden Aktenfunde in einer so kurzen Zeitspanne allerdings auch eine erfreulich zunehmende Sensibilisierung für das Gefahrenpotenzial ungesicherter personenbezogener Unterlagen.

§ 9 BDSG

Nach § 9 BDSG sind Unternehmen, die personenbezogene Daten verarbeiten, verpflichtet, alle technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die gesetzlichen Datenschutz- und Datensicherheitsanforderungen zu gewährleisten.

Dazu zählt insbesondere auch die Verpflichtung zu gewährleisten, dass personenbezogene Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle) und gegen Verlust geschützt sind (Verfügbarkeitskontrolle).

5. Arbeitskreis „Technische und organisatorische Datenschutzfragen“

Neben der sicherheitspolitisch geprägten Datenschutzdebatte in Deutschland spielen die rasanten technischen Entwicklungen und deren Folgen für das gesamte gesellschaftliche Leben eine maßgebliche Rolle für die künftige Aufgabenerfüllung der Datenschutzinstitutionen. Die Datenschutzbeauftragten des Bundes und der Länder befassen sich vor diesem Hintergrund in zunehmendem Maße mit technischen Datenschutzaspekten. Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ (AK Technik) berät und unterstützt unter meiner Federführung die Konferenz in diesem Bereich. Auch in diesem Berichtszeitraum trafen sich die Mitglieder des Arbeitskreises wieder zu vier turnusmäßigen Sitzungen.

Die 46. Sitzung des AK Technik fand im Februar 2006 in Schwerin statt. Schwerpunktthema dieser Sitzung waren Datenschutzfragen bei der Internettelefonie (VoIP). Die DVZ M-V GmbH stellte die Planungen zur Einführung von VoIP in der Landesverwaltung Mecklenburg-Vorpommerns zur Diskussion und erläuterte insbesondere die geplanten Sicherheitsmerkmale der gesamten Lösung (siehe auch Punkt 2.15.3). Die Teilnehmer konnten sich davon überzeugen, dass dem Datenschutz beim Betrieb des gesamten Verfahrens und insbesondere beim Umgang mit VoIP-Verkehrsdaten ein hoher Stellenwert eingeräumt wird.

Zur 47. Sitzung im September 2006 hatte die Gesellschaft für Telematikanwendungen im Gesundheitswesen (Gematik) nach Berlin eingeladen. Ich hatte die Gematik gebeten, die wesentlichen technischen Datenschutzaspekte der elektronischen Gesundheitskarte vorzustellen und mit den Teilnehmern zu diskutieren. Der Meinungsaustausch brachte zum einen den AK-Mitgliedern neue Erkenntnisse, von denen sie im Rahmen ihrer Beratungstätigkeit bei der flächendeckenden Einführung der Karte profitieren werden. Die Gematik erhielt zum anderen von den Datenschützern weitere Empfehlungen zur datenschutzgerechten Ausgestaltung der geplanten Telematik-Infrastruktur.

Ein weiterer Schwerpunkt dieser Sitzung waren Datenschutzfragen der RFID-Technologie. Der Arbeitskreis bereitete eine Entschließung zum Thema für die Datenschutzkonferenz vor und verabschiedete eine Orientierungshilfe zum datenschutzgerechten Einsatz von RFID (siehe Punkt 2.15.4).

Bei der Organisation der 48. Sitzung des AK Technik wurde ich maßgeblich von meinen Kollegen aus Niedersachsen unterstützt. Wir tagten im Februar 2007 in Hannover und berieten gemeinsam mit Fachleuten aus dem Informatikzentrum Niedersachsen über Fragen des datenschutzgerechten Identitätsmanagements. Unter anderem wurde über die Speicherung von Signatur-Zertifikaten in Verzeichnisdiensten diskutiert. Dabei wurde deutlich, dass der Aufbau und die Nutzung von Verzeichnisdiensten und Public-Key-Infrastrukturen (PKI) bundesweit sehr unterschiedlich ausgestaltet ist, wodurch deren Einbindung in länderübergreifende IT-Verfahren sehr erschwert wird. Im Ergebnis verständigten sich die AK-Mitglieder darauf, zunächst einen Forderungskatalog für PKIen und Verzeichnisdienste unter besonderer Berücksichtigung datenschutzrechtlicher Aspekte zu erstellen, der dann zur Vereinheitlichung dieser Infrastrukturkomponenten beitragen soll.

Zur 49. Sitzung des Arbeitskreises im September 2007 konnte ich die Mitglieder wieder nach Schwerin einladen. Im Mittelpunkt dieser Sitzung stand das Thema Informationssicherheits- und Datenschutzmanagement. Ich hatte Mitarbeiter der DVZ M-V GmbH gebeten, das für die Landesverwaltung Mecklenburg-Vorpommerns konzipierte Managementsystem vorzustellen. Die Arbeitskreismitglieder konnten sich davon überzeugen, dass die gemeinsam von den Datenschutzbeauftragten und vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlene Grundschutzmethodik (siehe auch Punkt 2.15.5) in der Verwaltung des Landes bereits in weiten Bereichen umgesetzt wurde.

Während dieser Sitzung befasste sich der Arbeitskreis auch mit den technischen Aspekten der sogenannten Online-Durchsuchung (siehe auch Punkt 2.1.1). Die Mitglieder verabschiedeten das Arbeitspapier „Technische Aspekte der Online-Durchsuchung“ (abrufbar aus meinem Internet-Angebot unter http://www.datenschutz-mv.de/dschutz/informat/internet/onlinedurchsuchung.pdf) und bereiteten eine entsprechende Entschließung für die Konferenz der Datenschutzbeauftragten des Bundes und der Länder vor (siehe Anlage1.20).

Neben den turnusmäßigen Sitzungen des AK Technik habe ich in diesem Berichtszeitraum begonnen, jährlich einen Workshop zu einem aktuellen Datenschutzthema mit Technikbezug als interne Weiterbildungsmaßnahme für Mitarbeiterinnen und Mitarbeiter der Datenschutzaufsichtsbehörden der Länder durchzuführen. Hintergrund dieses Angebots ist die Tatsache, dass die Landesdatenschutzbeauftragten in ihrer täglichen Kontroll- und Beratungspraxis in zunehmendem Maße mit technischen Fragestellungen konfrontiert werden. Von ihnen wird eine kompetente Beratung zu den jeweils erforderlichen technischen und organisatorischen Maßnahmen erwartet. Diese hohen Erwartungen werden sie nur dann erfüllen können, wenn sie sowohl den Stand der Technik als auch mögliche rechtliche Auswirkungen moderner technischer Verfahren kennen.

Gemeinsam mit dem Hessischen Datenschutzbeauftragten habe ich im Mai 2006 zum Workshop „Digitale Signaturen“ nach Frankfurt/Main eingeladen. Hochkarätige Referenten aus der Wirtschaft, der Verwaltung und von verschiedenen Hochschulen informierten die rund 100 Teilnehmer über technische und rechtliche Aspekte elektronischer Signaturen. So stimmte Professor Alfred Beutelspacher (Universität Gießen) die Teilnehmer mit einem sehr anschaulichen Grundlagenvortrag auf das Thema ein. Professor Alexander Rossnagel (Universität Kassel) erläuterte die rechtlichen Aspekte digitaler Signaturen und Arno Fiedler (TeleTrusT) gab seine Erfahrungen zu Fragen der Interoperabilität von Signaturen weiter. Abgerundet wurde der Workshop mit verschiedenen Vorträgen aus der Praxis, etwa zum Einsatz von Signaturen im OSCI-Umfeld oder zu Erfahrungen aus dem Betrieb eines Zertifizierungsdiensteanbieters. Im Ergebnis wurde deutlich, dass diese Form der Wissensvermittlung auf einhellige Zustimmung aller Teilnehmer stieß und dass auch die Referenten durch die Diskussion mit den Teilnehmern neue Erkenntnisse mitnehmen konnten, um sich in verstärktem Maße für eine datenschutzgerechte Ausgestaltung von Signaturverfahren einzusetzen.

Der zweite Workshop fand im Juli 2007 in Hannover statt zum Thema Informationssicherheits- und Datenschutzmanagement. Die Veranstaltung sollte unter anderem beleuchten, wie der Datenschutz in bereits etablierte Normen (etwa die BSI-Grundschutzstandards, die ISO 27001 oder die British Standards 7799 und 17799) und Musterprozesse aus dem Bereich des Sicherheitsmanagements (beispielsweise ITIL oder CobiT) dauerhaft und nachhaltig verankert werden kann. Es sollte verdeutlicht werden, auf welche Weise Synergieeffekte zwischen Sicherheits- und Datenschutzmanagement nutzbar gemacht werden können. Da sich das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD S-H) seit geraumer Zeit schwerpunktmäßig mit diesem Themenkomplex befasst, konnte ich für diesen Workshop im Wesentlichen auf Referenten aus den eigenen Reihen zurückgreifen. Neben einer Mitarbeiterin aus dem BSI bestritten die Veranstaltung daher ausschließlich Kollegen aus dem ULD S-H. Der Workshop konnte allen Teilnehmern den sehr engen Zusammenhang zwischen Managementfragen aus dem Bereich der Informationssicherheit und des Datenschutzes sehr anschaulich aufzeigen und somit aktuelles Wissen für die tägliche Kontroll- und Beratungstätigkeit vermitteln.

6. Öffentlichkeitsarbeit

6.1 Fachtagung 2006 - Datenschutz durch Technik

Die jährliche Fachtagung stand im Jahr 2006 unter dem Motto „Datenschutz durch Technik - Chancen für Unternehmen und öffentliche Verwaltung“. Gemeinsam mit der Landesarbeitsgemeinschaft der Industrie- und Handelskammern (IHK) in Mecklenburg-Vorpommern hatte ich Fachleute aus Politik, Verwaltung und Wirtschaft nach Rostock eingeladen, um darüber zu diskutieren, wie der Datenschutz zu einem Standortvorteil für die einheimische Wirtschaft entwickelt werden kann.

Im Mittelpunkt der Fachtagung stand das im Landesdatenschutzgesetz festgeschriebene Datenschutz-Audit-Verfahren (§ 5 Abs. 2 DSG M-V) mit seinen Vorteilen und Risiken sowohl für die IT-Branche in Mecklenburg-Vorpommern als auch für die beschaffenden Stellen in der Verwaltung. Während der Konferenz wurde deutlich, dass die Einführung eines Datenschutz-Gütesiegels die Vergabestellen in der öffentlichen Verwaltung deutlich entlasten würde, da die Prüfung der Datenschutzgerechtheit des Produktes entfallen und das Vergabeverfahren beschleunigt und qualitativ gesteigert werden kann. Für Unternehmen kann ein Datenschutz-Gütesiegel das Vertrauen in IT-Produkte und -Verfahren aus Mecklenburg-Vorpommern und somit deren Absatzchancen - auch über die Landesgrenzen hinaus - verbessern.

In dem Hauptvortrag „Datenschutz als Wettbewerbsvorteil“ befasste sich der damalige Konzerndatenschutzbeauftragte der DaimlerChrysler AG, Professor Dr. Alfred Büllesbach, mit der Rolle von Mensch und Technik in der Informationsgesellschaft, gesetzgeberischen Regulierungsansätzen und den Konsequenzen für den Datenschutz im Unternehmen. Die Globalisierung der Märkte, die weltweite Vernetzung und der damit ermöglichte Datenaustausch gefährdeten den Datenschutz in zunehmenden Maße und erforderten daher internationale Kooperation bei der Regulierung und datenschutzgerechten Gestaltung von Technologien. Um Vertrauen und Akzeptanz bei den sensibilisierten Kunden zu erreichen, benötigten Unternehmen ein modernes Datenschutzmanagement, das auch Auditierung und Gütesiegel nutzt.

Der Präsident der IHK Rostock, Wolfgang Hering, schilderte zunächst, wie wichtig der Kundendatenschutz in der Wirtschaft ist, hinterfragte jedoch, ob angesichts des angestrebten Bürokratieabbaus und des Prüfungsaufwandes die staatliche Einführung eines regionalen Datenschutzaudit sinnvoll sei. Der Landrat des Landkreises Ludwigslust, Rolf Christiansen, widmete sich dem Thema „Modellregion Westmecklenburg - Anforderungen an E-Government-Produkte“. Erste Ergebnisse einer Umfrage zum „Bedarf für ein Datenschutz-Gütesiegel für die IT-Firmen des Landes“ präsentierte das Vorstandsmitglied der IT-Initiative M-V, Andreas Scher. Barbara Trusch von der Firma HSH Soft- und Hardware Vertriebs GmbH, berichtete über die Auditierung der Meldebehördensoftware ihrer Firma beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD S-H). Schließlich hob der Leiter des ULD S-H, Dr. Thilo Weichert, die Bedeutung von Datenschutzzertifizierungen für ein modernes Datenschutzkonzept hervor und machte erste Vorschläge für ein europäisches Datenschutz-Gütesiegel. Abgerundet wurde die Fachtagung durch eine Ausstellung datenschutzgerechter Produkte und Verfahren.

Unter Punkt 2.15.1 habe ich bereits berichtet, dass die Landesregierung noch immer der Auffassung ist, in Mecklenburg-Vorpommern bestünde kein Bedarf für ein Gütesiegel. Die für die Durchführung des Audit-Verfahrens erforderliche Verordnung hat sie bisher nicht erlassen. Ich habe deshalb bereits Ende 2005 in Anlehnung an die bereits seit mehreren Jahren in Schleswig-Holstein verwendeten Dokumente sowohl einen Verordnungsentwurf als auch einen „Anforderungskatalog für die Begutachtung von IT-Produkten im Rahmen des Datenschutzauditverfahrens“ und einen „Informations- und Pflichtenkatalog für Sachverständige und sachverständige Prüfstellen“ erarbeitet und zur Diskussion gestellt.

6.2 Fachtagung 2007 - Der informierte Patient: Datenschutz im Gesundheitsland

Die Fachtagung 2007 habe ich am 9. Juli am Alfried Krupp Wissenschaftskolleg in Greifswald durchgeführt. Sie trug den Titel „Der informierte Patient: Datenschutz im Gesundheitsland“. Im Mittelpunkt standen die aktuellen Herausforderungen an den Schutz personenbezogener Daten in vernetzten Gesundheitsdienstleistungen und bei der Entwicklung der Gesundheitswirtschaft in Mecklenburg-Vorpommern. Meiner Einladung sind rund 100 Teilnehmer aus Politik und Wirtschaft, Forschung und Verwaltung, Verbänden und Vereinen gefolgt. Durch ihre sehr interessanten Diskussionsbeiträge haben sie alle zum Erfolg der Veranstaltung beigetragen. Die Tagung wurde von einer Fachausstellung begleitet. Zwölf Aussteller haben Produkte und Lösungen zur datenschutzgerechten Verarbeitung von Patientendaten vorgestellt.

Der Tagungsort war nicht zufällig gewählt: So pflegt meine Behörde schon seit vielen Jahren enge Kontakte mit dem Institut für Community Medicine der Ernst-Moritz-Arndt-Universität Greifswald und ortsansässigen Firmen, die sich mit der Verarbeitung von Patientendaten befassen. Die Wissenschaftler und Entwickler von informationstechnischen Lösungen haben stets frühzeitig meinen datenschutzrechtlichen Rat gesucht, was auch zur Akzeptanz ihrer Projekte bei den Patienten beigetragen hat.

Die Tagung wurde mit einem Grußwort des Zweiten Vizepräsidenten des Landtages Mecklenburg-Vorpommern, Herrn Andreas Bluhm, eröffnet. Daran schloss sich das Hauptreferat „Hippokrates online: Vom Heiler zum Gesundheitsmanager“ von Herrn Professor Hansjürgen Garstka, Berlin, an. Herr Professor Wolfgang Hoffmann, Greifswald, referierte zum Thema „Gesundheitsland M-V: Datenschutz tut gut“ und ging dabei auf verschiedene Projekte aus dem Bereich Community Medicine und deren datenschutzrechtliche Regeln ein. Weiterer Schwerpunkt der Tagung war die elektronische Gesundheitskarte sowie deren Realisierung. Die Vorsitzende des Ausschusses für Gesundheit des Deutschen Bundestages, Frau Dr. Martina Bunge, sprach zum Thema „Die Gesundheitskarte - Der Patient im Mittelpunkt der Gesundheitspolitik?!“, Herr Alexander Beyer von der Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) berichtete über den Stand der Entwicklung der Gesundheitskarte und Frau Dr. Waltraut Kotschy, Leiterin der Österreichischen Datenschutzkommission, stellte die österreichische Gesundheitskarte vor. Am Nachmittag wurden mehrere, teilweise bereits realisierte Projekte zur Verarbeitung von Patientendaten vorgestellt. Die Fachtagung wurde durch eine Podiumsdiskussion abgeschlossen, die vom Rektor der Ernst-Moritz-Arndt-Universität Greifswald, Herr Professor Rainer Westermann, moderiert wurde.
Die Tagungsbeiträge sind auf meiner Website veröffentlicht unter der URL http://www.datenschutz-mv.de/dschutz/veransta/infpat/vortraege.html.

7. Anlagen

Anlage 1 Öffentlicher Bereich

Anlage 1.1 Listen der Vereinten Nationen und der Europäischen Union über Terrorverdächtige

Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16./17. März 2006 in Magdeburg

In den vergangenen Monaten sind die vom Sanktionsausschuss der Vereinten Nationen (VN) erstellten Listen über terrorverdächtige Personen und Organisationen, die von der Europäischen Gemeinschaft durch entsprechende Verordnungen umgesetzt worden sind, in den Blickpunkt der Öffentlichkeit gerückt. Personen, die auf diesen Listen erscheinen, unterliegen umfangreichen Beschränkungen, die von Wirtschafts- und Finanzsanktionen über Einreiseverbote bis hin zum Einfrieren ihrer Gelder und anderer Vermögenswerte reichen.

Ein Eintrag in den genannten Listen greift in das informationelle Selbstbestimmungsrecht der betreffenden Personen ein und kann darüber hinaus gravierende existenzielle Folgen haben, die zum Beispiel die Verweigerung von Sozialleistungen umfassen können. Vielfach sind diese Personen nicht eindeutig bezeichnet. Auch in Deutschland lebende Personen sind von entsprechenden Maßnahmen betroffen. In jüngster Zeit gab es Verwechslungen mit schwerwiegenden Folgen für völlig unverdächtige Personen. Besonders kritisch ist zu werten, dass gegen die Aufnahme in die Listen kein Rechtsschutz besteht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher die Bundesregierung auf, bei den Vereinten Nationen und in der Europäischen Union auf die Einhaltung der rechtsstaatlich gebotenen Standards zu dringen. Dazu gehören insbesondere ein transparentes Listing-Verfahren, Entscheidungen auf einer gesicherten Tatsachenbasis, ein zweifelsfreier Identitätsnachweis und effektiver Rechtsschutz.

Anlage 1.2 Keine kontrollfreien Räume bei der Leistung von ALG II

Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16./17. März 2006 in Magdeburg

Die Datenschutzbeauftragten des Bundes und der Länder haben die Bundesagentur für Arbeit (BA) und die sonstigen verantwortlichen Stellen auf Bundes- und Länderebene in ihrer Entschließung vom 27./28. Oktober 2005 aufgefordert, die Datenschutzmissstände beim Arbeitslosengeld II zu beseitigen. Zu diesen Missständen gehört die wiederholte Weigerung der BA, Landesbeauftragten für den Datenschutz zu ermöglichen, ihre Kontrollaufgaben bei den Arbeitsgemeinschaften nach dem SGB II (ARGEn) zu erfüllen. Mit einer „Weisung“ vom 31. Januar 2006 versucht die BA, nunmehr alle ARGEn auf diese Linie zu verpflichten. Den Landesdatenschutzbeauftragten soll der für Kontrollzwecke notwendige Zugriff auf die zentralen automatisierten Verfahren verwehrt werden.

Der Bundesbeauftragte für den Datenschutz und die Landesdatenschutzbeauftragten bekräftigen ihre gemeinsame Auffassung, dass es sich bei den ARGEn um eigenverantwortliche datenverarbeitende Stellen der Länder handelt, die uneingeschränkt der Kontrolle der Landesbeauftragten für den Datenschutz unterliegen. Dass die BA Ressourcen für die Arbeitsgemeinschaften bereitstellt, ändert nichts an diesem Ergebnis.

Es muss gewährleistet sein, dass die Verarbeitung von Sozialdaten in den ARGEn von den jeweils zuständigen Landesbeauftragten umfassend und ohne inhaltliche Beschränkungen datenschutzrechtlich überprüft werden kann. Eine rechtliche Konstellation, durch die die Landesbeauftragten für den Datenschutz von der Kontrolle der ARGEn ausgeschlossen würden, würde gegen die bundesstaatliche Kompetenzordnung verstoßen und wäre einer effektiven Datenschutzkontrolle abträglich. Sie würde den Grundrechtsschutz der betroffenen Bürgerinnen und Bürger empfindlich beeinträchtigen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung dazu auf, umgehend einen rechtskonformen Zustand herzustellen.

Anlage 1.3 Mehr Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen

Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16./17. März 2006 in Magdeburg

Auf europäischer Ebene wird verstärkt über die Ausweitung des grenzüberschreitenden Informationsaustauschs für Zwecke der Polizei und Justiz mit dem Ziel diskutiert, einen Raum der Freiheit, der Sicherheit und des Rechts zu schaffen. Der Austausch personenbezogener Informationen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten setzt ein hohes und gleichwertiges Datenschutzniveau bei allen beteiligten Stellen voraus.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, dass die EU-Kommission einen Rahmenbeschluss zur Harmonisierung und zum Ausbau des Datenschutzes bei den Polizei- und Justizbehörden vorgelegt hat. Sie betonen, dass die Regelungen in enger Anlehnung an die allgemeine Datenschutzrichtlinie (95/46/EG) erfolgen müssen, damit der Datenschutz in der EU auf einem einheitlich hohen Niveau gewährleistet wird.

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen die Forderungen der Europäischen Datenschutzkonferenz in ihrem Beschluss vom 24. Januar 2006. Auch sie treten dafür ein, den Datenschutz im Zusammenarbeitsbereich der sog. „Dritten Säule“ der EU im Sinne der EU-Grundrechte-Charta zu gestalten.

Dies bedeutet unter anderem, dass Eingriffe in Freiheitsrechte nur im überwiegenden öffentlichen Interesse und im Rahmen der Verhältnismäßigkeit zulässig sind. Die Rahmenrichtlinie muss die Voraussetzungen der Datenverarbeitung und -übermittlung nach den jeweiligen Rollen der Verfahrensbeteiligten (Beschuldigte, Verdächtigte, Zeuginnen und Zeugen, Opfer) normenklar und differenziert regeln. Zudem müssen die Rechte der Betroffenen auf Auskunft, Berichtigung und Löschung gewährleistet werden.

Die Datenverarbeitung muss umfassend durch unabhängige Datenschutzbehörden kontrolliert werden können. Die Datenschutzkontrollrechte müssen - unter Beachtung der richterlichen Unabhängigkeit - gewahrt werden. Sie dürfen nicht mit der Begründung eingeschränkt werden, dass ein laufendes Verfahren vorliege oder die Gefahrenabwehr bzw. die Strafverfolgung behindert werde. Einheitliche Datenschutzregelungen müssen zudem alle Formen der Datenverarbeitung - auch sofern sie in Akten erfolgt - einbeziehen.

Daten von europäischen Polizei- und Justizbehörden dürfen an Drittstaaten außerhalb der EU nur übermittelt werden, wenn ihre Verarbeitung im Zielland nach rechtsstaatlichen Grundsätzen erfolgt und ein angemessener Datenschutz sichergestellt ist. Bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen muss ferner der Grundsatz der Zweckbindung beachtet werden. Abweichungen des ersuchenden Staates vom angegebenen Verwendungszweck müssen auf Ausnahmefälle von besonderem Gewicht beschränkt bleiben. Die Ausnahmen müssen für den ersuchten Staat umfassend und zeitnah kontrollierbar sein.

Zur Schaffung eines hohen und einheitlichen Datenschutzstandards in der Dritten Säule der EU gibt es keine Alternative. Es darf nicht dazu kommen, dass auf europäischer Ebene weitere Eingriffsbefugnisse für die Sicherheitsbehörden mit immer tieferen Einschnitten in die Grundrechte beschlossen werden, ohne dass gleichzeitig die Freiheitsrechte der hier lebenden Bürgerinnen und Bürger gestärkt und geschützt werden. Aus diesem Grund hält es die Konferenz für dringend erforderlich, entsprechende Datenschutzbestimmungen zügig zu verabschieden und umzusetzen, bevor der Datenaustausch weiter ausgebaut wird.

Anlage 1.4 Keine Aushöhlung des Fernmeldegeheimnisses im Urheberrecht

Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16./17. März 2006 in Magdeburg

Das Bundesministerium der Justiz hat den Referentenentwurf eines „Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums“ vorgelegt, das in Umsetzung einer europäischen Richtlinie stärkere Instrumente zum Schutz des Urheberrechts und anderer gewerblicher Schutzrechte einführen soll.

Der Gesetzentwurf gesteht den Rechteinhabenden in bestimmten Fällen Auskunftsansprüche auch gegenüber unbeteiligten Dritten zu, die selbst keine Urheberrechtsverletzungen begangen haben. So sollen etwa Internet-Provider auch über - durch das Fernmeldegeheimnis geschützte - Daten ihrer Nutzerinnen und Nutzer zur Auskunft verpflichtet werden. Damit sollen beispielsweise Anbietende und Nutzende illegal kopierter Musik- oder Videodateien oder Software leichter ermittelt werden können.

Die Datenschutzbeauftragten des Bundes und der Länder warnen vor der hiermit eingeleiteten Entwicklung. Zwar sind die vorgesehenen Eingriffe in das Fernmeldegeheimnis in dem Entwurf an formale Hürden geknüpft; insbesondere müssen Rechteinhabende eine richterliche Anordnung erwirken. Jedoch lassen die europarechtlichen Vorgaben den Mitgliedstaaten zugunsten des Datenschutzes so viel Spielraum, dass Eingriffe in das Fernmeldegeheimnis vermieden werden können. Das Bundesverfassungsgericht hat betont, dass gemeinschaftsrechtliche Spielräume zu nutzen sind.

Nachdem das grundrechtlich geschützte Fernmeldegeheimnis in den letzten Jahren immer stärker und in immer kürzeren Abständen für Zwecke der Strafverfolgung und der Geheimdienste eingeschränkt wurde, soll es nun auch erstmals zugunsten privater wirtschaftlicher Interessen nicht unerheblich weiter eingeschränkt werden. Es ist zu befürchten, dass damit ähnliche Begehrlichkeiten weiterer privater Interessengruppen geweckt werden. Dem grundrechtlich geschützten Fernmeldegeheimnis unterliegende Daten stünden am Ende der Entwicklung für kaum noch zu übersehende Zwecke zur Verfügung.

Es ist zu befürchten, dass durch die Auskunftsansprüche gegen Internet-Provider die gerade für die Verfolgung schwerer Straftaten beschlossene Verpflichtung zur Vorratsdatenspeicherung von Verkehrsdaten für die Durchsetzung privater Interessen genutzt wird. Angesichts der Tendenz, die Internet-Anbietenden in immer stärkerem Maße für die Kommunikationsinhalte ihrer Kunden verantwortlich zu machen, ist zudem zu befürchten, dass die Firmen vorsichtshalber weitere Verkehrsdaten speichern, um im Falle von Rechtsverletzungen Auskünfte erteilen zu können.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren deshalb an die Bundesregierung und an den Gesetzgeber, auf eine weitere Einschränkung des Fernmeldegeheimnisses - erstmals zur Durchsetzung wirtschaftlicher Interessen - zu verzichten. Es wäre völlig unakzeptabel, wenn Daten, deren zwangsweise Speicherung mit der Abwehr terroristischer Gefahren begründet wurde, nun auf breiter Basis für die Verfolgung von Urheberrechtsverletzungen genutzt würden. Musik- und Filmindustrie müssen selbst dafür Sorge tragen, dass durch technische Maßnahmen und neue Geschäftsmodelle unrechtmäßigen Nutzungen die Grundlage entzogen wird.

Anlage 1.5 Sachgemäße Nutzung von Authentisierungs- und Signaturverfahren

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (bei Enthaltung Schleswig-Holsteins) vom 11. Oktober 2006

Die Datenschutzbeauftragten des Bundes und der Länder beobachten einen Trend, abweichend von den bislang geltenden Vorgaben zur Nutzung der qualifizierten elektronischen Signatur in der öffentlichen Verwaltung zunehmend ungeeignete oder weniger sichere Verfahren zuzulassen. So soll beispielsweise infolge des Gesetzentwurfes der Bundesregierung zum Jahressteuergesetz 2007 (BR-Drs. 622/06) beim Verfahren Elster Online der Finanzverwaltung das in § 87 a AO Abs. 3 geforderte Verfahren zur qualifizierten elektronischen Signatur durch ein Verfahren ersetzt werden, das lediglich zur Authentisierung der Datenübermittler geeignet ist. Auch die Planungen zum Verfahren für den elektronischen Einkommensnachweis ELENA sehen zumindest für einen Übergangszeitraum den Verzicht auf die qualifizierte elektronische Signatur vor. Einer derartigen Fehlentwicklung muss mit Nachdruck entgegengetreten werden.

Obwohl Signatur- und Authentisierungsverfahren mit der asymmetrischen Verschlüsselung vergleichbare technische Verfahren nutzen, unterscheiden sie sich im Inhalt ihrer Aussagen und müssen unterschiedliche Rechtsfolgen für die Nutzenden nach sich ziehen. Der grundlegende Unterschied dieser Verfahren muss sowohl bei der Planung als auch bei ihrem Einsatz in Verwaltungsverfahren berücksichtigt werden.

Elektronische Signaturen liefern Aussagen über elektronische Dokumente, insbesondere über deren Authentizität und Integrität. Ausschließlich die qualifizierte elektronische Signatur ist durch rechtliche Regelungen der eigenhändigen Unterschrift in weiten Bereichen gleichgestellt und dient dem Nachweis der Echtheit elektronischer Dokumente. Zudem sind nur Verfahren zur Erzeugung elektronischer Signaturen rechtlich geregelt und sicherheitstechnisch genau definiert.

Authentisierungsverfahren liefern hingegen lediglich eine Aussage über die Identität einer Person oder einer Systemkomponente. Solche Verfahren sind beispielsweise zur Authentifizierung einer Person oder eines IT-Systems gegenüber Kommunikationspartnern oder zur Anmeldung an einem IT-System geeignet. Die hierbei ausgetauschten Informationen unterliegen in der Regel nicht dem Willen und dem Einfluss der Rechnernutzenden bzw. der Kommunikationspartner und beziehen sich ausschließlich auf den technischen Identifizierungsprozess. Daher dürfen an die Authentizität und Integrität solcher Daten nicht die gleichen Rechtsfolgen geknüpft werden wie an eine qualifizierte elektronische Signatur.

Die Aufrechterhaltung der unterschiedlichen Funktionalität und Verbindlichkeit von Signatur und Authentisierung liegt sowohl im Interesse von Bürgerinnen und Bürgern als auch der Verwaltung und ist rechtlich geboten. Die unsachgemäße Anwendung oder in Kauf genommene Funktionsvermischung dieser Verfahren mindert die Transparenz, die Sicherheit und die Verlässlichkeit bei der elektronischen Datenverarbeitung. Darüber hinaus sind erhebliche Nachteile für die Nutzenden zu erwarten.

Wird ein Authentisierungsschlüssel zum Signieren verwendet,
- kann fälschlicher Weise behauptet werden, dass Nutzende elektronische Dokumente signiert haben; da sie das Gegenteil nicht beweisen können, müssen sie befürchten, die damit verbundenen Rechtsfolgen tragen zu müssen,
- besteht die Möglichkeit, dass Authentisierungsverfahren (Single Sign On, Challenge Response etc.) gezielt missbräuchlich verwendet werden,
- wird den Nutzenden keine „Warnfunktion“ mehr angeboten wie bei der ausschließlichen Verwendung des Signaturschlüssels zum Signieren und
- sind die Verfahren und die daraus resultierenden Konsequenzen für die Nutzenden nicht mehr transparent.

Vor diesem Hintergrund fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass der Gesetzgeber weder ungeeignete noch weniger sichere Verfahren zulässt. Dies bedeutet, dass
- Nutzenden die Möglichkeit eröffnet werden muss, die elektronische Kommunikation mit der Verwaltung durch eine qualifizierte elektronische Signatur abzusichern,
- immer dann Signaturverfahren eingesetzt werden müssen, wenn Aussagen über Dokumente oder Nachrichten gefordert sind und Authentisierungsverfahren nur dort verwendet werden dürfen, wo es um Aussagen über eine Person oder eine Systemkomponente geht,
- die Transparenz der Verfahren und die Nutzbarkeit der Authentisierungsfunktion erhalten bleiben müssen.

Die Datenschutzbeauftragten appellieren darüber hinaus an die Verantwortlichen in der Verwaltung und bei den Projektträgern, gemeinsam die offenen Fragen beim Einsatz der qualifizierten elektronischen Signatur zu lösen und insbesondere die Entwicklung interoperabler, ökonomischer Verfahren zur Prüfung qualifizierter elektronischer Signaturen zu unterstützen. Hierfür ist die konstruktive Zusammenarbeit der Verantwortlichen von großen Anwendungsverfahren wie Elster Online, ELENA und Elektronische Gesundheitskarte unabdingbar.

Die Bundesregierung sollte verstärkt die Einführung von Verfahren mit qualifizierter elektronischer Signatur unterstützen, weil diese Verfahren für die sichere und authentische Kommunikation zwischen Bürgerinnen und Bürgern und der Verwaltung besonders geeignet sind. Die qualifizierte elektronische Signatur muss eine zentrale Komponente in E-Government-Anwendungen sein, und darf nicht durch ungeeignete oder weniger sichere Verfahren ersetzt werden. Die Bundesregierung sollte daher die Verbreitung von Chipkarten mit qualifiziertem Zertifikat fördern. Erst der flächendeckende Einsatz von qualifizierten elektronischen Signaturen ermöglicht niedrige Kosten bei der Bereitstellung der Karten und führt darüber hinaus zu rationellen und somit kostengünstigen Verwaltungsabläufen.

Anlage 1.6 Pressemitteilung: Datenschutz ist Maßstab der Freiheitlichkeit des Gemeinwesens

Pressemitteilung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. Oktober 2006 in Naumburg

Schwerpunkte der Tagung, welche unter dem Vorsitz Sachsen-Anhalts am 26. und 27. Oktober in Naumburg an der Saale stattfand, betrafen Themen aus den Bereichen Innere Sicherheit, Schulstatistik und Technikentwicklung. Der Datenhunger von Staat und Wirtschaft, verstärkt durch die rasante technische Entwicklung, wächst ständig. Die Wächteraufgabe der unabhängigen Datenschützer ist deshalb umso wichtiger. Notwendige Unterstützung erfährt der Datenschutz als Teil der rechtsstaatlichen Ordnung häufig durch die Gerichte, insbesondere durch das Bundesverfassungsgericht.

Die Konferenz erörterte intensiv die aktuellen Gesetzentwürfe der Sicherheitspolitiker, durch welche erneut verschärfte Eingriffsmöglichkeiten in die Grundrechte der Bürgerinnen und Bürger geschaffen werden sollen. Diesen wird ein erheblicher Sicherheitszuwachs unter anderem dadurch versprochen, dass Sicherheitsbehörden erlaubt wird, persönliche Daten bereits weit im Vorfeld eines weder tatsächlich noch zeitlich bestimmbaren Gefahrenereignisses zu verarbeiten und zu nutzen. Die Bestrebungen, so auch auf Daten unbescholtener Personen zuzugreifen, haben weiteren Fortgang gefunden.

Zu den neuen verfassungsrechtlichen Problemfällen zählt das zurzeit im Bundestag beratene Terrorismusbekämpfungsergänzungsgesetz, welches unter anderem den Geheimdiensten weitergehende Befugnisse einräumt. Eine Evaluation der bisherigen tiefgreifenden Instrumente unter unabhängiger wissenschaftlicher Verantwortung war zuvor nicht durchgeführt worden. Die Datenschutzbeauftragten konstatieren in einer hierzu gefassten Entschließung einen deutlichen Trend zum Präventionsstaat mit gravierenden Freiheitseinschränkungen. Daher müssen die tatsächlichen Möglichkeiten parlamentarischer Kontrollorgane dem Zuwachs an Macht bei den Sicherheitsbehörden korrespondieren.

Auch zu dem in gleichem Sachzusammenhang stehenden Entwurf eines Antiterrordatei-Gesetzes sah sich die Konferenz zu einer Entschließung veranlasst. Nach dem Gesetzentwurf sollen Nachrichtendienste und Sicherheitsbehörden in einer Art und Weise Zugriff auf Informationen der jeweils anderen Dienste erhalten, welche das verfassungsrechtliche Trennungsgebot zu beeinträchtigen geeignet ist.

Unter der Überschrift, dass verfassungsrechtlich nicht alles erlaubt ist, was technisch und praktisch umsetzbar erscheint, erörterte die Konferenz erneut die Themen Vorratsdaten-speicherung der Telefon- und Internetkommunikation sowie die Nutzung von Maut-Daten zur Strafverfolgung. Anlässlich der auch zur Sprache gekommenen europäischen Bezüge (z. B. Vorratsdatenspeicherung, Fluggastdaten) machten die Teilnehmenden unter anderem deutlich, dass es nicht akzeptabel ist, wenn Vorhaben, welche in Deutschland nicht durchsetzbar scheinen, von interessierten Stellen über die EU als europäischer Rechtsetzungsauftrag wieder eingebracht werden.

Die Konferenz hat Äußerungen der belgischen wie auch der schweizerischen Datenschutz-instanz zustimmend zur Kenntnis genommen, die nach Prüfung festgestellt haben, dass Datenübermittlungen von der SWIFT-Organisation an Empfängerbehörden in den USA in vielen Fällen unzulässig waren und sind. Die Datenschutzberatergruppe der EU-Kommission (Art. 29-Gruppe), deren Vorsitz der Bundesbeauftragte Schaar innehat, wird nach Prüfung des rechtstatsächlich schwierigen Beziehungsgeflechts zwischen SWIFT und den beteiligten Banken eine Stellungnahme abgeben. Auch diese unterliegen der datenschutzrechtlichen Verantwortlichkeit.

Besondere Aktualität erfährt derzeit die beabsichtigte Umstellung der Schulstatistik auf Individualdaten mit bundeseinheitlichem Kerndatensatz, insbesondere zu Zwecken der Bildungsplanung. Der föderalistischen Kompetenzverteilung entsprechend beraten die Landesbeauftragten für den Datenschutz die jeweilige oberste Kultusbehörde. Der Landesbeauftragte für den Datenschutz in Sachsen-Anhalt ist als Vorsitzender der Konferenz zum 5. Dezember 2006 von der Ständigen Konferenz der Kultusminister eingeladen, deren Kommission für Statistik zu den datenschutzrechtlichen Rahmenbedingungen des Vorhabens zu beraten. Zur Verdeutlichung der aktuellen datenschutzrechtlichen Bedenken hat die Konferenz eine Entschließung gefasst. Die Sinnhaftigkeit und Verhältnismäßigkeit des Vorhabens steht infrage.

Die Konferenz hat zudem über aktuelle Rechtsetzungsvorhaben (EU, Bund, Länder), E-Government-Vorhaben, die Informationsfreiheitsgesetzgebung sowie die Übermittlung von Fluggastdaten in die USA beraten.

Die Konferenz erörterte im Zuge der ständigen Begleitung des Projektes „Elektronische Gesundheitskarte“ den aktuellen Sachstand zu den Testverfahren im Zusammenhang mit der Karteneinführung. Trotz vielfältiger Detailprobleme, insbesondere im technischen Bereich, hat sie zustimmend zur Kenntnis genommen, dass Maßnahmen zur Wahrung differenzierter Steuerungsrechte der Patienten zu ihren medizinischen Daten frühzeitig in die Verfahren einbezogen werden.

Auch das Arbeitslosengeld II war wegen weiterer Gesetzesänderungen erneut Thema. Schwierigkeiten bereitet nach wie vor die Umsetzung der Datenschutzkontrolle. Obwohl die Datenschutzbeauftragten des Bundes und der Länder durch Konferenzentschließungen und Beratungen intensiv auf die Probleme unscharfer Kontrollzuständigkeiten hingewiesen haben, hat die zum 1. August 2006 wirksam gewordene Änderung des SGB II noch nicht zur ausreichenden Klarheit geführt. Die Datenschutzbeauftragten stellen dennoch in Abstimmung mit dem Bundesministerium für Arbeit und Soziales und der Bundesagentur für Arbeit eine effiziente datenschutzrechtliche Kontrolle der Leistungsträger und insbesondere der Arbeitsgemeinschaften sicher.

Gleichfalls bedarf die künftige Entwicklung der gesetzlichen Regelungen zum Arbeitslosengeld II der Begleitung der Datenschutzbeauftragten. Datenerhebungen müssen erforderlich, nicht aber durch publikumswirksame Schlagworte wie zum Beispiel „Missbrauch“ oder den Generalverdacht gegen Antragsteller motiviert sein.

Die Datenschutzbeauftragten haben sich über aktuelle Entwicklungen in der Informations- und Kommunikationstechnik unterrichten lassen. Der Trend, Alltagsgegenstände mit digitalen Etiketten (sog. RFID-Tags) auszustatten, weist auffällig nach oben. Da diese Etiketten tatsächlich kleine Rechner sind, entstehen durch die damit möglichen Funktionalitäten nicht kontrollierbare Risiken für Verbraucherinnen und Verbraucher. Die denkbaren Gefährdungen nehmen auch im staatlichen Bereich zu, wie die Einführung von mit RFID ausgerüsteten Ausweisen belegt. Im Rahmen der technischen Datenschutzthemen haben die Datenschutzbeauftragten daher hierzu eine Entschließung gefasst.

Der vom Europarat ausgerufene Europäische Datenschutztag wird künftig in der Woche um den 28. Januar terminiert werden, erstmals am Montag, dem 29. Januar 2007. Das Datum erinnert an die Eröffnung der Unterzeichnung des Übereinkommens zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten vom 28. Januar 1981, das insbesondere das Recht auf einen Persönlichkeitsbereich bei der automatisierten Verarbeitung schützen will. Hierzu hat sich die Konferenz auf Arten und Formen der Unterstützung und Beteiligung verständigt. Auf die beigefügte allgemeine Information wird verwiesen.

Anlage 1.7 Das Gewicht der Freiheit beim Kampf gegen den Terrorismus

Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. Oktober 2006 in Naumburg

Seit dem 11. September 2001 wandelt sich der Staat immer mehr zu einem Präventionsstaat, der sich nicht darauf beschränkt, Straftaten zu verfolgen und konkrete Gefahren abzuwehren. Der Staat verlagert seine Aktivitäten zunehmend in das Vorfeld der Gefahrenabwehr. Sicherheitsbehörden gehen der abstrakten Möglichkeit von noch nicht einmal geplanten Taten nach. Immer mehr Daten werden auf Vorrat gesammelt und damit eine Vielzahl unverdächtiger Menschen erfasst. Auch unbescholtene Bürgerinnen und Bürger werden als Risikofaktoren behandelt, ohne dass diese dafür Anlass gegeben haben.

Dieses neue Verständnis von innerer Sicherheit führt zu gravierenden Einschränkungen der Freiheitsrechte. Beispiele sind die von der Europäischen Union beschlossene Speicherung der Telekommunikationsverkehrsdaten oder die im Jahr 2002 verfassungswidrig durchgeführten Rasterfahndungen.

In diesem Zusammenhang ist auch der „Entwurf eines Gesetzes zur Ergänzung des Terrorismusbekämpfungsgesetzes“ kritisch zu bewerten. Die ursprünglich zur Terrorismusbekämpfung geschaffenen Befugnisse werden immer weiter ausgedehnt und nicht mehr nur auf Terrorverdächtige beschränkt.

Bei allen Gesetzen und Maßnahmen zur Terrorbekämpfung stellt sich die Frage nach deren Eignung und Verhältnismäßigkeit. Mehr Überwachung führt nicht automatisch zu mehr Sicherheit, aber stets zu weniger Freiheit. Es gibt keine absolute Sicherheit.

Die verfassungsrechtlich notwendige wissenschaftliche Evaluation der bisherigen Vorschriften zur Terrorismusbekämpfung durch eine unabhängige Stelle fehlt bislang. Der „Bericht der Bundesregierung zu den Auswirkungen des Terrorismusbekämpfungsgesetzes“ ist keine vollwertige Evaluation der bisherigen Vorschriften. Damit steht sowohl die Notwendigkeit einer Verlängerung als auch die Erforderlichkeit der Schaffung neuer Befugnisse in Zweifel.

Zunehmende Befugnisse verlangen nach zusätzlichen Kontrollen. Daher ist es unerlässlich, einen angemessenen Ausgleich zwischen den Befugnissen der Sicherheitsbehörden und den Kompetenzen der Kontrollorgane zu schaffen. Insbesondere müssen die Handlungsmöglichkeiten der parlamentarischen Kontrollorgane entsprechend ausgestaltet sein.

Anlage 1.8 Verfassungsrechtliche Grundsätze bei Antiterrordatei-Gesetz beachten

Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. Oktober 2006 in Naumburg

Mit dem Entwurf eines Gesetzes zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame-Dateien-Gesetz BT-Drs. 16/2950) - verschärft durch Forderungen aus dem Bundesrat - sollen in der Bundesrepublik Deutschland erstmals die rechtlichen Grundlagen für die Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten geschaffen werden. Von besonderer Bedeutung ist die beim Bundeskriminalamt zur Aufklärung und Bekämpfung des internationalen Terrorismus einzurichtende Antiterrordatei, in welcher umfangreiches Datenmaterial der beteiligten Sicherheitsbehörden zusammengeführt werden soll.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder verkennt nicht die zur Begründung des Gesetzentwurfs geltend gemachte hohe Bedrohung durch den internationalen Terrorismus und die Notwendigkeit zur Optimierung des Informationsaustauschs. Jede Intensivierung der informationellen Zusammenarbeit zwischen Polizeibehörden und Nachrichtendiensten muss jedoch den verfassungsrechtlichen Vorgaben, insbesondere dem Recht auf informationelle Selbstbestimmung, dem Grundsatz der Verhältnismäßigkeit und dem - in einigen Landesverfassungen ausdrücklich genannten - Trennungsgebot zwischen Polizei und Nachrichtendiensten entsprechen. Der vorliegende Entwurf zur Antiterrordatei enthält schwerwiegende verfassungs- und datenschutzrechtliche Risiken.

Insbesondere den folgenden brisanten Aspekten wird im Rahmen der anstehenden parlamentarischen Beratungen besondere Beachtung zu schenken sein:

- Die Anti-Terror-Datei sieht gravierende Erweiterungen des Datenaustauschs vor. Deshalb ist zumindest eine weitergehende Präzisierung der zu erfassenden Personen erforderlich. Insoweit ist insbesondere zu berücksichtigen, dass die Nachrichtendienste in der Antiterrordatei auch Personen erfassen, bei denen nur auf weichen Informationen beruhende tatsächliche Anhaltspunkte für eine Zuordnung zum internationalen Terrorismus bestehen. Diese Anhaltspunkte können auf legalem Verhalten beruhen, mit der Folge, dass auch unbescholtene Personen in der Antiterrordatei erfasst werden und deren Daten allen zugriffsberechtigten Behörden zur Verfügung stehen. Dass im Bereich der Vorfeldermittlungen ein besonders hohes Risiko einer Fehlprognose besteht, ist auch bereits verfassungsgerichtlich festgestellt.
- Die Definition der in der Datei zu erfassenden sog. Kontaktpersonen muss präzisiert werden und der Kreis der Betroffenen ist einzuschränken. Dies gilt insbesondere für solche Kontaktpersonen, gegen die keinerlei belastende Erkenntnisse vorliegen. Es muss sichergestellt werden, dass nicht bereits unverdächtige soziale Kontakte zu einer Erfassung von Personen aus dem Umfeld Verdächtigter führen.
- Die Aufnahme besonderer Bemerkungen, ergänzender Hinweise und Bewertungen in Freitextform eröffnet den am Verbund teilnehmenden Behörden die Möglichkeit, eine Vielzahl, auch weicher personenbezogener Informationen (z. B. nicht überprüfte Hinweise oder Vermutungen) ohne Bindung an hinreichend konkrete Festlegungen des Gesetzgebers in der Datei zu erfassen. Deshalb sollte darauf verzichtet werden.
- In diesem Zusammenhang ist auch der Zugriff von Polizeibehörden auf Vorfelderkenntnisse der Nachrichtendienste im Hinblick auf das Trennungsgebot kritisch zu hinterfragen. Besonders bedenklich erscheint dabei die Zulassung von Ausnahmen vom verfassungsrechtlichen Trennungsgebot in den sog. Eilfällen, in welchen den beteiligten Behörden ein unmittelbarer Online-Zugriff auf alle Daten gestattet wird.
- Die zugriffsberechtigten Sicherheitsbehörden sind nicht klar genug bezeichnet. Aufgrund der Speicherung auch höchst sensibler personenbezogener Vorfelddaten muss der Gesetzgeber aus rechtsstaatlichen Gründen selbst festlegen, welche Stellen zugriffsberechtigt sein sollen.
- Im Übrigen sind auch die bereits jetzt erkennbaren Tendenzen zu einer Erweiterung der Antiterrordatei über die Terrorismusbekämpfung hinaus nicht akzeptabel. Dies gilt insbesondere für die im Gesetzentwurf vorgesehene Nutzung der Datei im Rahmen der Strafverfolgung. Es darf nicht zu einer immer niedrigeren Eingriffsschwelle kommen.

Anlage 1.9 Verbindliche Regelungen für den Einsatz von RFID-Technologien

Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. Oktober 2006 in Naumburg

Der Einsatz von RFID-Tags (Radio Frequency Identification) hält unaufhaltsam Einzug in den Alltag. Schon jetzt werden sowohl im öffentlichen als auch im privatwirtschaftlichen Bereich viele Gegenstände mit diesen miniaturisierten IT-Systemen gekennzeichnet. Es ist zu erwarten, dass neben bereits jetzt mit RFID-Technik gekennzeichneten Lebensmitteln künftig auch Personalausweise, Geldscheine, Kleidungsstücke und Medikamentenpackungen mit RFID-Tags versehen werden. In wenigen Jahren könnten somit praktisch alle Gegenstände des täglichen Lebens weltweit eindeutig gekennzeichnet sein.

Die flächendeckende Einführung derart gekennzeichneter Gegenstände birgt erhebliche Risiken für das Recht auf informationelle Selbstbestimmung in sich. Die RFID-Kennungen verschiedenster Gegenstände können sowohl miteinander als auch mit weiteren personenbezogenen Daten der Nutzenden - in der Regel ohne deren Wissen und Wollen - zusammengeführt werden. Auf diese Weise werden detaillierte Verhaltens-, Nutzungs- und Bewegungsprofile von Betroffenen ermöglicht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet von allen Stellen, in deren Verantwortungsbereich RFID-Tags verwendet werden, insbesondere von Herstellern und Anwendern im Handels- und Dienstleistungssektor, alle Möglichkeiten der datenschutzgerechten Gestaltung dieser Technologie zu entwickeln und zu nutzen, und vor allem die Prinzipien der Datensparsamkeit, Zweckbindung, Vertraulichkeit und Transparenz zu gewährleisten. Der schnellen Umsetzung dieser Forderungen kann auch eine verbindliche Selbstverpflichtung von Herstellern und Anwendern der RFID-Technologie im Handels- und Dienstleistungssektor dienen.

Das Bundesverfassungsgericht hat den Gesetzgeber mehrfach darauf hingewiesen, dass wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels die technischen Entwicklungen aufmerksam zu beobachten sind und notfalls durch ergänzende Rechtsetzung korrigierend einzugreifen ist. Daher sind die besonderen Gegebenheiten, die mit dem Einsatz der RFID-Technologie verbunden sind, vom Gesetzgeber daraufhin zu untersuchen, ob für alle Risiken adäquate und rechtliche Schutzmechanismen vorhanden sind. In den Bereichen, in denen diese fehlen, hat der Gesetzgeber einzugreifen. Dies gilt insbesondere für den Fall, dass die Hersteller und Anwender sich auf eine verbindliche Selbstverpflichtung nicht einlassen.

Für den Schutz der Persönlichkeitsrechte Betroffener sind generell folgende Forderungen zu berücksichtigen:

- ***Transparenz:*** Alle Betroffenen müssen umfassend über den Einsatz, Verwendungszweck und Inhalt von RFID-Tags informiert werden.
- ***Kennzeichnungspflicht:*** Nicht nur die eingesetzten RFID-Tags selbst, sondern auch die Kommunikationsvorgänge, die durch die Chips ausgelöst werden, müssen für die Betroffenen leicht zu erkennen sein. Eine heimliche Anwendung darf es nicht geben.
- ***Keine heimliche Profilbildung:*** Daten von RFID-Tags aus verschiedenen Produkten dürfen nur so verarbeitet werden, dass personenbezogene Verhaltens-, Nutzungs- und Bewegungsprofile ausschließlich mit Wissen und Zustimmung der Betroffenen erstellt werden können. Soweit eine eindeutige Identifizierung einzelner Gegenstände für einen bestimmten Anwendungszweck nicht erforderlich ist, muss auf eine Speicherung eindeutig identifizierender Merkmale auf den RFID-Tags verzichtet werden.
- ***Vermeidung der unbefugten Kenntnisnahme:*** Das unbefugte Auslesen der gespeicherten Daten muss beispielsweise durch Verschlüsselung bei ihrer Speicherung und Übertragung unterbunden werden.
- ***Deaktivierung:*** Es muss vor allem im Handels- und Dienstleistungssektor die Möglichkeit bestehen, RFID-Tags dauerhaft zu deaktivieren, bzw. die darauf enthaltenen Daten zu löschen, insbesondere dann, wenn Daten für die Zwecke nicht mehr erforderlich sind, für die sie auf dem RFID-Tag gespeichert wurden.

Anlage 1.10 Keine Schülerstatistik ohne Datenschutz

Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. Oktober 2006 in Naumburg

Seit einigen Jahren arbeitet die Kultusministerkonferenz an der Einführung eines bundesweit einheitlichen Schulstatistiksystems, in dem weit über das bisherige Maß hinaus Daten aus dem Schulbereich personenbezogen verarbeitet werden sollen. Es soll auf Landesebene in einer Datei für jede Schülerin und jeden Schüler sowie für jede Lehrerin und jeden Lehrer für das gesamte „Schulleben“ ein umfangreicher Datensatz angelegt werden. Hierzu erhält jede Person eine Identifikationsnummer, was auf ein pseudonymisiertes Register hinausläuft. Die Länderdateien sollen überdies zu einer bundesweiten Datenbank zusammengefasst werden. Die spätere Ergänzung des Schülerdatensatzes mit sogenannten sozialökonomischen Daten über das Elternhaus sowie eine Einbeziehung der Kindergarten- und Hochschulzeit ist beabsichtigt. Eine präzise und einheitliche Zweckbestimmung lässt sich den bisherigen Äußerungen der Kultusministerkonferenz nicht entnehmen.

In datenschutzrechtlicher Hinsicht sind folgende Vorgaben zu beachten:

Wie das Bundesverfassungsgericht festgestellt hat, ist eine Totalerhebung nur zulässig, wenn der gleiche Erfolg nicht mit weniger einschneidenden Maßnahmen erreicht werden kann.
Im Hinblick auf die bereits gewonnenen Ergebnisse aus stichprobenartigen und weitgehend auf Freiwilligkeit beruhenden wissenschaftlichen Untersuchungen (wie PISA, IGLU oder TIMSS) erscheint die Notwendigkeit der geplanten Einrichtung eines bundesweiten zentralen schüler- bzw. lehrerbezogenen „Bildungsregisters“ nicht dargetan. Ein solches Register wäre ein nicht erforderlicher und damit unverhältnismäßiger Eingriff in das informationelle Selbstbestimmungsrecht.

Deshalb fordern die Datenschutzbeauftragten von der Kultusministerkonferenz bei diesem Vorhaben nachdrücklich den Verzicht auf eine ID-Nummer. Jede Möglichkeit einer Reidentifizierung von Individualdatensätzen ist durch geeignete Verfahren auszuschließen (kein schüler- oder lehrerbeziehbares Bildungsregister!).

Im Übrigen sind folgende verfassungsrechtliche Vorgaben und Grenzen unabdingbar:

- Der Umfang des Erhebungsprogramms ist auf den für die Statistikzwecke dienlichen Umfang zu beschränken.
- Bei allen Festlegungen sind die Grundsätze der Erforderlichkeit und Verhältnismäßigkeit zu beachten.
- Bei der Datenverarbeitung ist das Gebot der personellen, organisatorischen, räumlichen und verfahrensmäßigen Trennung von Verwaltungsvollzug und Statistik einzuhalten und das Statistikgeheimnis zu gewährleisten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass Schulministerien in mehreren Ländern das bisherige, datenschutzrechtlich bedenkliche Konzept nicht mehr weiter verfolgen, und strebt dies auch als Gesamtergebnis der mit der Kultusministerkonferenz zu führenden Gespräche und des angekündigten Workshops an.

Anlage 1.11 Information der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum 1. Europäischen Datenschutztag

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt die Initiative des Europarats für einen Europäischen Datenschutztag. Sie will mit verschiedenen Aktionen am 29. Januar 2007, dem ersten Europäischen Datenschutztag, die Menschen in Deutschland für ihre eigenen Datenschutzrechte sensibilisieren.

Der Europarat will über den Europäischen Datenschutztag das Bewusstsein für den Datenschutz bei den Bürgerinnen und Bürgern in Europa erhöhen. Alle mit dem Datenschutz befassten Stellen in Europa sind aufgerufen, sich durch eigene Aktionen an diesem Tag zu beteiligen. Der Tag wird zukünftig jährlich regelmäßig in der Woche um den 28. Januar terminiert werden, weil an diesem Datum die Unterzeichnung der Europaratskonvention 108 zum Datenschutz begonnen wurde. Mit der Konvention verpflichten sich die unterzeichnenden Staaten, für die Achtung der Rechte und Grundfreiheiten insbesondere des Persönlichkeitsbereichs bei der automatisierten Datenverarbeitung Sorge zu tragen.

Die Initiative für einen Datenschutztag wird begrüßt und unterstützt, weil sie einen Anlass gibt, in einer Zeit, in der Datenverarbeitung allgegenwärtig ist, die im Interesse des Schutzes von Privatsphäre notwendigen Grenzen darzustellen und zu verstehen. Die Konferenz möchte alle, die sich mit dem Thema Datenschutz befassen, ausdrücklich zu eigenen Aktionen und Informationen zum Datenschutz an diesem Tag ermuntern. Beispielhaft können Sprechstunden, Vorträge, Tage der offenen Tür, Preisausschreiben, Informationskampagnen zu einzelnen Themen, Aktionen mit speziellen Gruppen (z. B. Jugendliche, Reisende, Patientinnen/Patienten) etc. als Möglichkeiten für die Gestaltung des Tages genannt werden.

Soweit die Medien den Datenschutztag aufgreifen wollen, bieten die Mitglieder der Konferenz ihre Kooperation an und werden ihre fachlichen Kenntnisse zum Datenschutz gerne zur Verfügung stellen.

Anlage 1.12 GUTE ARBEIT in Europa nur mit gutem Datenschutz

Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. März 2007 in Erfurt

Die Ministerinnen und Minister für Beschäftigung und Soziales in Europa haben am 19. Januar 2007 neun Schlussfolgerungen für GUTE ARBEIT aufgestellt: GUTE ARBEIT bedeute Arbeitnehmerrechte und Teilhabe, faire Löhne, Sicherheit und Gesundheitsschutz bei der Arbeit sowie eine familienfreundliche Arbeitsorganisation. Gute und faire Arbeitsbedingungen sowie angemessener sozialer Schutz seien unabdingbar für die Akzeptanz der Europäischen Union bei den Bürgerinnen und Bürgern.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder nimmt diese Initiative zum Anlass und fordert dazu auf, auch den Beschäftigtendatenschutz zu stärken. Angesichts stetig wachsender technischer Möglichkeiten muss klar geregelt werden, welche Daten Unternehmen über ihre Beschäftigten erheben dürfen, wie sie damit verfahren müssen und wozu sie die Daten nutzen dürfen.

Deshalb fordert die Konferenz seit langem ein Arbeitnehmerdatenschutzgesetz. Bereits 2003 hat sie darauf hingewiesen, dass Persönlichkeitsrechte und Datenschutz im Arbeitsverhältnis vielfältig bedroht sind, zum Beispiel durch

- die Sammlung von Beschäftigtendaten in leistungsfähigen Personalinformationssystemen, die zur Erstellung von Persönlichkeitsprofilen genutzt werden,
- die Übermittlung von Beschäftigtendaten zwischen konzernangehörigen Unternehmen, für die nicht der Datenschutz der EG-Datenschutzrichtlinie gilt,
- die Überwachung des Arbeitsverhaltens durch Videokameras, die Protokollierung der Nutzung von Internetdiensten am Arbeitsplatz,
- die Erhebung des Gesundheitszustands, Drogen-Screenings und psychologische Testverfahren bei der Einstellung.

Die Achtung des Grundrechts auf informationelle Selbstbestimmung der Arbeitnehmerinnen und Arbeitnehmer zählt ebenso zu guten und fairen Arbeitsbedingungen wie Chancengleichheit oder gerechte Bezahlung. Beschäftigtendatenschutz erhöht zudem die Motivation, trägt und fördert die Arbeitszufriedenheit und bedeutet damit einen nicht zu unterschätzenden Standortvorteil.

Die Konferenz fordert die Bundesregierung auf, sich für einen hohen gemeinsamen Mindeststandard des Arbeitnehmerdatenschutzes in Europa einzusetzen und in Deutschland zeitnah einen entsprechenden Gesetzentwurf vorzulegen.

Anlage 1.13 Anonyme Nutzung des Fernsehens erhalten!

Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. März 2007 in Erfurt

Seit einiger Zeit werden in der Öffentlichkeit Pläne der großen privaten Fernsehveranstalter diskutiert, gemeinsam mit den Betreibern von Übertragungskapazitäten (Satellit, Kabel und DVB-T) ihre Programme nur noch verschlüsselt zu übertragen. Dabei werden vorrangig solche Geschäftsmodelle favorisiert, bei denen die kostenpflichtige Entschlüsselung des Signals nur mit personenbezogenen Smartcards möglich sein soll.

Die Datenschutzbeauftragten des Bundes und der Länder betrachten diese Entwicklung mit Sorge. Nachdem vor allem durch zahlreiche staatliche Eingriffe die verfassungsrechtlich gebotene unbeobachtete Nutzung von Telekommunikation und Internet kaum noch möglich ist, steht nun auch der seit jeher selbstverständliche anonyme und nicht registrierte Empfang von Rundfunkprogrammen auf dem Spiel. Gerade durch die Vermarktung individuell zugeschnittener Programmpakete im digitalen Rundfunk kann bei personenbezogener Abrechnung nachvollzogen werden, wer welche Angebote nutzt. Die entstehenden technischen Infrastrukturen werden zudem auch Möglichkeiten bieten, die konkrete Nutzung einzelner Sendungen zu registrieren. Damit wird die allgegenwärtige Bildung von Persönlichkeitsprofilen um detaillierte Kenntnisse über den Rundfunkkonsum ergänzt.

Die bisher bekannt gewordenen Pläne der Unternehmen widersprechen dem im Rundfunkstaatsvertrag geregelten Gebot, die Inanspruchnahme von Rundfunk und deren Abrechnung anonym zu ermöglichen und verstoßen gegen das Prinzip der Datenvermeidung. Dies wäre nicht akzeptabel, zumal datenschutzfreundliche Varianten der Abrechnung - beispielsweise durch den Einsatz von vorbezahlten Karten - ohne wirtschaftliche Einbußen zur Verfügung stehen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb die Länder auf, die Einhaltung der datenschutzrechtlichen Anforderungen des Rundfunkstaatsvertrages gegenüber den Veranstaltern durchzusetzen, und eine anonyme Nutzung von Rundfunkprogrammen auch in Zukunft sicherzustellen.

Angesichts der immer umfassenderen Individualisierung und Registrierbarkeit des Mediennutzungsverhaltens erinnert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder an ihre Forderung, das grundgesetzlich geschützte Fernmeldegeheimnis zu einem allgemeinen Mediennutzungsgeheimnis weiterzuentwickeln.

Anlage 1.14 Elektronischer Einkommensnachweis muss in der Verfügungsmacht der Betroffenen bleiben

Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. März 2007 in Erfurt
(beschlossen bei Enthaltung Nordrhein-Westfalens)

Mit dem Verfahren ELENA (elektronische Einkommensnachweise) sollen die Einkommensdaten sämtlicher abhängig Beschäftigter in einem bundesweiten Register gespeichert werden. Dieses Verfahren ist angesichts der Sensibilität und des Umfangs der dabei erfassten personenbezogenen Daten von erheblicher datenschutzrechtlicher Brisanz.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass ein derartiges Register nur dann eingerichtet werden darf, wenn die verfassungsrechtlichen Voraussetzungen erfüllt und die gesetzlichen und technisch-organisatorischen Vorkehrungen zum Schutz der dort gespeicherten Daten getroffen werden.

Zu den wesentlichen verfassungsrechtlichen Voraussetzungen für die Einrichtung des Registers gehören der Nachweis der Erforderlichkeit und die Verhältnismäßigkeit. Angesichts bestehender Zweifel daran, dass diese Voraussetzungen gegeben sind, muss belastbar dargelegt werden, dass die Daten für die jeweiligen Zwecke tatsächlich benötigt werden und dass der angestrebte Zweck nicht mit einem geringeren Eingriff in das Recht auf informationelle Selbstbestimmung erreicht werden kann.

Im Hinblick auf den vom Bundesministerium für Wirtschaft und Technologie erarbeiteten Referentenentwurf sieht die Konferenz darüber hinaus in den folgenden Punkten Klärungsbedarf:

- Es muss gesetzlich festgelegt werden, dass die Daten aus der Datenbank nur mit Mitwirkung der Teilnehmerinnen und Teilnehmer des Verfahrens zu entschlüsseln sind.
- Das Verfahren muss so ausgestaltet werden, dass die Ver- und Entschlüsselung der Daten ohne Vorliegen der Signaturkarte des Betroffenen nur in klar definierten Ausnahmefällen durch eine unabhängige Treuhänderstelle möglich ist.
- Sämtliche im Rahmen des Verfahrens verarbeiteten Daten müssen einem gesetzlichen Beschlagnahmeschutz unterworfen sein.
- Die technischen Komponenten müssen auf der Basis einer unabhängigen Prüfung zertifiziert werden.

Anlage 1.15 Keine heimliche Online-Durchsuchung privater Computer

Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. März 2007 in Erfurt

Bisher ist nur die offene Durchsuchung privater Computer gesetzlich geregelt. Trotzdem wollen staatliche Behörden auch heimliche Online-Durchsuchungen durchführen. Bei einer Online-Durchsuchung dringen Sicherheitsbehörden mittels sog. „Trojaner“ heimlich in den Rechner ein und verschaffen sich Zugriff auf alle gespeicherten Daten.

Der Bundesgerichtshof hat in seinem Beschluss vom 31. Januar 2007 (StB 18/06) die Auffassung der Datenschutzbeauftragten des Bundes und der Länder bestätigt, dass eine heimliche Online-Durchsuchung im Bereich der Strafverfolgung rechtswidrig ist. Weder die Bestimmungen zur Wohnungsdurchsuchung noch zur Telekommunikationsüberwachung können zur Rechtfertigung der heimlichen Durchsuchung und Ausforschung privater Computer herangezogen werden.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Einführung entsprechender Eingriffsgrundlagen sowohl im repressiven als auch im präventiven Bereich. Sie appellieren an die Gesetzgeber, es beim bisherigen Rechtszustand des „offenen Visiers“ zu belassen. Der Staat darf nicht jede neue technische Möglichkeit ungeachtet ihrer Eingriffstiefe zur Ausforschung einsetzen. Dies gilt auch dann, wenn wichtige Belange, wie zum Beispiel die Strafverfolgung, betroffen sind. Hier ist ein Umdenken erforderlich. Es muss ein Raum der Privatsphäre bleiben, der nicht durch heimliche staatliche Überwachungsmaßnahmen ausgehöhlt werden darf.

Eine heimliche Online-Durchsuchung greift tief in die Privatsphäre ein. Die auf einem Computer gespeicherten Daten können aufgrund ihrer Vielzahl und besonderen Sensibilität Einblick in die Persönlichkeit der Betroffenen geben. Der Schutz des Kernbereichs privater Lebensgestaltung wird gefährdet, wenn der Staat heimlich und fortdauernd in private Computer eindringt, um dort personenbezogene Daten auszuspähen. Dies gilt umso mehr, wenn Nachrichtendienste die Möglichkeit heimlichen Zugriffs auf diese Informationen erhalten, obwohl ihnen nicht einmal die offene Erlangung durch eine Beschlagnahme gestattet ist.

Es ist Aufgabe des Staates dafür Sorge zu tragen, dass den Einzelnen die Möglichkeit zur Entfaltung ihrer Persönlichkeit bleibt. Diese Möglichkeit würde unvertretbar eingeschränkt, wenn Durchsuchungsmaßnahmen zugelassen würden, bei denen aufgrund ihrer Heimlichkeit keine Person wissen kann, ob, wann und in welchem Umfang sie von ihnen bereits betroffen ist oder in Zukunft betroffen sein wird. Der Gesetzgeber sollte deshalb davon absehen, derartige neue Eingriffsbefugnisse zu schaffen, nur weil sie ihm technisch möglich erscheinen und ihre Zweckmäßigkeit behauptet wird. Die technische Entwicklung allein kann nicht der Maßstab für die Rechtfertigung von Eingriffen sein.

Die Konferenz befürchtet massive Sicherheitseinbußen, weil zu erwarten ist, dass sich Computernutzer vor staatlicher Ausforschung zu schützen versuchen, indem sie etwa Softwaredownloads unterlassen. Somit werden aber auch die sicherheitstechnisch wichtigen Software-Updates verhindert und Computer anfälliger gegen Angriffe Krimineller. Die Einführung von Befugnissen zur Online-Durchsuchung würde das Ansehen des Rechtsstaats und das Vertrauen in die Sicherheit von Informationstechnik, insbesondere von E-Government und E-Commerce, massiv beschädigen. Schließlich würden die hohen Aufwendungen für IT-Sicherheit in Staat und Wirtschaft konterkariert. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert deshalb an die Bundesregierung, die Landesregierungen und die Parlamente, auf die Einführung derartiger Befugnisnormen zu verzichten.

Anlage 1.16 Pläne für eine öffentlich zugängliche Sexualstraftäterdatei verfassungswidrig

Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. März 2007 in Erfurt

In der aktuellen Diskussion um einen verbesserten Schutz von Kindern vor Sexualstraftätern wird unter anderem die Einrichtung einer öffentlich zugänglichen Sexualstraftäterdatei mit Wohnsitzangaben gefordert. Es wird vorgeschlagen, die Namen und Adressen von verurteilten Sexualstraftätern, z. B. über das Internet, zu veröffentlichen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont, dass an Kindern begangene Sexualstraftaten mit allen zur Verfügung stehenden rechtsstaatlichen Mitteln bekämpft werden müssen. Dies schließt jedoch die Anwendung eindeutig rechtsstaatswidriger Mittel aus. Um ein solches verfassungswidriges Mittel würde es sich aber bei einer solchen Datei handeln. Dadurch würden die Betroffenen an eine Art elektronischen Pranger gestellt. Sie würden durch die öffentliche Bloßstellung sozial geächtet. Tätern würde die Möglichkeit der Resozialisierung genommen, die ihnen nach unserer Rechtsordnung zusteht.

Der Vorschlag ist lediglich dazu geeignet, Misstrauen und Selbstjustiz zu fördern. Die Betroffenen könnten damit eher zu einem erhöhten Gefahrenpotenzial werden. Er sollte deshalb nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder nicht weiter verfolgt werden.

Anlage 1.17 Vorratsdatenspeicherung, Zwangsidentifikation im Internet, Telekommunikationsüberwachung und sonstige verdeckte Ermittlungsmaßnahmen

Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. März 2007 in Erfurt

Die gesetzlichen Regelungen der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sollen nach der Ankündigung der Bundesregierung unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts einer umfassenden Neuregelung unterzogen werden. Die Bundesregierung will in diesem Zusammenhang auch die europäische Richtlinie zur Vorratsspeicherung von Telekommunikationsverkehrsdaten umsetzen. Das Bundesministerium der Justiz hat zwischenzeitlich einen Referentenentwurf vorgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont erneut, dass die Vorratsdatenspeicherung deutschem Verfassungsrecht widersprechen würde. Nach der Rechtsprechung des Bundesverfassungsgerichts ist die Speicherung von Daten auf Vorrat zu nicht hinreichend bestimmbaren Zwecken verfassungswidrig. Zudem würde die für eine freiheitliche Gesellschaft konstitutive unbefangene Kommunikation erheblich beeinträchtigt. Die Konferenz fordert die Bundesregierung auf, die Umsetzung der Europäischen Richtlinie zur Vorratsdatenspeicherung zumindest solange zurückzustellen, bis der bereits angerufene Europäische Gerichtshof über deren Rechtmäßigkeit entschieden hat.

Die geplante Ausweitung der Vorratsdatenspeicherung geht weit über die europarechtliche Umsetzungsverpflichtung hinaus und wäre ein zusätzlicher unverhältnismäßiger Eingriff in die Kommunikationsfreiheit der Bürgerinnen und Bürger. So sollen die Daten auch zur Verfolgung von Straftaten von erheblicher Bedeutung sowie mittels Telekommunikation begangener Straftaten genutzt werden. Zudem soll die Möglichkeit zur anonymen E-Mail-Kommunikation abgeschafft und die Nutzenden öffentlich zugänglicher E-Mail-Dienste sollen zur Angabe ihres Namens und ihrer Adresse verpflichtet werden. Diese Angaben sollen außerdem einer Vielzahl von Behörden zum Online-Abruf zur Verfügung gestellt werden, darunter der Polizei, den Staatsanwaltschaften, den Nachrichtendiensten, dem Zoll und der Bundesanstalt für Finanzdienstleistungsaufsicht. Auch dies begegnet erheblichen datenschutzrechtlichen Bedenken.

Zwar stärken einige der vorgesehenen Änderungen der Strafprozessordnung die rechtsstaatlichen und grundrechtlichen Sicherungen bei verdeckten strafprozessualen Ermittlungsmaßnahmen. Es besteht jedoch noch erheblicher Verbesserungsbedarf, insbesondere im Hinblick auf den Schutz des Kernbereichs privater Lebensgestaltung, den Schutz von Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern und die Voraussetzungen der Telekommunikationsüberwachung:

- Mit einer erneuten Ausweitung des Straftatenkatalogs für die Telekommunikationsüberwachung würde die Tendenz zunehmender Überwachungsmaßnahmen in verstärktem Maße fortgesetzt. Der Katalog sollte deshalb mit dem Ziel einer deutlichen Reduzierung kritisch überprüft werden. Es sollten nur Straftaten aufgenommen werden, deren Aufklärung in besonderem Maße auf die Telekommunikationsüberwachung angewiesen ist, die mit einer bestimmten gesetzlichen Mindeststrafe (z. B. ein Jahr) bedroht sind und die auch im Einzelfall schwerwiegen.

- Die vorgesehene Kernbereichsregelung ist ungenügend. Sie nimmt in Kauf, dass regelmäßig auch kernbereichsrelevante Informationen erfasst werden. Für solche Informationen muss stattdessen grundsätzlich ein Erhebungsverbot gelten. Erkenntnisse aus dem Kernbereich der privaten Lebensgestaltung, die dennoch erlangt werden, müssen zudem einem absoluten Verwertungsverbot unterliegen, nicht nur für Strafverfahren.
- Der Schutz des Kernbereichs privater Lebensgestaltung ist nicht nur in den Bereichen der Wohnraum- und Telekommunikationsüberwachung zu gewährleisten. Auch für alle anderen verdeckten Ermittlungsmaßnahmen ist eine Regelung zum Schutz des Kernbereichs zu treffen.
- Für die Kommunikation mit Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern sollte ein absolutes Erhebungs- und Verwertungsverbot geschaffen werden, das dem jeweiligen Zeugnisverweigerungsrecht entspricht. Dieses sollte unterschiedslos für alle Berufsgeheimnisträgerinnen und Berufsgeheimnisträger und deren Berufshelferinnen und Berufshelfer gelten. Die im Entwurf enthaltene Differenzierung zwischen bestimmten Gruppen von Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern ist sachlich nicht gerechtfertigt.
- Für Angehörige im Sinne von § 52 StPO sollte ein Erhebungs- und Verwertungsverbot für die Fälle vorgesehen werden, in denen das öffentliche Interesse an der Strafverfolgung nicht überwiegt. Die besonderen verwandtschaftlichen Vertrauensverhältnisse dürfen nicht ungeschützt bleiben.
- Für teilnehmende Personen von Kernbereichsgesprächen, die weder Berufsgeheimnisträgerinnen und Berufsgeheimnisträger noch Angehörige im Sinne von § 52 StPO sind, sollte insoweit ein Aussageverweigerungsrecht aufgenommen werden. Andernfalls bleibt der Kernbereich teilweise ungeschützt.
- Für die sogenannte Funkzellenabfrage, die alle Telefonverbindungen im Bereich einer oder mehrerer Funkzellen erfasst, sollten klare und detaillierte Regelungen mit engeren Voraussetzungen normiert werden. Diese sollten vorsehen, dass im Rahmen einer besonderen Verhältnismäßigkeitsprüfung die Anzahl der durch die Maßnahmen betroffenen unbeteiligten Dritten berücksichtigt und die Maßnahme auf den räumlich und zeitlich unbedingt erforderlichen Umfang begrenzt wird. Die Unzulässigkeit der Maßnahme zur Ermittlung von Tatzeuginnen und Tatzeugen sollte ins Gesetz aufgenommen werden.
- Die aufgrund einer Anordnung der Staatsanwaltschaft bei Gefahr in Verzug erlangten Daten dürfen nicht verwertet werden, wenn die Anordnung nicht richterlich bestätigt wird. Dieses Verwertungsverbot darf nicht - wie im Entwurf vorgesehen - auf Beweiszwecke begrenzt werden.
- Art und Umfang der Begründungspflicht für den richterlichen Beschluss der Anordnung der Telekommunikationsüberwachung sollte wie bei der Wohnraumüberwachung im Gesetz festgeschrieben werden. Im Sinne einer harmonischen Gesamtregelung sollten darüber hinaus qualifizierte Begründungspflichten für sämtliche verdeckte Ermittlungsmaßnahmen geschaffen werden.
- Zur Gewährleistung eines effektiven Rechtsschutzes ist sicherzustellen, dass sämtliche Personen, die von heimlichen Ermittlungsmaßnahmen betroffen sind, nachträglich von der Maßnahme benachrichtigt werden, soweit diese bekannt sind oder ihre Identifizierung ohne unverhältnismäßige weitere Ermittlungen möglich ist und nicht überwiegende schutzwürdige Belange anderer Betroffener entgegenstehen. Darüber hinaus sollte bei Massendatenerhebungen über eine ergänzende Benachrichtigung durch eine öffentliche Bekanntmachung der Maßnahme nachgedacht werden.

- Die für die Telekommunikationsüberwachung vorgesehenen Berichts- und Statistikpflichten sollten um Angaben zur Dauer der Überwachung, zur Anzahl der Gespräche und zur Benachrichtigung Betroffener ergänzt werden.
- Die im Entwurf enthaltenen erweiterten Eingriffsgrundlagen sollten befristet und einer unabhängigen, gründlichen und wissenschaftlich unterstützten Evaluation unterzogen werden.

Anlage 1.18 Telekommunikationsüberwachung und heimliche Ermittlungsmaßnahmen dürfen Grundrechte nicht aushebeln

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 8. Juni 2007

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wendet sich mit Nachdruck gegen die von Bundesregierung und Bundesratsgremien geplante Einführung der Vorratsspeicherung von Telekommunikationsverkehrsdaten und die Verschärfungen verdeckter Ermittlungsmaßnahmen, vor allem durch Telekommunikationsüberwachung:

Die Datenschutzbeauftragten haben am 8./9. März 2007 auf ihrer Konferenz in Erfurt einen ersten Gesetzentwurf als verfassungswidrig beanstandet. Insbesondere haben sie vor heimlichen Online-Durchsuchungen und der Vorratsdatenspeicherung gewarnt. Damit würde tief in die Privatsphäre eingegriffen und das Kommunikationsverhalten der gesamten Bevölkerung - ob via Telefon oder Internet - pauschal und anlasslos erfasst.

Die einhellige Kritik der Datenschutzbeauftragten und ihre Aufforderung, stattdessen verhältnismäßige Eingriffsregelungen zu schaffen, wurden von der Bundesregierung nicht beachtet. In ihrem Gesetzentwurf vom 27. April 2007 wird demgegenüber der Schutz der Zeugnisverweigerungsberechtigten verringert, Benachrichtigungspflichten gegenüber betroffenen Personen werden aufgeweicht, Voraussetzungen für die Erhebung von Standortdaten in Echtzeit und für den Einsatz des IMSI-Catchers erheblich ausgeweitet und die Verwendungszwecke für die auf Vorrat gespeicherten Daten über die europarechtlichen Vorgaben hinaus auch auf leichte Straftaten, auf Zwecke der Gefahrenabwehr und sogar der Nachrichtendienste erstreckt.

Die nun im Bundesratsverfahren erhobenen zusätzlichen Forderungen zeugen von mangelndem Respekt vor den Freiheitsrechten der Bürgerinnen und Bürger. Dies zeigen folgende Beispiele: Die ohnehin überzogene Speicherdauer aller Verkehrsdaten wird von 6 auf 12 Monate verlängert. Die Überwachungsintensität erhöht sich durch eine Verschärfung der Prüfpflichten der Telekommunikationsunternehmen - bis zum Erfordernis des Ablichtens und Aufbewahrens von Identitätsnachweisen aller Personen, die Prepaid-Produkte nutzen wollen. Die Sicherheitsbehörden erhalten Auskunft über Personen, die bestimmte dynamische IP-Adressen nutzen. Ausschüsse des Bundesrates wollen die Nutzung dieser Daten sogar zur zivilrechtlichen Durchsetzung der Rechte an geistigem Eigentum gestatten und bewegen sich damit weit jenseits des durch die EG-Richtlinie zur Vorratsspeicherung abgesteckten Rahmens, die Nutzung auf die Verfolgung schwerer Straftaten zu beschränken.

Weiterhin ist eine Ausdehnung der Auswertung von Funkzellendaten von Mobiltelefonen mit dem Ziel der Ermittlung des Aufenthaltes von möglichen Zeuginnen und Zeugen geplant. Daten, die Beweiserhebungs- oder -verwertungsverboten unterliegen, sollen nicht unmittelbar gelöscht, sondern nur gesperrt werden.

Ganz nebenbei will der Innenausschuss des Bundesrats eine Rechtsgrundlage für die heimliche Online-Durchsuchung von Internet-Computern schaffen. Allein die Zulassung dieser Maßnahme würde rechtsstaatlichen Grundsätzen eklatant widersprechen und das Vertrauen in die Sicherheit der Informationstechnik massiv beschädigen.

Das Bundesverfassungsgericht hat in letzter Zeit eine Reihe von Sicherheitsgesetzen mit heimlichen Erhebungsmaßnahmen aufgehoben. Auch europäische Gerichte haben Sicherheitsmaßnahmen für rechtswidrig erklärt. Eine Entscheidung des Europäischen Gerichtshofs über die Verpflichtung zur Vorratsdatenspeicherung von Telekommunikationsverbindungsdaten sollte abgewartet werden ebenso wie die Entscheidung des Bundesverfassungsgerichtes zur nordrhein-westfälischen Regelung, die dem Verfassungsschutz die Online-Durchsuchung erlaubt.

Die Forderungen im Gesetzgebungsverfahren zeugen von einem überzogenen Sicherheitsdenken. Sie führen dazu, dass die Freiheitsrechte der Bevölkerung untergraben werden. Sicherheit in der Informationsgesellschaft ist nicht mit überbordenden Überwachungsregelungen zu erreichen, sondern nur durch maßvolle Eingriffsbefugnisse mit effektiven grundrechtssichernden Verfahrensregelungen und durch deren besonnene Anwendung. Die betroffenen Grundrechte verkörpern einen zu hohen Wert, als dass sie kurzfristigen Sicherheitsüberlegungen geopfert werden dürfen.

Anlage 1.19 Gesetzesinitiative der Bundesregierung zu Auskunfteien und Scoring: Nachbesserung bei Auskunfteienregelungen gefordert

Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. bis 26. Oktober 2007 in Saalfeld

Die fortschreitende technologische Entwicklung führt zu immer weitreichenderer Erfassung und Verknüpfung von persönlichen Daten und ermöglicht deren Auswertung für Kontroll- und Präventionszwecke. In der Privatwirtschaft ist daher ein engmaschiges Netz verschiedener Auskunftssysteme und branchenübergreifender Zentraldateien entstanden, die durch Profilbildung das Verhalten eines jeden Menschen ohne dessen Wissen und Wollen abbilden und bewerten können.

Vor diesem Hintergrund begrüßt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass das Bundesministerium des Innern endlich damit begonnen hat, die gesetzlichen Regelungen zu den Auskunfteien zu überarbeiten und neue Regelungen zum Scoring zu schaffen.

Die vorgesehenen Regelungen zu den Auskunfteien verschlechtern die Rechtsposition der Betroffenen. Sie tragen dem sich ständig weiter entwickelnden Auskunfteimarkt und den dadurch hervorgerufenen Bedrohungen für das Recht auf informationelle Selbstbestimmung nicht hinreichend Rechnung. Ziel einer gesetzlichen Regelung muss es sein, den rasant wachsenden, branchenübergreifenden Datenaustausch zu beschränken. Es kann nicht hingenommen werden, dass Auskunfteidienste nur einseitig das Informationsinteresse der angeschlossenen Unternehmen bedienen. Sie müssen auch in stärkerem Maße die schutzwürdigen Belange der betroffenen Bürgerinnen und Bürgern berücksichtigen. Mit der im Entwurf vorgesehenen Möglichkeit, die Auskunftstätigkeit auf jegliche rechtliche und wirtschaftliche Risiken zu erstrecken, wäre zu befürchten, dass letztlich bei allen vertraglichen Beziehungen - also auch bei Versicherungs- und Arbeitsverträgen - vorab Auskunfteien eingeschaltet werden. Damit würden die allgemeinen Vertragsrisiken im Wirtschaftsleben in nicht mehr angemessener Weise einseitig auf die Kundinnen und Kunden verlagert.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert den Gesetzgeber auf, die Situation der Verbraucherinnen und Verbraucher deutlich zu verbessern und mit dem Gesetzesvorhaben einen fairen Ausgleich zwischen den Interessen der Wirtschaft und der betroffenen Verbraucherinnen und Verbraucher zu schaffen. Die Konferenz hält es für dringend erforderlich, die Auskunfteitätigkeit auf kreditorische Risiken zu begrenzen. Zudem fordert die Konferenz, Auskunfteidienste branchenspezifisch zu begrenzen.

Der vorgelegte Referentenentwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes sieht beim Scoring nun Ansätze für ein transparenteres Verfahren für die Betroffenen vor. Es muss jedoch darauf geachtet werden, dass dieser Ansatz auch vorbehaltlos umgesetzt wird. Das Scoring, bei dem mittels einer mathematisch-statistischen Formel das zukünftige vertragstreue Verhalten eines Menschen durch einen Zahlenwert ausgedrückt wird, dringt seit Jahren in immer mehr Bereiche des Wirtschaftslebens vor. Den Betroffenen wurde jedoch bisher das Wissen darüber, wie sich der Scorewert zusammensetzt, vorenthalten. Diese Praxis soll der Gesetzentwurf beenden. Die Betroffenen sollen Auskunft darüber erhalten, welche Daten mit welcher Gewichtung in den jeweiligen Scorewert eingeflossen sind. Die vorgeschlagenen Regelungen gehen jedoch noch nicht weit genug. Unbedingt zu streichen ist etwa eine im Entwurf enthaltene Regelung, wonach die Auskunft mit der Begründung verweigert werden kann, es würden Geschäftsgeheimnisse offenbart.

Anlage 1.20 Nein zur Online-Durchsuchung

Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. bis 26. Oktober 2007 in Saalfeld

Der Computer hat im täglichen Leben der meisten Menschen eine zentrale Bedeutung für die Aufbewahrung und Gestaltung privatester Informationen, wie Fotografien, Reiseberichte, Tagebuchaufzeichnungen, persönliche Briefe, Eindrücke, Vorstellungen und Gefühle.

Die heimliche Online-Durchsuchung führt deshalb zu erheblichen Eingriffen in Grundrechte (informationelles Selbstbestimmungsrecht, Unverletzlichkeit der Wohnung, Telekommunikationsgeheimnis usw.). Die Installation von Überwachungssoftware etwa mit Hilfe des Internets oder die Versendung von E-Mails unter dem Namen einer anderen Behörde wird erwogen, sogar das unbemerkte Eindringen in Wohnungen zu diesem Zweck wird nicht ausgeschlossen.

Bei dem geforderten heimlichen Zugriff auf informationstechnische Systeme geht es nicht nur um „Online-Durchsicht“ als einmalige Durchsuchung und die damit verbundene Übertragung von Festplatteninhalten an die Strafverfolgungs- oder Sicherheitsbehörden, sondern auch um die anhaltende Überwachung, um das Ausspähen von Passworten und die Protokollierung aller elektronischen Aktivitäten. Auch sollen andere Kommunikations- und Datenverarbeitungssysteme, wie Computernetze, Mobiltelefone, PDA usw. in die heimliche Durchsuchung einbezogen werden. Dabei ist die Feststellung des Computers einer Zielperson technisch ohne Zusatzinformationen nicht ohne Weiteres möglich. Die Gefahr ist daher sehr groß, dass von einer solchen Maßnahme eine Vielzahl von - auch unverdächtigen - Nutzerinnen und Nutzern betroffen sein werden.

Es steht fest, dass sich der unantastbare Kernbereich privater Lebensgestaltung bei Online-Durchsuchungen durch technische Mittel bei der Datenerhebung nicht schützen lässt. Ein automatisierter Kernbereichsschutz ist somit nicht realisierbar.

Darüber hinaus wird eingeräumt, dass sich mit Hilfe der entsprechenden Software die auf den Festplatten gespeicherten Inhalte manipulieren ließen, was die Beweiseignung der gewonnenen Erkenntnisse und damit - jedenfalls bei der Verfolgung von Straftaten - die Geeignetheit der Online-Durchsuchung infrage stellt.

Derzeit wird zwar versichert, dass der Einsatz nur auf die Bekämpfung des Terrorismus sowie die Verfolgung schwerster Straftaten und insgesamt auf wenige Fälle beschränkt wird. Die Erfahrungen zeigen aber, dass solche Beschränkungen nicht von langer Dauer sein werden. So begründen z. B. die drohende Aufweichung der Zweckbindung der Mautdaten und die Entwicklung der Telekommunikationsüberwachung die Befürchtung, dass Online-Durchsuchungen entsprechend dem technischen Fortschritt als Standardmaßnahme künftig auch bei Gefahren und Straftaten von geringerer Bedeutung eingesetzt werden. Zudem ist davon auszugehen, dass Terrorverdächtige Mittel und Wege finden werden, durch geeignete Gegenmaßnahmen eine erfolgreiche Online-Durchsuchung zu verhindern. Die heimliche Online-Durchsuchung führt deshalb voraussichtlich nicht zu mehr Sicherheit, aber sicher zur Einschränkung der Freiheit.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen daher ihre im Rahmen der 73. Konferenz im März 2007 erhobene Forderung an die Bundesregierung, die Landesregierungen und die Parlamente, auf die Einführung der repressiven und präventiven Online-Durchsuchung zu verzichten.

Sie halten es für zwingend notwendig, dass das Urteil des Bundesverfassungsgerichts in dem Verfahren gegen die Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalens abgewartet wird.
Weiterführende Informationen: Technische Aspekte der Online-Durchsuchung

Weiterführendes Material zur Anlage 1.20:

Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder
21. September 2007

Technische Aspekte der Online-Durchsuchung

0. Vorbemerkung

Das vorliegende Dokument soll den Ablauf und die technischen Verfahren der geplanten Online-Durchsuchung erläutern und aus technischer Sicht bewerten.

In den Abschnitten 1 bis 4 wird die Online-Durchsuchung beschrieben. Diese Beschreibung basiert auf den Antworten des BMI vom 22. August 2007 zu den Fragenkatalogen des BMJ und der SPD-Bundestagsfraktion. In diesen Abschnitten werden vorwiegend Begriffe verwendet, die aus dem Fragenkatalog stammen, auch wenn sie nicht allgemein anerkannt bzw. akzeptiert sind.

Im Abschnitt 5 werden die Abläufe und Verfahren aus technischer Sicht bewertet. Die Beschreibungen und Schlussfolgerungen hat der AK Technik zusammengestellt. Die Bewertungen gehen von derzeit technisch grundsätzlich möglichen Szenarien aus. In vielen Punkten besteht allerdings noch erheblicher Klärungsbedarf.

1. Begriffe

Informationstechnisches System:
- Gegenstand der Online-Durchsuchung
- System aus Hardware, Software und Daten, das der Erfassung, Speicherung, Verarbeitung, Übertragung und Anzeige von Informationen und Daten dient
- kann bspw. Personalcomputer, Server, vernetzte Verbünde von Computern, Infrastrukturkomponenten (Router, Switche, DE-CIX-Einrichtungen), externe Speichermedien
  (z. B. CD-ROMs, DVDs, externe Festplatten, USB-Speicher), Fax-Geräte, Mobilgeräte (z. B. Handys, Smartphones, Blackberrys) betreffen

Online-Durchsuchung:
- Oberbegriff für Online-Durchsicht und Online-Überwachung

Online-Durchsicht:
- einmalige Durchsuchung eines informationstechnischen Systems

Online-Überwachung:
- Überwachung eines informationstechnischen Systems über einen gewissen Zeitraum
- Inhalte aktueller Telekommunikationsvorgänge sind nicht Gegenstand der Online-Überwachung

Quellen-TKÜ:
- ausschließliche Erhebung von Telekommunikationsinhalten; betrifft nicht sonstige, auf der Festplatte abgelegte Inhalte

Remote-Forensic-Software (RFS):
- interne Bezeichnung des BKA für die zu verwendende Software

2. Phasen der Online-Durchsuchung

2.1 Technische Vorabklärung

2.1.1 Art der Informationsgewinnung
- Telekommunikationsüberwachung
- Portscan
- herkömmliche Ermittlungsmaßnahmen
- Einsatz von V-Leuten
- Einsatz von verdeckten Ermittlern

2.1.2 Art der zu beschaffenden Informationen über das Zielsystem
- Betriebssystemtyp und -version
- Internetzugang
- Browsertyp und -version
- installierte Software (Produkte und Versionen)
- Online-Verhalten der Zielperson
- Möglichkeiten der Einbringung der RFS

2.2 Technische Vorbereitung

2.2.1 Einbringungsmöglichkeiten der RFS

2.2.1.1 Aussagen des BMI im Fragenkatalog vom 22. August 2007

Das BMI bleibt bei der Beantwortung der Fragen hinsichtlich der Möglichkeiten der Einbringung sehr unkonkret und beschränkt sich auf Aussagen wie:

„Es gibt eine Vielzahl von Einbringungsmöglichkeiten, die auf Tauglichkeit für den jeweiligen Einsatz überprüft und eventuell angepasst werden müssen.“

„Eine generelle Aussage zur genauen Einbringungsmethode ist nicht möglich ...“

„Es besteht Einigkeit darüber, dass kein Interesse daran besteht, Hintertüren in Betriebs- und Anwendungssysteme einzubauen ...“

„Die Einbringung der RFS im Wege der E-Mail-Kommunikation kann je nach Einzelfall ein geeignetes Mittel darstellen.“

2.3 Technische Umsetzung

2.3.1 Zielstellung

Online-Durchsicht:

Was hat die Zielperson bezogen auf ihr informationstechnisches System in der Vergangenheit gemacht?

Online-Überwachung:

Was macht die Zielperson bezogen auf ihr informationstechnisches System aktuell?

2.3.2 Informationen/Aktivitäten

Folgende Informationen sollen erhoben bzw. Aktivitäten durchgeführt werden:
Online-Durchsicht:

- Informationen über das System selbst,
- auf dem Zielsystem gespeicherte Daten,
- Suche nach Dateien mit bestimmten Namen,
- Suche nach Dateien mit bestimmten Dateiendungen,
- Suche nach Eigenschaften/Attributen (z. B. Zugriffsdaten),
- Schlüsselwortsuche,
- Suche in bestimmten Verzeichnissen,
- Suche nach Dateien eines bestimmten Dateityps.

Online-Überwachung:

- alle Funktionen der Durchsicht und zusätzlich,
- Erfassung flüchtiger Daten (Passworteingaben; Texte, die nicht übertragen werden; in Bearbeitung befindliche verschlüsselte Dateien),
- Erfassung von Klartexten vor einer Verschlüsselung,
- Erfassung von Klartexten nach einer Entschlüsselung,
- Einsatz von Key-Loggern zum Abfangen von Tatstatureingaben, beispielsweise von kryptographischen Schlüsseln.

An den Computer angeschlossene oder mit diesem kommunizierende Geräte wie Mikrofone, Webcams oder Scanner sollen nicht überwacht werden. Mit diesen Geräten erhobene und auf dem informationstechnischen System gespeicherte Daten können jedoch Gegenstand der Durchsicht/Überwachung sein.

Online-Durchsicht und Online-Überwachung sollen sich ebenfalls nicht auf Telekommunikationsdaten erstrecken. Die technische Vorgehensweise ist vergleichbar und offensichtlich wird auch der gleiche „technische Baukasten“, wenn auch mit unterschiedlichen Bausteinen, genutzt.

Wie eine Vermischung beider Maßnahmen verhindert werden soll, wird nicht beschrieben.

2.3.3 Auswahl/Eingrenzung der zu erhebenden Informationen

Die zu sichernde Datenmenge soll anhand von vorher festgelegten Suchkriterien begrenzt werden. Folgende Möglichkeiten sollen dabei technisch umsetzbar sein:
- Erfassen der Inhalte von Dateien,
- Recherche mittels Suchbegriffen,
- Recherche in gelöschten Texten,
- Überwachung von Befehlen und genutzten Funktionen,
- Recherche nach und Erhebung von Passwörtern, Signaturen und -schlüsseln,
- Einschränkung auf ein tägliches Überwachungszeitfenster (z. B. 20.00 - 22.00 Uhr),
- Einschränkung auf bestimmte Nutzer.

2.3.4 Umgehungs-/Überwindungsmöglichkeiten von Kryptierungen

Das BMI sieht mehrere Möglichkeiten, Kryptierungen zu umgehen, von denen jedoch nicht alle genutzt werden sollen.

a) Abzweigen von Klar-Informationen vor der Ver- bzw. nach der Entschlüsselung
   - soll genutzt werden

b) Zugriff auf Schlüssel mit Sniffer-Software und/oder Key-Loggern
   - ist eine der vorgesehenen Online-Maßnahmen

c) Verwendung von absichtlich geschwächten Verschlüsselungsprodukten
   - „Der generelle Einbau von staatlichen Hintertüren ist derzeit politisch nicht gewollt."

d) treuhänderische Hinterlegung von kryptographischen Schlüsseln (key escrow)
   - „... in Deutschland politisch nicht durchsetzbar ... und technisch wenig erfolgversprechend ..."

2.3.5 Ausleitung der Informationen

Die gewonnenen Ergebnisse werden so lange auf dem informationstechnischen System zwischengelagert, bis eine Internetverbindung durch die Zielperson hergestellt wird. Die Daten werden verschlüsselt abgelegt. Nach der Übertragung auf den Rechner der Sicherheitsbehörde werden die Daten auf dem informationstechnischen System gelöscht.

2.4 Dauer und Beendigung der Maßnahme

2.4.1 Dauer der Maßnahme

2.4.1.1 Online-Durchsicht

Die Dauer der Durchsicht und der anschließenden Übermittlung ist abhängig
- von dem Online-Verhalten der Zielperson,
- vom Durchsuchungszweck,
- von der Anzahl und der Größe der zu übertragenden Dateien,
- von der Bandbreite des TK-Anschlusses des Zielsystems,
- vom Betriebszustand des Systems,
- von den Sicherungsmaßnahmen, die die Zielperson getroffen hat.

Die Durchsicht und die anschließende Übertragung kann einen Zeitraum von wenigen Minuten bis zu mehreren Tagen in Anspruch nehmen.

2.4.1.2 Online-Überwachung

Die Überwachungsdauer ist in der Regel wesentlich länger als bei der Online-Durchsicht und soll sich aus dem dann gesetzlich festgelegten Überwachungszeitraum ergeben.

2.4.2 Zeitpunkt und Art der Beendigung

Die Maßnahme soll planmäßig beendet werden, wenn
- die erhobenen Daten als ausreichend angesehen werden,
- der ursprüngliche Verdacht entkräftet wurde,
- die Durchsuchungserlaubnis aufgehoben wurde oder
- der gesetzlich zulässige Überwachungszeitraum erreicht ist.

In diesen Fällen soll sich die RFS auf ein entsprechendes Kommando hin (manuelle Auslösung) selbst deinstallieren.

Darüber hinaus soll die RFS ein Verfallsdatum und Zähler erhalten, die eine Selbst-Deinstallation der Software gewährleisten. Auf diese Weise soll auch eine ungewollte, erneute Aktivierung der RFS etwa nach dem Wiederaufsetzen des Systems mittels Datensicherungen (Back-Up) verhindert werden.

Unter Umständen ist es erforderlich, dass die Maßnahme nicht planmäßig beendet werden muss, bspw.
- bei erfolgloser Kontaktaufnahme mit dem Zielsystem (falls bspw. keine Internet-verbindung durch die Zielperson aufgebaut wird) oder bei
- (der eigentlich ausgeschlossenen) Entdeckung der RFS durch Antivirenprogramme, IDS-Systeme oder ähnliche Tools.

Die Deinstallation soll sich ausschließlich auf die RFS auswirken und keine Beeinträchtigungen des Zielsystems nach sich ziehen.

Es ist nicht beabsichtigt, den „Ursprungszustand“ des Zielsystems nach der Deinstallation der RFS herzustellen, da sich das Zielsystem während der Laufzeit der RFS ohnehin ständig verändert. Lediglich Änderungen, die die RFS an der Systemkonfiguration vorgenommen hat, sollen bei der Deinstallation der RFS rückgängig gemacht werden.

3. IT-Sicherheitsrisiko für Zielrechner

Mit der selbstentwickelten Software RFS sollen keine Daten auf dem Zielsystem manipuliert werden. Durch Hinterlegung des Quellcodes der RFS etwa beim genehmigenden Richter soll die Nachprüfbarkeit dieser Aussage in einem späteren Verfahren garantiert werden können.

Sensible Infrastrukturen in Staat und Wirtschaft sollen nicht gefährdet sein, da keine Online-Durchsuchung von Rechnern in Behörden oder Unternehmen vorgesehen ist.

Die Nutzung der RFS durch Dritte für eigene Zwecke soll nicht möglich sein, da „... die Software keine eigenen Verbreitungsroutinen und auch einen wirksamen Schutz gegen Missbrauch beinhaltet.“

Es soll sichergestellt sein, dass die Software RFS „... nicht ohne erheblichen Aufwand ...“ dazu veranlasst werden kann, an einen anderen als den von den Sicherheitsbehörden benutzten Server zurückzumelden und dass die Software weder von außen erkannt noch angesprochen werden kann.

Der generelle Einbau von „staatlichen Hintertüren“ in Verschlüsselungsprodukte ist derzeit politisch nicht gewollt. Es besteht Einigkeit darüber, dass kein Interesse daran besteht, „Hintertüren“ in Betriebs- und Anwendungssysteme einzubauen. Sie hätten nicht nur für die IT-Sicherheit, sondern auch für die deutsche Wirtschaft fatale Konsequenzen.

4. Beweissicherheit/Computer-Forensik

4.1 „Konventionelle“ Beweiserhebung auf Computersystemen

Das BMI beschreibt die konventionelle Durchführung einer Datenträgeruntersuchung (DTU) nur sehr kurz:

- Kopie anfertigen,
- Verifizierung der Kopie,
- Erstellen einer Sicherheitskopie,
- Auswertungen anhand der Kopie, ausführliche Dokumentation.

4.2 Beweiskraft der Online-Durchsuchung

Das BMI hat keine Zweifel an der Beweiskraft der Online-Durchsuchung und verweist auf Folgendes:

- Die Online-Durchsuchung soll lückenlos dokumentiert werden (z. B. die Einbringung der RFS, alle Remote-Zugriffe, alle auf dem Zielrechner durchgeführten Befehle).
- Die Integrität der übertragenen Daten soll durch Hash-, Verschlüsselungs- und Signaturverfahren sichergestellt werden.

Das BMI räumt jedoch ein, dass eine Wiederholung der Überwachungsaktivitäten „... wegen des dynamischen Charakters ...“ der gesamten Maßnahme nicht möglich ist.
Nach Ansicht des BMI ist die Beweiskraft jedoch nicht immer relevant. Lediglich bei der Nutzung der Online-Durchsuchung im Bereich der Strafverfolgung ist die forensische Beweiserhebung Zweck der Maßnahme. Bei der Nutzung als Maßnahme zur Gefahrenabwehr ist die Erkenntnisgewinnung einziger Zweck.

5. Bewertung und Schlussfolgerungen

5.1 Einbringung der RFS

Der „Erfolg“ der Online-Durchsuchung hängt maßgeblich davon ab, ob es technisch und organisatorisch möglich ist, die RFS unbemerkt in das Zielsystem einzubringen. Nachfolgend werden die Erfolgsaussichten bei den bisher diskutierten Einbringungsmethoden diskutiert und generelle Schutzmaßnahmen erläutert.

5.1.1 Einbringungsmöglichkeiten

Da das BMI nicht detailliert auf Einbringungsmöglichkeiten eingeht (vgl. Punkt 2.2.1.1), werden hier einige Möglichkeiten vorgestellt, die - nach dem derzeitigen Stand der Technik - prinzipiell geeignet sind, fremde Rechner unbemerkt mit Software zu infiltrieren.

a) mit „Hilfe“ der Zielperson:
   - verheißungsvolle E-Mails/Instant Messages mit der RFS als Anhang,
   - offizielle E-Mails von Behörden mit der RFS als Anhang,
   - E-Mails, bei denen der Absender gefälscht wurde, und dem Adressaten vertrauenswürdig erscheint,
   - manipulierte Web-Seiten, von denen die RFS heruntergeladen wird,
   - Herumliegenlassen/Zusenden von CD’s, USB-Sticks und ähnlichen Datenträgern;

b) ohne Hilfe der Zielperson:
- Ausnutzen von Software-Sicherheitslücken mit spezieller, auf die jeweilige Lücke zugeschnittener Software (sog. Exploits),
- Zero-Day-Exploit: erscheint meist am selben Tag, an dem eine Sicherheitslücke allgemein bekannt wird,
- Less-Than-Zero-Day-Exploit: wird bereits vor bekannt werden einer Sicherheitslücke angeboten,
- von Herstellern eingebaute Hintertüren,
- Hintertüren in staatlichen E-Government-Anwendungen,
- Infektion von Downloads „on the fly“,
- physischer Zugriff auf den Zielrechner durch Eindringen in die von der Zielperson benutzten Räume.

5.1.2 „Erfolgsaussichten“ bei der Einbringung

a) mit „Hilfe“ der Zielperson:
- verheißungsvolle E-Mails/Instant Messages mit der RFS als Anhang
  → geringe Erfolgsaussichten, weil sensibilisierte Zielpersonen kaum solche E-Mails öffnen werden

- offizielle E-Mails von Behörden mit der RFS als Anhang
  → geringe Erfolgsaussichten, weil sensibilisierte Zielpersonen kaum solche E-Mails öffnen werden

- E-Mails, bei denen der Absender gefälscht wurde, und dem Adressaten vertrauenswürdig erscheint
  → mittlere Erfolgsaussichten, sofern die Zielperson dem Absender ungeprüft vertraut

- manipulierte Web-Seiten, von denen die RFS heruntergeladen wird
  → mittlere Erfolgsaussichten, sofern die Zielperson keine Sandbox einsetzt und konfiguriert

- Herumliegenlassen/Zusenden von CD’s, USB-Sticks und ähnlichen Datenträgern
  → geringe Erfolgsaussichten, weil sensibilisierte Zielpersonen kaum ihnen unbekannte Datenträger auf Rechnern mit sensiblen Inhalten nutzen werden

b) ohne Hilfe der Zielperson:
- Ausnutzen von Software-Sicherheitslücken (bekannte Lücken oder Zero-Day-Exploits/Less-Than-Zero-Day-Exploits)
  → mittlere Erfolgsaussichten bei bereits länger bekannten Lücken, sofern keine aktuellen Patches eingespielt wurden
  → hohe Erfolgsaussichten bei Zero-Day-Exploits, weil Schutzmöglichkeiten noch nicht verfügbar sind
  → sehr hohe Erfolgsaussichten bei Less-Than-Zero-Day-Exploits, weil praktisch kein Schutz möglich ist

- von Herstellern eingebaute Hintertüren
  → geringe Erfolgsaussichten, sofern die Zielperson Open-Source-Software einsetzt

- Hintertüren in E-Government-Anwendungen
  → geringe Erfolgsaussichten, weil die Zielpersonen solche Anwendungen kaum nutzen werden

- Infektion von Downloads „on the fly“
  → hohe Erfolgsaussichten, da nur wenige Downloads digital signiert sind
  → hohe Erfolgsaussichten auch bei signierten Downloads, sofern die Hersteller mitwirken

- physischer Zugriff auf die IT-Zielsysteme
  → geringe Erfolgsaussichten bei Einzelsystemen, da ständig unter Kontrolle der Nutzer (z. B. Notebooks)
  → hohe Erfolgsaussichten bei komplexen Systemen und Infrastrukturkomponenten, da Eingriffe nur schwer feststellbar sind

5.1.3 Generelle Gegenmaßnahmen und ihre Schutzwirkung

- Nutzung von zwei PCs (ein Online- und ein Offline-System)
  - Daten durchlaufen den Online-PC beim Senden und Empfangen nur verschlüsselt
  - Übertragung der Daten zum Bearbeiten (Lesen, Schreiben) bspw. per USB-Stick auf den Offline-PC
    → verhindert das Auslesen mit hoher Wahrscheinlichkeit
- Live-System von CD/DVD
  - dauerhafte Änderungen am Betriebssystem mit Hilfe der RFS sind nicht möglich
  - nach jedem Neustart von CD/DVD ist der Originalzustand wieder hergestellt
    → verhindert das Auslesen mit hoher Wahrscheinlichkeit
- Nutzung eines virtuellen Zweitsystems
  - geschützte Umgebung für das Betriebssystem
  - sicherer Kanal in das Gastsystem möglich
    → verhindert das Auslesen aus der geschützten Umgebung mit hoher Wahrscheinlichkeit
- Einsatz von Virenscannern
  - einfache Scanner finden nur Schadsoftware mit bekannten Mustern (Signaturen)
    → RFS soll hochspezialisiert sein und von handelsüblichen Scannern angeblich nicht entdeckt werden
  - gute Produkte suchen nicht nur nach bekannten Mustern, sondern versuchen, das Verhalten von Software zu analysieren (proaktive Verfahren wie Heuristik oder Sandbox-Technologie)
    → ob hier die RFS unentdeckt bleibt, ist zumindest fraglich
- Einsatz von Intrusion Detection Systemen (IDS)
  - erkennen von Angriffsmustern und von Veränderungen der Systemkonfiguration
  - schon das Erkennen der Tatsache, dass ein System verändert wurde, könnte auf die RFS hindeuten
    → ob hier die RFS unentdeckt bleibt, ist zumindest fraglich

- Einsatz von Firewalls
  - vom Nutzer zugelassene Kommunikation (E-Mails, Downloads) werden nicht unterbunden
  - verschlüsselter Datenverkehr ist ebenfalls nicht filterbar
    → Schutz vor RFS kaum realisierbar
- Einsatz des TPM (Trusted Platform Modul)
  - erlaubt dem Betriebssystem, Veränderungen zu erkennen
  - gewollte Downloads werden möglicher Weise nicht als Risiko erkannt
  - Hintertüren von Softwareherstellern werden nicht erkannt
    → Schutz vor RFS zurzeit nicht abschließend bewertbar
- Nutzung des Systems ausschließlich nach Anmeldung mit Kennung und Passwort
  - bei Nutzerkennungen ohne Admin-Rechten können Installationsmöglichkeiten eingeschränkt werden
  - Software-Installation nur mit Admin-Rechten zulassen
    → erschwert das Einbringen der RFS unter bestimmten Umständen
- komplette Festplattenverschlüsselung
  - Installationsmöglichkeiten insbesondere bei physikalischem Zugriff kaum gegeben
    → erschwert das Einbringen der RFS unter bestimmten Umständen

5.2 Reichweite der Eingriffe

Die Tatsache, dass nicht nur Personalcomputer sondern beispielsweise auch Server (bspw. Mailserver), vernetzte Verbünde von Computern und komplexe Infrastrukturkomponenten (z. B. Router, Switche, DE-CIX-Einrichtungen) von der Online-Durchsuchung betroffen sein können (vgl. Punkt 1), verdeutlicht die Reichweite und damit die Eingriffstiefe dieser Maßnahme. Werden derartige IT-Komponenten überwacht, muss davon ausgegangen werden, dass nicht nur Einzelpersonen, sondern immer eine kaum einzugrenzende Anzahl von Betroffenen überwacht wird. Das BMI weist zwar darauf hin, dass bei Systemen, die unter der administrativen Betreuung Dritter stehen, anstelle der Online-Überwachung grundsätzlich der direkte Weg zu den jeweiligen Stellen gesucht würde, der aktuelle Gesetzentwurf schließt den Einsatz der RFS jedoch auch hier nicht aus.

Zudem lässt sich die Reichweite schon deshalb kaum einschätzen, weil es einer konkreten Definition des Begriffs „Verbund“ mangelt. Es kann sich dabei sowohl um ein kleines lokales Netz handeln als auch um ausgedehnte Firmen-Netze (Intranets). Dass unter diesen Voraussetzungen die Online-Durchsuchung nicht einmal mehr auf Deutschland beschränkt werden kann, bleibt vom BMI völlig unerwähnt.

Im Übrigen ist bereits bei der Online-Durchsuchung von Einzelsystemen wie Personalcomputern oder Laptops davon auszugehen, dass nicht nur Einzelpersonen überwacht werden. Auch in diesen Fällen ist nicht auszuschließen, dass mehrere Personen das System nutzen, und somit von der Maßnahme betroffen sind.

Die Reichweite der Eingriffe kann auch anhand der Art der zu erhebenden Informationen (vgl. Punkt 2.3.2) verdeutlicht werden. Die Suche nach bestimmten Dateien bedeutet nämlich in der Praxis, dass bspw. gezielt nach E-Mail-Adressbüchern, Kontaktlisten, Logdateien, Schlüsselbünden, Konfigurationsdateien, Cache-Dateien, Browser-Historien oder Sicherheitskopien gesucht werden kann.

5.3 IT-Sicherheitsrisiko für den Zielrechner

Da grundsätzlich zu bezweifeln ist, dass eine komplexe Software wie die RFS vollständig fehlerfrei programmiert wurde, ist äußerst fraglich, ob
- die Software weder durch Antivirenprogramme noch durch IDS-Systeme entdeckt werden kann,
- die Nutzung der RFS durch Dritte für eigene Zwecke wirklich ausgeschlossen werden kann,
- die RFS nicht doch dazu veranlasst werden kann, Daten an einen anderen als den von den Sicherheitsbehörden benutzten Server zu senden und ob
- die Software tatsächlich einen wirksamen Schutz gegen Missbrauch beinhaltet (vgl. Punkt 3).

Im Übrigen schließt das BMI nicht vollständig aus, dass die RFS missbraucht werden kann. Zitat:

„Speziell wird sichergestellt, dass die Software nicht ohne erheblichen Aufwand dazu veranlasst werden kann, an einen anderen als den von den Sicherheitsbehörden benutzten Server zurückzumelden und dass die Software weder von außen erkannt noch angesprochen werden kann."

Wie hoch der Aufwand tatsächlich ist, wäre zu prüfen.

Jedenfalls ist das BMI in der Pflicht, belastbare Nachweise für die Behauptungen vorzulegen, dass
- tatsächlich keine Daten auf dem Zielsystem manipuliert werden,
- sensible Infrastrukturen in Staat und Wirtschaft nicht gefährdet sind,
- die Nutzung der RFS durch Dritte für eigene Zwecke nicht möglich ist,
- die Software nicht dazu veranlasst werden kann, an einen anderen als den von den Sicherheitsbehörden benutzten Server zurückzumelden,
- die Software weder von außen erkannt noch angesprochen werden kann und
- keine Hintertüren oder absichtlich eingebaute Schwachstellen in Hard- und Software verwendet werden.

5.4 Beweissicherheit

5.4.1 Konventionelle Computer-Forensik

Um elektronisch gespeicherte Daten auf Computersystemen als rechtskräftige Beweise verwenden zu können, sind eine Reihe technisch-organisatorischer Anforderungen umzusetzen. Hansen/Krause erläutern den Ablauf wie folgt:

In der Regel sind vier Schritte erforderlich:

1) Identifizierung
   - Klärung, welche Informationen als Beweise erhoben werden sollen
   - Festlegen der Vorgehensweise und der Mittel/Werkzeuge

2) Sicherstellung
   - Sicherstellung der Zielrechner in Anwesenheit von Zeugen und gegebenenfalls Eigner
   - gegebenenfalls Sicherstellung weiterer Dateninhalte aus flüchtigen Speichern vor der Abschaltung des Systems
   - Sicherung der Datenträger gegen nachträgliche Veränderungen (z. B. Schreibschutz, kryptographische Verfahren zur digitalen Signatur)
   - Erstellen eine Image Kopie
3) Analyse
   - die Analyse durch sachverständige Kriminaltechniker
   - Analyse nie am Originalsystem, sondern immer an der Kopie
4) Aufbereitung und Präsentation
   - Zusammenfassung der Analyse in einem Bericht

5.4.2 Beweissicherheit der Online-Durchsuchung

Im Gegensatz zur konventionellen Computer-Forensik, die auf die garantierte Unveränderheit des Untersuchungsgegenstandes setzt, ist bei der Online-Durchsuchung die Veränderung des Untersuchungsgegenstandes - bedingt durch das Einbringen der RFS - die Voraussetzung für die Beweiserhebung. Schon diese Tatsache widerspricht allen Vorgaben der klassischen Computer-Forensik. Ob mit dem Start der RFS auf dem Zielsystem tatsächlich (weitere) Änderungen sicher ausgeschlossen werden können (vgl. Punkt 3), kann kaum zweifelsfrei bewiesen werden. Damit ist auch der Beweiswert der erhobenen Daten äußerst fraglich.

Ob es darüber hinaus möglich ist, die zu untersuchenden Daten bei der Übertragung zum Server der Sicherheitsbehörde verlässlich vor Manipulation und Veränderung zu schützen, ist fraglich. Es dürfte kaum möglich sein, auf einem fremdkontrollierten Zielsystem (nämlich durch die Zielperson) verlässlich kryptographische Verfahren, wie etwa die digitale Signatur, durchzuführen.

Auch die angeblich lückenlose Protokollierung aller Aktivitäten und die Hinterlegung des Quellcodes der RFS (vgl. Punkt 4.2) kann nicht garantieren, dass Daten auf dem Zielsystem verändert werden - und sei es durch Software-Fehler in der RFS oder im Betriebssystem des Zielsystems.

Der Nutzen der Hinterlegung des Quellcodes ist ohnehin mehr als fragwürdig. Mit dieser Maßnahme will das BMI offenbar sicherstellen, dass der Quellcode im Bedarfsfall vollständig analysiert werden kann. Zieht man jedoch in Betracht, dass eine Quellcodeanalyse einen erheblichen Aufwand an Zeit und hochqualifiziertem Fachpersonal erfordert, wird eine solche Analyse wohl kaum vor dem Einsatz der Software angefordert werden. Vielmehr ist anzunehmen, dass lediglich eine nachträgliche Quellcode-Analyse angefordert wird, um bspw. in einem strafrechtlichen Verfahren die „ordnungsgemäße“ Funktion der RFS beweisen zu können.

Doch selbst dieser Beweis muss unvollständig bleiben. Es ist davon auszugehen, dass der Vorgang der Online-Durchsuchung von den Sicherheitsbehörden von außen „gesteuert“ wird. So wird beispielsweise die Möglichkeit bestehen, durch „Nachladen“ von Softwarekomponenten im Laufe der Online-Durchsuchung die Originalsoftware zu verändern, um sie aktuellen Anforderungen entsprechend anpassen zu können (etwa Nachladen erweiterter Suchkriterien). Dass durch diese Maßnahme der Beweiswert des hinterlegten Quellcodes nichtig ist, versteht sich von selbst.

Der Beweiswert der mit der Online-Durchsuchung erhobenen Daten bleibt daher in jedem Fall äußerst fragwürdig.

5.5 Schutz des Kernbereichs der privaten Lebensgestaltung

Dass eine Online-Durchsuchung solche Bereiche unberücksichtigt lässt, die durch bestimmte Dateinamen oder Dateiendungen adressiert werden, ist kaum anzunehmen. Allein die Tatsache, dass eine Datei mit „Liebesbrief.doc“ bezeichnet ist, wird sicher nicht dazu führen, dass Inhalte dieser Datei nicht an den Server der Sicherheitsbehörde übertragen werden.

Auch die Suche nach Eigenschaften/Attributen wird kaum zu Einschränkungen führen, weil eine verlässliche Schlussfolgerung auf Inhalte nicht möglich ist.

Ebenso ist die Suche nach Schlüsselworten, die Suche in bestimmten Verzeichnissen oder die Suche nach Dateien eines bestimmten Dateityps keine geeignete Methode, Daten aus dem Kernbereich der privaten Lebensgestaltung zu schützen.

Selbst wenn Erkennungsalgorithmen entwickelt werden könnten, in deren Ergebnis der Kernbereich definiert werden kann, wäre immer eine Durchsuchung des Gesamtdatenbestandes nötig, um entsprechende Indexierungen zu ermöglichen. Es ist somit kein technisches Verfahren erkennbar, mit dem ein „automatisierter Kernbereichsschutz“ realisiert werden kann.

Das BMI räumt folgerichtig ein, dass „... der Schutz des Kernbereichs anderer Nutzer wie auch des Beschuldigten allein mit technischen Mitteln nicht abschließend garantiert werden kann ...“, und dieser Schutz nur im Rahmen der Auswertung der erhobenen Daten gewährleistet werden kann.

Im Ergebnis ist festzustellen, dass der Kernbereich der privaten Lebensgestaltung bei einer Online-Durchsuchung durch technische Mittel nicht angemessen geschützt werden kann.

Die Erklärungen des BMI und des BKA zur Zahl der zu erwartenden Online-Durchsuchungen (bisher wird von maximal 10 Maßnahmen pro Jahr gesprochen) darf nicht dazu führen, den Eingriff in den Kernbereich der privaten Lebensgestaltung zu verharmlosen und in der Folge die Online-Durchsuchung zu legitimieren. Selbst wenn die Online-Durchsuchung - angesichts geringer Fallzahlen - als angemessenes Mittel zur Terrorismus- bzw. Extremismusbekämpfung angesehen werden würde, darf nicht außer acht bleiben, dass der technische Fortschritt sehr schnell dazu führen kann, dass die Online-Durchsuchung zu einem Standardwerkzeug der Sicherheitsbehörden werden kann.

Dann wäre vor dem Hintergrund der jetzigen technischen Möglichkeiten ein Eingriffsinstrument legitimiert worden, das bei fortschreitender Technikentwicklung völlig unangemessen wäre.

Im Übrigen ist angesichts der künftig abnehmenden Anzahl der Festnetzanschlüsse und der zunehmenden Kommunikation per IP-Telefonie ohnehin zu hinterfragen, welche Fallzahlen künftig zu erwarten sind und ob die bisher vom BMI betonte Trennung der Online-Durchsuchung von der „Quellen-TKÜ“ Bestand haben wird. Aus den Aussagen des BMI zum Problem der verschlüsselten Kommunikation wird deutlich, dass die mit der RFS verbundenen technischen Möglichkeiten die Grundlage darstellen sollen, um angesichts der technischen Entwicklungen (Konvergenz der Netze, Verschlüsselung, Vielfalt der Kommunikationsdienste) die Strafverfolgungsbehörden technisch nicht den Anschluss verlieren zu lassen und ihnen die Möglichkeiten zu erhalten, über die sie gegenwärtig bei der TKÜ verfügen.

5.6 Auswirkungen auf das Vertrauen in die IT-Infrastruktur und Folgen für die Akzeptanz von E-Government-Verfahren

IT-Sicherheit und Datenschutz sind die zentralen Akzeptanzkriterien der sich herausbildenden Informationsgesellschaft und der weltweiten Daten- und Kommunikationsnetze. Eine Folge der heimlichen Online-Durchsuchung wird eine tiefgreifende Vertrauenskrise sein. Bürgerinnen und Bürger und möglicherweise auch Unternehmen werden nicht mehr bereit sein, staatliche E-Government-Angebote zu nutzen, da sie den Missbrauch dieser Verfahren für die Zwecke der Online-Durchsuchung befürchten.

So hat beispielsweise die Finanzverwaltung schon jetzt massive Bedenken geäußert, dass ihre Bemühungen um die breite Nutzung der elektronischen Steuererklärung (ELSTER) durch die Diskussionen um die Online-Durchsuchung konterkariert werden. Schon jetzt - vor dem Einsatz der Online-Durchsuchung - werden sinkende Nutzungszahlen erwartet.

Selbst die elektronische Kommunikation zwischen Bürgerinnen und Bürgern bzw. Unternehmen mit staatlichen Stellen per E-Mail wird künftig gemieden werden, weil das BMI nicht ausschließt, dass die RFS mittels E-Mails verbreitet wird.

Auch die elektronische Kommunikation mit der Wirtschaft wird in Mitleidenschaft gezogen werden. Wenn Kunden sich nicht mehr der Vertraulichkeit der elektronischen Kommunikation sicher sein können, werden sie wieder auf die konventionelle Kommunikationswege zurückgreifen. Sie werden dann möglicherweise auf Anwendungen wie Online-Banking und E-Commerce-Verfahren verzichten.

Zudem ist zu befürchten, dass etwa Personalcomputer nicht mehr auf dem aktuellen Sicherheitsstand gehalten werden. Aus Furcht vor infiltrierten Downloads könnten Nutzer beispielsweise auf die regelmäßigen Sicherheits-Updates verzichten. Dies wird zu einem Anstieg der Computerkriminalität führen, da Sicherheitslücken nicht mehr beseitigt werden.

Das BMI weist zwar darauf hin, dass sogenannte Hintertüren nicht eingebaut werden sollen. Es ist jedoch - zumindest aus technischer Sicht - mit ziemlicher Sicherheit davon auszugehen, dass vorhandene Hintertüren und unveröffentlichte Sicherheitslücken genutzt werden.

Insbesondere damit konterkariert das BMI jedoch die Beteuerungen der Bundesregierung, den Bürgern und der Wirtschaft eine sichere und vertrauenswürdige IT-Infrastruktur zur Verfügung zu stellen. Es ist nämlich zu befürchten, dass (evtl. zunächst nur) dem BMI bekannte Sicherheitslücken nicht so schnell wie möglich publiziert werden, damit Schutzmaßnahmen ergriffen werden können, sondern dass diese Lücken bewusst über längere Zeit offen gehalten werden, um sie für die Zwecke der Online-Durchsuchung zu nutzen. Damit kann insbesondere der Wirtschaft erheblicher Schaden zugefügt werden (Stichwort Computer-Spionage). Die Wahrscheinlichkeit ist nämlich sehr hoch, dass das BMI gerade nicht exklusive „Nutzungsrechte“ an solchen Sicherheitslücken hat.

Fraglich ist in diesem Zusammenhang auch, welche Rolle das Bundesamt für Sicherheit in der Informationstechnik (BSI) künftig spielen soll bzw. noch spielen kann. Das BMI weist zwar ausdrücklich darauf hin, dass das BSI angewiesen wurde, sich nicht aktiv an der Entwicklung der für die Online-Durchsuchung einzusetzenden Software zu beteiligen. Ob das BMI tatsächlich dauerhaft auf den Sachverstand des BSI verzichtet wird, darf zumindest bezweifelt werden. Das Vertrauen in das BSI als glaubwürdigem Berater in Fragen der IT-Sicherheit ist schon jetzt sowohl in der Wirtschaft als auch bei Bürgern nachhaltig beeinträchtigt.

Schließlich darf nicht außer acht gelassen werden, dass auch Kriminelle das Verfahren der Online-Durchsuchung oder zumindest bewusst in Kauf genommene Sicherheitslücken nutzen werden. Die Tatsache, dass Sicherheitsbehörden beharrlich davon ausgehen, dass die Online-Durchsuchung technisch durchführbar ist, wird Kriminelle in zunehmendem Maße veranlassen, sich diese Methode für ihre Zwecke nutzbar zu machen. Selbst wenn die Online-Durchsuchung für Sicherheitsbehörden nicht verwendet werden dürfte - etwa infolge einer Entscheidung des Bundesverfassungsgerichts - ist selbstverständlich davon auszugehen, dass Kriminelle alle technischen Möglichkeiten künftig nutzen werden.

Schon allein dieser Aspekt verdeutlicht, wie wichtig es künftig sein wird, alle Nutzer von Informations- und Kommunikationstechnik weiter zu sensibilisieren. Es ist auch Aufgabe der Datenschutzbeauftragten des Bundes und der Länder, sowohl die Verantwortlichen in Wirtschaft und Verwaltung als auch Bürgerinnen und Bürger zu informieren und zu beraten, um auch dadurch ein höheres Sicherheitsbewusstsein zu erreichen.

Anlage 1.21 Zentrale Steuerdatei droht zum Datenmoloch zu werden

Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. bis 26. Oktober 2007 in Saalfeld

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es für inakzeptabel, dass die Bundesregierung mit dem Jahressteuergesetz 2008 im Schnelldurchgang ohne ausführliche parlamentarische Beratung die beim Bundeszentralamt für Steuern aufzubauende zentrale Steuerdatei um zusätzliche - teilweise sensible - Daten anreichern will. Zugleich droht die Steueridentifikationsnummer (Steuer-ID) bereits vor ihrer endgültigen Einführung zu einem allgemeinen Personenkennzeichen zu werden.

Der Gesetzentwurf sieht die Ablösung des Lohnsteuerkartenverfahrens durch ein elektronisches Abrufverfahren (ElsterLohn II) ab 2011 vor. Bereits am 9. November 2007 soll das Gesetz abschließend im Bundestag beraten werden. Geplant ist unter anderem, die in Zusammenhang mit der seit dem 1. Juli 2007 vergebenen Steuer-ID errichtete Datenbank um weitere Daten zu ergänzen, etwa um die Religionszugehörigkeit, Ehepartner/Ehepartnerinnen/Kinder und deren Steuer-ID, dazu Angaben über Steuerklassen. Hierbei werden auch zahlreiche Datensätze auf Vorrat aufgenommen, da auch Personen betroffen sind, die (noch) keine Arbeitnehmerinnen/Arbeitnehmer sind.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert vom Bundestag und Bundesrat, dieses Vorhaben der Umstellung auf ein elektronisches Verfahren mit dem Jahressteuergesetz 2008 nicht zu beschließen. Folgende Punkte sind datenschutzrechtlich kritisch:

- Der durch die Vergabe der Steueridentifikationsnummer an alle Steuerpflichtigen und damit für alle Einwohnerinnen und Einwohner der Bundesrepublik entstehende Datenpool erhält eine neue Dimension. Zwar sind die Lohnsteuerabzugsmerkmale auch bisher auf der Lohnsteuerkarte vermerkt. Die Speicherung dieser Daten in einer zentralen Datenbank würde aber erhebliche datenschutzrechtliche Fragen aufwerfen. In den zentralen Datenbestand würden die Daten aller Personen mit Lohnsteuerkarten einfließen, also auch von solchen Personen, die sich nicht in einem lohnsteuerpflichtigen Beschäftigungsverhältnis befinden. Es ist zweifelhaft, ob die Aufnahme dieses Personenkreises dem Erforderlichkeitsgrundsatz entspricht. Nützlichkeitserwägungen sind für eine Datenhaltung auf Vorrat in keinem Fall ausreichend.
- Die Daten würden bundesweit annähernd vier Millionen Arbeitgebern zur Verfügung stehen. Als einzige Sicherung ist dabei vorgesehen, dass nur ein autorisierter Arbeitgeber die Lohnsteuerabzugsmerkmale abrufen kann. Klärungsbedürftig ist allerdings, wie dies sichergestellt werden kann. Zwar ist ein Authentifizierungsverfahren für den Arbeitgeber vorgesehen. Die Frage ist jedoch, ob damit tatsächlich eine rechtswidrige Informationsbeschaffung Dritter auszuschließen ist. Zumindest sollten die Daten aus der zentralen Datenbank nur unter Mitwirkung der Betroffenen abgerufen werden können.
- Die gesetzlich vorgeschriebene Evaluierung des Verfahrens (§ 87 a Abs. 6 AO) ist noch nicht erfolgt. Gleichzeitig existieren bereits jetzt Bestrebungen, die Kommunikationsplattform „Elster“ für Nutzungen durch andere Verwaltungszweige zu öffnen (OpenElster). Dies aber bedeutete, dass damit die Steuer-ID auch für die Identitätsfeststellung bei steuerfremden Anwendungen herangezogen werden könnte, ohne damit der strikten Zweckbindung nach § 139 b Abs. 5 Abgabenordnung zu rein steuerlichen Zwecken Rechnung zu tragen.

Diese Zweckbindung kann nach § 139 b Abs. 2 AO auch nicht durch die jeweilige Einwilligung der betroffenen Bürgerinnen und Bürger überwunden werden. Mit OpenElster sollen diese Vorkehrungen offenbar aufgeweicht werden, bevor die Steuer-ID überhaupt eingeführt wurde. Allein dies macht deutlich, dass jede Erweiterung des zentralen Datenbestandes kritisch hinterfragt werden muss.

Schließlich ist zu befürchten, dass die vorgesehene Erweiterung der Datenbank beim BZSt nicht den Schlusspunkt darstellt. Die im neuen Datenpool gespeicherten Daten wären auch für Sozialleistungsträger und Strafverfolgungsbehörden interessant. Es gibt zahlreiche Beispiele, dass Daten, die zunächst nur für einen engen Zweck gespeichert werden dürfen, später für viele andere Zwecke verwendet werden: Die für steuerliche Zwecke erhobenen Daten über Freistellungsaufträge werden mit den ebenfalls beim BZSt gespeicherten Daten der Empfänger von BAföG- und anderen Sozialleistungen abgeglichen. Die Mautdaten, die zunächst nur zur Mautberechnung erhoben wurden, sollen zukünftig auch zur Strafverfolgung verwendet werden. Der zunächst ausschließlich zur Terrorismusbekämpfung und der Bekämpfung der organisierten Kriminalität eingeführte Kontendatenabruf steht heute auch Finanzämtern und anderen Behörden wie z. B. der Bundesagentur für Arbeit über das BZSt offen. Das BZSt enthält so einen einzigartigen aktuellen Datenpool aller Bundesbürgerinnen und -bürger, der wesentliche Meldedaten, Bankkontenstammdaten und Steuerdaten zentral verknüpfen kann.

Anlage 1.22 Zuverlässigkeitsüberprüfungen bei Großveranstaltungen

Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. bis 26. Oktober 2007 in Saalfeld

Anlässlich der Fußball-WM 2006 wurden im Rahmen der Akkreditierung umfassende Zuverlässigkeitsüberprüfungen nach einem auf Verwaltungsebene festgelegten Verfahren durchgeführt. Dabei wurde auf die Datenbestände der Polizei- und Verfassungsschutzbehörden des Bundes und der Länder zurückgegriffen. Dieses gesetzlich nicht vorgesehene Verfahren soll nunmehr beliebigen weiteren Veranstaltungen als Vorbild dienen.

Solche Zuverlässigkeitsüberprüfungen greifen in das Grundrecht auf informationelle Selbstbestimmung ein. Grundrechtseingriffe dürfen nicht unter Umgehung gesetzlicher Vorschriften durchgeführt werden, die Voraussetzungen und Begrenzungen solcher Verfahren regeln. Die Sicherheitsüberprüfungsgesetze des Bundes und der Länder sind für die Durchführung von allgemeinen Zuverlässigkeitsprüfungen, z. B. anlässlich von Veranstaltungen, nicht einschlägig. Eine generelle rechtliche Grundlage für Zuverlässigkeitsüberprüfungen besteht außerhalb der spezialgesetzlichen Bestimmungen nicht.

Einwilligungen können - auch wenn die Betroffenen über die Umstände informiert wurden - diese Maßnahme alleine nicht legitimieren. Dies nicht nur deshalb, weil Betroffene oft Nachteile befürchten müssen, wenn sie die Einwilligung verweigern und insoweit eine echte Freiwilligkeit fehlt. Viele Regelungen zu Überprüfungsverfahren verlangen - zusätzlich - zu den materiellen und verfahrensrechtlichen Regelungen die Mitwirkung der betroffenen Personen in Form einer schriftlichen Erklärung bei der Einleitung einer solchen Überprüfung. Außerdem sollen die Vorschriften ein transparentes Verfahren gewährleisten, in dem unter anderem die Rechte Betroffener geregelt sind, so etwa das Recht auf Auskunft oder Anhörung vor negativer Entscheidung. Diese flankierenden Schutzmechanismen sind bei Überprüfungsverfahren unerlässlich.

Anlage 2 Nichtöffentlicher Bereich

Anlage 2.1 Die Entwicklung und Anwendung von RFID-Technologie ist insbesondere im Handel und im Dienstleistungssektor datenschutzkonform zu gestalten!

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 8./9. November 2006 in Bremen - Empfehlung der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich

Die gegenwärtige Entwicklung der RFID-Technologie (Radio Frequency Identification) und ihr Einsatz im Handel und im Dienstleistungssektor kann Kosteneinsparungspotenziale beispielsweise im Rahmen von Logistik- und Produktionsprozessen eröffnen. Sie birgt allerdings auch erhebliche Risiken für das Persönlichkeitsrecht von Verbraucherinnen und Verbrauchern. Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich halten es deswegen für erforderlich, dass die RFID-Technologie datenschutzkonform entwickelt und eingesetzt wird. Bereits jetzt sollten Hersteller und Anwender im Handel und im Dienstleistungssektor die Möglichkeiten der datenschutzgerechten Gestaltung dieser Technologie nutzen.

RFID ist eine Technik, um Daten mit Hilfe von Funkwellen auf einem Chip berührungslos und ohne Sichtkontakt lesen, speichern und gegebenenfalls verarbeiten zu können. Mit RFID-Chips gekennzeichnete Gegenstände können mit einem Lesegerät abhängig von der Reichweite bzw. Sendestärke identifiziert und lokalisiert werden. Ungeachtet der zahlreichen Vorteile des Einsatzes von RFID-Chips ist zu befürchten, dass zukünftig massenhaft personenbezogene Daten verarbeitet werden, indem nahezu alle Gegenstände des täglichen Lebens (einschließlich Kleidung, Lebensmittel- und andere Verpackungen, Medikamente usw.) über Hintergrundsysteme dauerhaft den Betroffenen zugeordnet werden können. RFID ermöglicht damit technisch die von den Verbraucherinnen und Verbrauchern unbemerkte Ausforschung ihrer Lebensgewohnheiten und ihres Konsumverhaltens etwa zu kommerziellen Zwecken.

Diese technologische Entwicklung stellt den Datenschutz vor neue Herausforderungen. Ob auf RFID-Chips gespeicherte Daten einen Personenbezug aufweisen, wird häufig von den konkreten Umständen des Einzelfalls abhängen. Selbst Informationen, die zunächst keinen Personenbezug haben, weil sie allein ein Produkt kennzeichnen, könnten über die Lebensdauer des Chips gesehen - zum Beispiel mit Hilfe von Hintergrundsystemen - später einer konkreten Person zugeordnet werden.

Damit würden rückwirkend alle gespeicherten Daten über einen mit einem RFID-Chip gekennzeichneten Gegenstand zu personenbezogenen Daten. Ein datenschutzkonformer Einsatz der RFID-Technologie wird deshalb immer schwerer kontrollierbar sein. Die Ausübung der verfassungsrechtlich begründeten, datenschutzrechtlich unabdingbaren Rechte der Verbraucherinnen und Verbraucher auf Auskunft sowie auf Löschung und Berichtigung von unrichtigen personenbezogenen Daten wird - insbesondere wegen der geringen Größe der RFID-Chips - künftig erheblich erschwert.

Angesichts dieses Gefährdungspotenzials der RFID-Technologie erscheint es fraglich, ob die bestehenden gesetzlichen Regelungen ausreichen, den wirksamen Schutz der Persönlichkeitsrechte der Betroffenen zu gewährleisten.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich halten es für erforderlich, dass bereits bei der technologischen Ausgestaltung von RFID das Recht auf informationelle Selbstbestimmung der Betroffenen gewahrt wird. Dazu gehört vor allem, dass Verbraucherinnen und Verbrauchern nach dem Kauf von Produkten die RFID-Chips auf einfache Weise unbrauchbar machen können. Daneben sind auch die Datenschutzrechte der betroffenen Arbeitnehmerinnen und Arbeitnehmer im Produktions- und Logistikprozess zu wahren. Zugleich sind unter anderem der Handel und der Dienstleistungssektor und insbesondere die entsprechenden Verbände aufgerufen, umfassende, verbindliche und nachprüfbare Selbstverpflichtungen für eine datenschutzfreundliche Ausgestaltung der RFID-Technologie abzugeben.

Für den Schutz der Persönlichkeitsrechte der betroffenen Verbraucherinnen und Verbraucher sind dabei folgende Regeln unabdingbar:

Transparenz/Benachrichtigungspflicht

Die Verbraucherinnen und Verbraucher müssen wegen des möglichen Personenbezugs der auf RFID-Chips gespeicherten Daten umfassend über den Einsatz, Verarbeitungs- und Verwendungszweck und Inhalt von RFID-Chips informiert werden. Werden durch ihren Einsatz personenbezogene Daten gespeichert, sind die Betroffenen hiervon zu benachrichtigen.

Kennzeichnungspflicht

Nicht nur die eingesetzten RFID-Chips selbst, sondern auch die Kommunikationsvorgänge, die durch die Chips, Lesegeräte bzw. dazugehörige Hintergrundsysteme ausgelöst werden, müssen für die Verbraucherinnen und Verbraucher transparent und leicht zu erkennen sein. Eine heimliche Anwendung „hinter dem Rücken“ der Betroffenen darf es nicht geben.

Deaktivierung

Den betroffenen Verbrauchern muss ab dem Kauf von mit RFID-Chips versehenen Produkten die Möglichkeit eröffnet werden, die RFID-Chips jederzeit dauerhaft zu deaktivieren bzw. die darauf enthaltenen Daten zu löschen, insbesondere dann, wenn Daten für die ursprünglichen Speicherzwecke nicht mehr erforderlich sind. Dieses Recht darf nicht durch Gewährleistungsbeschränkungen in Allgemeinen Geschäftsbedingungen beeinträchtigt werden.

Datensicherheit

Die Vertraulichkeit der gespeicherten und der übertragenen Daten ist durch Sicherstellen der Authentizität der beteiligten Geräte (Peripherie) und durch Verschlüsselung zu gewährleisten. Das unbefugte Auslesen der gespeicherten Daten muss wirksam verhindert werden.

Keine heimliche Profilbildung

Daten von RFID-Chips aus verschiedenen Produkten dürfen nur so verarbeitet werden, dass personenbezogene Verhaltens-, Nutzungs- und Bewegungsprofile ausschließlich mit Wissen und Einwilligung der Betroffenen erstellt werden können. Soweit eine eindeutige Identifizierung einzelner Gegenstände für einen bestimmten Anwendungszweck nicht erforderlich ist, muss auf eine Speicherung eindeutig identifizierender Merkmale auf den RFID-Chips verzichtet werden.

Anlage 2.2 SWIFT: Datenübermittlung im SWIFT-Verfahren in die USA

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 8./9. November 2006 in Bremen

Es wird festgestellt, dass die gegenwärtige Spiegelung von Datensätzen im SWIFT-Rechenzentrum in den USA und die anschließende Herausgabe von dort gespeicherten Daten an US-amerikanische Behörden wegen fehlender Rechtsgrundlage sowohl nach deutschem Recht als auch nach EG-Datenschutzrecht unzulässig ist. Insbesondere verfügen die USA über kein angemessenes Datenschutzniveau im Sinne des Artikels 25 Abs. 1 und Abs. 2 der EG-Datenschutzrichtlinie. Rechtlich verantwortlich für die Übermittlung der Daten in die USA sind sowohl die in Belgien ansässige SWIFT, als auch die deutschen Banken, die sich trotz des Zugriffs der amerikanischen Behörden auf die bei SWIFT/USA gespeicherten Datensätze auch weiterhin der Dienstleistungen von SWIFT bedienen.

Die Banken werden aufgefordert, unverzüglich Maßnahmen vorzuschlagen, durch die im SWIFT-Verfahren entweder eine Übermittlung von Daten in die USA unterbunden werden kann oder aber zumindest die übermittelten Datensätze hinreichend gesichert werden, damit der bislang mögliche Zugriff der US-amerikanischen Sicherheitsbehörden künftig ausgeschlossen ist. Eine Möglichkeit besteht nach Ansicht der Aufsichtsbehörden in der Verlagerung des zurzeit in den USA gelegenen Servers in einen Staat mit einem angemessenen Datenschutzniveau. Eine weitere Möglichkeit besteht in einer wirksamen Verschlüsselung der in die USA übermittelten Zahlungsverkehrsinformationen. Es muss ausgeschlossen sein, dass die US-amerikanischen Behörden in die Lage versetzt sind, die auf dem dortigen Server gespeicherten Datensätze zu dechiffrieren. Die Aufsichtsbehörden erwarten eine ernsthafte Auseinandersetzung der Banken mit den aufgezeigten Möglichkeiten. Allgemeine Hinweise auf eine faktische oder ökonomische Unmöglichkeit sind nicht akzeptabel. Der Verweis auf einen in der Zukunft liegenden und noch keinesfalls feststehenden Abschluss eines völkerrechtlichen Abkommens zwischen dem EU-Rat und der US-Regierung vermag nicht den gegenwärtigen Handlungsbedarf zu beseitigen.

Unabhängig davon müssen die Banken gemäß § 4 Abs. 3 Bundesdatenschutzgesetz ihre Kundinnen und Kunden darüber informieren, dass im Falle der Weiterleitung von grenzüberschreitenden Zahlungsaufträgen die Datensätze auch an ein in den USA ansässiges SWIFT Operating Center übermittelt werden. Dabei bleibt es den Banken überlassen, ob sie alle Kundinnen und Kunden über die Übermittlung der Datensätze an SWIFT/USA informieren oder nur diejenigen, für die die Dienste von SWIFT genutzt werden. Die Unterrichtung der Kundinnen und Kunden ist eine notwendige, wenn auch nicht hinreichende Mindestvoraussetzung für die Zulässigkeit der Übermittlung der Daten an SWIFT/USA. Sie ist unverzüglich umzusetzen.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich nehmen das Anliegen der deutschen Banken zur Kenntnis, aus Gründen des Wettbewerbs eine europaweit einheitliche Lösung zu erreichen. Es soll in Zusammenarbeit mit den übrigen europäischen Datenschutz-Aufsichtsbehörden eine einheitliche Handhabung angestrebt werden.

Anlage 2.3 Weitergabe von Kundendaten durch Versandhandelsunternehmen an Auskunfteien

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 19./20. April 2007 in Hamburg

Die Übermittlung von personenbezogenen Daten über das vertragsgemäße Zahlungs- und Geschäftsabwicklungsverhalten ihrer Kunden sowie die Übermittlung von Scorewerten, die auf der Grundlage dieses Verhaltens berechnet wurden, durch Versandhandelsunternehmen an Auskunfteien zur Nutzung für deren eigene Geschäftszwecke ist unzulässig, es sei denn, die Kunden haben ausdrücklich in die Weitergabe dieser Daten eingewilligt.

Ein Datenschutzhinweis in den Allgemeinen Geschäftsbedingungen eines Versandhandelsunternehmens entspricht weder der Form noch dem Inhalt nach den Anforderungen an eine wirksame Einwilligung im Sinne von § 4 a BDSG. Eine Einwilligung der Kunden setzt voraus, dass diese ausdrücklich darauf hingewiesen werden, welche Daten zu welchem Zweck an wen weitergegeben werden sollen.

Die Zulässigkeit einer Weitergabe von Kundendaten in dem genannten Umfang kann nicht auf § 28 BDSG gestützt werden, da sie nicht der Zweckbestimmung des Vertragsverhältnisses des Versandhandelsunternehmens mit dem Kunden dient (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG) und die schutzwürdigen Interessen der Kunden an dem Ausschluss der Weitergabe ihrer Daten an Auskunfteien überwiegen (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG). Die Kunden, die im Versandhandel bestellen, müssen nicht damit rechnen, dass ihr bisheriges Kundenverhalten gegenüber einem Versandhaus entscheidend dafür sein kann, ob sie Lieferungen von anderen Unternehmen erhalten, die bei einer Auskunftei Bonitätsauskünfte einholen. Die Kunden dürfen nicht zum Objekt wirtschaftlichen Handelns dadurch gemacht werden, dass der Handel selbst definiert, was für die Kunden bzw. ihre Daten gut ist. Sie haben daher ein überwiegendes schutzwürdiges Interesse an dem Ausschluss der Vermarktung ihrer positiven Bonitätsdaten.

Anlage 2.4 Weitergabe von umzugsbedingten Adressänderungen durch Versandhandelsunternehmen

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 19./20. April 2007 in Hamburg

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich stellen dazu fest: Übermittelt ein Unternehmen Umzugsadressen seiner Kunden an andere Unternehmen zur weiteren Übermittlung dieser Adressänderungen an angeschlossene Unternehmen zum Zwecke des Adressabgleichs, so ist dies nur mit einer ausdrücklichen Einwilligung der Betroffenen gemäß § 4 a BDSG zulässig.

Ein Datenschutzhinweis in den Allgemeinen Geschäftsbedingungen eines Versandhandelsunternehmens entspricht weder der Form noch dem Inhalt nach den Anforderungen an eine wirksame Einwilligung im Sinne von § 4 a BDSG. Eine Einwilligung der Kunden setzt voraus, dass diese ausdrücklich darauf hingewiesen werden, welche Daten zu welchem Zweck an wen weitergegeben werden sollen.

Anlage 2.5 Erhebung von Positivdaten zu Privatpersonen bei Auskunfteien

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 19./20. April 2007 in Hamburg

Nicht nur sog. Verbraucherauskunfteien wie beispielsweise die SCHUFA, sondern auch Handels- und Wirtschaftauskunfteien erheben und verarbeiten zunehmend Bonitätsdaten zu Privatpersonen, die nicht gewerblich tätig sind. Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen in diesem Zusammenhang darauf hin, dass die Handels- und Wirtschaftsauskunfteien insoweit die selben datenschutzrechtlichen Vorgaben zu beachten haben wie die „Verbraucherauskunfteien“.

Handels- und Wirtschaftsauskunfteien können daher sog. Positivdaten zu Privatpersonen grundsätzlich nicht auf Grundlage des § 29 Abs. 1 BDSG erheben. Denn bei Positivdaten - das sind Informationen, die keine negativen Zahlungserfahrungen oder sonstiges nicht vertragsgemäßes Verhalten zum Inhalt haben - überwiegt das schutzwürdige Interesse der betroffenen Personen, selbst über die Verwendung ihrer Daten zu bestimmen. Werden die Daten übermittelt, ist insoweit bereits die Übermittlung nach § 28 BDSG regelmäßig unzulässig.

Will eine Auskunftei Positivdaten zu Privatpersonen erheben, bedarf es dafür einer wirksamen Einwilligung der Betroffenen im Sinne des § 4 a BDSG. Sofern die Auskunftei oder ihre Vertragspartner zu diesem Zweck eine für eine Vielzahl von Fällen vorformulierte Einwilligungsklausel verwenden, die als Allgemeine Geschäftsbedingung im Sinne des § 305 BGB zu werten ist, muss eine entsprechende Einwilligung darüber hinaus den Anforderungen des § 307 BGB genügen.

Anlage 2.6 Mahnung durch Computeranruf

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 19./20. April 2007 in Hamburg

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich stellen dazu fest:

Eine telefonische Mahnung durch Computeranruf ist wegen der hohen Gefahr, dass ein anderer als der vorgesehene Empfänger die Nachricht erhält und so personenbezogene Daten einem Dritten unbefugt offenbart werden, unzulässig.

Anlage 2.7 Kreditscoring/Basel II

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 19./20. April 2007 in Hamburg

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich beurteilen die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten beim Einsatz von Scoring-Verfahren im Bereich der Kreditwirtschaft wie folgt:

I. Welche personenbezogenen Merkmale dürfen für die Berechnung des Scores genutzt werden?

1. Es dürfen nur Parameter genutzt werden, deren Bonitätsrelevanz mittels eines den wissenschaftlichen Standards entsprechenden mathematisch-statistischen Verfahrens nachgewiesen wurde. Die statistische Relevanz eines Parameters ist für die Einstellung in das Scoring-Verfahren eine notwendige, aber noch keine hinreichende Bedingung.
2. Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG dürfen nur Daten erhoben und gespeichert werden, soweit dies zur Zweckbestimmung eines Vertragsverhältnisses erforderlich ist. Die Tatsache, dass ein Scoring-Verfahren durchgeführt wird, ändert daran nichts und erweitert nicht den Berechtigungsrahmen der Banken. Es dürfen daher nur Daten in ein Scoring-Verfahren eingestellt werden, die das Institut im Rahmen eines Kreditvertrages erheben darf (Erforderlichkeitsprinzip). Soweit Daten für andere Zwecke, etwa aufgrund von Vorgaben des KWG oder des WpHG erhoben und gespeichert wurden, dürfen diese Daten nur für diese Zwecke, nicht jedoch für Scoring-Verfahren verwendet werden. (Da sensitive Daten im Sinne des § 3 Abs. 9 BDSG nicht nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG erhoben und verarbeitet werden, dürfen diese auch nicht in die Score-Berechnung einfließen.)
3. Das Scoring-Verfahren selbst stellt eine Datennutzung dar. Für diese gilt § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Danach ist die Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Ein berechtigtes Interesse der Banken an der Nutzung der für das Scoring-Verfahren verwendeten Parameter kann in der Regel angenommen werden. Wenn das Kreditinstitut die Möglichkeit hat, konkrete, unmittelbar bonitätsrelevante Daten zu erheben, darf es nicht auf Daten zurückgreifen, die nur Indizcharakter haben.

Soweit ein berechtigtes Interesse der Banken vorliegt, ist bei jedem einzelnen Parameter zu überprüfen, ob der Betroffene überwiegende schutzwürdige Interessen am Ausschluss der Datennutzung geltend machen kann. Die hier vorzunehmende Abwägung stellt einen normativen Prozess dar; die bloße statistische Relevanz eines Kriteriums führt noch nicht dazu, dass nicht von überwiegenden schutzwürdigen Interessen des Betroffenen auszugehen ist.

Bei der Abwägung können die gesetzgeberischen Wertungen aus § 10 Abs. 1 Satz 3 ff. KWG herangezogen werden. § 10 Abs. 1 KWG gilt zwar als bankenaufsichtsrechtliche Norm nur für die Erhebung und Verarbeitung personenbezogener Daten zur internen Risikobemessung (Eigenkapitalausstattung), nicht jedoch für das Scoring im Außenverhältnis zu den (potenziellen) Kundinnen und Kunden. Die Wertungen aus § 10 Abs. 1 Satz 3 ff. KWG können allerdings als gesetzgeberisches Leitbild in die Auslegung des BDSG einfließen. Das gilt insbesondere für die Anforderungen an Scoring-Merkmale. Die Merkmale müssen daher nicht nur mathematisch-statistisch erheblich sein, sondern eine ebenso hohe Stringenz aufweisen wie die im Merkmalskatalog des § 10 Abs. 1 Satz 6 KWG aufgeführten Regelbeispiele. So sind Angaben zur Staatsangehörigkeit bereits aufgrund des ausdrücklichen Verbots in § 10 Abs. 1 Satz 3 KWG als Score-Merkmale ausgeschlossen.

Bei der Abwägung sind darüber hinaus Wertungen des Grundgesetzes wie auch des einfachen Rechts daraufhin zu überprüfen, ob eine Benachteiligung der (potenziellen) Kundinnen und Kunden aufgrund eines bestimmten Kriteriums unzumutbar ist.

4. Auch wenn sich Basel II vornehmlich mit der Eigenkapitalhinterlegung der Institute befasst, wird der Einsatz von Scoring-Verfahren zunehmend dazu führen, jeden Kredit entsprechend dem individuellen Risiko zu bezinsen. Nur wenn in einer Gesamtschau der Kriterien sichergestellt ist, dass diesem Anliegen Rechnung getragen wurde, erfolgt die Datennutzung zur Wahrung berechtigter Interessen und sind keine überwiegenden schutzwürdigen Interessen der Betroffenen tangiert.

II. Wie transparent müssen die Bewertungen für die Betroffenen sein?

Für die Betroffenen (wie auch für die Aufsichtsbehörden) muss nachvollziehbar sein,

1. welche personenbezogenen Merkmale in die Berechnung des Score-Wertes einfließen;
2. welche konkreten personenbezogenen Daten der kreditsuchenden Person dafür genutzt wurden;
3. welches die maßgeblichen Merkmale sind, die den konkreten Score-Wert der betroffenen Person negativ beeinflusst haben. Diese maßgeblichen Merkmale sollen nach ihrer Bedeutung bzw. den Grad ihres Einflusses auf den konkreten Score-Wert aufgelistet werden, wobei sich die Auflistung auf die vier bedeutsamsten Merkmale beschränken soll.

Darüber hinaus ist bei der Anwendung von Scoring-Verfahren der § 6 a BDSG zu beachten.

Anlage 2.8 Internationaler Datenverkehr

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 19./20. April 2007 in Hamburg

1. Der Düsseldorfer Kreis beschließt das anliegende **Positionspapier** zum internationalen Datenverkehr. Der BlnBDI wird gebeten, das Papier als Vorsitzender der AG „Internationaler Datenverkehr“ an die damals beteiligten Wirtschaftsvertreter zu versenden, die zugleich darauf hingewiesen werden sollen, dass weitere Fallkonstellationen in einer allgemein zugänglichen Handreichung näher dargestellt werden.

   Die im Positionspapier genannten Auffassungen können von den Aufsichtsbehörden bei der Beratung auch anderer Wirtschaftsvertreter genutzt werden.

2. Der Düsseldorfer Kreis beschließt ferner die anliegende **Handreichung** zur rechtlichen Bewertung von Fallgruppen zur internationalen Auftragsdatenverarbeitung. Sie beinhaltet die häufigsten Fallkonstellationen und soll den Unternehmen die rechtliche Bewertung erleichtern. Im Einzelfall kann eine abweichende Bewertung erforderlich sein. Deshalb verbieten sich schematische Lösungen. Den Aufsichtsbehörden wird anheim gestellt, die Handreichung im Internet zu veröffentlichen oder auf andere Weise interessierten Unternehmen zugänglich zu machen.

Anmerkung: Positionspapier und Handreichung sind auf meiner Website unter http://www.datenschutz-mv.de/dschutz/ddk/int-daten.html zu finden.

Anlage 2.9 Gesetzesinitiative der Bundesregierung zu Auskunfteien und Scoring

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 08./09. November 2007 in Hamburg

Im modernen Wirtschaftsleben kommt Auskunfteien eine ständig wachsende Bedeutung zu. Diese sammeln eine Vielzahl von persönlichen Daten auch über Privatpersonen, um sie Dritten insbesondere für die Beurteilung der Kreditwürdigkeit ihrer Geschäftspartner gegen Entgelt zur Verfügung zu stellen.

Während in der Vergangenheit vor allem Kreditinstitute, der Versandhandel und Telekommunikationsunternehmen Auskünfte abgefragt haben, werden Informationen zur Beurteilung der Kreditwürdigkeit zunehmend auch von Vermietern, Versicherungen und sonstigen Unternehmen eingeholt. Von den Auskunfteien wird dabei vielfach ein sogenannter Scorewert übermittelt. Hierbei handelt es sich um einen Wert, der auf der Grundlage eines mathematisch-statistischen Verfahrens aus den bei der Auskunftei vorhandenen Angaben errechnet wird und eine Aussage über die Wahrscheinlichkeit des künftigen Zahlungsverhaltens der Betroffenen und damit über ihre Kreditwürdigkeit enthält.

Der Aufbau und die Erweiterung der zentralen Datenbestände über Betroffene bei Auskunfteien und die branchenübergreifende Bereitstellung dieser Informationen für eine Vielzahl von Unternehmen sowie der zunehmende Einsatz von Scoring-Verfahren gefährden nachhaltig das Recht auf informationelle Selbstbestimmung der Betroffenen.

Vor diesem Hintergrund begrüßt der Düsseldorfer Kreis im Grundsatz den vom Bundesministerium des Innern vorgelegten Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes, mit dem die Rechte der Betroffenen gestärkt und insbesondere auch die Transparenz beim Einsatz von Scoring-Verfahren verbessert werden sollen.

Nach Auffassung des Düsseldorfer Kreises bedarf der vorliegende Gesetzentwurf allerdings einer grundlegenden Überarbeitung, um das Ziel der Stärkung der Rechte der Betroffenen auch tatsächlich zu erreichen.

Dabei muss insbesondere sichergestellt werden, dass die bei Auskunfteien gesammelten Daten die Erstellung umfassender Persönlichkeitsprofile von Betroffenen nicht zulassen. Darüber hinaus ist gesetzlich eindeutig zu regeln, dass die Einholung einer Bonitätsauskunft auch in Zukunft an das Vorliegen eines finanziellen Ausfallrisikos geknüpft bleibt. Die im Entwurf derzeit vorgesehene Regelung, wonach jedes rechtliche oder wirtschaftliche Interesse einschließlich der Vermeidung allgemeiner Vertragsrisiken ein berechtigtes Interesse darstellen kann, würde die Rechte der Betroffenen unverhältnismäßig beeinträchtigen.

Des Weiteren muss eindeutig klargestellt werden, dass nur vertragsrelevante Daten in die Berechnung eines Scorewerts einbezogen werden dürfen. Im Übrigen dürfen die Auskunftsrechte der Betroffenen nicht durch die pauschale Berufung auf ein Geschäftsgeheimnis vereitelt werden.

Anlage 2.10 Anwendbarkeit des Bundesdatenschutzgesetzes auf Rechtsanwälte

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 8./9. November 2007 in Hamburg

Der Düsseldorfer Kreis begrüßt, dass die Bundesregierung in ihrer Stellungnahme zum 21. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erklärt hat, dass die Erhebung und Verwendung personenbezogener - auch mandatsbezogener - Daten durch Rechtsanwälte den Vorschriften des Bundesdatenschutzgesetzes unterliegt und dass die Aufsichtsbehörden der Länder zuständig sind, die Datenschutzkontrolle durchzuführen.

Der Düsseldorfer Kreis sieht darin die Bestätigung seiner Auffassung, dass das Bundesdatenschutzgesetz (BDSG) - auch hinsichtlich mandatsbezogener Daten - auf Rechtsanwälte anwendbar ist. In der Bundesrechtsanwaltsordnung (BRAO) befinden sich aus datenschutzrechtlicher Hinsicht nur punktuelle Regelungen (§ 43a Abs. 2 BRAO Schweigepflicht, § 50 BRAO Handakten). Die Vorschriften des BDSG treten gemäß § 1 Abs. 3 BDSG lediglich insoweit zurück, als bereichsspezifische Datenschutzvorschriften bestehen. Durch das anwaltliche Berufsgeheimnis werden die Informationsrechte der Aufsichtsbehörden nach § 38 BDSG in Verbindung mit § 24 Abs. 6 und 2 BDSG nicht eingeschränkt.

Anlage 3 Modernisierung des Datenschutzes: Herausforderungen durch die Technik

Stellungnahme des Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern zur Anhörung des Innenausschusses des Deutschen Bundestages am 5. März 2007

1. Modernisierung des Datenschutzes

Die Risikoanalyse des Ersten Senats des Bundesverfassungsgerichts in seinem Urteil vom 15. Dezember 1983 - 1 BvR 209/83 u. a. - stellt die gesetzgeberische Herausforderung durch moderne Informations- und Kommunikationstechnologien auch weiterhin mit der überzeugenden Schlussfolgerung eines staatlichen Gewährleistungsanspruches dar:

„Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. ...

Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann bei welcher Gelegenheit über sie weiß.“

Datenschutzfreundliche Technologien

Die Datenschutzbeauftragten haben 1997 eine Arbeitsgruppe aus ihrem Kreis „Datenschutzfreundliche Technologien“ beauftragt der Frage nachzugehen, inwieweit datenschutzfreundliche Technologien einen Beitrag zur Bewältigung dieser Herausforderungen leisten können, deren Arbeitspapier im Folgenden immer noch einen aktuellen Einstieg in die Problematik leisten kann (www.datenschutz-mv.de/dschutz/informat/dsftechn/apdsftec.pdf).

Anonymität

Bereits 1983 hat das Bundesverfassungsgericht im Volkszählungsurteil - am Beispiel der Statistik - den Anspruch auf Anonymisierung anerkannt. Gemäß der bekannten Auffassung des Bundesverfassungsgerichts heißt es dort:

„Für den Schutz des Rechts auf informationelle Selbstbestimmung ist - und zwar auch schon für das Erhebungsverfahren - ... die Einhaltung des Gebots einer möglichst frühzeitigen faktischen Anonymisierung unverzichtbar, verbunden mit Vorkehrungen gegen die Deanonymisierung“ (BVerfGE 65, 1-49-).

In der Rechtsprechung zum Medienrecht ist das Recht auf Anonymität ebenfalls seit längerem als besondere Ausprägung des Persönlichkeitsrechts anerkannt, beispielsweise vom Bundesgerichtshof:

„Das Recht auf informationelle Selbstbestimmung schützt ... davor, aus dem Bereich der Anonymität in den einer persönlichen Bekanntheit gerückt zu werden“ (BGH AfP 1994, 306, 307).

Auch der Rat für Forschung, Technologie und Innovation, der unter Federführung des Bundeskanzleramts und des Bundesministers für Bildung, Wissenschaft, Forschung und Technologie einen ausführlichen Bericht über Chancen, Innovationen und Herausforderungen der Informationsgesellschaft erstellt hat, hat das Thema Anonymisierung aufgegriffen. Der Rat führt in Kapitel 2.5 über Datenschutz Folgendes aus:

„Den Vorrang verdienen Verfahren, die den Betroffenen ein Höchstmaß an Anonymität gegenüber Netzbetreibern und Dienstleistungsanbietern sichern“.

Entsprechende Passagen finden sich auch in den Bundestags- und Bundesratsdrucksachen über „Deutschlands Weg in die Informationsgesellschaft“ wieder (Entschließung zu der Empfehlung an den Europäischen Rat „Europa und die globale Informationsgesellschaft“ und zu der Mitteilung der Kommission „Europas Weg in die Informationsgesellschaft: Ein Aktionsplan“, Bundesrat, Drucksache 776/96, 10.10.1996, Bonn).

Problematische Systemelemente

Betrachtet man traditionelle informationsverarbeitende Systeme in ihrer komplexen Gesamtheit, so sind einige klassische Einzelprozesse (Systemelemente) identifizierbar, in denen üblicherweise solche Daten, die zur Identifizierung des Benutzers geeignet sind, anfallen, bearbeitet und gespeichert werden:

1. Identifizierung/Identifikation
   Eine Identifizierung ist der Vorgang, der zum eindeutigen Erkennen einer Person oder eines Objektes dient (Feststellung der Identität einer Person).
2. Identitätsfeststellung
   Als Identitätsfeststellung wird die Überprüfung bezeichnet, welche Personalien (Identität) einer natürlichen Person zuzuordnen sind.
3. Authentisierung
   Authentisierung ist der Vorgang des Nachweises der eigenen Identität.
4. Authentifizierung
   Authentifizierung ist der Vorgang der Überprüfung (Verifikation) der behaupteten Identität eines Gegenübers.
5. Autorisierung
   Autorisierung bezeichnet in der Informationstechnologie die Zuweisung und Überprüfung von Zugriffsrechten auf Daten und Dienste an Systemnutzer. Die Autorisierung erfolgt meist nach einer erfolgreichen Authentifizierung.
6. Zugriffskontrolle
   Prüfung des Berechtigungsprofils relativ zu der gewünschten Aktion/Dienstleistung des Systems.

7. Protokollierung
   Festhalten von Aktionen gemeinsam mit Angaben zum Benutzer zum Zwecke der Nachweisführung.
8. Abrechnung
   Rechnungsstellung der erbrachten und in Anspruch genommenen Systemleistungen an den Benutzer.

Als Begründung für die jeweils erhobenen, anfallenden, gespeicherten und verarbeiteten personenbezogenen Daten werden überwiegend Abrechnungszwecke, verbesserte Kundenbetreuung, statistische sowie Kontrollzwecke angegeben.

Identitätsfeststellung des Benutzers nicht erforderlich

Die Feststellung der tatsächlichen Identität des Benutzers ist für die Funktionalität eines IuK-Systems grundsätzlich jedoch nicht erforderlich. Allenfalls in bestimmten Fällen zur Autorisierung, Abrechnung und Protokollierung könnte die tatsächliche Identität des Benutzers erforderlich sein und müsste dort offen gelegt werden bzw. bekannt sein. In den übrigen Prozessen ist dies nicht notwendig.

Wenn in einem System stattfindende Aktionen nachträglich kontrolliert werden müssen, so ist eine Protokollierung erforderlich. So ist z. B. die in den Datenschutzgesetzen des Bundes und der Länder vorgeschriebene Eingabekontrolle (z. B. Nr. 5 der Anlage zu § 9 BDSG) in der Regel nur mit Hilfe der Protokollierung realisierbar, da die Zulässigkeit der Datenerhebung bzw. der Datenspeicherung nicht maschinell geprüft werden kann.

Bereits bei der Konzeption von IuK-Systemen sollte daher generell und für jeden einzelnen Prozess untersucht werden, ob Daten zur wahren Identität des Einzelnen zur Verfügung stehen müssen oder ob eine anonyme oder pseudonyme Gestaltung infrage kommt.

Technikfolgenabschätzung

Soweit diese Feststellungen weiter Gültigkeit beanspruchen, muss sich der Gesetzgeber aber im Rahmen einer vorausschauenden Technikfolgenabschätzung mit den Herausforderungen neuer Technologien und neuer Geschäftsfelder auseinandersetzen und die Frage beantworten, ob die bisherigen Konzeptionen zukunftsfest sind.

Datenschutzkonzeption zukunftsfest?

Ein Ausgangspunkt für Überlegungen zu einem Modernisierungsbedarf des Datenschutzrechtes in Deutschland besteht in der Analyse der Zukunftsfähigkeit der hieraus entwickelten Datenschutzkonzeptionen vor dem Hintergrund der Herausforderungen der Informationsgesellschaft durch technische und technologische Entwicklungen.

Dies kann und soll in der vorliegenden Stellungnahme nur schlaglichtartig erfolgen und basiert auf einem Kurzbericht des Arbeitskreises „Technische und organisatorische Datenschutzfragen“, den der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern leitet, wie er zur 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vorgelegt wurde.

Die folgenden Beispiele aktueller oder mittelfristig zu erwartender technischer Entwicklungen verändern unser alltägliches Leben und stellen vor allem die datenschutzrechtlichen Konzeptionen:

- Trennungsgebot,
- Transparenzgebot,
- Zweckbindungsgebot,
- Datenverarbeitung auf der Grundlage einer freiwilligen Einwilligung,
- Dezentralisierung vor Zentralisierung von Datenbeständen,
- Privilegierung der privaten Verwendung,
- Personenbeziehbarkeit von Daten als personenbezogene Daten,
- Grundrechtsschutz durch staatliche Überwachung im Wege einer Zufallskontrolle und die
- Wertungsunterschiede zwischen der Datenverarbeitung öffentlicher und nicht-öffentlicher Stellen

grundsätzlich infrage.

Konvergenz von Techniken und Netzen

Konvergenz bezeichnet allgemein das Zusammenstreben verschiedener Teilbereiche und deren Aufgehen in einem Ganzen neuer Qualität. Entwicklungen dieser Art können auf verschiedenen Gebieten der Technik beobachtet werden, unter anderem in der Telekommunikation. Beispielsweise führt die Einführung von Voice over IP zu einer Konvergenz zwischen Sprach- und Datennetzen. Auch das unten erwähnte Triple Play resultiert aus einer Konvergenz von Kabelfernsehnetzen, Datennetzen und klassischen Telefonnetzen.

2. Besondere Risikofelder

Neben den spezifischen Risiken, die von den einzelnen Diensten ausgehen, sind Wechselwirkungen und Kumulationseffekte zu befürchten (Beispiele: siehe unter IPTV und Triple Play), die eine datenschutzrechtliche Regelung zunehmend erschweren.

IPTV

IPTV ist die Übertragung von Fernsehen und Filmen über digitale Datennetze mit Hilfe des IP (Internet Protocol), auf dem auch die Datenübertragung im Internet basiert. Datenschutzrechtlich interessant sind hier sogenannte Rückkanäle, mit denen die Nutzer Kontakt zu den Programmveranstaltern aufnehmen können. Über solche Rückkanäle können Nutzer beispielsweise weitere Daten vom Anbieter oder Dritten abrufen oder spielen.

Mittlerweile haben einige Anbieter in Metropolregionen IPTV auf den Markt gebracht. Eine weitere Möglichkeit, die jedoch bislang selten angeboten wird, ist die gezielte Bestellung von Filmen (Video on Demand). Die Übertragung der Fernsehsignale erfolgt häufig nicht in offenen Netzen wie dem Internet, Rückkanäle werden jedoch in der Regel über das Internet aufgebaut. Hier werden insbesondere Daten zu den (Medien-)Konsumgewohnheiten übertragen.

In Abhängigkeit davon, welche weiteren Dienste und Kommunikationsmöglichkeiten integriert sind, können auch Daten aus anderen Lebensbereichen übertragen werden. (Beispiel: In einer Fernsehsendung wird ein Auto einer bestimmten Marke gezeigt. Gleichzeitig kann der Zuschauer für dieses Auto eine Probefahrt beim nächstgelegenen Vertragshändler vereinbaren.) Diese können sowohl von den Anbietern selbst als auch von Dritten gesammelt und missbraucht werden („gläserner Zuschauer“).

Triple Play

Unter dem Stichwort Triple Play wird das gebündelte Anbieten von Fernsehen, Telefonie (z. B. als Voice over IP) und Internetzugang verstanden. Entsprechende Angebote werden derzeit beispielsweise von Kabelnetzbetreibern unterbreitet.

Neben den spezifischen Risiken, die von den einzelnen Diensten ausgehen, sind Wechselwirkungen und Kumulationseffekte zu befürchten. Insbesondere können sich Sicherheitslücken in einem Dienst auf einen anderen auswirken (z. B. von IPTV auf den Internetzugang, der gegebenenfalls zum Electronic Banking benutzt wird). Datensammlungen eines Triple-Play-Anbieters können zur Bildung umfassenderer Profile führen, als bei Anbietern von Einzeldiensten.

Spam/UBE

Spam oder UBE (unsolicited bulk e-mail) ist unerwünschte elektronische Post. Spam führt zu erheblichen Produktivitätsverlusten bei der Nutzung des Mediums E-Mail. Viele der Spam-Absender residieren im Ausland und können so kaum belangt werden, obwohl ihr Handeln in immer mehr Rechtsordnungen strafbar ist.

Spam ist ein Massenphänomen. Spam gefährdet die Verfügbarkeit des E-Mail-Dienstes, weil der massenweise Eingang von Nachrichten zur Überlastung der Empfängersysteme führen kann. Um dem Spam-Aufkommen zu begegnen, setzen viele Anwender Filtermechanismen ein. Filter müssen den Kopfzeilen wie Absender und Betreff und Versandweg sowie den Inhalt der Nachrichten auswerten, um diese sinnvoll klassifizieren zu können. Dabei besteht die Gefahr, dass auch Unbefugte E-Mails lesen können. Außerdem können Nachrichten infolge einer fehlerhaften Klassifikation unterdrückt werden.

Utility Computing und Application Service Providing

Unter Utility Computing werden Techniken und Geschäftsmodelle verstanden, mit denen ein Service Provider seinen Kunden (standardisierte) IT-Dienstleistungen zur Verfügung stellt, die nach Verbrauch abgerechnet werden („IT aus der Steckdose“). Der Begriff Application Service Providing ist nahezu synonym.

Es gibt Application Service Provider am Markt, das Geschäftsmodell ist zumindest in einigen Bereichen etabliert. Künftig wird mit einer höheren Marktdurchdringung zu rechnen sein.

Utility Computing ist praktisch immer Datenverarbeitung im Auftrag. Diese Art von Dienstleistungen dürften künftig immer stärker standardisiert werden, sodass der Auftraggeber immer weniger Informatik-Wissen für Einkauf und Betrieb dieser Leistungen benötigt. Der Application Service Provider gestaltet die Technik weitgehend selbst und könnte daran interessiert sein, dass wichtige Gestaltungselemente als Betriebsgeheimnisse angesehen werden. Dies führt dazu, dass die Auftraggeber ihre Verantwortung bei der Auswahl und der Überwachung des Auftragnehmers immer schlechter wahrnehmen können.

Web 2.0

Bei Web 2.0 handelt es sich um einen unscharfen und umstrittenen Begriff, der neue interaktive Dienste im Internet und eine geänderte Wahrnehmung des Internet beschreiben soll. Dem Web 2.0 zugerechnete Anwendungen basieren technisch häufig auf Web-Service-APIs, Ajax (Asynchronous JavaScript and XML) und Abonnement-Diensten wie RSS. Auch die Integration von sogenannter sozialer Software wie Blogs und Wikis wird als Teil des Web 2.0 angesehen.

In der Wahrnehmung der Netzteilnehmer verschwindet zusehends die Trennung zwischen lokaler und zentraler Datenhaltung, lokalen und netzbasierten Anwendungen, Editoren und Nutzern sowie zwischen einzelnen Diensten. Außerdem können Anwendungen viel einfacher und mitunter ohne Programmierkenntnisse erstellt oder neu zusammengesetzt werden (siehe auch Webanwendungen).

In diesem Zusammenhang postulieren einige Autoren das Ende des Software-Lebenszyklus, weil sich die neuen Anwendungen ständig im Beta-Stadium befinden. Kritiker wie Tim Berners-Lee vom W3C lehnen den Begriff Web 2.0 ab, weil niemand angeben könne, was er bedeutet. Vom W3C wurde der verwandte Begriff „Semantic Web“ (semantisches Web) geprägt: Maschinenlesbare Daten sollen nach diesem Konzept die Semantik der Web-Inhalte zum Ausdruck bringen und damit vielfältige Möglichkeiten der Verknüpfung und Auswertung bieten. Die erwähnten Techniken sind am Markt verfügbar.

Die genannten Anwendungen führen häufig zur Veröffentlichung von Daten des Anwenders oder seines sozialen Umfeldes. Außerdem werden oft Nutzerprofile gebildet. Ob sich alle Anwender der möglichen Folgen bewusst sind, muss bezweifelt werden. Nach Medienberichten sind Anwender beispielsweise von den Folgen der Veröffentlichung von privaten Videoclips überrascht worden.

Wichtig sind in diesem Zusammenhang jedoch vor allem die Folgen für Dritte. Eine weitere Auswirkung könnte darin bestehen, dass die Anwender Techniken aus diesem Bereich in ungeeigneten Umgebungen nutzen (beispielsweise unausgereifte Webanwendungen in ihrem Arbeitsumfeld zu dienstlichen Zwecken).

Standortbezogene Dienste

Standortbezogene Dienste sind über ein Netzwerk erbrachte mobile Dienste, die positions- und gegebenenfalls zeit- oder personenabhängig sind.

Am Markt verfügbar sind insbesondere standortbezogene Dienste im Bereich des GSM- oder UMTS-Mobilfunks, wie Routenplaner, Restaurant-Finder oder Positionsbestimmungen des eigenen oder eines fremden Mobiltelefons. Dienste dieser Art können zu umfangreichen Bewegungsprofilen führen, die mit weiteren Daten über Tätigkeiten, Beziehungen oder Vorlieben des Benutzers angereichert sind. Standortbezogene Dienste können als Vorstufe des Ubiquitous Computing (siehe dort) angesehen werden.

Elektronische Ausweisdokumente; Biometrie in Ausweisen

In Ausweisdokumenten sollen in zunehmendem Maße biometrische Daten gespeichert werden. Außerdem ist offenbar geplant, auch Kryptochips und Schlüsselmaterial dort zu integrieren.

Hinsichtlich der Speicherung biometrischer Daten stellen sich zahlreiche Fragen, welche die Qualität der verwendeten Verfahren betreffen. So ist nach der Zuverlässigkeit bei der Erzeugung der Referenzdaten (Enrolment) sowie der Wiedererkennung (Parameter wie Falschzulassungsrate und Falschabweisungsrate) und nach der Langzeitstabilität zu fragen. Wichtig ist auch, ob die biometrischen Daten fälschungssicher und vertraulich gespeichert werden und wer darauf zugreifen kann (Gestaltung und Überwindungssicherheit des Zugriffsschutzes).

Werden Kryptochips samt Schlüsselmaterial in die Ausweise integriert, sind insbesondere das Schlüsselmanagement und der Zugriffsschutz zu prüfen.

RFID

Radio-Frequency Identification (RFID) Technologie wird zunehmend für eine Reihe unterschiedlicher Zwecke eingesetzt. Während es Situationen gibt, in denen diese Technologie positive und günstige Auswirkungen hat, sind auch negative Folgen für die Privatsphäre möglich. RFID-Etiketten werden bisher vorwiegend zur Identifikation und Organisation von Gegenständen (Produkten), zur Kontrolle der Logistik oder zum Schutz der Authentizität einer Produktmarke (Warenzeichen) verwendet; sie können aber auch mit personenbezogenen Informationen wie Kreditkarten-Daten verknüpft werden und auch zur Erhebung solcher Informationen oder zur Lokalisierung oder Profilbildung über Personen benutzt werden, die Gegenstände mit RFID-Etiketten besitzen.

Diese Technologie würde die unbemerkte Verfolgung und das Aufspüren von Individuen ebenso wie die Verknüpfung erhobener Daten mit bestehenden Datenbanken ermöglichen. (Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 2004 in Saarbrücken, Entschließung der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vom 20. November 2003). Der Arbeitskreis Technik der Konferenz hat inzwischen zum Thema eine Orientierungshilfe verabschiedet (www.datenschutz-mv.de/dschutz/informat/rfid/ohrifd.pdf).

Voice over IP

Die Internet-Telefonie verbreitet sich rasant. Mittlerweile bieten alle großen Provider in Deutschland das Telefonieren über das Internet an. Dabei ist den Kundinnen und Kunden oft nicht bekannt, dass diese Verbindungen oft unsicherer sind als ein Telefongespräch über das herkömmliche Festnetz. Während nämlich bei separaten, leitungsvermittelten Telekommunikationsnetzen Sicherheitskonzepte vorzulegen sind, ist dies bei VoIP bisher nicht die Praxis.

Bei Telefongesprächen über das Internet kommt die Internet-Technologie Voice over IP (VoIP) zum Einsatz. Dabei werden Sprach-Daten mit Hilfe des aus der Internetkommunikation bekannten Internet-Protokolls (IP) in Datenpakete unterteilt und paketweise über bestehende lokale Computernetze und/oder das offene Internet übermittelt.

Eine derartige Integration von Sprache und Daten in ein gemeinsames Netzwerk stellt den Datenschutz vor neue Herausforderungen. Das Fernmeldegeheimnis ist selbstverständlich auch für die Internet-Telefonie zu gewährleisten. Die aus der Internetnutzung und dem Mail-Verkehr bekannten Unzulänglichkeiten und Sicherheitsprobleme können sich bei der Integration der Telefonie in die Datennetze jedoch auch auf die Inhalte und näheren Umstände der VoIP-Kommunikation auswirken und den Schutz des Fernmeldegeheimnisses beeinträchtigen. Beispielsweise können VoIP-Netzwerke durch automatisierte Versendung von Klingelrundrufen oder Überflutung mit Sprachpaketen blockiert, Inhalte und nähere Umstände der VoIP-Kommunikation mangels Verschlüsselung ausgespäht, kostenlose Anrufe durch Erschleichen von Authentifizierungsdaten geführt oder Schadsoftware wie Viren oder Trojaner aktiv werden.

Darüber hinaus ist nicht auszuschließen, dass das Sicherheitsniveau der vorhandenen Datennetze negativ beeinflusst wird, wenn sie auch für den VoIP-Sprachdaten-Verkehr genutzt werden.

Personenbezogene Daten der VoIP-Nutzenden können außerdem dadurch gefährdet sein, dass Anbieter von VoIP-Diensten ihren Sitz mitunter im außereuropäischen Ausland haben und dort möglicherweise weniger strengen Datenschutzanforderungen unterliegen als Anbieter mit Sitz in der Europäischen Union (EU). (Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. Oktober 2005 in Lübeck, der BfDI erstellt zurzeit eine Handlungsempfehlung zu diesem Thema und unterstützt das BSI bei der Formulierung datenschutztechnischer Handlungsempfehlungen.)

SPIT

SPIT (SPam over IP Telephony) ist das massenhafte automatisierte Anrufen von VoIP-Telefonen. SPIT ist die Weiterentwicklung der automatisierten Anrufe, die bereits heute zu Werbezwecken eingesetzt werden. SPIT ist jedoch erheblich billiger als ein automatischer Anruf, weil keine spezielle Hardware erforderlich ist und weil die Verbindungskosten verschwindend gering sind. Mit der zunehmenden Nutzung von VoIP ist auch mit dem Auftreten von SPIT zu rechnen.

Es ist mit vergleichbaren Auswirkungen wie bei Spam zu rechnen (siehe dort). Unerwünschte Anrufe, die nicht ausgefiltert werden, greifen jedoch erheblich stärker in die Privatsphäre des Betroffenen ein als unerwünschte E-Mails, da solche Anrufe zu jeder Zeit eingehen können und nach sofortiger Aufmerksamkeit und Reaktion verlangen.

Identitätsmanagement

Unter Identitätsmanagement versteht man das Verwalten von Identitäten und/oder von Identitätsdaten. Hierbei handelt es sich um zu einer (natürlichen) Person gehörende Daten (die nicht notwendigerweise für alle Datenverarbeiter auch unmittelbar personenbezogen sein müssen). Ein Identitätsmanagementsystem ist ein IT-System (einschließlich organisatorischer Komponenten), das Identitätsmanagement unterstützt. Insoweit handelt es sich bei dem Wort „Identitätsmanagement“ um einen Sammelbegriff, der für eine Vielzahl von bereits bestehenden datenschutzrelevanten Techniken verwendet werden kann.

Heutzutage findet man drei hauptsächliche Ausprägungen vor, die häufig in Mischformen vorkommen:

1. Accountmanagement innerhalb einer Organisation, was Authentisierung, Autorisierung und Accounting umfasst, z. B. mit Hilfe von Verzeichnisdiensten und Single Sign-On-Lösungen;
2. Profiling von Nutzerdaten von Organisationen, z. B. mit Hilfe von Data Warehouses;
3. Nutzerkontrolliertes, kontextabhängiges Pseudonym- und Rollenmanagement, wobei sich Teilfunktionalität z. B. in E-Mail-Clients, Internet-Browsern oder Form-Fillern findet.

Viele Identitätsmanagementsysteme oder Teilkomponenten sind bereits auf dem Markt. Der Grad der Selbstbestimmung und Transparenz für den Nutzer unterscheidet sich stark in den verschiedenen Systemen. Parallel zu den Fortschritten, die Profiling-Techniken machen, und deren zunehmender Verbreitung zeigt sich in anderen Bereichen des Identitätsmanagements ein Trend weg von rein zentralisierten Speicher- und Managementkonzepten hin zu einem verstärkten Einbeziehen des Nutzers. Es gibt datenminimierende Techniken wie die „anonymen Credentials“, bei denen Nutzer ihre erworbenen Berechtigungen in Form von Zertifikaten unter verschiedenen Pseudonymen nachweisen können, ohne dass dies verkettbar wäre.

An vielen Stellen und bei vielen Beteiligten können beim Identitätsmanagement Daten anfallen, deren Verkettbarkeit zueinander und zu Personen im Einzelfall zu untersuchen ist. Auch der Nutzer selbst kann grundsätzlich große Teile seiner Kommunikation mitspeichern und verfügt damit in der Regel nicht nur über eine gute Übersicht seines eigenen digitalen Lebens, sondern diese Daten betreffen häufig auch seine Kommunikationspartner und damit Daten von anderen Personen und Organisationen.

Verbindung von Videoüberwachung, Biometrie, RFID

Videoüberwachung, biometrische Identifikationsverfahren und RFID sind bereits oder werden demnächst massenweise verfügbar.

Damit rückt auch die Vernetzung dieser Techniken in greifbare Nähe. Dies könnte zu einer Bildung von sehr aussagekräftigen Bewegungsprofilen von Menschen führen. Es erscheint möglich, sowohl große Personengruppen (z. B. Kunden oder Benutzer einer bestimmten Institution) als auch Einzelpersonen gezielt zu überwachen.

Ubiquitous Computing/Pervasive Computing/Ambient Intelligence/Smart Dust

Ubiquitous Computing (ubiquitäre/allgegenwärtige Computertechnik, Abk. UbiComp) bezeichnet die Allgegenwärtigkeit von Informationsverarbeitung im Alltag von Menschen in verschiedenen Lebensbereichen. Computer werden in die Umgebung eingebettet und bilden ein mobiles Netz, dessen Teile sich ständig ändern können und das sich selbst organisiert bzw. konfiguriert. Mit diesem Begriff verwandt sind Pervasive Computing (alles/den gesamten Alltag durchdringende Computertechnik), Ambient Intelligence (Umgebungsintelligenz) und Smart Dust (intelligenter Staub = extrem miniaturisierte Computer, die beispielsweise mit Sensoren ausgestattet sind). Erste Entwicklungen sind am Markt verfügbar. Hierzu zählen beispielsweise RFID-Tags.

Bei UbiComp lässt sich immer schwerer eine datenverarbeitende Stelle sinnvoll festlegen bzw. ermitteln. Auch der Begriff der Datenübermittlung passt innerhalb einer UbiComp-Umgebung kaum noch. Demgegenüber können sich in UbiComp-Netzwerken je nach Gestaltung unterschiedliche, gegebenenfalls sensible Lebensgewohnheiten widerspiegeln oder durch Profilbildung ermittelt werden.

Quantenkryptographie

Durch Nutzung von Effekten aus der Quantenphysik hoffen Forscher, eine Klasse von Computern schaffen zu können, die bestimmte Aufgaben wesentlich effizienter löst als die jetzt verfügbaren Rechner. Mit solchen Geräten könnten insbesondere heute übliche kryptographische Verfahren gebrochen werden. So ist bereits ein Algorithmus bekannt, mit dem das Problem der Faktorisierung mit geringem Aufwand gelöst und so Kryptoverfahren wie RSA gebrochen werden können (sogenannter Shor-Algorithmus).

Quanteneffekte lassen sich aber auch zu neuen Formen geheimer Kommunikation nutzen, bei denen der Empfänger von Nachrichten jeden Abhörversuch bemerkt (zum Beispiel beim sogenannten BB84-Protokoll).

Quantencomputer sind derzeit als Labormuster sehr geringer Leistung verfügbar. Quanteneffekte konnten bereits erfolgreich zur Geheimhaltung von Nachrichten genutzt werden; hierzu gibt es Labormuster bzw. Prototypen. Quantencomputer stellen künftig ein enormes Risiko für die Vertraulichkeit, Integrität und Zurechenbarkeit von Daten dar, die mit heutigen kryptographischen Methoden gesichert werden. Quantenkryptographie stellt hier einen Ausweg dar.

Mittels Quantenkryptographie gesicherte Nachrichten lassen sich auch von solchen Stellen nicht unbemerkt abhören, denen dies gesetzlich zugestanden ist.

Nanotechnologie

Nanotechnologie ist die populäre Umschreibung für Forschung in Physik, Chemie und Maschinenbau, die sich mit der Trennung, dem Zusammenbau und der Verformung von Werkstoffen auf der Ebene einzelner Atome und Moleküle beschäftigt. Die Eigenschaften solcher Werkstoffe werden viel stärker durch die Oberflächeneigenschaften und durch quantenmechanische Effekte bestimmt als bei herkömmlichen Materialien.

Auf diesem Gebiet wird derzeit vor allem Grundlagenforschung betrieben. Es gibt vereinzelte Anwendungen etwa bei der Veredelung von Oberflächen und in der medizinischen Diagnostik und Therapie. Viele Auswirkungen der Nanotechnologie sind jedoch noch nicht ausreichend verstanden, so die Auswirkungen von Nanopartikeln auf die menschliche Gesundheit.

Die Nanotechnologie könnte zur Miniaturisierung, Leistungssteigerung und Verbilligung von Informations- und Kommunikationstechnik beitragen. Sie könnte auch die Entwicklung von Quantencomputern und Smart Dust beschleunigen. Dies kann sich mittelbar über die jeweiligen Basistechniken auf den Datenschutz auswirken.

Wegen des frühen Entwicklungsstandes der Nanotechnologie können Aussagen zu möglichen Folgen vorerst nur vage sein.

3. Rechtlicher Modernisierungsbedarf - eine Ethische Diskussion

Im gleichen Maße, wie der wirtschaftliche Wert personenbezogener Informationen steigt, scheint die gesellschaftliche Wertschätzung der Privatheit zu sinken. Im Schatten der sicherheitspolitisch determinierten politischen Diskussion eines angeblichen verfassungsmäßigen Rechtes auf „Sicherheit“ werden die bürgerlichen Freiheiten und insbesondere das Recht auf informationelle Selbstbestimmung zunehmend und - entgegen ständiger Beteuerungen dauerhaft - nicht nur im Bereich öffentlicher Datenverarbeitung eingeschränkt, sondern damit Individualität und Privatheit auch im nicht-öffentlichen Bereich delegitimiert.

Das „klassische“ Abwehrkonzept gegen staatliche Überwachung weicht zunehmend der Gefahr für die private Gestaltungsfreiheit durch die informationstechnische Vernetzung aller Lebensbereiche. Informationstechnik ist die bestimmende Infrastruktur für das öffentliche, das berufliche und immer mehr auch das private Umfeld der Menschen. Über diese Infrastruktur hat der Einzelne immer weniger Kontrolle, selbst ein kompletter Entzug ist real ohne gravierende Einschnitte in die Lebenswirklichkeit undenkbar geworden.

Datenschutz nach „Prinzip Zufall“

Diese fehlende Kontrollmöglichkeit können die Aufsichtsbehörden gegenwärtig nicht kompensieren, sondern üben ihren gesetzlichen Auftrag nach dem „Prinzip Zufall“ aus. Das Konzept der Transparenz zur Eröffnung einer Ausweichmöglichkeit erfüllt seine Funktion dann nicht mehr, wenn es keine Ausweichmöglichkeit mehr gibt. Die Einholung freiwilliger Einwilligungen wird zur wirkungslosen Bürokratie, wo die Nicht-Erteilung der Einwilligung zu erheblichen Nachteilen führt. Die Gefährdung für personenbezogene Daten durch zentrale Datenbestände ist keine besondere mehr, wenn die Vernetzung vieler kleiner Datenbestände durch den Einsatz von Recherchetechniken zum selben oder besseren Ergebnissen führt. Die Trennung zwischen öffentlichen und nicht-öffentlichen Bereich verliert ihren Schutzcharakter, wenn öffentliche Stellen auf die Datensammlungen von Privaten ungehindert zugreifen können und umgekehrt.

Jede Modernisierung ist nur eine Zwischenstation

„Für wie immer verstandene Modernisierungsversuche gilt nichts anderes als für alle bisherigen und künftigen Datenschutzregelungen. Sie entstehen im Vorzeichen einer sich ständig wandelnden Technologie und können deshalb nur so lange auf die Verwendung personenbezogener Daten Einfluss nehmen wie die mit ihr verbundenen sozialen und ökonomischen Folgen relativ konstant bleiben. Modernisierungen sind, anders und schärfer ausgedrückt, nicht mehr als Zwischenstationen eines unverändert offenen Regelungsprozesses.“ (Simitis, BDSG, 6. Aufl., Einl., Rn. 106)

Datenschutz als Grundrechtsgewährung

Maßstab in diesem Regelungsprozess muss die in der Entscheidung des Bundesverfassungsgerichtes konkretisierte Wertung des Grundgesetzes bleiben, dass die Selbstbestimmungsmöglichkeit des Einzelnen Funktionsbedingung für die Demokratie ist und bleibt. Diese Selbstbestimmungsmöglichkeit zu erhalten erfordert einerseits Zurückhaltung des Gesetzgebers bei der Anpassung der Datenschutzvorschriften an vermeintliche Sicherheitsinteressen, Globalisierungszwänge oder Innovationshemmnisse, andererseits effektive und unabhängige Aufsichtsbehörden in Verbindung mit gefährdungsadäquaten Sanktionsmöglichkeiten, schadensadäquaten Straftatbeständen und Ersatzpflichten auch für Nicht-Vermögensschäden bei Verletzungen dieses Rechtes durch öffentliche oder nicht-öffentliche Stellen.

4. Datenschutz-Audit

Die Auditierung von Produkten auf freiwilliger Basis ist ein erster Schritt zur Durchsetzung technischer Standards, die datenschutzgerechten Technologien zum Durchbruch verhelfen können. Aus den bisher als freiwillig konzipierten Produktauditierungen könnten technische Zulassungsverfahren entwickelt werden, die wie die Straßenverkehrszulassung neuer Fahrzeuge oder die Zulassung von Medikamenten die Unbedenklichkeit von IT-Produkten und -Verfahren gewährleisten.

Auditierung in Länderkompetenz

Der Vollzug des BDSG unterliegt gemäß Art. 83 GG der Länderkompetenz, womit auf die Aufsichtsbehörden nach BDSG die Aufgabe zukommt, eine einheitliche Ausgestaltung der Auditierungen fachlich kompetent und (wirtschafts-)politisch unabhängig i. S. der EG-Datenschutzrichtlinie sicherzustellen. Diese Unabhängigkeit ist neben der fachlichen Kompetenz, die personelle Ressourcen voraussetzt, die Grundvoraussetzung für eine Akzeptanz einer Auditierung.

Verfahren durch die Aufsichtsbehörden

Sie gewinnt für Hersteller und Anwender ihren entscheidenden Wert durch die sich hieraus ergebene Sicherheit auf Seiten beider Vertragspartner, dass die Datenschutzgerechtigkeit des zu verwendenden Produktes durch die gegebenenfalls prüfende Datenschutzaufsichtsbehörde festgestellt und bestätigt wurde.

Unabhängigkeit der Aufsichtsbehörden

Die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EG-Datenschutzrichtlinie) verlangt, dass die Einhaltung datenschutzrechtlicher Vorschriften in den Mitgliedsstaaten von Stellen überwacht wird, die ihre Aufsichtaufgaben in völliger Unabhängigkeit wahrnehmen. Die Unabhängigkeit ist eine Grundvoraussetzung für die Akzeptanz eines Auditierungsverfahrens. In vielen deutschen Bundesländern ist demgegenüber die Datenschutzaufsicht über die Privatwirtschaft (sogenannte nicht-öffentliche Stellen) immer noch in den jeweiligen Innenministerien angesiedelt und damit in den hierarchischen Weisungsstrang des Ministeriums eingebunden.

Diese Aufsichtsstruktur bei der Datenschutzkontrolle verstößt nach Feststellung der Europäischen Kommission gegen europäisches Recht und ist Gegenstand eines Vertragsverletzungsverfahrens gegen die Bundesrepublik Deutschland. In Mecklenburg-Vorpommern ist die Funktion der Aufsichtsbehörde gemäß § 33 a Landesdatenschutzgesetz (DSG M-V) 2004 dem Landesbeauftragten für den Datenschutz übertragen worden.

Koordinierung durch Düsseldorfer Kreis

Als Koordinierungsgremium der Aufsichtsbehörden verfügt der sogenannte Düsseldorfer Kreis infolge der geringen personellen Ausstattung der zuständigen Bereiche in den Innenministerien gegenwärtig weder über die personellen noch die fachlichen Ressourcen im IT-Bereich, um eine bundesweit koordinierte Auditierung sicherstellen zu können.

Audit auf landesrechtlicher Grundlage

Das DSG M-V regelt seit 2002 in § 5 Absatz 2:

„(2) Informationstechnische Produkte, deren Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit in einem Prüfverfahren festgestellt wurde, sollen vorrangig eingesetzt werden. Die Landesregierung regelt durch Rechtsverordnung Inhalt, Ausgestaltung und die Berechtigung zur Durchführung des Verfahrens.“

Der Landesgesetzgeber hat die Voraussetzungen dafür geschaffen, dass Hersteller und Vertriebsfirmen ihre IT-Produkte (Hardware, Software und Verfahren), die grundsätzlich auch für den Einsatz in der öffentlichen Verwaltung geeignet sind, auf ihre Datenschutzfreundlichkeit prüfen und im Erfolgsfalle mit einem Gütesiegel versehen lassen können. Dieses Datenschutzauditverfahren muss durch eine Rechtsverordnung geregelt werden.

Diese steht auch in Mecklenburg-Vorpommern seit 2002 immer noch aus. Hierfür wird seit Inkrafttreten der Regelung angeführt, dass auf die Umsetzung der bundesgesetzlichen Regelung gewartet werden soll, da nur eine bundesweite Verwendbarkeit des Audits sinnvoll sei.

Der Erlass einer solchen Verordnung würde nicht nur einen entscheidenden Qualitätsschritt für den präventiven Datenschutz im IT-Sektor bedeuten. Für die im Lande entwickelten IT-Produkte würde diese formelle Qualitätsbestätigung durch Auditierung zugleich auch einen nicht unbeträchtlichen Marketing- und Absatzfaktor darstellen. Hersteller und Vertriebsfirmen von IT-Produkten hätten bei einer Auditierung in Mecklenburg-Vorpommern Standortvorteile, denn nach § 5 Abs. 2 Satz 1 DSG M-V sind öffentliche Stellen des Landes grundsätzlich verpflichtet, vorrangig auditierte Produkte einzusetzen.

Auditierte Produkte im öffentlichen Bereich

Dementsprechend ist die gesamte Landes- und Kommunalverwaltung gehalten, bei Ausschreibungen zunehmend das Kriterium der Auditierung in die Anforderungskataloge aufzunehmen. Das Datenschutz-Gütesiegel wirkt im Ausschreibungsverfahren dann als Nachweis der datenschutzrechtlichen Zulässigkeit des Produktes. Es entlastet Verwaltung und Unternehmen von der ansonsten bei jeder Ausschreibung erforderlichen Einzelfallprüfung der Geeignetheit des Produktes für den geplanten Einsatz.

Vergaberechtlich zulässige Berücksichtigung

Eine solche Regelung begegnet auch keinen durchgreifenden vergaberechtlichen Bedenken, wenn die Verfahrensausgestaltung der Vergaben eine Gleichbehandlung auditierter Produkte mit solchen, die in vergleichbarer Weise ihre Eignung nachweisen, sicherstellt.

Eine Zertifizierung kann somit nur als Bevorzugung von Bietern in dem Sinne wirken, als bei ihnen die Vorlage von besonderen Eignungsnachweisen obsolet wird.

Wie bei der Ausschreibung mit Hilfe sogenannter „Leitprodukte" kann ein auditiertes Produkt mit dem Zusatz „oder gleichwertig" gefordert werden (vgl. § 8 Nr. 3 Abs. 5 VOL/A). Erforderlich ist aber, dass die Produkteigenschaften und Qualitätsanforderungen des auditierten Produkts allen Bietern bekannt sind oder sein können. Es ist ratsam, die Kriterien einer für das ausgeschriebene Produkt möglichen Auditierung in der Ausschreibung anzugeben.

Zugunsten der Anbieter auditierter Produkte kann - wie bei bieterbezogenen Anforderungen - darauf verzichtet werden, die Vorlage weiterer Nachweise (Gutachten, Prüfzeugnisse o. ä.) zu verlangen. Auf diese Weise werden einerseits Auditierungen bevorzugt, andererseits behalten andere Bieter die Chance zu belegen, dass ihre (bislang noch) nicht auditierten Produkte (mindestens) gleiche Anforderungen erfüllen wie die auditierten.

Marketinginstrument

Neben den Wettbewerbsvorteilen im Bereich der öffentlichen Verwaltung würde sich die Auditierung auch in der Privatwirtschaft positiv auf die Vermarktung des Produktes auswirken. Hersteller und Vertriebsfirmen könnten die Qualität ihres Produktes durch das Zertifikat in Werbung und Marketing absatzsteigernd hervorheben. Privaten Kaufinteressenten würde ein Produkt angeboten, das sich durch ein amtliches, datensicherheitstechnisch und datenschutzrechtlich relevantes „Prüfsiegel" gegenüber Konkurrenzprodukten positiv abhebt.

Kunden und Abnehmer könnten diese Datenschutzeigenschaften - gerade beim IT-Einsatz in sensiblen Bereichen - in ihre Kaufentscheidung einbeziehen.

Entlastung öffentlicher Vergabestellen

In der öffentlichen Verwaltung würde die Einführung eines Datenschutzaudits gleichzeitig die Arbeit der Vergabestellen entlasten, weil wesentliche technische Komponenten, deren Datenschutzniveau der Anwender oft nur schwer beurteilen kann, bereits vorab sachverständig geprüft sind. Hierin liegt der entscheidende Vorteil für die Aufsichtsbehörden in Prüfverfahren. Sie kann die Prüfung auf die Fragen der rechtlich zulässigen Anwendung der Technik beschränken. Die Prüfung der technischen Sicherheit des Produktes könnte entfallen, die hinsichtlich der datenschutzrechtlichen Zulässigkeit der konkreten Anwendungen erleichtert. Das Prüfverfahren im Rahmen der Vergabe würde beschleunigt und qualitativ verbessert.

E-Goverment nur mit Audit

In allen E-Goverment-Verfahren wird eine umfassende datenschutzrechtliche Prüfung erforderlich sein, die alle technischen Aspekte bereits in der Konzipierung mit einschließt. Ein Auditierungsverfahren würde hierfür den geeigneten rechtlichen und technischen Rahmen bieten.

Rechtsklarheit für Entwickler

Eine Auditierung trägt zu Rechtsklarheit in Verwaltung und Wirtschaft bei, da sie gleichzeitig ein einheitlich anzuwendender Verfahrensmaßstab nach transparenten, nachprüfbaren Kriterien ist. Diese helfen den Entwicklern in den Unternehmen bereits im Konzeptstadium von Produkten.

Kostenreduzierung

Die Anhebung des Datensicherheitsniveaus wirkt sich darüber hinaus auf die Betriebssicherheit der eingesetzten Systeme aus. Fehlerhafte und redundante Anwendungen werden verringert beziehungsweise ausgeschlossen. Bearbeitungszeiten werden verkürzt - die Gesamtkosten reduziert.

Die frühzeitige Berücksichtigung datenschutzrechtlicher Anforderungen verhindert nachträglichen Entwicklungs- und Kostenaufwand.

Entlastung der Aufsichtbehörden

Im Rahmen einer tiefgehenden Kontrolle technischer Einrichtungen durch die Aufsichtsbehörden wird regelmäßig ein Großteil der technischen Parameter geprüft, die auch im Rahmen einer Auditierung zu prüfen sein würden. Ein Audit-Verfahren muss mithin sicherstellen, dass alle Aufsichtsbehörden einheitliche Maßstäbe anlegen und die Ergebnisse gegenseitig anerkennen.

Wirksamkeitssteigerung von Prüfungen

Das Auditierungsverfahren für ein Produkt führt in dem Unternehmen zu einem Kompetenzzuwachs, der sich in den künftigen Produkten wiederfinden wird. Zugleich wird das Produkt selbst zum Werbeträger für Datenschutz und bedient so eine wachsende Nachfrage.

Entwurf einer Rechtsverordnung für M-V

Am 6. Dezember 2005 habe ich in Warnemünde einen Workshop „Datenschutz durch Technik“ durchgeführt, auf dem Mitarbeiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein die oben dargestellten Auswirkungen des Datenschutz-Gütesiegels eindrucksvoll dargestellt und mit Zahlen belegt haben. Des Weiteren wurden dort
- der Entwurf für eine Datenschutz-Gütesiegel-Verordnung Mecklenburg-Vorpommern,
- die Anforderungskataloge für die zu akkreditierenden Sachverständigen und
- für IT-Produkte

sowie die Bedingungen für die vergaberechtliche Zulässigkeit des Verfahrens diskutiert.

Verfahrensablauf

Das Auditierungsverfahren beginnt mit der Prüfung der Produkte durch unabhängige, beim Landesbeauftragten für den Datenschutz auf der Basis eines Informations- und Pflichtenkataloges für Sachverständige und sachverständige Prüfstellen akkreditierte Sachverständige anhand des von mir veröffentlichten Kriterienkataloges. Deren Gutachten bilden die Grundlage für die Entscheidung des Landesbeauftragten für den Datenschutz über die Erteilung des Gütesiegels.

Gutachterakkreditierung

Dieses Akkreditierungverfahren wäre ein weiterer Vorteil für die Wirtschaft im Land. Fachleute aus Mecklenburg-Vorpommern könnten so ihre Qualifikation im technischen und/oder rechtlichen Datenschutz quasi „öffentlich beglaubigt“ und zu weit geringeren Kosten als für eine öffentliche Bestellung und Vereidigung als Gutachter durch die IHK nach § 36 Gewerbeordnung nachweisen.

Elektronische Gesundheitskarte als Modellprojekt

Das SGB X regelt die Auditierungsmöglichkeit in § 78 c SGB X - unter der Überschrift Datenschutzaudit wie folgt:

„Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt. Die Sätze 1 und 2 gelten nicht für öffentliche Stellen der Länder mit Ausnahme der Sozialversicherungsträger und ihrer Verbände.“

Für die elektronische Gesundheitskarte nach § 291 a SGB V wäre bei Umsetzung des gesetzgeberischen Auftrages die Auditierung ein wirksamer Weg zur Akzeptanzsteigerung dieses wichtigen Infrastrukturprojektes, aber nur eines der Beispiele.

Anlage 4 Fachtagung 2006 und Unterlagen zum Audit

Anlage 4.1 Entwurf einer Datenschutzgütesiegel-Landesverordnung
Stand : 7. Dezember 2005

Entwurf

Landesverordnung über ein Auditverfahren zur Erteilung des Datenschutzgütesiegels im Land Mecklenburg-Vorpommern (Datenschutzgütesiegel-Landesverordnung - DSGü LVO M-V)

Vom 2006
(GVOBl. S. ... / GS M.-V. Gl. Nr. ...)

Aufgrund des § 5 Abs. 2 Satz 2 Landesdatenschutzgesetz - DSG M-V in der Fassung der Bekanntmachung vom 28. März 2002 (GVOBl. M-V S. 154), zuletzt geändert am (GVOBl. M-V S. ...) verordnet die Landesregierung:

Inhaltsübersicht

§ 1 Auditierung von IT-Produkten

(1) Informationstechnische Produkte (IT-Produkte) erhalten auf Antrag der Hersteller- oder Vertriebsfirmen vom Landesbeauftragten für den Datenschutz das Datenschutzgütesiegel, wenn das IT-Produkt den Rechtsvorschriften über den Datenschutz und die Datensicherheit entspricht. Das Gütesiegel wird auf der Grundlage des Anforderungskatalogs des Landesbeauftragten für den Datenschutz für die Begutachtung von IT-Produkten im Rahmen des Auditverfahrens erteilt. Es wird befristet. Es kann widerrufen werden, wenn die Voraussetzungen für die Erteilung nicht mehr vorliegen.

(2) IT-Produkte im Sinne dieser Verordnung sind Hardware, Software und Verfahren, die zur Nutzung durch öffentliche Stellen des Landes Mecklenburg-Vorpommern geeignet sind.

(3) Erfolgreich auditierte IT-Produkte können durch ein Gütesiegel nach der Anlage zu dieser Verordnung gekennzeichnet werden. Die Anlage ist Bestandteil dieser Verordnung. Das Gütesiegel muss die Registrierungsnummer und die Gültigkeitsdauer enthalten. Das graphische Symbol darf die in der Anlage dargestellte Mindestgröße nicht unterschreiten.

(4) Der Landesbeauftragte für den Datenschutz führt ein Register über alle IT-Produkte mit Gütesiegel, das dort eingesehen werden kann und in geeigneter Weise veröffentlicht wird.

(5) Für IT-Produkte, die nach einem vergleichbaren Auditverfahren beim Bund oder in einem anderen Bundesland ein Gütesiegel erhalten haben, stellt der Landesbeauftragte für den Datenschutz auf Antrag fest, ob die Voraussetzungen des § 5 Abs. 2 Satz 1 DSG M-V erfüllt sind. Für IT-Produkte nach Satz 1 ist in der Regel keine gesonderte Auditierung gemäß Absatz 1 erforderlich.

§ 2 Verfahren

(1) Voraussetzung für einen Antrag nach § 1 Abs. 1 ist die Überprüfung des IT-Produktes durch hierfür vom Landesbeauftragten für den Datenschutz anerkannte Sachverständige nach § 3. Die Sachverständigen sind von den Hersteller- oder Vertriebsfirmen zu beauftragen.

(2) Erfüllt ein IT-Produkt nach den Feststellungen des Sachverständigen die datenschutzrechtlichen Anforderungen, legt der Antragsteller das entsprechende Gutachten mit einer schriftlichen Dokumentation der Prüfung dem Landesbeauftragten für den Datenschutz mit folgenden Angaben vor:

1. Zeitpunkt der Prüfung,
2. detaillierte Bezeichnung des IT-Produktes,
3. Zweck und Einsatzbereich,
4. besondere Eigenschaften des IT-Produktes, insbesondere zur Datenvermeidung (§ 5 Abs. 1 Satz 1 DSG M-V), Datensicherheit (§§ 21 und 22 DSG M-V), Gewährleistung der Rechte der Betroffenen (§§ 24 bis 27 DSG M-V),
5. Bewertung der besonderen Eigenschaften,
6. Zusammenfassung der Prüfung zum Zweck der Veröffentlichung durch den Landesbeauftragten für den Datenschutz.

Der Landesbeauftragte für den Datenschutz kann ergänzende Angaben und die Vorlage des zu auditierenden IT-Produktes anfordern.

§ 3 Anerkennung von Sachverständigen

(1) Der Landesbeauftragte für den Datenschutz erteilt die Anerkennung zum Sachverständigen auf Antrag, wenn die erforderliche Fachkunde, Zuverlässigkeit und Unabhängigkeit nachgewiesen wird. Die Erteilung der Anerkennung erfolgt auf der Grundlage des Pflichtenkatalogs für Sachverständige des Landesbeauftragten für den Datenschutz. Sie kann fachlich beschränkt werden, wenn die Fachkunde nur für einen Teilbereich des Datenschutzes besteht. Die Voraussetzungen für die Anerkennung erfüllt in der Regel auch, wer durch eine vergleichbare Anerkennung als Sachverständiger beim Bund oder einem anderen Bundesland zugelassen wurde.

(2) Liegen die Voraussetzungen für eine Anerkennung nach Abs. 1 nicht mehr vor, widerruft der Landesbeauftragte für den Datenschutz die Anerkennung.

(3) Der Landesbeauftragte für den Datenschutz führt eine Liste der anerkannten Sachverständigen, die auch fachliche Beschränkungen der Prüfungstätigkeit ausweist. Die Liste kann beim Landesbeauftragten für den Datenschutz eingesehen und in geeigneter Weise veröffentlicht werden.

§ 4 Gebühren

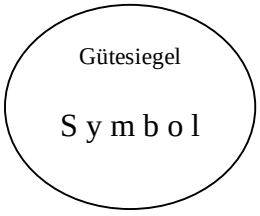
Der Landesbeauftragte für den Datenschutz kann für die ihm durch diese Verordnung übertragenen Aufgaben Gebühren nach Maßgabe einer Gebührenordnung erheben.

§ 5 Inkrafttreten

Diese Verordnung tritt am Tage nach ihrer Verkündung in Kraft.

Anhang:

Gütesiegel



Bei der Darstellung des Gütesiegels soll eine Größe von 24 mm Durchmesser nicht unterschritten werden. Es ist zusammen mit dem folgenden Text zu verwenden:

„Vom Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern zum Einsatz bei öffentlichen Stellen in Mecklenburg-Vorpommern empfohlen gemäß § 5 Abs. 2 DSG M-V. Registriernummer (lfd. Nr.), [befristet bis (Datum)], weitere Informationen unter www.datenschutz-mv.de.“

Anlage 4.2 FAQ zum Datenschutz-Audit-Projekt des Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern

1) Wird das Gütesiegel bundesweit anerkannt?

Es versteht sich von selbst, dass keinem Hersteller eines IT-Produkts zugemutet werden sollte, 16 oder 17 verschiedene Gütesiegel beantragen zu müssen, damit die Datenschutzfreundlichkeit des betreffenden Produktes bundesweit anerkannt wird. Der Verordnungsentwurf berücksichtigt dieses Anliegen in § 1 Abs. 5 und legt fest, dass für Produkte, die nach einem vergleichbaren Auditverfahren beim Bund oder in einem anderen Bundesland ein Gütesiegel erhalten haben, in der Regel keine gesonderte Auditierung erforderlich sein soll.

Darüber hinaus habe ich bereits Gespräche mit dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein mit dem Ziel geführt, ein unbürokratisches und transparentes Audit-Verfahren zu entwickeln. Ich strebe ein Antragsverfahren an, bei dem der Hersteller nur einen Ansprechpartner für den gesamten Audit-Prozess hat, unabhängig vom künftigen Einsatzort seines Produktes.

2) Haben die Marktführer Interesse an einem Datenschutz-Gütesiegel?

Es wird befürchtet, dass große Hersteller wie die Firma Microsoft wegen ihrer marktbeherrschenden Stellung kein Interesse an der Auditierung ihrer Produkte haben. Diese Befürchtung teile ich nicht.

Als Vorsitzender des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder stehe ich in engem Kontakt etwa zur Firma Microsoft. Microsoft ist maßgeblicher Initiator der Initiative „Deutschland sicher im Netz“. In der im Januar 2005 gestarteten bundesweiten Initiative haben sich unter Schirmherrschaft des Bundesministers für Wirtschaft und Arbeit namhafte Partner aus Politik, Wirtschaft und Gesellschaft zusammengeschlossen. Die Initiative will die Sicherheitsrisiken bei der Nutzung des Internet verringern, indem sie für ein sicherheitsbewusstes Verhalten im Umgang mit dem Internet sensibilisiert. In diesem Zusammenhang hat sich gerade die Firma Microsoft für das Produkt-Audit eingesetzt und prüft derzeit, welche Softwarebestandteile des eigenen Produktportfolios für die Erteilung des Datenschutz-Gütesiegels geeignet sind.

3) Rechnet sich das Produkt-Audit nur mit Fördermitteln?

Es wird vermutet, dass die Erfolge des Produkt-Audits in Schleswig-Holstein vorwiegend auf die Fördermittel zurückzuführen sind, die in den ersten drei Jahren nach Projektstart ausgereicht worden sind.

Nach Auslaufen der Förderung ging die Zahl der Audit-Verfahren jedoch nicht zurück, sondern stieg sogar an. Folgende Zahlen zu verliehenen Gütesiegeln in Schleswig-Holstein belegen dies:

- 2002: 1 Gütesiegel,
- 2003: 10 Gütesiegel (davon 9 gefördert),
- 2004: 7 Gütesiegel (davon 4 gefördert),
- Ende 2004: Auslaufen der Förderung,
- 2005: 13 Gütesiegel bis November, 2 Re-Zertifizierungen.

Dass diese Fördermöglichkeiten die Akzeptanz des Gütesiegels wesentlich unterstützt haben, ist sicher unstrittig. Vor diesem Hintergrund habe ich das Landesförderinstitut Mecklenburg-Vorpommern (LfI M-V) gebeten zu prüfen, ob das Audit-Verfahren auch in unserem Bundesland förderwürdig sei. Dies wurde mir ausdrücklich bestätigt (Zitat):

„Die (geförderte) Entwicklung und spätere Durchführung eines Datenschutz-Audits in Mecklenburg-Vorpommern kann damit in die Europäische Entwicklungsstrategie eingeordnet werden und ist prinzipiell aus den Strukturfonds ERFE und ESF (aus- und weiterbildungsbezogene Projektanteile) in der Förderperiode 2007 bis 2013 förderwürdig."

4) Kann der Wettbewerbsvorteil die Audit-Kosten aufwiegen?

Sicher wird nicht jeder Hersteller eines auditierten Produkts von messbaren Vermarktungsvorteilen berichten können. Einer Umfrage in Schleswig-Holstein zur Folge haben aber mehr als die Hälfte dieser Hersteller positive Erfahrungen gemacht und bestätigen, dass es einfacher war, Aufträge aus der Verwaltung und der Wirtschaft zu erhalten.

Auch das LfI M-V bestätigt in seiner Stellungnahme, dass das Angebot auditierter Produkte einen positiven Effekt auf die Wirtschaft der Region haben kann. Die Vertrauenswürdigkeit von IT-Produkten ist insbesondere bei internetbasierten Anwendungen ausschlaggebend für das Nutzerverhalten. Das LfI M-V stellt folgendes fest (Zitat):

„Für Unternehmen in Mecklenburg-Vorpommern, die zum Teil erheblich unter der geographischen Marktferne des Landes leiden, können sich hier hervorragende Chancen eröffnen. Für kleine und unbekannte Firmen ist aber für die Vermarktung der Vertrauensaspekt ein Erfolgskriterium. Die Verwendung staatlich zertifizierter und datenschutzrechtlich unbedenklicher DV-Anwendungen kann helfen, die Konversionsrate wesentlich zu steigern und damit den überregionalen Absatz einheimischer Unternehmen zu steigern."

5) Widerspricht die Verordnung dem Wunsch nach Deregulierung?

Eines der wohl bürokratischsten Vorgänge der öffentlichen Verwaltung ist das Beschaffungswesen. Sowohl das Erstellen von Angeboten seitens der Hersteller als auch das Auswerten dieser Angebote durch öffentliche Stellen ist regelmäßig mit einem erheblichen zeitlichen, finanziellen und personellen Aufwand verbunden. Hier sind wesentliche Vereinfachungen und Einsparungen zu erwarten, wenn das Vorhandensein eines Gütesiegels zu einem zusätzlichen Auswahlkriterium wird. Der Anbieter kann seine Produktbeschreibung wesentlich vereinfachen, indem er auf den Zertifizierungsreport verweist und der Einkäufer kann sich bei der Bewertung eines auditierten Produkts auf das Urteil eines externen Sachverständigen verlassen. Somit unterstützt die vorgeschlagene Landesverordnung für ein Audit-Verfahren die Bemühungen um Deregulierung.

Anlage 5 Organigramm

Der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern

Landesbeauftragter für Informationsfreiheit
Aufsichtsbehörde gemäß § 38 BDSG

Stand: 01.05.2008

Landesbeauftragter
Karsten Neumann
5 94 94-36

- europäischer und internationaler Datenschutz
- Grundsatzangelegenheiten der Informationsfreiheit

Vorzimmer
Ute Bache
5 94 94-35

LD 1 Recht, Verwaltung

Ina Schäfer
5 94 94-31

Birka Paul
5 94 94-53

Thomas Ahrens
behördlicher Datenschutzbeauftragter
5 94 94-32

- Grundsatzangelegenheiten
- des Datenschutzes
- Informationsfreiheit
- Justiz
- Polizei
- Verfassungsschutz
- Verkehr
- Ausländerrecht
- Finanzen und Steuern
- Telekommunikations-
- und Medienrecht
- Kommunal- und Einwohnerwesen
- Bau-, Wohnungs- und Liegenschaftswesen
- Statistik
- Religionsgesellschaften

LD 2 Wirtschaft und Soziales

Dr. Manfred Oberbeck
5 94 94-34

Rolf Hellwig
5 94 94-42

Hiltraud Bockholt
5 94 94-43

- Aufsicht nach BDSG
- Sozialversicherungen
- Gesundheitswesen
- Personalwesen
- Schulen, Hochschulen
- Wissenschaft, Forschung
- Land-, Forst- und Wasserwirtschaft
- Eigenbetriebe
- Umweltschutz
- gewerbliche Dienst-
- leistungen, freie Berufe
- Kredit- und Versicherungswirtschaft
- Handel und Versandhandel
- Auskunfteien
- SCHUFA
- Werbewirtschaft

LD 3 Technik, allg. Verwaltung

Gabriel Schulz
Stellvertreter
5 94 94-37

Technik

René Weichelt
5 94 94-41

Thomas Brückmann
5 94 94-51

- Informations- und Kommunikationstechnik
- E-Government
- Internet
- Betriebssysteme
- Netzwerke
- Standardsoftware
- Verschlüsselung, Signatur
- Biometrie
- baulicher Datenschutz
- Sicherheitskonzepte
- Verfahrensverzeichnis
- IT der Dienststelle

Verwaltung

Iris Dahlmann
5 94 94-45

Diana Lokatis
5 94 94-55

Carolin Dobschanski
5 94 94-57

Auszubildende/r
5 94 94-56

- Öffentlichkeitsarbeit
- Haushalt
- Personal
- Betreuung der Auszubildenden
- Schreibdienst
- Registratur
- Bibliothek
- Informationsmaterial

Besuchsanschrift
Johannes-Stelling-Straße 21
19053 Schwerin

Postanschrift
Schloss Schwerin
19053 Schwerin

Telefon: 03 85/5 94 94-0
Telefax: 03 85/5 94 94-58
E-Mail: datenschutz@mvnet.de
Internet: www.datenschutz-mv.de
www.informationsfreiheit-mv.de

Anlage 6 Aktenplan

0. Organisation, Verwaltung und Grundsatzangelegenheiten
0.1 Organisation
0.1.0 Allgemeines
0.1.1 Geschäftsverteilungs- und Organisationsplan
0.1.3 Aktenplan
0.1.4 Statistiken - eigene
0.1.5 Ordnungen und Regelungen
0.1.6 Veranstaltungen (eigene Vorträge unter 0.5.7)
0.1.7 Verschiedenes
0.2 Verwaltung
0.2.0 Allgemeines
0.2.1 Haushaltsplan, Stellenplan, Kassenwesen
0.2.2 Dienstgrundstück, Dienstgebäude, Diensträume, Kfz
0.2.3 Beschaffung und Materialverwaltung
0.2.4 Post und Telefax
0.2.5 Personal
0.2.6 Bibliothek
0.3 Zusammenarbeit, Sitzungen, Arbeitskreise, Landtag/Landesregierung,
0.3.0 Allgemeines
0.3.1 Konferenz der Datenschutzbeauftragten des Bundes und der Länder
0.3.2 Arbeitskreise/Arbeitsgruppen/Arbeitsgemeinschaften zu 0.3.1
0.3.3 Düsseldorfer Kreis (ab 2005)
0.3.4 Zusammenarbeit mit BfD, LfD, Aufsichtsbehörden und anderen Datenschutzbeauftragten
0.3.5 Zusammenarbeit mit Organisationen
0.3.6 Zusammenarbeit mit dem Landtag
0.3.7 Zusammenarbeit mit der Landesregierung und den Ministerien
0.3.8 Arbeitsgruppen des Düsseldorfer Kreises und Workshops der AB
0.3.9 Konferenz der Informationsfreiheitsbeauftragten (IFK) ehem. AGID
0.4 Datenschutz in den Ländern, beim Bund und im Ausland
0.4.0 Allgemeines, Hinweise, Informationen, Pressemitteilungen
0.4.1 Gesetze, Rechtsverordnungen, Verwaltungsvorschriften in den Ländern
0.4.2 Gesetze, Rechtsverordnungen, Verwaltungsvorschriften beim Bund
0.4.3 Tätigkeitsberichte - Pressemitteilungen (BfD/LfD/AB)
0.4.4 Arbeitsverzeichnis für Tätigkeitsberichte
0.4.5 Datenschutz im Ausland
0.4.6 Datenübermittlung ins Ausland
0.5 Presse/Öffentlichkeitsarbeit
0.5.0 Allgemeines
0.5.1 Organisation von eigenen Veranstaltungen
0.5.2 allgemeine Anfragen
0.5.3 Pressearbeit
0.5.4 Medienverteiler
0.5.5 Zusammenarbeit mit Dritten
0.5.6 Druckvorlagen; PDF-Dateien zur Veröffentlichung
0.5.7 Eigene Vorträge/angeforderte Manuskripte
0.5.8 Versand von Publikationen u. a. Materialien
0.6 Datenschutz in der EG/EU u. im Europarat

0.6.0 Allgemeines
0.6.1 EU-Richtlinien/Übereinkommen
0.6.2 Verordnungen
0.6.3 Sonstige Rechtsakte/Äußerungen der EU
0.6.4 Gerichtsentscheidung
0.6.5 Aufsätze/Literatur
0.6.6 Konferenzen
0.6.7 Europarat/OECD
0.6.8 Einzelprobleme

1. Datenschutz allgemein, Statistik, Religionsgesellschaften
1.0 Allgemeine Fragen des Datenschutzes
1.0.0 Allgemeines
1.0.1 Landesdatenschutzgesetz DSG M-V
1.0.2 Rechtsverordnungen
1.0.3 Verwaltungsvorschriften, Richtlinien, Erlasse
1.0.4 Gerichtsentscheidungen
1.0.5 Aufsätze
1.0.7 Kontroll- und Informationsbesuch
1.0.8 Einzelprobleme
1.0.9 BDSG (Grundsätzliche Auslegungsfragen)
1.1 Statistik und Wahlen
1.1.0 Allgemeines
1.1.1 Gesetze
1.1.2 Rechts- und EG-Verordnungen
1.1.3 Verwaltungsvorschriften, Richtlinien, Erlasse
1.1.4 Gerichtsentscheidungen
1.1.5 Aufsätze
1.1.7 Kontroll- und Informationsbesuche
1.1.8 Einzelprobleme
1.2 Religionsgesellschaften
1.2.0 Allgemeines
1.2.1 Evangelische Kirche
1.2.2 Katholische Kirche
1.2.3 Sonstige
1.2.4 Literatur
1.3 Medien in den Ländern
1.3.0 Allgemeines
1.3.1 Verfassungsbeschwerden/Gerichtsentscheidungen/Aufsätze
1.3.2 Rundfunk/Fernsehen
1.3.3 frei
1.3.4 Presse
1.3.5 Onlinedienste/Btx
1.4 Polizei und Verkehr
1.4.0 Allgemeines
1.4.1 Gesetze
1.4.2 Rechtsverordnungen
1.4.3 Verwaltungsvorschriften, Richtlinien, Erlasse
1.4.4 Gerichtsentscheidungen
1.4.5 Aufsätze

1.4.7 Kontroll- und Informationsbesuche
1.4.8 Einzelprobleme
1.5 Verfassungsschutz
1.5.0 Allgemeines
1.5.1 Gesetze
1.5.2 Rechtsverordnungen
1.5.3 Verwaltungsvorschriften, Richtlinien, Erlasse
1.5.4 Gerichtsentscheidungen
1.5.5 Aufsätze
1.5.7 Kontroll- und Informationsbesuche
1.5.8 Einzelprobleme
1.6 Rechtswesen
1.6.0 Allgemeines
1.6.1 Gesetze
1.6.2 Rechtsverordnungen
1.6.3 Verwaltungsvorschriften, Richtlinien, Erlasse
1.6.4 Verfassungsbeschwerden/Gerichtsentscheidungen
1.6.5 Aufsätze
1.6.7 Kontroll- und Informationsbesuche
1.6.8 Einzelprobleme
1.7 Finanzwesen
1.7.0 Allgemeines
1.7.1 Gesetze
1.7.2 Rechtsverordnungen
1.7.3 Verwaltungsvorschriften, Richtlinien, Erlasse
1.7.4 Gerichtsentscheidungen
1.7.5 Aufsätze
1.7.7 Kontroll- und Informationsbesuche
1.7.8 Einzelprobleme
1.8 Einwohnerwesen
1.8.0 Allgemeines
1.8.1 Gesetze
1.8.2 Rechtsverordnungen
1.8.3 Verwaltungsvorschriften, Richtlinien, Erlasse
1.8.4 Gerichtsentscheidung
1.8.5 Aufsätze
1.8.7 Kontroll- und Informationsbesuche
1.8.8 Einzelprobleme
1.9 Bau-, Wohnungs- und Liegenschaftswesen
1.9.0 Allgemeines
1.9.1 Gesetze
1.9.2 Rechtsverordnungen
1.9.3 Verwaltungsvorschriften, Richtlinien, Erlasse
1.9.4 Gerichtsentscheidungen
1.9.5 Aufsätze
1.9.7 Kontroll- und Informationsbesuche
1.9.8 Einzelprobleme

2 Sozialwesen, Sozialversicherungen, Gesundheitswesen, Personalwesen, Bildung und Kultur, Wissenschaft und Forschung, Wirtschaft
2.0 Allgemeines
2.0.1 Gesetze
2.0.3 Verwaltungsvorschriften, Richtlinien, Erlasse
2.0.4 Gerichtsentscheidungen
2.0.5 Veröffentlichungen
2.0.7 Kontroll- und Informationsbesuche
2.0.8 Einzelprobleme
2.1 Sozialwesen
2.1.0 Allgemeines
2.1.1 Gesetze
2.1.2 Rechtsverordnungen
2.1.3 Verwaltungsvorschriften, Richtlinien, Erlasse
2.1.4 Gerichtsentscheidungen
2.1.5 Veröffentlichungen
2.1.7 Kontroll- und Informationsbesuche
2.1.8 Einzelprobleme
2.2 Sozialversicherungen
2.2.0 Allgemeines
2.2.1 Sozialversicherung
2.2.2 Rentenversicherung
2.2.3 Krankenversicherung
2.2.4 Unfallversicherung
2.2.5 Pflegeversicherung
2.2.7 Kontroll- und Informationsbesuche
2.2.8 Einzelprobleme
2.3 Gesundheitswesen
2.3.0 Allgemeines
2.3.1 Gesetze
2.3.2 Rechtsverordnungen
2.3.3 Verwaltungsvorschriften, Richtlinien, Erlasse
2.3.4 Gerichtsentscheidungen
2.3.5 Veröffentlichungen
2.3.7 Kontroll- und Informationsbesuche
2.3.8 Einzelprobleme
2.4 Personalwesen
2.4.0 Allgemeines
2.4.1 Gesetze
2.4.2 Rechtsverordnungen
2.4.3 Verwaltungsvorschriften, Richtlinien, Erlasse
2.4.4 Gerichtsentscheidungen
2.4.5 Veröffentlichungen
2.4.7 Kontroll- und Informationsbesuche
2.4.8 Einzelprobleme
2.5 Bildung, Kultur, Wissenschaft und Forschung
2.5.0 Allgemeines
2.5.1 Gesetze
2.5.2 Rechtsverordnungen

2.5.3 Verwaltungsvorschriften, Richtlinien, Erlasse
2.5.4 Gerichtsentscheidungen
2.5.5 Veröffentlichungen
2.5.7 Kontroll- und Informationsbesuche
2.5.8 Einzelprobleme
2.6 Wirtschaft, Gewerbe
2.6.0 Allgemeines
2.6.1 Gesetze
2.6.2 Rechtsverordnungen
2.6.3 Verwaltungsvorschriften, Richtlinien, Erlasse
2.6.4 Gerichtsentscheidungen
2.6.5 Veröffentlichungen
2.6.7 Kontroll- und Informationsbesuche
2.6.8 Einzelprobleme
2.7 Land-, Forst-, Wasserwirtschaft und Umweltschutz
2.7.0 Allgemeines
2.7.1 Gesetze
2.7.2 Rechtsverordnungen/Satzungen
2.7.3 Verwaltungsvorschriften, Richtlinien, Erlasse
2.7.4 Gerichtsentscheidungen
2.7.5 Veröffentlichungen
2.7.7 Kontroll- und Informationsbesuche
2.7.8 Einzelprobleme
2.8 Nicht öffentlicher Bereich
2.8.0 Allgemeines
2.8.1 Gesetze
2.8.2 Rechtsverordnungen
2.8.3 Verwaltungsvorschriften, Richtlinien, Erlasse
2.8.4 Gerichtsentscheidungen
2.8.7 Kontroll- und Informationsbesuche
2.8.8 Einzelprobleme
2.9 Eigenbetriebe, sog. öffentliche Unternehmen
2.9.0 Allgemeines
2.9.1 Gesetze
2.9.2 Rechtsverordnungen
2.9.3 Verwaltungsvorschriften, Richtlinien, Erlasse
2.9.4 Gerichtsentscheidungen
2.9.5 Veröffentlichungen
2.9.7 Kontroll- und Informationsbesuche
2.9.8 Einzelprobleme

3. Technik allgemein, Hardware, Software, Betriebssysteme,
3.0 E-Government/Internet/Telekommunikation/Standards
3.0.0 Allgemeines
3.0.1 Kooperation
3.0.2 Zusammenarbeit mit Aufsichtsbehörden
3.0.3 Vorschrift und Praxis
3.0.4 Begriffsbestimmungen
3.0.5 E-Government/Automationsvorhaben

3.6.0 Allgemeines
3.6.2 Kontroll- u. Informationsbesuche
3.6.3 Prüfkataloge
3.6.4 Anfragen
3.6.5 Hinweise, Ratschläge zu Informations- und Kontrollbesuchen
3.6.8 Einzelprobleme/Beratungsersuchen
3.7 Registerführung
3.7.0 Allgemeines
3.7.1 Dateienregister
3.7.2 gesonderte Register
3.7.3 Verfahrensbeschreibungen M-V
3.7.4 Auftragsdatenverarbeitung
3.7.5 Verfahrensbeschreibungen nach §§ 4 d, 4 e BDSG (untergliedert nach Branchen)
3.7.8 Einzelprobleme/Beratungsersuchen
3.8 Firmenkontakte
3.8.0 Allgemeines
3.8.1 Eigene Firmenkontakte
3.8.2 sonstige Informationsveranstaltungen und -material
3.8.3 Beeinflussung von Entwicklungsarbeiten
3.8.8 Einzelprobleme/Beratungsersuchen
3.9 Test
3.9.0 Test VDS-Doku

4. Nicht-öffentlicher Bereich
4.0 Allgemeines und Aufsicht
4.0.0 Regelungen, Rechtssprechung, Presse, Aufsätze
4.0.1 Aufsicht nach § 38 BDSG
4.0.2 Aufsicht nach spezialgesetzlichen Regelungen
4.0.3 Firmenakten
4.0.4 Kontroll- und Informationsbesuche
4.0.5 Praxishilfen, Empfehlungen, Richtlinien
4.0.6 Allgemeine Themen/Probleme
4.0.7 Owi - und Zwangsgeldverfahren
4.0.8 frei
4.0.9 Sonstige Einzelprobleme
4.1 Auskunfteien (inkl. SCHUFA)
4.1.0 Regelungen, Rechtsprechung, Presse, Aufsätze
4.1.1 Kontroll- und Informationsbesuche
4.1.2 frei
4.1.3 Allgemeine Themen/Probleme
4.1.4 Allgemeines zu bestimmten Auskunfteien
4.1.5 Einzelprobleme bei Handels- und Wirtschaftsauskunfteien
4.1.6 Einzelprobleme bei der SCHUFA
4.1.7 Scoring
4.1.8 frei
4.1.9 Sonstige Einzelprobleme
4.2 Markt- und Meinungsforschung
4.2.0 Regelungen, Rechtsprechung, Presse, Aufsätze
4.2.1 Kontroll- und Informationsbesuche

4.2.2 frei
4.2.3 Allgemeine Themen/Probleme
4.2.4 Umfragen
4.2.5 frei
4.2.6 frei
4.2.7 frei
4.2.8 frei
4.2.9 Sonstige Einzelprobleme
4.3 Banken/Kreditwirtschaft
4.3.0 Regelungen, Rechtsprechung, Presse, Aufsätze
4.3.1 Kontroll- und Informationsbesuche
4.3.2 frei
4.3.3 Allgemeine Themen/Probleme (auch: credit scoring/Basel II)
4.3.4 Kreditinstitutbezogene Einzelprobleme
4.3.5 frei
4.3.6 frei
4.3.7 frei
4.3.8 frei
4.3.9 Sonstige Einzelprobleme
4.4 Versicherungswirtschaft
4.4.0 Regelungen, Rechtsprechung, Presse, Aufsätze
4.4.1 Kontroll- und Informationsbesuche
4.4.2 frei
4.4.3 Allgemeine Themen/Probleme
4.4.4 Private Krankenversicherungen
4.4.5 Kfz -Versicherungen
4.4.6 frei
4.4.7 frei
4.4.8 frei
4.4.9 Sonstige Einzelprobleme
4.5 Handel, Versandhandel
4.5.0 Regelungen, Rechtsprechung, Presse, Aufsätze
4.5.1 Kontroll- und Informationsbesuche
4.5.2 frei
4.5.3 Allgemeine Themen/Probleme
4.5.4 Rabattsysteme
4.5.5 Bonitätsprüfung und -absicherung / Warenumtausch
4.5.6 Warndateien
4.5.7 E-Commerce
4.5.8 frei
4.5.9 Sonstige Einzelprobleme
4.6 Werbung, Adress- und Telefonbuchverlage, Adressenweitergabe
4.6.0 Regelungen, Rechtsprechung, Presse, Aufsätze
4.6.1 Kontroll- und Informationsbesuche
4.6.2 frei
4.6.3 Allgemeine Themen/Probleme
4.6.4 Verzeichnisse auf CD-ROM
4.6.5 Adressenvermietung, -vermittlung
4.6.6 Adress- und Telefonbuchverlage

4.6.7 Werbung
4.6.8 frei
4.6.9 Sonstige Einzelprobleme
4.7 Energieversorgung, Transport und Verkehr (nur privat), Sport, Tourismus und Reisen
4.7.0 Regelungen, Rechtsprechung, Presse, Aufsätze
4.7.1 Kontroll- und Informationsbesuche
4.7.2 frei
4.7.3 Allgemeine Themen/Probleme
4.7.4 Kfz-Vermietung, Taxen
4.7.5 Deutsche Bahn AG
4.7.6 Schifffahrt
4.7.7 Sonstiges/Einzelfälle zu Energieversorgung, Transport und Verkehr
4.7.8 Reisen
4.7.9 Tourismus, Sport
4.8 Gewerbliche Dienstleistungen und freie Berufe (auch Detekteien, Private Sicherheitsdienste etc.)
4.8.0 Regelungen, Rechtsprechung, Presse, Aufsätze
4.8.1 Kontroll- und Informationsbesuche
4.8.2 frei
4.8.3 Allgemeine Themen/Probleme
4.8.4 Steuerberater, Unternehmensberater, Wirtschaftsprüfer
4.8.5 Rechtsanwälte und andere private Rechtsschutz-Institutionen
4.8.6 Private im Gesundheits- und Veterinärwesen (nicht Krankenhäuser)
4.8.7 Private Sicherheitsdienste, Detekteien
4.8.8 Inkassounternehmen
4.8.9 Sonstige Gewerbe/freie Berufe
4.9 Übrige Bereiche, Auftragsdatenverarbeitung und sonstige Einzelfälle
4.9.0 Regelungen, Rechtsprechung, Presse, Aufsätze
4.9.1 Kontroll- und Informationsbesuche
4.9.2 frei
4.9.3 Allgemeine Themen/Probleme
4.9.4 Auftragsdatenverarbeiter
4.9.5 Mieterdatenschutz
4.9.6 Vereine, soziale Einrichtungen
4.9.7 Videoüberwachung durch Private
4.9.8 Wirtschaftskriminalität
4.9.9 Sonstiges

5. Informationsfreiheit
5.0 Allgemeines
5.0.1 Allgemeine Anfragen
5.1 Gesetze im Land
5.1.0 Informationsfreiheitsgesetz M-V
5.1.1 andere Gesetze
5.1.2 frei
5.2 Rechtsverordnungen, Verwaltungsvorschriften, Richtlinien, Erlasse
5.2.0 Rechtsverordnungen
5.2.1 Verwaltungsvorschriften
5.2.2 Erlasse

5.3 Tätigkeits- und Evaluierungsberichte
5.3.0 Evaluierung
5.4 Informationsfreiheit in den Ländern, beim Bund, in der EU und im Ausland
5.4.0 Allgemeines, Hinweise, Informationen, Veröffentlichungen
5.4.1 Gesetze, Verordnungen, Richtlinien in den Ländern
5.4.2 Gesetze, Verordnungen, Richtlinien beim Bund
5.4.3 Informationsfreiheit in der EU und im Ausland
5.5 Gerichtsentscheidungen
5.5.0 Verfassungsgerichte und EuGH
5.5.1 OVG und Verwaltungsgerichte
5.5.2 andere Gerichte
5.6 Aufsätze/Veröffentlichungen
5.6.0 Aufsätze
5.6.1 Veröffentlichungen
5.7 Kontroll- und Informationsbesuche
5.8 Einzelprobleme
5.8.0 Allgemeines
5.8.1 Sachgebiete

6. Projektbereich
6.1 Projekt Grunddatenerfassung
6.1.1 Projekt Grunddatenerfassung

8. Abkürzungsverzeichnis

ABS	Anti-Blockier-System
ADV	Automatisierte Datenverarbeitung
AGnES	Arztentlastende Gemeindenahe E-Health gestützte Systemische Intervention
AK Technik	Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Ständigen Konferenz der Datenschutzbeauftragten des Bundes und der Länder
AKLS	Automatisches Kfz-Kennzeichen-Lesesystem
AMF	Amt für Migration und Flüchtlingsangelegenheiten
AO	Abgabenordnung
ARGE	Arbeitsgemeinschaft
AuslDatV	Ausländerdateienverordnung
BAO KAVALA	Besondere Aufbauorganisation für den G8-Gipfel
BDSG	Bundesdatenschutzgesetz
BEM	betriebliches Eingliederungsmanagement
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BMF	Bundesministerium der Finanzen
BMFSFJ	Bundesministerium für Familie, Senioren, Frauen und Jugend
BMI	Bundesministerium des Innern
BMWi	Bundesministerium für Wirtschaft und Technologie
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
CobIT	Control Objectives for Information and Related Technology
DCS	Data Center Steuern
DDV	Deutscher Direkt-Marketing-Verband
DIN	Deutsches Institut für Normung e. V.
DSG M-V	Landesdatenschutzgesetz
DVZ M-V GmbH	Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH
EKG	Elektrokardiographie
ELENA	Elektronischer Einkommensnachweis
ERFA-Kreis	Erfahrungsaustauschkreis
EU	Europäische Union
EuroPriSe	European Privacy Seal
EZB	Europäische Zentralbank
FHH	Freie und Hansestadt Hamburg
FIDIS	Future of Identity in the Information Society
FStrPrivFinG	Fernstraßenbauprivatfinanzierungsgesetz
GDD	Gesellschaft für Datenschutz und Datensicherung e. V.
GewO	Gewerbeordnung
GG	Grundgesetz
GPS	Global Positioning System
HandwO	Handwerksordnung
HTTP	Hypertext Transport Protocol
I. D. I.	Interessenverband Deutsches Internet e. V.
ID	Identifikationsnummer
IFG M-V	Informationsfreiheitsgesetz Mecklenburg-Vorpommern

IHK	Industrie- und Handelskammer
IM M-V	Innenministerium Mecklenburg-Vorpommern
IP	Internet Protocol
IPSEC	Internet Protocol Security
ISO	International Organization for Standardization
ITIL	IT Infrastructure Library
KAG M-V	Kommunalabgabengesetz Mecklenburg-Vorpommern
KoopA ADV	Kooperationsausschuss Automatisierte Datenverarbeitung Bund/Länder/Gemeinden
KV M-V	Kommunalverfassung des Landes Mecklenburg-Vorpommern
KWG	Kreditwesengesetz
LaGuS	Landesamt für Gesundheit und Soziales
LArchivG M-V	Landesarchivgesetz Mecklenburg-Vorpommern
LBG M-V	Landesbeamtengesetz
LKA M-V	Landeskriminalamt Mecklenburg-Vorpommern
LKHG M-V	Landeskrankenhausgesetz für das Land Mecklenburg-Vorpommern
LKV	Landes- und Kommunalverwaltung
LM M-V	Ministeriums für Ernährung, Landwirtschaft, Forsten und Fischerei
LMG M-V	Landesmeldegesetz Mecklenburg-Vorpommern
LRKG M-V	Landesreisekostengesetz des Landes Mecklenburg-Vorpommern
OSCI	Online Services Computer Interface
OWiG	Gesetzes über Ordnungswidrigkeiten
PassDEÜV	Passdatenerfassungs- und Übermittlungsverordnung
PIN	Persönliche Identifikationsnummer
PKI	Public-Key-Infrastruktur
RFID	Radio Frequency Identification
SCHUFA	SCHUFA Holding AG
SchulG M-V	Schulgesetz Mecklenburg-Vorpommern
SGB I	Sozialgesetzbuch Erstes Buch
SGB II	Sozialgesetzbuch Zweites Buch
SGB IX	Sozialgesetzbuch Neuntes Buch
SGB VII	Sozialgesetzbuch Siebtes Buch
SGB VIII	Sozialgesetzbuch Achtes Buch
SGB X	Sozialgesetzbuch Zehntes Buch
SOG M-V	Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommern
SRTP	Secure Real-Time Transport Protocol
StDÜV	Steuerdatenübermittlungsverordnung
Steuer-ID	Steueridentifikationsnummer
StPO	Strafprozessordnung
SWIFT	Society for Worldwide Interbank Financial Telekommunications
TLS	Transport Layer Security
TMG	Telemediengesetz
TMS M-V	Travel-Management-Systems des Landes Mecklenburg-Vorpommern
ULD S-H	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

VERA	Vergleichsarbeiten in der Grundschule
Verf M-V	Verfassung des Landes Mecklenburg-Vorpommern
VermKatG	Gesetz über die Landesvermessung und das Liegenschaftskataster des Landes Mecklenburg-Vorpommern
VPN	Virtual Private Network
VwGO	Verwaltungsgerichtsordnung
VwVfG M-V	Verwaltungsverfahrensgesetz Mecklenburg-Vorpommern
WGA	Microsoft Windows Genuine Advantage
ZIR	zentrales Informationsregister
ZKA	Zentraler Kreditausschuss

Stichwortverzeichnis

10. Publikationen

Beim Landesbeauftragten für den Datenschutz sind derzeit folgende Publikationen kostenlos erhältlich:

Broschüren

1. Tätigkeitsbericht für den Zeitraum 1992/1993
2. Tätigkeitsbericht für den Zeitraum 1994/1995
3. Tätigkeitsbericht für den Zeitraum 1996/1997
5. Tätigkeitsbericht für den Zeitraum 2000/2001
6. Tätigkeitsbericht für den Zeitraum 2002/2003

Datenschutzgerechtes eGovernment (Handlungsempfehlungen und datenschutzfreundliche Lösungen für die Verwaltung)

Vom Bürgerbüro zum Internet – Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung

Datenschutz im Krankenhaus

Die Virtuelle Poststelle im datenschutzgerechten Einsatz

Datenschutz bei Dokumentenmanagementsystemen - Orientierungshilfe

Infoblätter

Datenschutz und Statistik

Datenschutz und Telefax

Meine Daten - Mein Recht ... auch in der Schule

Meine Daten - Mein Recht ... als Kunde und Verbraucher

Ihre Rechte auf Schutz Ihrer Daten

Ihr Recht auf Widerspruch bei der Meldebehörde

Das Recht auf Informationsfreiheit in Mecklenburg-Vorpommern

Zulässigkeit und gesetzliche Grenzen von Videoüberwachungsanlagen

Ihre Auskunftsrechte als Patient

Ihre Rechte gegenüber Handels- und Wirtschaftsauskunfteien

Muster (Kopien)

Mustervertrag zur Verarbeitung personenbezogener Daten im Auftrag

Mustervertrag zur datenschutzgerechten Vernichtung von Schriftgut mit personenbezogenen Daten

Musterdienstvereinbarung über die Nutzung der Telekommunikationsanlage

Musterdienstvereinbarung zur Nutzung von Internetdiensten

Muster einer Verpflichtungserklärung zum Datengeheimnis gemäß § 6 DSG M-V

Muster einer Bestellung zur oder zum behördlichen Datenschutzbeauftragten

Orientierungshilfen (Kopien)

Empfehlungen zur Passwortgestaltung und zum Sicherheitsmanagement
Transparente Software - eine Voraussetzung für datenschutzfreundliche Technologien
Forderung an Wartung und Fernwartung von DV-Anlagen
Data Warehouse und Data Mining im öffentlichen Bereich (Datenschutzrechtliche und -technische Aspekte)
Datenschutz bei Windows XP Professional
TCPA, Palladium und DRM
Datensicherheit bei USB-Geräten
Datenschutzfragen zum Anschluss von Netzen der öffentlichen Verwaltung an das Internet
Datenschutzrechtliche Aspekte beim Einsatz von Verzeichnisdiensten
Datenschutzgerechte Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz
Datenschutzfragen zur Präsentation von öffentlichen Stellen im Internet
Datenschutz und Internet in der Schule
Datenschutzgerechte Vernichtung von Schriftgut mit personenbezogenen Daten
Anforderungen zur informationstechnischen Sicherheit bei Chipkarten
Datenschutzrechtliche Aspekte beim Einsatz optischer Datenspeicherung
Datenschutz und Telefax
Datenschutz in kommunalen Vertretungsorganen
Datenschutz und Telemedizin - Anforderungen an Medizinnetze
Datenschutz bei Telearbeit
Datenschutz in drahtlosen Netzen
Datenschutz bei Dokumentenmanagementsystemen
Einsatz kryptografischer Verfahren
Datenschutz bei technikunterstützten Verfahren der Personal- und Haushaltsbewirtschaftung
Common Criteria Protection Profile - Software zur Verarbeitung von personenbezogenen Bilddaten
Datenschutzgerechter Einsatz von RFID

Formulare (Kopien)

Verfahrensbeschreibung nach § 18 DSG M-V; Hinweise zur Führung der Verfahrensbeschreibung
Widerspruch gegen die Weitergabe meiner Daten gemäß §§ 32, 34 a, 35 Meldegesetz für das Land Mecklenburg-Vorpommern

Unsere Informationsmaterialien zum Download und weitere Informationen:

www.datenschutz-mv.de
www.informationsfreiheit-mv.de

Informationen über den Datenschutz auch unter:

www.bfdi.bund.de
www.datenschutz.de (Virtuelles Datenschutzbüro)