LANDTAG MECKLENBURG-VORPOMMERN **Drucksache 5/3844**
5. Wahlperiode **13.10.2010**

UNTERRICHTUNG

durch den Landesbeauftragten für den Datenschutz

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

und

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

Berichtszeitraum: 1. Januar 2008 bis 31. Dezember 2009

Zugeleitet mit Schreiben des Landesbeauftragten für den Datenschutz vom 11. Oktober 2010.

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 Neunte Tätigkeitsbericht gemäß § 33 Abs. 1 DSG M-V sowie der Vierte Tätigkeitsbericht gemäß § 38 Abs. 1 BDSG umfassen den Zeitraum vom 1. Januar 2008 bis zum 31. Dezember 2009.

Wie in der Vergangenheit 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

Seite

0. Einleitung

Im Berichtszeitraum 2008 und 2009 haben sich die Meldungen zum Thema Datenschutz förmlich überschlagen. Datenskandale machten die Runde und erreichten ein Maß an Öffentlichkeit, wie es diesem Thema in den letzten Jahrzehnten selten beschert war. Nicht nur das Bundesverfassungsgericht sah sich zum Handeln bewegt, sondern auch der Europäische Gerichtshof und die europäische sowie die nationale Politik mussten handeln.

Den gesetzgeberischen Bemühungen ist gegenwärtig allerdings eher eine symbolische als eine wirklich überzeugende Kraft beizumessen. Begrüßenswert ist jedoch das wachsende öffentliche Bewusstsein für die Herausforderungen an den demokratischen Rechtsstaat, die aus der Entwicklung der Informations- und Kommunikationswirtschaft resultieren. Diese Entwicklung hat aber auch nachdrücklich gezeigt, dass eine umfassende Novellierung des Bundesdatenschutzgesetzes dringend erforderlich ist. Bisher hat nicht zuletzt die Lobbyarbeit auf den Gängen des Deutschen Bundestages wirklich überzeugende Schritte aber verhindert.

Die Datenschutzbeauftragten von Bund und Ländern haben wiederholt ihre Bereitschaft zu einer fachlichen Mitwirkung erklärt. Diese Mitwirkung soll sich aber nicht auf die Teilnahme an „Gipfeltreffen“ beschränken. Erfreulicherweise findet das Angebot zunehmend in der alltäglichen Politik und der Medienberichterstattung Gehör.

Auch der Landtag von Mecklenburg-Vorpommern hat die Diskussion aufgegriffen und meine Behörde sowohl personell als auch institutionell gestärkt. Zum Januar 2010 erhielt ich eine zusätzliche Stelle des höheren Dienstes. Dies ist zwar keinesfalls ausreichend, angesichts der Bemühungen der Landesregierung um Personalabbau aber doch eine keineswegs selbstverständliche und daher besonders begrüßenswerte Verstärkung. Zudem wurden meine Beteiligungsrechte im Gesetzgebungsverfahren durch eine Änderung der Gemeinsamen Geschäftsordnung der Landesregierung und in der Geschäftsordnung des Landtages gestärkt. Ich habe nunmehr die Möglichkeit, frühzeitig in die datenschutzrechtlich bedeutsamen Gesetzesvorhaben einbezogen zu werden, und hoffe, dass die Landesregierung davon vollständig Gebrauch machen wird.

Die öffentliche Wahrnehmung des Datenschutzes führte aber auch zu einem enormen Anstieg bei den Petitionen von Bürgerinnen und Bürgern. Schwerpunkt waren vor allem die Themen Videoüberwachung im nicht-öffentlichen Bereich und Sozialdatenschutz bei Hartz-IV-Leistungsbezug. Die Zahl der Petitionen war so stark gestiegen, dass mitunter die Arbeitsfähigkeit der Behörde bedroht war.

Die Beratungs- und Fortbildungsangebote meiner Behörde wurden in einem erfreulichen Umfang angenommen. In den Jahren 2008 und 2009 konnte ich gemeinsam mit meinen Mitarbeiterinnen und Mitarbeitern in ca. 85 Veranstaltungen rund 2.000 Teilnehmerinnen und Teilnehmer aus der öffentlichen Verwaltung, den Schulen und Hochschulen sowie den Unternehmen des Landes erreichen. Den angefragten Bedarf konnte ich damit jedoch nicht decken.

Meine Datenschutz-Fachtagungen zu den Themen „Datenschutz im Tourismusland“ (siehe Punkt 5.1) und „Privatsphäre - gefangen im Netz der Koordinaten“ (siehe Punkt 5.2) mit jeweils mehr als hundert Teilnehmern haben dazu beigetragen, mit zahlreichen Fachleuten aus Wissenschaft, Wirtschaft und Verwaltung des Landes zu aktuellen Themen ins Gespräch zu kommen. Mit den jährlichen Fachtagungen hat sich ein breit akzeptiertes Informations- und Diskussionspodium für Führungskräfte und Datenschützer etabliert.

Als eine weitere erfolgreiche Form der inhaltlichen Schwerpunktsetzung habe ich 2009 ein Projekt zum Thema „Elektronische Verwaltung und Datenschutz“ durchgeführt (siehe Punkt 6). Im Rahmen des Projektes habe ich auf kommunaler Ebene die Umsetzung der Regelungen zum Datenschutz am Beispiel des elektronisch zu führenden Melderegisters untersucht. Im Ergebnis war es erstmalig möglich, statistisch aussagekräftige Ergebnisse zur E-Government-Fähigkeit der Kommunen zu erhalten. Zugleich konnte ich Kommunen vor Ort fachkundig beraten. Die Ergebnisse dieser Untersuchung belegen in aller Deutlichkeit einen enormen Handlungsbedarf des Landes. Die in der Mehrzahl sehr kleinen Kommunalverwaltungen sind mit ihrer gegenwärtigen personellen Ausstattung und technischen Infrastruktur nicht in der Lage, auch nur die geringsten Datensicherheitsanforderungen durchgängig sicherzustellen. Auch wenn durch den E-Government-Zweckverband mit der Beschäftigung von Datenschutzexperten in vielen Kommunen deutliche Fortschritte erzielt wurden, so ist doch das Land in der Pflicht, die Kommunen bei der Einführung von E-Government-Verfahren wesentlich intensiver und frühzeitiger zu unterstützen.

Mein Neunter Tätigkeitsbericht gemäß § 33 Abs. 1 DSG M-V belegt einerseits die steigenden fachlichen und persönlichen Anforderungen an meine Mitarbeiterinnen und Mitarbeiter. Er verdeutlicht andererseits aber auch die zunehmenden Anforderungen an die Verantwortlichen in Verwaltungen und Unternehmen. Dort sollte der Datenschutz nicht länger als Hindernis betrachtet, aber auch nicht als „Feigenblatt“ benutzt werden. Vielmehr muss Datenschutz als einzig geeignetes Mittel begriffen werden, mit dem das Recht auf informationelle Selbstbestimmung der von den Datenverarbeitungen betroffenen Bürgerinnen und Bürger des Landes im alltäglichen Handeln geschützt werden kann. Das Bundesverfassungsgericht hat mit seiner Forderung nach einer staatlichen Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme den Weg in einer überzeugenden Weise aufgezeigt.

1. Empfehlungen

1.1 Zusammenfassung aller Empfehlungen

Ich empfehle der Landesregierung, bei den Beratungen zum IT-Staatsvertrag die Berücksichtigung datenschutzrechtlicher Grundsätze einzufordern und auf einer angemessenen Beteiligung von Bund und Ländern bei Entscheidungen in grundrechtssensiblen Fragen zu bestehen. Auf Landesebene muss ein Verfahren gefunden werden, wie der Landtag in die wichtigsten strukturbestimmenden Entscheidungen frühzeitig einbezogen wird und wie die Beteiligung des Landesbeauftragten für den Datenschutz sichergestellt werden kann (Punkt 2.1.3).

Ich empfehle der Landesregierung, von diesem Beteiligungsrecht umfassend Gebrauch zu machen, um die IT-Sicherheit zu gewährleisten, ohne den Datenschutz der Bürgerinnen und Bürger einzuschränken (Punkt 2.1.4).

Ich empfehle der Landesregierung sicherzustellen, dass die erforderlichen Maßnahmen zur Datensicherheit und zum Datenschutz in den hierfür erforderlichen Sicherheitskonzepten festgeschrieben und ausnahmslos umgesetzt werden. Außerdem müssen Regelungen zum Einsatz von elektronischen Signaturen getroffen werden (Punkt 2.1.8).

Ich empfehle der Landesregierung, §§ 34 Abs. 6 i. V. m. Abs. 5 SOG M-V in der Novellierung des Sicherheits- und Ordnungsgesetzes zu berücksichtigen (Punkt 2.2.2).

Ich empfehle der Landesregierung, darauf hinzuwirken, dass durch den zuständigen parlamentarischen Gesetzgeber eine normenklare und verhältnismäßige gesetzliche Grundlage zur Videoüberwachung im Straßenverkehr geschaffen wird (Punkt 2.2.3).

Ich empfehle der Landesregierung deshalb, darauf hinzuwirken, dass künftige Wahltermine so festgelegt und veröffentlicht werden, dass eine fristgerechte Bekanntmachung der Widerspruchsmöglichkeit durchgeführt werden kann (Punkt 2.6.3).

Ich empfehle der Landesregierung, die bei der Einführung des elektronischen Reisepasses gewonnenen Erkenntnisse detailliert auszuwerten und die Pass- und Personalausweisbehörden sowohl beim Betrieb des Passantragsverfahrens als auch bei der Einführung der neuen Personalausweise zu unterstützen (Punkt 2.4.8).

Ich empfehle der Landesregierung, die Personalausweisbehörden bei der Einführung der neuen elektronischen Personalausweise aktiv zu unterstützen und darauf hinzuwirken, dass ausreichend finanzielle Mittel und genügend qualifiziertes Personal in den Kommunen zur Verfügung steht, damit die zahlreichen neuen Aufgaben auf sichere und datenschutzgerechte Weise bearbeitet werden können.
Die Personalausweisbehörden sollten Bürgerinnen und Bürger bei der Ausgabe des neuen Personalausweises auf die erforderliche Sicherheitsausstattung des privaten Personalcomputers hinweisen und ausdrücklich die Nutzung von Lesegeräten mit eigenem Tastaturfeld empfehlen (Punkt 2.4.9).

Ich empfehle dem Landtag, mit einer Änderung des DSG M-V dem Landesdatenschutzbeauftragten im Bereich der Rechtspflege bei Gerichten eine Prüfungsbefugnis über technische und organisatorische Maßnahmen zur Datensicherheit einzuräumen. Um im Bereich der äußeren Datensicherheit (etwa in Bezug auf die Erforderlichkeit von Sicherheitskonzept, Verfahrensbeschreibung und Freigabe) mehr Rechtsklarheit zu schaffen, sollte der Anwendungsbereich des DSG M-V auf den Bereich der Rechtspflege bei Gerichten ausgeweitet werden. Die Unabhängigkeit der Gerichte bliebe gewahrt, wenn gleichzeitig festgeschrieben wird, dass die §§ 30, 31 und 32 im Bereich der Rechtspflege keine Anwendung finden (Punkt 2.4.10).

Ich empfehle der Landesregierung, statistische Angaben über die ermittelten Konten und Depots, die aufgrund von Kontenabfragen ermittelt werden konnten, zur Verfügung zu stellen, um Feststellungen darüber zu ermöglichen, ob die diesbezüglich zu verzeichnenden Erfolge in einem angemessenen Verhältnis zu der Anzahl der durchgeführten Kontenabrufe stehen (Punkt 2.7.3).

Ich empfehle dem Landtag erneut, durch eine Änderung des § 5 Abs. 2 Landesdatenschutzgesetz (DSG M-V) die erforderliche gesetzliche Grundlage für die Durchführung eines Auditierungsverfahrens zu schaffen (Punkt 2.10.5).

Ich empfehle der Landesregierung, vor dem Einsatz von EPOS in jeder Dienststelle das behördenspezifische Sicherheitskonzept zu erarbeiten und das Verfahren vor der Inbetriebnahme formell freizugeben. Das Innenministerium sollte zudem gemeinsam mit dem Software-Hersteller unverzüglich die im Sicherheitskonzept geforderte Datenbankverschlüsselung realisieren (Punkt 2.11.6).

Ich empfehle der Landesregierung erneut, ihre Beschlüsse zur Basiskomponente Signatur entschlossen umzusetzen und sich für eine stärkere Verbreitung der qualifizierten elektronischen Signatur einzusetzen. In Mecklenburg-Vorpommern sollte sie Anwendungen der qualifizierten elektronischen Signatur sowohl in der Verwaltung als auch in der Wirtschaft fördern (Punkt 2.14.3).

Ich empfehle der Landesregierung, dem Projekt „IT-Management-System“ den erforderlichen Stellenwert beizumessen. Um die sichere und datenschutzgerechte Funktion der Informations- und Kommunikationstechnik gewährleisten zu können, muss unverzüglich ein IT-Management-System mit den oben beschriebenen Komponenten realisiert werden (Punkt 2.14.4).

Ich empfehle der Landesregierung, insbesondere bei der Entwicklung und beim Betrieb moderner E-Government-Verfahren die Grundsätze der Datensparsamkeit und der Datenvermeidung zu beachten und den Einsatz datenschutzfördernder Identitätsmanagementsysteme voranzutreiben (Punkt 2.14.5).

Ich empfehle der Landesregierung, die öffentlichen Stellen des Landes für eine datenschutzgerechte Ausgestaltung der Webseitenprotokollierung mit entsprechender Anonymisierung zu sensibilisieren (Punkt 2.14.6).

Ich empfehle der Landesregierung, sich dafür einzusetzen, dass die Kritikpunkte der Datenschutzbeauftragten von Bund und Ländern am Entwurf des Bürgerportalgesetzes bei der Ausgestaltung des De-Mail-Gesetzes berücksichtigt werden (Punkt 2.14.7).

Ich empfehle der Landesregierung, die Kernaussagen der Orientierungshilfen des AK Technik in ihre entsprechenden Planungsgrundsätze, etwa das IT-Sicherheitsrahmen-Konzept der Landesverwaltung, zu übernehmen und somit verbindlich einzuführen (Punkt 2.14.8).

Ich empfehle der Landesregierung, die „Besonderen Beförderungsbedingungen“ um eine entsprechende Regelung zu ergänzen und dabei eine Löschungsfrist von einem Jahr vorzusehen (Punkt 3.6).

1.2 Umsetzung der Empfehlungen des 8. Tätigkeitsberichtes

Lfd. Nr.:	Empfehlung	Umsetzungsstand	Gliederungs-punkt
1	Ich empfehle der Landesregierung und dem Landtag, Zuverlässigkeitsüberprüfungen bei (Groß-)Veranstaltungen auf eine spezifische gesetzliche Grundlage zu stellen.	Der Empfehlung wurde nicht gefolgt.	2.2.2
2	Ich empfehle der Landesregierung, die neu eingefügten und befristeten Befugnisse gründlich zu evaluieren und auf ihre Erforderlichkeit hin zu überprüfen.	Der Empfehlung wurde überwiegend nicht gefolgt.	2.2.3
3	Ich empfehle der Landesregierung, meine Vorschläge bei der nächsten Novellierung des Sicherheits- und Ordnungsgesetzes zu berücksichtigen.	Der Empfehlung wurde überwiegend nicht gefolgt.	2.2.4
4	Ich empfehle der Landesregierung, gesetzlich die Durchführung von Maßnahmen der Verkehrsüberwachung mittels Videotechnik zu regeln.	Der Empfehlung wurde nicht gefolgt.	2.2.6
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.	Zwar wurde der Empfehlung gefolgt, eine gesetzliche Grundlage zu schaffen; jedoch ist diese aus datenschutzrechtlicher Sicht nicht tragfähig.	2.3.1
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 Internet-diensten am Arbeitsplatz“ der Datenschutz-beauftragten des Bundes und der Länder beachtet werden. Besondere Aufmerksamkeit ist geboten, wenn kommunale Vertretungen die technische Infrastruktur der Stadt- und Gemeindeverwal-tungen mit nutzen.	Von entsprechenden Aktivitäten habe ich keine Kenntnis.	2.4.2

Lfd. Nr.:	Empfehlung	Umsetzungsstand	Gliederungs-punkt
7	Ich empfehle der Landesregierung, künftig die Kommunen bei der Einführung zentraler E-Governmentverfahren 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.	Der Empfehlung wurde zum Teil gefolgt. Die Landesregierung beabsichtigt, im Bereich des Personenstandswesens eine Vermittlungsstelle einzurichten. Die Vermittlungsstelle soll den Kommunen insoweit zugute kommen, als diese sonst für jedes einzelne Standesamt die für die elektronische Datenverarbeitung erforderlichen Standards selbst vorhalten müssten.	2.4.7
8	Ich empfehle dem Landtag, im Kommunalabgabengesetz eine Klarstellung dahingehend aufzunehmen, dass die Ermittlung von Steuerpflichtigen nicht im Wege einer Auskunftspflicht Dritter erfolgen darf.	Die Empfehlung wurde nicht umgesetzt, da das KAG M-V nicht novelliert worden ist.	2.5.4
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.	Die Empfehlung wurde nicht umgesetzt.	2.5.5
10	Ich empfehle der Landesregierung, sich umgehend um die Schaffung einer verfassungsgemäßen Rechtsgrundlage zu bemühen und bis dahin das Verfahren LUNA 2.0 einzustellen.	Die Empfehlung wurde nicht umgesetzt.	2.5.6
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.	Von entsprechenden Aktivitäten habe ich keine Kenntnis.	2.5.7
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.	Von entsprechenden Aktivitäten habe ich keine Kenntnis.	2.6.2

Lfd. Nr.:	Empfehlung	Umsetzungsstand	Gliederungs-punkt
13	Ich empfehle der Landesregierung erneut, dem ELENA-Verfahrensgesetz im Bundesrat nur dann zuzustimmen, wenn die Verfassungs-mäßigkeit des Verfahrens nachgewiesen, die Sicherheit der Daten garantiert und eine Kontrolle durch unabhängige Stellen gewährleistet ist.	Der Empfehlung wurde nicht gefolgt. Mecklenburg-Vorpommern hat dem ELENA-Verfahrensgesetz im Bundesrat zugestimmt.	2.8.1
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.	Der Empfehlung wurde nicht gefolgt. In einzelnen Fachverfahren nutzt die Landesregierung Verschlüsselung und fortgeschrittene elektronische Signaturen oder bereitet dies vor. Qualifizierte elektronische Signaturen fördert die Landesregierung nicht. Ebenso wenig wurde die Ausstattung mit Kartenlesern verbessert.	2.10.1
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.	Der Empfehlung wurde insoweit gefolgt, dass die Landes-regierung über die unteren Schulaufsichtsbehörden an die Schulträger eine entsprechende Empfehlung aussprechen wird.	2.11.1
16	Ich empfehle dem Landtag klarzustellen, dass keinem Mitarbeiter wegen der Anrufung des Landesbeauftragten für den Datenschutz oder des behördlichen Datenschutzbeauftragten Nachteile entstehen dürfen.	Von entsprechenden Aktivitäten habe ich keine Kenntnis.	2.12.3
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.	Der Empfehlung wurde nicht gefolgt.	2.15.1
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.	Der Empfehlung wurde nicht gefolgt. In einzelnen Fachverfahren nutzt die Landesregierung fortgeschrittene elektronische Signaturen oder bereitet dies vor. Qualifizierte elektronische Signaturen fördert die Landesregierung nicht.	2.15.2
19	Ich empfehle dem Landtag, die technische Entwicklung von RFID-Systemen aufmerksam zu beobachten und sofort gesetzgeberisch aktiv zu werden, wenn die rechtlichen Schutz-mechanismen den neuen Risiken nicht mehr gerecht werden.	Von entsprechenden Aktivitäten habe ich keine Kenntnis.	2.15.4

Lfd. Nr.:	Empfehlung	Umsetzungsstand	Gliederungs-punkt
20	Ich empfehle der Landesregierung, Informationssicherheits- und Datenschutzfragen künftig in engem Zusammenhang zu bearbeiten und die vom BSI beschriebenen Management-prozesse bei der Planung, der Einrichtung, dem Betrieb und nach der Außerbetriebnahme von IT-Verfahren vollständig umzusetzen.	Die Landesregierung verfolgt die von mir empfohlenen Vorgehensweisen im Projekt „IT-Management-System“ (siehe Punkt 2.14.4). Das Projekt ist noch nicht praxisrelevant, der Zeitplan konnte nicht eingehalten werden.	2.15.5

2. Öffentlicher Bereich

2.1 Rechtswesen/Europa

2.1.1 Stockholmer Programm

Die Europäische Union will im Stockholmer Programm ihre politischen Ziele zur Entwicklung eines Raums der Freiheit, der Sicherheit und des Rechts bis 2015 festschreiben.

In dem von der Kommission vorgelegten Entwurf werden die Wahrung der persönlichen Freiheitsrechte und der Schutz der Privatsphäre zwar angesprochen. Auch werden Aufklärungskampagnen zum Datenschutz und die Förderung von datenschutzrechtlichen Technologien genannt. Jedoch hinkt ein verbesserter Datenschutz deutlich hinter den Zielsetzungen für eine verbesserte Sicherheitsarchitektur hinterher. So enthält der Kommissionsentwurf einen umfangreichen Katalog besonders eingriffsintensiver Maßnahmen wie beispielsweise ein elektronisches Registrier- sowie Vorabgenehmigungssystem für Ein- und Ausreisen in die/aus der EU. Zudem wird eine einheitliche Plattform der Informationsverarbeitung mit geradezu beliebig vielen Datenverarbeitungsmöglichkeiten angestrebt, welche ohne angemessene Ausgleichsmaßnahmen zur Gewährleistung von Datenschutz und Datensicherheit die Bürgerrechte gefährdet.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher am 8. und 9. Oktober 2009 in Berlin eine Entschließung verabschiedet, in der sie Maßnahmen vorschlägt, die das Verhältnis zwischen Sicherheit und Freiheit besser austarieren (siehe Anlage 1.30). Dazu zählen: die Weiterentwicklung des Rahmenbeschlusses zu einem harmonisierten Datenschutzrecht, das im Bereich der polizeilichen und justiziellen Zusammenarbeit ein hohes Datenschutzniveau gewährleistet, die Beachtung von zwingenden Datenschutzgrundsätzen beim Abschluss von Übereinkommen mit Drittstaaten sowie ein unabhängiges datenschutzrechtliches Beratungs- und Kontrollgremium für alle Bereiche der polizeilichen und justiziellen Zusammenarbeit der EU- Mitgliedsstaaten.

Die Bundesregierung wird aufgefordert, sich für diese Forderungen im weiteren Verfahren einzusetzen.

2.1.2 INSPIRE-Richtlinie, Geodaten

Mit der INSPIRE-Richtlinie (Richtlinie 2007/2/EG des Europäischen Parlaments und des Rates) ist den Mitgliedsstaaten aufgegeben worden, Vorschriften über den digitalen Zugang zu Geodaten in nationales Recht umzusetzen. Ziel dieser Richtlinie ist die Bereitstellung von amtlichen Geodaten nach einheitlichen Standards für europaweite behördliche, kommerzielle und private Nutzungen.

Zunächst hatte der Bund hierzu ein Gesetz verabschiedet, welches am 10. Februar 2009 in Kraft getreten ist. Das Gesetz zum Zugang zu digitalen Geodaten (GeoZG) soll insbesondere den rechtlichen Rahmen für den Zugang zu Geodaten sowie die Nutzung dieser Daten - insbesondere für Maßnahmen, die Auswirkungen auf die Umwelt haben können - schaffen.

Aus verfassungsrechtlichen Gründen ist auch Mecklenburg-Vorpommern verpflichtet, die INSPIRE-Richtlinie in Landesrecht umzusetzen. Das Innenministerium Mecklenburg-Vorpommern hat mir hierzu den Entwurf eines Gesetzes über das amtliche Vermessungs- und Geoinformationswesen (VermGeoG M-V) übersandt. Meine Stellungnahme hierzu führte unter anderem zu folgenden Änderungen im Entwurf des VermGeoG M-V:

- Stellen und Personen außerhalb des öffentlichen Bereiches werden personenbezogene Daten aus Geobasisdaten nur unter Berücksichtigung datenschutzrechtlicher Grundsätze bereitgestellt. Konkret müssen diese Privaten ein berechtigtes Interesse an der Kenntnis der begehrten Daten glaubhaft darlegen und der Betroffene darf kein schutzwürdiges Interesse am Ausschluss der Bereitstellung haben (§ 22 VermGeoG M-V).

- Die Aufbewahrungsfrist der Protokolldaten bei einem automatisierten Abruf von Geobasisdaten des Liegenschaftskatasters (§ 25 VermGeoG M-V) wurde verlängert, um die Revisionsfähigkeit, wie sie § 21 Abs. 2 Nr. 4 DSG M-V vorschreibt, sicherzustellen.

- Die Regelungen zum Zugang und zur Verwendung von Geodaten und Geodatendiensten und dabei insbesondere die Bestimmungen zum Schutz öffentlicher und sonstiger Belange (§ 35 VermGeoG M-V) wurden im Einklang mit den Regelungen zum IFG M-V überarbeitet. Dieses betraf vor allem die Zugangsbeschränkungen bei einer möglichen Offenbarung schutzwürdiger personenbezogener Daten und Betriebs- oder Geschäftsgeheimnisse.

Das VermGeoG M-V ist durch den Landtag des Landes Mecklenburg-Vorpommern noch nicht verabschiedet worden. Ich werde den weiteren Fortgang und die praktische Umsetzung dieses Gesetzes aufmerksam beobachten.

2.1.3 IT im Grundgesetz/IT-Planungsrat

Am 1. August 2009 ist im Zuge der Föderalismusreform II mit der Grundgesetzänderung der neue Artikel 91c Grundgesetz in Kraft getreten (BGBl. 2009 I S. 2248 ff.). Er regelt, dass Bund und Länder bei der Planung, der Errichtung und dem Betrieb der für ihre Aufgabenerfüllung benötigten informationstechnischen Systeme zusammenwirken können. Zudem schafft er die Grundlage für den Bund, ein sogenanntes Verbindungsnetz zwischen den informationstechnischen Netzen von Bund und Ländern einzurichten, um einen reibungslosen Datenaustausch zu fördern. Näheres dazu regelt das am 18. August 2009 in Kraft getretene „Gesetz über die Verbindung der informationstechnischen Netze des Bundes und der Länder (IT-NetzG)".

Art. 91c GG sieht vor, dass die Grundlagen der Zusammenarbeit **für einzelne nach Inhalt und Ausmaß bestimmte Aufgaben** gemeinsam von Bund und Ländern zu bestimmen sind. Die Bundesregierung hat am 4. November 2009 den vom Bundesminister des Innern vorgelegten Entwurf eines Gesetzes über die Bund-Länder-Zusammenarbeit im Bereich der öffentlichen Informationstechnik und die Errichtung des IT-Planungsrates beschlossen. Der IT-Planungsrat löst die bisherigen Gremien „Arbeitskreis der Staatssekretäre für E-Government in Bund und Ländern" und „Kooperationsausschuss von Bund und Ländern für automatisierte Datenverarbeitung" (Koop A ADV) ab und tritt in deren Rechtsnachfolge ein. Der IT-Staatsvertrag, der am 1. April 2010 in Kraft treten soll, sieht den IT-Planungsrat als zentrales bundes- und länderübergreifendes Steuerungsorgan vor. Er soll die Zusammenarbeit zwischen Bund und Ländern koordinieren, fachunabhängige und fachübergreifende IT-Interoperabilitäts- und Sicherheitsstandards beschließen, bundesweite E-Government-Projekte steuern und die Festlegungen gemäß IT-NetzG für das Verbindungsnetz treffen.

Grundsätzlich begrüße ich die Einrichtung des IT-Planungsrates, weil damit die Möglichkeit einer effektiven Kooperation zwischen Bund und Ländern bei der Planung, der Errichtung und dem Betrieb bundesweiter informationstechnischer Systeme ermöglicht wird. Der IT-Staatsvertrag soll allerdings eine umfassende Rahmenregelung für die gesamte IT-Zusammenarbeit zwischen Bund und Ländern schaffen. Es ist fraglich, ob eine solche **umfassende Übertragung** von Bund/Länder-Kompetenzen auf den IT-Planungsrat verfassungsrechtlich tatsächlich legitimiert ist.

Es ist jedoch absehbar, dass die informationstechnische Kooperation von Bundes- und Landesbehörden in zunehmendem Maße die Verarbeitung personenbezogener Daten betreffen wird, die durch angemessene und dem Stand der Technik entsprechende Maßnahmen zu schützen sind. Das Bundesverfassungsgericht hat die besondere Bedeutung der informationellen Selbstbestimmung und der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme in seiner Entscheidung vom 27. Februar 2008 hervorgehoben. Das betrifft insbesondere auch die Festlegung von Standards im IT-Bereich. Entscheidungen des IT-Planungsrates über Fragen der Gewährleistung von IT-Sicherheit können über die Bestimmungen des IT-Staatsvertrages rechtsverbindlich werden. Derartige Regelungen müssen aber regelmäßig Gegenstand parlamentsgesetzlicher Regelungen sein. Es droht somit eine Umkehrung der gesetzlichen Bezüge zwischen Exekutive und Legislative. Der IT-Planungsrat muss daher die Vorgaben des Bundesverfassungsgerichts berücksichtigen und bei Entscheidungen in grundrechtssensiblen Fragen die Parlamente in Bund und Ländern beteiligen.

Der IT-Staatsvertrag sieht in § 3 Abs. 1 außerdem vor, dass der IT-Planungsrat vorrangig lediglich bestehende Marktstandards beschließen soll. Damit besteht die Gefahr, dass moderne datenschutzfreundliche Technologien keine Berücksichtigung finden und Verfahren ohne angemessenen Datenschutz beschlossen werden. Darauf hat auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 8./9. Oktober 2009 hingewiesen (siehe Anlage 1.27). Sie begrüßt, dass der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit an den Sitzungen des IT-Planungsrates teilnehmen soll, hält es allerdings für geboten, dass auch die Landesdatenschutzbeauftragten einbezogen werden.

Ich empfehle der Landesregierung, bei den Beratungen zum IT-Staatsvertrag die Berücksichtigung datenschutzrechtlicher Grundsätze einzufordern und auf einer angemessenen Beteiligung von Bund und Ländern bei Entscheidungen in grundrechtssensiblen Fragen zu bestehen. Auf Landesebene muss ein Verfahren gefunden werden, wie der Landtag in die wichtigsten strukturbestimmenden Entscheidungen frühzeitig einbezogen wird und wie die Beteiligung des Landesbeauftragten für den Datenschutz sichergestellt werden kann.

2.1.4 Novellierung des BSI-Gesetzes

Das Bundeskabinett hat im Januar 2009 den „Gesetzentwurf zur Stärkung der Sicherheit in der Informationstechnik des Bundes“ beschlossen. Mit dem am 20. August 2009 in Kraft getretenen Gesetz wurden dem Bundesamt für Sicherheit in der Informationstechnik (BSI) weitere Befugnisse eingeräumt, um Gefahren für die Sicherheit der Informationstechnik des Bundes abzuwehren. So sollte das BSI ermächtigt werden, die gesamte Sprach- und Datenkommunikation aller Unternehmen und Bürger mit Bundesbehörden zu überwachen und auszuwerten. Das Bundesamt sollte zudem personenbezogene Daten an Strafverfolgungsbehörden schon dann übermitteln dürfen, wenn sie zur Aufklärung von nicht erheblichen Straftaten, die mittels Telekommunikation begangen wurden, genutzt werden. Schließlich sollte das BSI ihm bekannt gewordene Sicherheitslücken und Schadprogramme zunächst geheimhalten dürfen. Der Gesetzentwurf sah zudem eine Änderung des Telemediengesetzes vor, die Diensteanbietern von Telemedien zur Störungsbeseitigung die umfassende Protokollierung des Surfverhaltens von Nutzern im Internet ermöglichen sollte.

Der Gesetzentwurf stieß nicht nur bei Datenschützern und Bürgerrechtlern, sondern auch bei zahlreichen Bundestagsabgeordneten und im Bundesrat auf massive Kritik. Einerseits war absehbar, dass durch die Geheimhaltung von Sicherheitslücken insbesondere die ordnungsgemäße Abwicklung von Verwaltungsaufgaben beeinträchtigt werden könnte. Andererseits würden die neuen Überwachungsbefugnisse erhebliche Gefahren für die Persönlichkeitsrechte von Bürgerinnen und Bürgern mit sich bringen.

Der Bundesrat verlangte unter anderem zu prüfen, ob die vorgesehenen Überwachungsbefugnisse den hohen verfassungsrechtlichen Anforderungen an die Rechtfertigung von Eingriffen in das Fernmeldegeheimnis und das Recht auf informationelle Selbstbestimmung gerecht werden. Sowohl die Geheimhaltungsbefugnis des BSI bei Sicherheitslücken als auch die Befugnisse von Diensteanbietern zur Protokollierung des Surfverhaltens der Nutzer akzeptierte der Bundesrat in dem vorgesehenen Umfang nicht.

In ihrer Entschließung vom 18. Februar 2009 fordern auch die Datenschutzbeauftragten des Bundes und der Länder eine Überarbeitung des Gesetzentwurfs. Sie begrüßen zwar grundsätzlich alle Aktivitäten, in den gewachsenen, vernetzten IT-Strukturen des Bundes das Niveau der IT-Sicherheit zu erhöhen. Gleichzeitig fordern sie jedoch, dass die zur Risikobegrenzung eingeführten Maßnahmen nicht den Datenschutz beeinträchtigen dürfen. Schon bei der Konzeption von IT-Sicherheitsmaßnahmen sei daher datenschutzgerechten Lösungen der Vorzug zu geben. So wären insbesondere Anonymisierungs- und Pseudonymisierungsverfahren geeignet, um die unnötige Registrierung des Nutzerverhaltens und die Überwachung der Kommunikation zu vermeiden.

Mit den Stimmen der großen Koalition hat der Bundestag am 19. Juni 2009 den umstrittenen Gesetzentwurf zur Kompetenzerweiterung des Bundesamtes für Sicherheit in der Informationstechnik verabschiedet. Die große Koalition hatte sich zuvor darauf geeinigt, den umstrittenen Gesetzentwurf der Bundesregierung in Kernpunkten zu entschärfen. Eine Reihe der auch von Datenschützern angemahnten Änderungen wurde berücksichtigt. So wurde die Erlaubnis für Anbieter von Telemedien gestrichen, Nutzerdaten wie IP-Adressen zum Zweck der Störungsbekämpfung zu speichern. Korrekturen hat die Koalition auch an der geplanten Befugnis für das BSI beschlossen, „Protokolldaten“ einschließlich personenbeziehbarer Nutzerinformationen unbegrenzt erheben und automatisiert auswerten zu dürfen. So wurde eine Pflicht zur Pseudonymisierung der Protokolldaten eingeführt, um die Erstellung von Kommunikationsprofilen zu verhindern. Die Befugnis zur Übermittlung der Daten an Sicherheitsbehörden wurde zudem eingeschränkt auf Straftaten nach den §§ 202a, 202b, 303a oder 303b in der Strafprozessordnung (die sogenannten Hackerparagraphen).

Der Bundesrat hat den Gesetzentwurf am 10. Juli 2009 gebilligt. Die Länderkammer fasste eine zusätzliche Entschließung. Darin bringt sie ihre Erwartung zum Ausdruck, dass die Länder unter anderem an der Erarbeitung der Regelungen, die sich auf die Informationstechnik in der Verantwortung der Länder und Kommunen auswirken können, „umfassend und rechtzeitig“ beteiligt werden.

Ich empfehle der Landesregierung, von diesem Beteiligungsrecht umfassend Gebrauch zu machen, um die IT-Sicherheit zu gewährleisten, ohne den Datenschutz der Bürgerinnen und Bürger einzuschränken.

2.1.5 Vereinfachungen bei der Freigabe von IT-Verfahren

In der Landesverwaltung und in den Kommunalverwaltungen werden in zunehmendem Maße Behörden übergreifende IT-Verfahren zur Verarbeitung personenbezogener Daten eingesetzt, die aus zentral betriebenen und dezentral in den jeweiligen Behörden eingesetzten Verfahrensteilen bestehen. Ein typisches Beispiel hierfür ist die elektronische Melderegisterauskunft, die ich im Achten Tätigkeitsbericht beschrieben habe (siehe dort Punkt 2.4.3).

Das Landesdatenschutzgesetz verlangt von der für die Verarbeitung personenbezogener Daten verantwortlichen Stelle, ein IT-Sicherheitskonzept und eine Verfahrensbeschreibung zu erstellen, ggf. eine Vorabkontrolle durchzuführen und das gesamte Verfahren formell freizugeben.

Für die oben genannten Verfahren sind diese Vorgaben mitunter objektiv schwer umzusetzen, da oft keiner der Beteiligten das gesamte Verfahren vollständig überblicken und datenschutzrechtlich bewerten kann. Für das elektronische Meldewesen hatte ich seinerzeit daher akzeptiert, dass das Innenministerium einen Teil der Aufgaben der Meldeämter übernimmt, etwa die Erstellung des zentralen Sicherheitskonzeptes und die Freigabe der zentralen Verfahrensteile, obwohl weder das Melderecht noch das Landesdatenschutzgesetz eine solche Aufgabenteilung vorsehen.

Vor diesem Hintergrund hat der Städte- und Gemeindetag im Zusammenhang mit den Beratungen der Interministeriellen Arbeitsgruppe „Deregulierung und Bürokratieabbau“ vorgeschlagen, mit einer Änderung des Landesdatenschutzgesetzes das Freigabeverfahren zu vereinfachen. Es wurde angeregt, eine zentrale Freigabestelle einzurichten, die häufig genutzte Verfahren stellvertretend für jede nutzende Behörde datenschutzrechtlich freigibt.

Die Vorschläge des Städte- und Gemeindetages sollten mit dem Vierten Gesetz zur Deregulierung und zum Demokratieabbau umgesetzt werden. Den vom Innenministerium vorgelegten Gesetzentwurf habe ich im Rahmen der Ressortanhörung jedoch abgelehnt. Die dort vorgesehene Änderung des Landesdatenschutzgesetzes hätte dazu geführt, dass das Prinzip der Verantwortlichkeit der Daten verarbeitenden Stelle für die im jeweiligen Verfahren verarbeiteten personenbezogenen Daten aufgegeben würde und somit grundlegende Datenschutzstandards der Europäischen Datenschutzrichtlinie missachtet würden.

Unstrittig war jederzeit, dass moderne E-Government-Verfahren, die viele Stellen des Landes betreffen, mit den bestehenden Regelungen des Landesdatenschutzgesetzes kaum zu erfassen und daher kaum datenschutzgerecht einzuführen und zu betreiben sind. Landesweit bereits eingesetzte oder geplante Verfahren wie das Meldewesen, die Antragsverfahren für den elektronischen Reisepass bzw. den neuen Personalausweis oder das elektronische Personenstandswesen erfordern tatsächlich praxistauglichere Regelungen etwa zur Übertragung der Verantwortlichkeit zentraler Verfahrensbestandteile oder zur Freigabe der einzelnen Teilverfahren.

Ich habe dem Innenministerium daher weiterführende Vorschläge zur Novellierung des Landesdatenschutzgesetzes unterbreitet. Kerngedanke dieser Vorschläge ist die Möglichkeit, komplexe IT-Verfahren in mehrere Teilverfahren aufzuteilen, die aus datenschutzrechtlicher Sicht dann wie selbständige Verfahren betrachtet werden. Dadurch wäre es beispielsweise möglich, die datenschutzrechtliche Verantwortung für zentrale Teile eines von mehreren Stellen genutzten Verfahrens beispielsweise auf den Betreiber dieses Teilverfahrens zu übertragen. Dieser wäre dann verpflichtet, hierfür das IT-Sicherheitskonzept und die Verfahrensbeschreibung zu erstellen, ggf. eine Vorabkontrolle durchzuführen und das Teilverfahren formell freizugeben. Für die dezentralen Verfahrensteile blieben die nutzenden Stellen weiterhin verantwortlich und die oben genannten Pflichten würden bezüglich dieser Verfahrensbestandteile dort verbleiben.

Das Innenministerium hat meine Vorschläge weitgehend aufgegriffen und den Ressortentwurf zum Vierten Gesetz zur Deregulierung und zum Demokratieabbau im Vorfeld der Verbandsanhörung entsprechend geändert. Mit Ablauf dieses Berichtszeitraumes war die Verbandsanhörung noch nicht abgeschlossen. Ich werde das Gesetzgebungsverfahren auch weiterhin begleiten.

2.1.6 Endlich ein Untersuchungshaftvollzugsgesetz

Bisher gab es noch kein spezielles Gesetz zum Vollzug der Untersuchungshaft, sondern nur wenige einzelne Bestimmungen in der Strafprozessordnung (StPO), im Strafvollzugsgesetz (StVollzG) und im Jugendgerichtsgesetz (JGG). Zwölf Bundesländer, darunter auch Mecklenburg-Vorpommern, haben einen weitgehend einheitlichen Gesetzentwurf erarbeitet. Aus datenschutzrechtlicher Sicht ist dem in der Untersuchungshaft geltenden Grundsatz der Unschuldsvermutung in einigen Bereichen noch nicht ausreichend Rechnung getragen worden. Dies bezieht sich insbesondere auch auf die Regelungen zur Datenverarbeitung im medizinischen Bereich.

Gegenüber dem Justizministerium und dem Landtag Mecklenburg-Vorpommern habe ich Folgendes empfohlen:

Vorgesehen ist, dass die Anstalt mit außervollzuglichen Einrichtungen eng zusammenarbeiten soll, um den Untersuchungsgefangenen soziale Hilfe zukommen zu lassen. Ich habe darauf hingewiesen, dass mit der Vorschrift keine Befugnisse zur Verarbeitung personenbezogener Daten verbunden sein darf. Dieses Erfordernis wurde in die Gesetzesbegründung aufgenommen.

Der Gesetzentwurf bestimmt weiter, dass andere Gefangene beim Zugangsgespräch „in der Regel“ nicht zugegen sein dürfen. In der Begründung wird aufgeführt, dass beispielsweise bei unüberwindlichen sprachlichen Verständnisschwierigkeiten ein zuverlässiger Mitgefangener hinzugezogen werden kann. Aus datenschutzrechtlicher Sicht ist jedoch ein anderer - wenn auch zuverlässiger - Gefangener grundsätzlich unbefugt, die sensiblen personenbezogenen Daten des aufzunehmenden Gefangenen, welche im Zugangsgespräch erörtert werden, zur Kenntnis zu nehmen. Allenfalls könnte die Hinzuziehung eines anderen Gefangenen von der Einwilligung des Betroffenen abhängig gemacht werden, wobei an die Freiwilligkeit besondere Anforderungen zu stellen wären. Darüber hinaus müsste dieser andere Gefangene zur Verschwiegenheit verpflichtet werden.

Es ist geregelt, dass, wenn Besuche optisch überwacht werden, die Betroffenen vorher darauf hinzuweisen sind. Weder aus dem Gesetzeswortlaut noch aus der Begründung ist ersichtlich, wie dieser Hinweis erfolgen soll. Dies sollte aus meiner Sicht jedoch ausdrücklich gesetzlich geregelt werden.

Im Hinblick auf die Bedeutung des Grundrechts des Briefgeheimnisses (Art. 10 Grundgesetz), des Grundrechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz) und im Hinblick auf die geltende Unschuldsvermutung während der Untersuchungshaft sollte geregelt werden, dass eine Anordnung der Textkontrolle nur in Einzelfällen erfolgt.

Die vorgesehene Erfassung biometrischer Merkmale soll der Identitätsfeststellung dienen. Die Regelung ist sehr weit und unbestimmt, da unter den Begriff der biometrischen Merkmale zahlreiche Merkmale fallen. Zweifel an der Erforderlichkeit ergeben sich aufgrund der Gesamtschau. So ist bereits vorgesehen, Finger- und Handflächenabdrucke, Lichtbilder und äußerliche körperliche Merkmale zur Identitätsfeststellung zu erheben. Hier sollte zumindest in der Gesetzesbegründung eine Klarstellung erfolgen, aus welchen Gründen noch zusätzliche biometrische Merkmale erforderlich sind.

Im Gesetzentwurf wird den Berufsgeheimnisträgern eine Pflicht zur Offenbarung von Geheimnissen gegenüber der Anstaltsleitung auferlegt, was einen schweren Eingriff in das durch die Berufsgeheimnisse geschützte Vertrauensverhältnis zwischen dem Untersuchungsgefangenen und dem Berufsgeheimnisträger bedeutet. Um einen besseren Schutz des Vertrauensverhältnisses zu gewährleisten, wäre aus meiner Sicht eine bloße Offenbarungsbefugnis die bessere Lösung. Keinesfalls darf die Offenbarungspflicht so weit gehen, als „dies für die Aufgabenerfüllung der Anstalt oder der Aufsichtsbehörde ... erforderlich ist“. Diese Regelung halte ich nicht mehr für verhältnismäßig.

Die Löschfrist soll für Daten in Dateien fünf Jahre betragen im Gegensatz zur entsprechenden Regelung im Strafvollzugsgesetz, wo lediglich eine zweijährige Frist vorgesehen ist. Aus datenschutzrechtlicher Sicht wird auch hier empfohlen, die Frist auf zwei Jahre zu begrenzen.

In der Beschlussempfehlung des Europa- und Rechtsausschusses vom 4. Dezember 2009 wurde der Gesetzentwurf im Wesentlichen unverändert übernommen. Mein Vorschlag, dass andere Gefangene beim Aufnahmegespräch allenfalls dann zugegen sein dürfen, wenn der aufzunehmende Gefangene einwilligt, wurde insofern modifiziert aufgegriffen, als die Formulierung nun so lautet, dass ein anderer Gefangener „nur“ anwesend sein darf, „wenn anders eine sprachliche Verständigung nicht möglich ist“.

Das Gesetz ist am 1. Januar 2010 in Kraft getreten.

2.1.7 Neues Dolmetschergesetz M-V

Das Justizministerium hat mich frühzeitig am Gesetzgebungsverfahren beteiligt. So war im Entwurf eines Ersten Gesetzes zur Änderung des Dolmetschergesetzes zunächst vorgesehen, dass die Dolmetscher- und Übersetzerlisten in elektronischer Form geführt und im Internet veröffentlicht werden können. Zudem sollte die Prüfung eines berechtigten Interesses von einsichtnehmenden Personen seitens der Justizbehörden wegfallen, da dies nicht mehr zeitgemäß sei.

Ich habe dem Ministerium empfohlen, dass, wenn eine solche Prüfung entfallen soll, aus datenschutzrechtlicher Sicht für eine frei zugängliche Veröffentlichung im Internet zumindest eine informierte Einwilligungserklärung des Dolmetschers bzw. Übersetzers erforderlich ist.

Angesichts der weltweiten Zugriffs- und unbeschränkten Verarbeitungs- und Speichermöglichkeiten auf die personenbezogenen Daten dieses Personenkreises muss es diesem selbst überlassen bleiben zu entscheiden, ob eine weltweite Veröffentlichung gewünscht ist oder nicht. In diesem Zusammenhang ist zu berücksichtigen, dass viele Dolmetscherinnen und Übersetzerinnen ihre Dienste von ihrer privaten Wohnanschrift und mit privater Telefon- und Telefaxnummer anbieten dürften, sodass es sich nicht nur um rein berufliche Daten handelt. Die Privatsphäre ist damit in gleichem Maße tangiert.

Des Weiteren habe ich empfohlen, die personenbezogenen Daten, die in die Liste aufgenommen und veröffentlicht werden, wie Name, Anschrift, Telekommunikationsanschlüsse, Beruf und die jeweilige Sprache, im Gesetz selbst zu benennen. Ebenso sollte der Gesetzgeber im Gesetz selbst bestimmen, welches Veröffentlichungsmedium genutzt werden soll.

Das Justizministerium hat meine Empfehlungen in den Gesetzestext aufgenommen. Das Gesetz wird in Kürze verabschiedet werden.

2.1.8 Umsetzung der EG-Dienstleistungsrichtlinie

Bis Ende 2009 musste die Europäische Dienstleistungsrichtlinie (RL 2006/123/EG) umgesetzt werden. Ziel dieser Richtlinie ist es, den grenzüberschreitenden Handel mit Dienstleistungen zu fördern, bestehende Hindernisse abzubauen und damit zur Verwirklichung des einheitlichen, europäischen Binnenmarktes beizutragen. Dabei soll die Aufnahme und Ausübung von Dienstleistungstätigkeiten künftig deutlich leichter werden. Ein wichtiges Instrument hierfür bilden die sogenannten "Einheitlichen Ansprechpartner".

Das Ministerium für Wirtschaft, Arbeit und Tourismus Mecklenburg-Vorpommern (WM M-V) hat einen Gesetzentwurf vorgelegt, mit dem die Anforderungen der EG-Dienstleistungsrichtlinie umgesetzt werden sollen. In das Gesetzgebungsverfahren wurde meine Behörde frühzeitig einbezogen. Schwerpunkt der datenschutzrechtlichen Betrachtung war neben den Änderungen einiger spezialgesetzlicher Vorschriften insbesondere der Entwurf des Einheitlicher-Ansprechpartner-Errichtungsgesetzes Mecklenburg-Vorpommern (EAPG M-V). Danach sollen die Industrie- und Handelskammern sowie die Handwerkskammern des Landes die Aufgaben des Einheitlichen Ansprechpartners wahrnehmen.

In dem betreffenden Gesetzentwurf wurde auf eine spezielle datenschutzrechtliche Regelung verzichtet. Das WM M-V war der Auffassung, dass es keiner derartigen Regelung bedarf, solange die Einheitlichen Ansprechpartner im Rahmen und in Erfüllung der ihnen zugewiesenen Aufgaben handeln. Ich habe das Ministerium jedoch darauf hingewiesen, dass das EAPG M-V eine datenschutzrechtliche Regelung enthalten muss. Insbesondere müssen die zu schaffenden gesetzlichen Vorschriften zur Umsetzung der EG-Dienstleistungsrichtlinie den Zweck und die Verarbeitung personenbezogener Daten festlegen und beschränken.

Der Einheitliche Ansprechpartner tritt als Kontaktstelle bzw. Kontaktperson in Erscheinung, mit dessen Hilfe jeder Dienstleistungserbringer alle Verfahren, Formalitäten und Anfragen abwickeln kann. Über ihn werden alle europäischen Dienstleister (auch aus der Ferne) Formalitäten elektronisch abwickeln können. Um diese Aufgabe durchführen zu können, muss der Einheitliche Ansprechpartner die gleichen (aber auch nicht mehr) Befugnisse wie die für die Aufgabenerfüllung originär zuständige Behörde haben. Hierzu habe ich dem WM M-V eine entsprechende Regelung vorgeschlagen, die in der Folge gesetzlich festgeschrieben wurde.

Gleichzeitig lag mir ein Entwurf der Landesregierung zu einem Gesetz zur verwaltungsrechtlichen Umsetzung der EG-Dienstleistungsrichtlinie in das Landesrecht von Mecklenburg-Vorpommern (EG-DLRG M-V) vor. Mit diesem Gesetzentwurf sollen allgemeine verwaltungsrechtliche Anforderungen der EG-Dienstleistungsrichtlinie im Verwaltungsverfahrensgesetz umgesetzt werden. Aufgrund der sogenannten Simultangesetzgebung (Gleichklang der Verwaltungsverfahrensgesetze des Bundes und der Länder) orientierte man sich dabei an Bestimmungen des Bundes.

In dieses gesetzgeberische Verfahren wurde ich nicht einbezogen, sodass ich meine Stellungnahme hierzu direkt an den Vorsitzenden des Innenausschusses des Landtages (federführender Ausschuss) richtete. Gleichzeitig habe ich gegenüber dem Innenministerium eine Beanstandung wegen des Verstoßes gegen die Beteiligungspflicht nach § 33 Abs. 2 Satz 3 DSG M-V sowie § 4 Abs. 3 GGO II ausgesprochen.

In meiner Stellungnahme wies ich darauf hin, dass der Einheitliche Ansprechpartner einen umfangreichen Zugriff auf alle personenbezogenen Daten eines Dienstleisters hat. Voraussetzung hierfür ist, dass der Dienstleister seinen Antrag an den Einheitlichen Ansprechpartner richtet. Aufgrund des Umfangs und der Sensibilität dieser Daten muss technisch und organisatorisch sichergestellt werden, dass die Datensicherheit und der Datenschutz auf einem angemessen hohen Niveau sind. Beispielsweise müssen die Authentizität und die Integrität der Daten durch die Verwendung von elektronischen Signaturen gesichert und für die Wahrung der Vertraulichkeit kryptographische Verschlüsselungsverfahren eingesetzt werden. Ich habe empfohlen, hierzu konkrete gesetzliche Regelungen zu treffen.

In dem betreffenden Gesetzentwurf sind ebenfalls Regelungen zur Europäischen Verwaltungszusammenarbeit enthalten, bei denen es sich nicht um Datenübermittlungsbefugnisse, sondern um Amtshilfevorschriften handelt. Durch Amtshilfevorschriften können aber Eingriffe in die Grundrechtsposition der Betroffenen nicht legitimiert werden. Folglich bedarf es hier einer gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen ergeben. Ich habe dem Innenausschuss des Landtages empfohlen, Befugnisnormen für die Datenverarbeitung bereichsspezifisch zu regeln.

Ich empfehle der Landesregierung sicherzustellen, dass die erforderlichen Maßnahmen zur Datensicherheit und zum Datenschutz in den hierfür erforderlichen Sicherheitskonzepten festgeschrieben und ausnahmslos umgesetzt werden. Außerdem müssen Regelungen zum Einsatz von elektronischen Signaturen getroffen werden.

Nach Redaktionsschluss hat mir der Innenminister den Entwurf einer Rechtsverordnung vorgelegt, in der vor allem Vorgaben zur Sicherstellung der elektronischen Verfahrensabwicklung und der elektronischen Kommunikation unter Berücksichtigung der Maßnahmen zur Datensicherheit nach den §§ 21 und 22 DSG M-V getroffen werden. Zu diesem Entwurf habe ich Stellung genommen und dabei insbesondere auf die Erforderlichkeit der qualifizierten elektronischen Signatur hingewiesen.

2.2 Polizei/Ordnungsbehörden

2.2.1 Kfz-Scanning durch die Polizei

In meinem Achten Tätigkeitsbericht (Punkt 2.2.4) hatte ich über den Einsatz des automatisierten Kfz-Kennzeichen-Lesesystems (AKLS) beim G8-Gipfel berichtet und kritisiert, dass es mir aufgrund der Löschung der Dateien nicht möglich war zu prüfen, inwieweit der Einsatz des AKLS einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt.

Inzwischen hat das Bundesverfassungsgericht mit seiner Entscheidung vom 11. März 2008 (1 BvR 2074/05 und 1 BvR 1254/07) die automatische Erfassung von Autokennzeichen in Hessen und Schleswig-Holstein für verfassungswidrig und nichtig erklärt. Es hat die Verwendung des Begriffes „Fahndungsbestand“ als zu unbestimmt bezeichnet, sodass letztlich nicht ausgeschlossen werden kann, dass auch Ausschreibungen zur polizeilichen Beobachtung einbezogen sind. Das hat zur Folge, dass eine systematische, räumlich weit reichende Sammlung von Informationen über das Bewegungsverhalten von Fahrzeugen und damit auch von Personen mit technisch geringem Aufwand möglich ist. Ebenso haben die höchsten Richter kritisiert, dass der Vorschrift eine hinreichende Zweckbestimmung fehle.

Damit dürften auch die entsprechenden Regelungen in Mecklenburg-Vorpommern die Autofahrer in ihrem Grundrecht auf informationelle Selbstbestimmung verletzen.
Die Voraussetzungen für die Möglichkeit der Polizei, gemäß § 43 a Abs. 2 SOG M-V die Kfz-Kennzeichen nicht nur mit dem Fahndungsbestand, sondern auch mit anderen polizeilichen Dateien abzugleichen, sind viel zu unpräzise formuliert.

Unter Hinweis auf die Rechtsprechung des Bundesverfassungsgerichts und ein im Auftrag des Allgemeinen Deutschen Automobilclubs e. V. (ADAC) erstelltes Rechtsgutachten zu diesem Thema, welches ebenfalls zu dem Ergebnis kommt, dass § 43 a Abs. 2 SOG M-V teilweise zu unbestimmt und unverhältnismäßig und daher teilweise verfassungswidrig sei, habe ich die Landesregierung aufgefordert, eine entsprechende Änderung der gesetzlichen Ermächtigungsnormen vorzunehmen und mich frühzeitig an dem Gesetzgebungsverfahren zu beteiligen.

2.2.2 Regelungen bei verdeckten Datenerhebungen

In meinem Achten Tätigkeitsbericht (Punkt 2.2.4) hatte ich meine datenschutzrechtlichen Bedenken über die im Zusammenhang mit dem G8-Gipfel durchgeführten Observationen der BAO KAVALA dargelegt und der Landesregierung empfohlen, meine Vorschläge bei der nächsten Novellierung des Sicherheits- und Ordnungsgesetzes Mecklenburg-Vorpommern (SOG M-V) zu berücksichtigen.

Auf meine Kritik, dass für die Observationsdauer in § 33 Abs. 1 Satz 1 2. Alternative SOG M-V keine zeitliche Obergrenze festgelegt ist, hat die Landesregierung entgegnet, dass dies nicht notwendig sei und im Übrigen aus polizeilicher Sicht nicht praktikabel erscheine. In den fraglichen Observationsanordnungen sei eine Befristung der Maßnahmen in jedem der vorliegenden Fälle vorgenommen worden. Die entsprechenden Anordnungen hierzu würden vom Behördenleiter schriftlich unter Angabe der für sie maßgeblichen Gründe erfolgen. Das Vorliegen der Voraussetzungen für solche intensiven Maßnahmen werde selbstverständlich stetig überprüft.

Zu meiner weiteren Kritik am Einsatz von Observationsmaßnahmen bei sogenannten Kontakt- und Begleitpersonen hat die Landesregierung auf § 33 Abs. 2 Satz 2 SOG M-V verwiesen, wonach die Polizei solche Personen nur dann observieren kann, wenn diese mit Personen, bei denen tatsächliche Anhaltspunkte dafür bestehen, dass sie Straftaten erheblicher Bedeutung (§ 49 SOG M-V) begehen werden, bzw. mit Personen, die an diesen Straftaten beteiligt sind, hierzu in Verbindung stehen. Insofern fordere die Maßnahme der Observation von Kontakt- und Begleitpersonen, dass tatsächliche Anhaltspunkte vorliegen.

Auch hatte ich bemängelt, dass in den Anordnungen zu den betreffenden Observationen eine Feststellung darüber fehlt, dass die Aufklärung des Sachverhaltes zum Zweck der Verhütung solcher Straftaten oder ihrer möglichen Verfolgung auf andere Weise nicht möglich ist (ultima ratio). Hierauf hat die Landesregierung entgegnet, dass der BAO KAVALA keine anderen Möglichkeiten zur Verfügung gestanden hätten, die Vorhaben der betreffenden Personen - anlassbezogene Straftaten hinsichtlich des WWG 8 - zu verhindern.

Aufgrund meiner schwerwiegenden Bedenken im Hinblick auf die fehlende Unterrichtung des Betroffenen und damit die fehlende rechtliche Nachprüfbarkeit der Maßnahme hat die Landesregierung mitgeteilt, dass die entsprechende Regelung überprüft werde.

Diese Überprüfung ist jedoch bislang nicht erfolgt, sodass ich der Landesregierung empfehle, §§ 34 Abs. 6 i. V. m. Abs. 5 SOG M-V in der Novellierung des Sicherheits- und Ordnungsgesetzes zu berücksichtigen.

2.2.3 Anlassloses „Blitzen“ im Straßenverkehr - Beschluss des Bundesverfassungsgerichts vom 11. August 2009

Das Bundesverfassungsgericht hat sich im Jahr 2006 mit einer Geschwindigkeitsmessung beschäftigt, welche auf einem in Mecklenburg-Vorpommern gelegenen Autobahnabschnitt durchgeführt wurde. Die Videoaufzeichnung wurde mit dem Verkehrskontrollsystem Typ VKS vorgenommen.

Dem Beschwerdeführer warf man eine Geschwindigkeitsüberschreitung vor. In dem Bußgeldbescheid wurde als ausreichende Rechtsgrundlage der Erlass zur Überwachung des Sicherheitsabstandes nach § 4 StVO des Wirtschaftsministeriums Mecklenburg-Vorpommern angegeben. Hiergegen wandte sich der Beschwerdeführer und führte dabei an, dass die Videoaufzeichnung des Verkehrsverstoßes mangels konkreten Tatverdachts ohne ausreichende Rechtsgrundlage angefertigt worden sei.

Die zweite Kammer des Zweiten Senats des Bundesverfassungsgerichts hat in ihrem Beschluss vom 11. August 2009 (2 BvR 941/08) festgestellt, dass „die Rechtsauffassung, die mittels einer Videoaufzeichnung vorgenommene Geschwindigkeitsmessung könnte auf einen Erlass eines Ministeriums gestützt werden, unter keinem rechtlichen Aspekt vertretbar und daher willkürlich“ ist.

Das Bundesverfassungsgericht hat schlussfolgernd die vorinstanzlichen Entscheidungen (Urteil des Amtsgerichts Güstrow und Beschluss des Oberlandesgerichts Rostock) aufgehoben und die Sache zur erneuten Entscheidung an das Amtsgericht Güstrow zurückverwiesen.

Ich habe bereits bei verschiedenen Gelegenheiten und so insbesondere auch jetzt gegenüber verschiedenen Landesministerien darauf hingewiesen, dass nach § 46 Abs. 1 Ordnungswidrigkeitengesetz (OWiG) die Vorschriften der Strafprozessordnung (StPO) zwar „sinngemäß“ anzuwenden sind, dies allerdings nur generell für die allgemeinen Gesetze über das Strafverfahren, die wegen der unterschiedlichen Bedeutung beider Verfahren nicht immer im vollen Umfang auf das Bußgeldverfahren übertragbar sind, gilt. So dürfen nach § 100 h Abs. 1 Nr. 1 StPO auch ohne Wissen des Betroffenen außerhalb von Wohnungen Bildaufnahmen hergestellt werden, wenn die Erforschung des Sachverhaltes oder die Übermittlung des Aufenthaltsortes eines Beschuldigten auf andere Weise weniger Erfolg versprechend oder erschwert wäre. Ob diese Vorschrift, die für den Bereich der Strafverfolgung geschaffen worden ist, tatsächlich in verhältnismäßiger Weise für Verkehrsordnungswidrigkeitsverstöße herangezogen werden kann, erscheint mir insbesondere unter Berücksichtigung der Vorgaben des Volkszählungsurteils (BVerfGE 65, 1 ff.) und der ständigen Rechtsprechung des Bundesverfassungsgerichts zur Normenklarheit und Bestimmtheit gesetzlicher Eingriffsbefugnisse in das Recht auf informationelle Selbstbestimmung fraglich. Insofern sollte der Beschluss des Bundesverfassungsgerichts auch für das Innenministerium Mecklenburg-Vorpommern Anlass sein, die Rechtsgrundlagen für die Videoüberwachung durch Polizei im Bereich der präventiven Verkehrsüberwachung zu überprüfen.

Das Amtsgericht Güstrow hat das Verfahren in dem betreffenden Bußgeldverfahren nach § 47 Abs. 2 OWiG nunmehr eingestellt.

Ich empfehle der Landesregierung, darauf hinzuwirken, dass durch den zuständigen parlamentarischen Gesetzgeber eine normenklare und verhältnismäßige gesetzliche Grundlage zur Videoüberwachung im Straßenverkehr geschaffen wird.

2.2.4 Homepageüberwachung beim BKA

Anlässlich einer Kontrolle zu einem DNA-Massentest bei einer Kriminalpolizeiinspektion hat mir der zuständige Beamte Folgendes mitgeteilt: Beim Bundeskriminalamt (BKA) gebe es eine Fahndungsseite, die nicht primär dem Ziel der Information der Öffentlichkeit diene, sondern vielmehr dazu angelegt sei, damit das BKA Zugriffe auf diese Internetseite verfolgen könne. Es würde von der Vermutung ausgegangen, dass der potentielle Täter die Seite gegebenenfalls häufiger aufruft, um sich über Neuigkeiten in dem Fall auf dem Laufenden zu halten. Daher würden die Zugriffe auf die Internetseiten durch das BKA registriert und verfolgt. In einem Fall sei die ermittelnde Kriminalpolizei durch das BKA über häufige Zugriffe informiert worden. Ein Zusammenhang des Nutzers mit der Tat konnte jedoch nach der Befragung durch die Kriminalpolizei ausgeschlossen werden.

Da mir dieses Vorgehen aus datenschutzrechtlicher Sicht problematisch erschien, habe ich den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) gebeten, dies beim BKA näher zu prüfen.

Die Homepageüberwachung wird technisch dergestalt durchgeführt, dass die Protokolldaten, die bei Zugriffen auf bestimmte Fahndungsseiten auf dem Webserver des BKA anfallen, in einem separaten Auswertungs-Server gespeichert werden. Sofern der Browser des Nutzers dies zulässt, werden „Cookies“ gesetzt. Das Verfahren funktioniert aber auch, wenn Cookies deaktiviert sind. Die Auswertung erfolgt mit einer speziellen Anwendung. Es werden die Zugriffe mit folgenden Daten aufgelistet: interne Nummer, Anzahl der aufgerufenen Seiten, Zeitpunkt und IP-Adresse der ersten Nutzung, Zeitpunkt und IP-Adresse der letzten Nutzung, Informationen zum Provider. Somit ist das Internetnutzungsverhalten einer konkreten Person zuzuordnen.

Rechtsgrundlage für die polizeiliche Auswertung stellt nach Auffassung des Bundesministeriums des Innern und des BKA § 163 Abs. 1 Strafprozessordnung (StPO) dar. Wenn derartige Maßnahmen ergriffen werden, sei regelmäßig ein entsprechender Anfangsverdacht gegeben. Die verdeckte Recherche zur weiteren Sachverhaltserforschung sei daher durch die oben genannte Rechtsgrundlage gedeckt.

Der BfDI hat dazu die Auffassung vertreten, dass die StPO hier nicht zur Anwendung kommt. Stellt ein Anbieter eine Website ins Netz, so handelt es sich hierbei um ein Angebot im Bereich der Telemedien. Die beim Aufruf eines solchen Angebots beim Anbieter entstehenden sog. Nutzungsdaten sind Daten, die im Rahmen der Telekommunikation zum Zwecke der Erbringung des Dienstes zwangsläufig anfallen. Der Umgang mit diesen Nutzungsdaten richtet sich nach dem Telemediengesetz (TMG). § 15 TMG gewährt keine Befugnis für die hier streitige Verwendung der Nutzungsdaten durch das BKA, da der Diensteanbieter personenbezogene Daten eines Nutzers nur erheben und verwenden darf, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Zudem liegt keine Anordnung einer Strafverfolgungsbehörde vor. § 100g StPO scheidet hier aus, da die Regelung nicht auf Nutzungsdaten nach dem TMG anwendbar ist.

Wegen der Intensität des Grundrechtseingriffs bei einer Homepageüberwachung im Hinblick auf die Heimlichkeit der Maßnahme und auch den Umfang der dadurch betroffenen Personenkreise ist grundsätzlich schon der Rückgriff auf die Generalklausel der §§ 161, 163 StPO äußerst fraglich. Daher fehlte es an einer tragfähigen Rechtsgrundlage für die vom BKA praktizierte Homepageüberwachung.

Die Bundesregierung hat sich dieser Rechtsauffassung im Wesentlichen angeschlossen. Das Bundesministerium des Innern hat das BKA angewiesen, mit den betroffenen Staatsanwaltschaften Einvernehmen über die Beendigung etwaiger laufender Maßnahmen herzustellen und künftig das Instrument der Homepageüberwachung nicht mehr einzusetzen.

2.2.5 Videoüberwachung des Marktplatzes in Neubrandenburg

Die Polizeidirektion (PD) Neubrandenburg hat bei mir angefragt, ob ich eine geplante Videoüberwachung des Marktplatzes Neubrandenburg und angrenzender Teilbereiche aus datenschutzrechtlicher Sicht für rechtmäßig erachte, und mir den Entwurf einer Anordnung des Behördenleiters übersandt. Der Marktplatz Neubrandenburg sowie der sich anschließende Umgebungsbereich des Marktplatzcenters sollten nach der Konzeption der PD Neubrandenburg videoüberwacht werden. Der Marktplatz wurde zum Zeitpunkt unseres Vororttermins baulich komplett umgestaltet. Es befinden sich dort ein Hotel und Cafes, welche auf dem Platz Tische und Stühle aufgestellt haben. Auf einer Seite des Platzes am „Haus der Kultur und Bildung“ (HKB) befindet sich eine Freitreppe, die in der Vergangenheit sehr viel von Jugendlichen, jungen Erwachsenen und „Szenegängern“ als Treffpunkt genutzt wurde. Auch diese Freitreppe wird baulich umgestaltet und soll erhalten bleiben. Es handelt sich insgesamt gesehen um einen belebten und beliebten Platz, der auch durch das angrenzende Marktplatzcenter eine der zentralen Einkaufsmöglichkeiten der Stadt darstellt.
In der Vergangenheit kam es gehäuft zu Straftaten in diesem Bereich. Dies wurde durch statistische Zahlen aus den Jahren 2004 bis 2008 untermauert.

Die PD Neubrandenburg führt § 32 Abs. 3 Satz 2 SOG M-V als einschlägige Rechtsgrundlage an. Danach dürfen Bilder offen aufgezeichnet werden, soweit an diesen Orten wiederholt Straftaten begangen worden sind und Tatsachen die Annahme rechtfertigen, dass dort künftig mit der Begehung von Straftaten zu rechnen ist. Der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern sieht grundsätzliche verfassungsrechtliche Probleme im Hinblick auf die Regelung des § 32 Abs. 3 SOG M-V. Selbst wenn man sich über diese Bedenken hinwegsetzen würde und die Auffassung verträte, dass auch eine Häufung von einfachen und mittelschweren Straftaten an einem Ort einen Kriminalitätsbrennpunkt (so die Gesetzesbegründung, vgl. Drucksache 4/2116 vom 22. Februar 2006, S. 21) darstellen kann, müsste dies seitens der PD Neubrandenburg aufgrund von objektiv nachvollziehbaren, ortsbezogenen Lageerkenntnissen dargelegt werden. Letztendlich ist die Videoüberwachung im vorliegenden Fall aus Gründen der Verhältnismäßigkeit abzulehnen. Der Grundsatz der Verhältnismäßigkeit gebietet es, dass die Einbußen an grundrechtlich geschützter Freiheit nicht in unangemessenem Verhältnis zu den Gemeinwohlzwecken stehen dürfen, denen die Grundrechtseinschränkung dient.
Die Kriminalitätsbelastung müsste sich deutlich von derjenigen vergleichbarer anderer Orte abheben. Die absoluten Zahlen zur Straßenkriminalität waren in dem betreffenden videozuüberwachenden Gebiet rund um den Marktplatz nicht sonderlich hoch und mit denen anderer Großstädte nicht zu vergleichen. Bei einem Großteil der Delikte handelte es sich um Fahrraddiebstähle, die dem Bereich der einfachen und mittleren Kriminalität zuzurechnen sind. Diese Zahlen rechtfertigen jedoch nicht den Grundrechtseingriff, den eine Vielzahl von sich normgerecht verhaltenden Bürgern hinzunehmen hätte, die sich an einem zentralen Marktplatz einfach nur entspannen möchte, indem sie die umliegenden Cafes nutzt oder ihre Einkäufe erledigt. Ebenso dürfe auch das „Haus der Kultur und Bildung“, welches zurzeit unseres Vororttermins umgebaut wurde und künftig als Kultur- und Kongresszentrum genutzt wird, einen weiteren kommunikativen Treffpunkt darstellen, den Menschen unbeobachtet von Videokameras nutzen können sollten.

Tatsachen, die die Annahme künftiger Straftatenbegehungen als Voraussetzungen des § 32 Abs. 3 Satz 2 SOG M-V rechtfertigen würden, sind nicht überzeugend vorgetragen worden.

Ich hatte der PD Neubrandenburg empfohlen, von der geplanten Videoüberwachung des Marktplatzes Abstand zu nehmen. Dieser Empfehlung ist die PD gefolgt.

2.2.6 Speicherung Strafunmündiger im Kriminalaktennachweis (KAN)

Das Bundesministerium des Innern (BMI) übersandte den Innenministerien der Länder Änderungen in der Errichtungsanordnung zum Kriminalaktennachweis (KAN). Ich habe in einer Stellungnahme gegenüber unserem Innenministerium erhebliche datenschutzrechtliche Bedenken hinsichtlich der Speicherung Strafunmündiger im KAN geäußert. Wegen der besonderen Eingriffstiefe, die von der Speicherung personenbezogener Daten zur Vorsorge für die spätere Strafverfolgung für die Strafunmündigen ausgeht, und der Gefahr einer Stigmatisierung bedarf es einer normenklaren Rechtsgrundlage. Insbesondere halte ich die bundesweite Speicherung dieses Personenkreises weder für erforderlich noch für verhältnismäßig.

§ 8 BKAG dient der Verhütung von Straftaten und der Vorsorge für die künftige Strafverfolgung. Mit der Erfassung von Daten Strafunmündiger würden damit Daten von Personen auf Vorrat aufgenommen werden, denen auf Grund ihres geistigen und seelischen Entwicklungsstadiums die Einsichtsfähigkeit in die von ihnen begangenen Handlungen fehlt. Die Speicherung erfolgt also zu einem Zeitpunkt, in dem die weitere Entwicklung des Kindes nicht absehbar ist. Wegen dieser Unsicherheit in der Prognose besteht meines Erachtens die Gefahr, dass durch die ständige Verlängerung der Aussonderungsprüffristen „Jugendsünden“ über einen längeren Zeitraum abgebildet werden. Anknüpfungspunkt für die Speicherung von Kindern sollte zumindest sein, dass sie bereits strafbare Handlungen begangen haben.

Das BMI hält jedoch in seiner Erwiderung eine Speicherung im KAN für unabdingbar. Diese sei auf Intensivtäter beschränkt, bei denen die Prognose besteht, dass sie auch nach Erreichen des 14. Lebensjahres weiterhin Straftaten von erheblicher Bedeutung begehen werden. Die strengen Tatbestandsvoraussetzungen würden ausschließen, dass „Jugendsünden“ zu einer Speicherung führen. Die Speicherung sei nur gestattet, wenn bestimmte Tatsachen die Annahme rechtfertigen, dass die Betroffenen Straftaten von erheblicher Bedeutung begehen werden. Die Prognose, dass der Strafunmündige in der Zukunft irgendwelche (geringfügigen) Straftaten begehen wird, reicht nach Aussage des BMI für eine Speicherung nicht aus, weshalb eine „Jugendsünde“ die Speicherung gerade nicht rechtfertigt. Inzwischen ist die Änderung in der Errichtungsanordnung vollzogen worden.

Ich werde dementsprechend bei den Polizeidienststellen Stichproben durchführen, um zu gewährleisten, dass die strengen Einschränkungen auch umgesetzt werden.

2.2.7 Musikfestival - Anforderung einer Liste sämtlicher Mitarbeiter durch die Ordnungsbehörde

Der Veranstalter eines Musikfestivals hatte sich an mich gewandt, weil er von der Gemeinde aufgefordert worden war, im Vorfeld der Veranstaltung die personenbezogenen Daten aller mit dem Festival Beschäftigten, wie Sicherheitskräfte, Versorgungsunternehmen und Mitarbeiter des Veranstalters, mitzuteilen. Diese Forderung wurde von der Gemeinde und von der Polizei damit begründet, dass es bei dem Festival im vorherigen Jahr einen schweren Unfall gegeben habe, bei dem es dem Veranstalter auf Grund der Unfallzeit außerhalb der Dienstzeiten der Mitarbeiter im betreffenden Bereich erst Stunden nach dem Unfall gelang, den Unfallfahrer zu benennen. Nach Auffassung des Veranstalters hätte die Polizei auch mit einer Liste der Namen und Adressen aller Beschäftigten den Fahrer nicht schneller ausfindig machen können. Der Rechtsvertreter des Veranstalters hatte Bedenken hinsichtlich des Arbeitnehmerdatenschutzes und bat mich daher um eine datenschutzrechtliche Bewertung.

Das zuständige Amt hatte als Rechtsgrundlage für die Anforderung einer Liste sämtlicher Mitarbeiter § 34c und § 55 ff. Gewerbeordnung (GewO) angegeben. § 34c GewO ist jedoch nicht einschlägig. In dieser Vorschrift geht es um die Erlaubnis zur Gewerbetätigkeit von Maklern, Anlageberatern, Bauträgern und Baubetreuern. Darunter fällt der Veranstalter nicht. Er zieht für jedes Festival Fachfirmen heran, welche die fliegenden Bauten wie Zelte und Bühnen errichten. Die Bauten dieser Firmen werden von der zuständigen unteren Baubehörde abgenommen; der Petent kauft die Leistungen der Fachfirmen einschließlich der Abnahmen der unteren Baubehörde ein. Diese kümmert sich also um die Sicherheit der Besucher, was die fliegenden Bauten anbelangt. Eine Liste der für die Aufbauten hinzuzuziehenden Fachfirmen mit den Namen der Geschäftsführer wurde dem Amt bereits zugesagt.

Wer gewerbsmäßig Leben und Eigentum fremder Personen bewachen will, muss gemäß § 34a GewO eine Erlaubnis seitens der zuständigen Behörde einholen. Zu diesem Zweck können von Personen weitere personenbezogene Daten gemäß § 34a Abs. 1 Satz 4 GewO eingeholt werden. Um die Beantragung einer solchen Erlaubnis handelt es sich hier jedoch offenkundig nicht, sodass auch diese Vorschrift als Ermächtigungsnorm zur Abfrage weiterer personenbezogener Daten nicht einschlägig wäre. Gleichwohl hatte der Veranstalter eine namentliche Aufstellung der Sicherheitskräfte und die Vorlage der notwendigen Nachweise zugesichert.

Ebenso verhielt es sich mit der Versorgung der Festivalbesucher. Die Händler, die die Versorgung übernehmen, werden von dem Veranstalter aufgrund von Mietverträgen verpflichtet. Diese Händler sind nach den Angaben des Veranstalters sämtlich im Besitz von Reisegewerbekarten gemäß §§ 55 ff. GewO. Sie verfügen auch über die notwendigen Hygienescheine. Die lebensmittelrechtlichen Vorschriften werden eingehalten und von dem zuständigen Hygieneamt - und nicht von der Gemeinde - kontrolliert.

Insofern war es aus datenschutzrechtlicher Sicht nicht nachvollziehbar, warum eine namentliche Aufstellung aller Beschäftigten eingereicht werden sollte, um die Einhaltung der lebensmittelrechtlichen Vorschriften zu gewährleisten. Auch hier reicht für das zuständige Hygieneamt ein Ansprechpartner für den Fall, dass eine Versorgungsfirma die Hygienevorschriften nicht einhält.

Nach Auskunft des Rechtsvertreters des Veranstalters hat sich dieser letztendlich mit dem Amt darüber geeinigt, dass im Vorfeld der Veranstaltung eine Liste mit den Firmen und deren Geschäftsführern/Inhabern sowie eine namentliche Aufstellung der Sicherheitskräfte und die notwendigen Nachweise vorgelegt werden.

2.3 Verfassungsschutz

2.3.1 Elektronische Vorgangsbearbeitung beim Verfassungsschutz

Bereits im Siebten Tätigkeitsbericht (Punkt 2.3.1) hatte ich die Verfassungsschutzbehörde darauf hingewiesen, dass für die elektronische Vorgangsbearbeitung eine gesetzliche Grundlage zu schaffen ist. Am Gesetzgebungsverfahren bin ich beteiligt worden. Der Gesetzentwurf sah vor, dass die Sicherheitsakte und die Sicherheitsüberprüfungsakte auch in elektronischer Form geführt werden dürfen. Des Weiteren ist eine Abfrage personenbezogener Daten mittels automatisierter Verarbeitung nur zulässig, wenn für sie die Voraussetzung der Speicherung vorliegt.

Hintergrund dieser Ergänzung ist, dass die Verfassungsschutzbehörde schon vor einigen Jahren begonnen hat, die Vorgangsbearbeitung auf eine elektronische Basis umzustellen. Ich hatte die Verfassungsschutzbehörde in der Vergangenheit wiederholt auf die Gefahren hingewiesen, die mit einer automatisierten Datenverarbeitung einhergehen. Insbesondere habe ich darauf aufmerksam gemacht, dass im Rahmen von Sicherheitsüberprüfungen Daten sogenannter Randpersonen, wie Auskunfts- und Referenzpersonen, nicht elektronisch gespeichert werden dürfen.

Es ist davon auszugehen, dass auch künftig nur ein Teil der Korrespondenz in elektronischer Form abgewickelt wird. Um in Papierform eingehende Dokumente in elektronischer Form weiter zu verarbeiten, wird regelmäßig das Einscannen der Posteingänge erforderlich sein. Wenn vor dem Scannen nicht geprüft wird, ob die Schreiben personenbezogene Daten sogenannter Randpersonen enthalten, ist nicht auszuschließen, dass deren Daten vorschriftswidrig elektronisch gespeichert werden. Wenn die eingescannten Dokumente zudem nicht mit einer Texterkennungssoftware behandelt werden, besteht auch keine Möglichkeit, etwa durch eine Volltextsuche unzulässig gespeicherte Daten zu finden, um sie wenigstens nachträglich zu löschen. Im Ergebnis ist zu befürchten, dass somit auch personenbezogene Daten von Betroffenen, die nicht zu dem Kreis der sicherheitszuüberprüfenden Personen gehören, von der Verfassungsschutzbehörde im EDV-System gespeichert und wieder auffindbar sind.

Zusätzlich begegnet die elektronische Vorgangsbearbeitung im Sicherheitsüberprüfungsbereich Bedenken insofern, als immer noch die Wahrnehmung der Aufgaben des Geheimschutzbeauftragten des Innenministeriums (als zuständiger Stelle für die Einleitung und Durchführung der Sicherheitsüberprüfung) und der Aufgaben des stellvertretenden Leiters der Verfassungsschutzabteilung/Referatsleiter für den Bereich Sicherheitsüberprüfungsakten (als mitwirkender Behörde, § 4 Abs. 3 Sicherheitsüberprüfungsgesetz (SÜG M-V)) in einer Person stattfindet.

Der Gesetzgeber hat jedoch eine ausdrückliche Trennung beider Stellen vorgesehen. Intention des Gesetzgebers war es, dass die zuständige Stelle die Sicherheitsüberprüfung durchführt und die Verfassungsschutzbehörde eben „nur“ mitwirkt. Aufgrund der jetzigen Praxis kann nicht sichergestellt werden, dass die Informationen aus den jeweiligen Aufgabenfeldern nur in dem gesetzlich zulässigen Umfang in die Bewertung des zu beurteilenden Sachverhalts einfließen. Dadurch wird das Recht auf informationelle Selbstbestimmung der von Sicherheitsüberprüfungen betroffenen Mitarbeiterinnen und Mitarbeiter des Innenministeriums verletzt. Ich habe das Ministerium wiederholt auf diese Problematik hingewiesen, ohne dass bisher eine Umstrukturierung in Erwägung gezogen wurde.

Leider sind die oben genannten Regelungen - ohne meine datenschutzrechtlichen Bedenken aufzugreifen - durch das Gesetz zur Änderung von Vorschriften den Verfassungsschutz betreffend vom 28. Januar 2009 unverändert in Kraft getreten.

2.4 Einwohnerwesen/Kommunales

2.4.1 Wenn Asylbewerber Freunde oder Verwandte besuchen wollen

Der Flüchtlingsrat Mecklenburg-Vorpommern e. V. hat mir den vom Innenministerium herausgegebenen Vordruck „Antrag auf Erlaubnis zum vorübergehenden Verlassen des Bereichs der Duldung gemäß § 12 Abs. 5 i. V. m. § 61 Abs. 1 Aufenthaltsgesetz“ zur datenschutzrechtlichen Prüfung übersandt.

Der Vordruck war aus datenschutzrechtlicher Sicht widersprüchlich gestaltet. Einerseits waren die Angaben Geburtsdatum und Staatsangehörigkeit der zu besuchenden Person nicht als Pflichtangaben gekennzeichnet, andererseits aber enthielt der Vordruck am Ende den Satz „Nur vollständig ausgefüllte Anträge werden bearbeitet!“. So war es für einen Asylbewerber aus unserem Bundesland zum Beispiel unklar, ob er, wenn er einen Freund in Hamburg besuchen wollte, auch einzelne Angaben weglassen darf und ob sein Antrag dann trotzdem noch bearbeitet werden würde.

Es ist durchaus wahrscheinlich, dass ein Asylbewerber nicht zwangsläufig das Geburtsdatum jeder Person kennt, die er besuchen möchte. Zudem ist fraglich, ob die Ausländerbehörde in jedem Falle wissen muss, welche Staatsangehörigkeit die zu besuchende Person hat.

Dem Innenministerium als zuständiger Fachaufsichtsbehörde habe ich meine Bedenken mitgeteilt und darüber hinaus angemerkt, dass im vorliegenden Sachverhalt nicht hinreichend deutlich wird, dass die Ausländerbehörde stets (unabhängig von einem Vordruck) bei jeder Entscheidung über ein vorübergehendes Verlassen des beschränkten Aufenthaltsbereiches ihr Ermessen pflichtgemäß ausüben muss. Das Ministerium hat meine Hinweise zum Anlass genommen und sowohl die Hinweise überarbeitet, die die Ausübung des Ermessens betreffen, als auch den Vordruck insofern geändert, dass nunmehr deutlich wird, welche Felder auch weiterhin nur optional ausgefüllt werden müssen.

Den Flüchtlingsrat Mecklenburg-Vorpommern e. V. habe ich über das Ergebnis informiert.

2.4.2 Auch Amtswehrführer haben Rechte

Petenten haben mich gebeten zu prüfen, ob eine Veröffentlichung ihrer personenbezogenen Daten rechtmäßig war.

In diesem Fall ging es um die Veröffentlichung einer Übersicht aller Amtswehrführungen im amtlichen Bekanntmachungsblatt des Landkreises. Hier waren neben den Namen der Amtswehrführer und ihrer Stellvertreter auch Angaben zu deren Wohnanschriften und Telefonnummern (einschließlich Mobilfunknummern) enthalten.

Eine Rechtsgrundlage, die eine solche Veröffentlichung erlaubt, konnte der Landkreis nicht benennen. Demzufolge hätten die Betroffenen vor dieser Veröffentlichung schriftlich ihre Einwilligung hierzu erteilen müssen (§ 8 Abs. 1 DSG M-V). Da dies nicht geschehen ist, hätten die vorgenannten Daten nicht veröffentlicht werden dürfen.

Der Landkreis hat zugesagt, künftig derartige Daten nur noch dann zu veröffentlichen, wenn die erforderliche Einwilligung vorliege. Außerdem wolle man bei vorgesehenen Veröffentlichungen personenbezogener Daten den behördlichen Datenschutzbeauftragten mit einbeziehen.

2.4.3 Bürgeranfragen nur anonymisiert ins Internet

Eine Stadt hat auf ihrer Internetseite den Namen und die Wohnanschrift eines Bürgers veröffentlicht, der zu einer Bürgerfragestunde eine schriftliche Anfrage an den Vorsitzenden der Stadtvertretung gerichtet hatte. Mit dieser Art der Veröffentlichung war der Bürger nicht einverstanden und hat sich mit der Bitte um Überprüfung an mich gewandt.

Die Stadtverwaltung hat die Veröffentlichung der Anfrage samt der personenbezogenen Daten damit begründet, dass hierdurch in transparenter Art und Weise für die Öffentlichkeit die Arbeit der Stadtvertretung dargestellt wird. Außerdem seien die Angaben erforderlich, um prüfen zu können, ob es sich bei dem Bürger um einen Einwohner der Stadt handele. Dieses und der Umstand, dass der Betroffene das 14. Lebensjahr vollendet haben muss, ist nach der Hauptsatzung eine formale Voraussetzung dafür, um derartige Fragen überhaupt stellen zu können.

Die Prüfung dieser Voraussetzungen obliegt nach meinem Dafürhalten allein der Verwaltung (interner Verwaltungsvorgang). Ein öffentlicher Umgang mit Namen, Alter und Anschrift ist in diesem Falle nicht erforderlich.

Die Stadtverwaltung hat des Weiteren das Argument angeführt, dass man im vorliegenden Fall von einem Einverständnis des Bürgers zur Veröffentlichung seiner personenbezogenen Daten ausgehen konnte, da ein derartiger öffentlicher Umgang mit Daten gängige Praxis in anderen Bürgerforen sei. Außerdem würden diejenigen Bürger, die in der Bürgerfragestunde etwas fragen möchten, vor der eigentlichen Frage persönlich ihren Namen, ihr Lebensalter und ihre Wohnanschrift offenbaren.

Hier wurde die Tatsache nicht beachtet, dass die Betroffenen ihre persönlichen Daten selbstbestimmt preisgeben und dass diese Informationen während der Bürgerfragestunde nur jeweils einem begrenzten Personenkreis zugänglich sind. Die Veröffentlichung von personenbezogenen Daten im Internet stellt jedoch eine ganz andere Qualität dar, als es bei einem mündlichen Vortragen während der Bürgerfragestunde der Fall ist.

Dieses und der Umstand, dass hier die Anforderungen, die § 8 DSG M-V an eine Einwilligung stellt, nicht erfüllt waren, führten zu meiner Empfehlung, bei Bürgeranfragen künftig auf die Veröffentlichung der personenbezogenen Daten im Internet zu verzichten. Auch ohne diese Angaben ist aus meiner Sicht ein öffentlicher und transparenter Umgang mit dem jeweiligen Anliegen möglich.

Dieser Empfehlung ist die Stadtverwaltung gefolgt. Ebenso hat sie - bereits unmittelbar, nachdem der Petent seine Bedenken der Verwaltung gegenüber zum Ausdruck gebracht hatte - das Dokument, in dem seine personenbezogenen Daten enthalten waren, aus ihrem Internetangebot entfernt.

2.4.4 Erhalten Parteien immer Auskünfte aus dem Melderegister?

Immer wieder (so auch zur Kommunalwahl am 7. Juni 2009) treten Parteien und andere Wahlvorschlagsträger an Meldebehörden mit der Bitte um Übermittlung von Melderegisterauskünften heran. Diese Art der Melderegisterauskünfte ist nach § 35 Abs. 1 LMG erlaubt, es sei denn, der Betroffene hat hiergegen Widerspruch eingelegt oder es liegt eine Vollauskunftssperre nach § 34 Abs. 5 LMG vor.

Damit die Wahlberechtigten ihr Widerspruchsrecht zur Kenntnis nehmen können, muss die Meldebehörde nach § 35 Abs. 1 Satz 4 LMG bei der Anmeldung und spätestens acht Monate vor der Wahl (also hier vor dem 7. Oktober 2008) durch öffentliche Bekanntmachung hierauf hinweisen. Ich habe die Kommunalwahl 2009 zum Anlass genommen, um alle 119 Meldebehörden des Landes noch einmal auf diese Bekanntmachungsfrist hinzuweisen. Gleichzeitig bat ich um Übersendung einer Kopie der jeweiligen Bekanntmachung.

Von 116 Meldebehörden erhielt ich eine Antwort. In Auswertung dieser Antworten stellte ich fest, dass hiervon lediglich 32 Meldebehörden fristgerecht, dass heißt acht Monate vor der Wahl, gesondert auf dieses Widerspruchsrecht hingewiesen haben. Bei 62 Meldebehörden erfolgte die Bekanntmachung nicht fristgerecht. 22 Meldebehörden äußerten sich zu unkonkret, um einschätzen zu können, ob die Bekanntmachung innerhalb der vorgegebenen Frist erfolgte. Einige Meldebehörden teilten mir mit, dass sie auf diese Bekanntmachung verzichten würden, da sie generell keine Melderegisterauskünfte an Parteien oder andere Wahlvorschlagsträger übermitteln würden. Andere wiederum bedankten sich für die Hinweise und sagten zu, die Bekanntmachungsfrist zukünftig genauer zu beachten.

Fraglich ist, welche rechtlichen Auswirkungen die fehlende Bekanntmachung auf die Rechtmäßigkeit der Wahlhandlung hat. Zumindest wäre in diesem Fall die Erteilung von Auskünften rechtswidrig. Nach meinen Feststellungen trifft diese Vermutung auf die Beauskunftungen, die durch das Amt Bützow-Land, das Amt Friedland, das Amt Neukloster-Warin, das Amt Zarrentin, die Hansestadt Stralsund, die Hansestadt Anklam und die Stadt Boizenburg/Elbe durchgeführt wurden, zu. In Auswertung der von den vorgenannten Verwaltungen eingeholten Stellungnahmen kam ich insbesondere zu der Einschätzung, dass eine fristgemäße öffentliche Bekanntmachung (bis zum 7. Oktober 2008) nur bedingt möglich war, da der konkrete Wahltermin erst mit Amtsblatt vom 22. September 2008 veröffentlicht wurde. Unter Beachtung der für amtliche Bekanntmachungsblätter bestehenden Redaktionsfristen und deren vertraglich geregelten Erscheinen war eine fristgerechte Veröffentlichung, wie sie § 35 Abs. 1 Satz 4 LMG vorschreibt, nicht mehr in jedem Fall möglich.

Ich empfehle der Landesregierung deshalb, darauf hinzuwirken, dass künftige Wahltermine so festgelegt und veröffentlicht werden, dass eine fristgerechte Bekanntmachung der Widerspruchsmöglichkeit durchgeführt werden kann.

Das Ergebnis dieser Umfrage ist für mich ein klares Indiz dafür, dass das Widerspruchsrecht Schwächen aufweist, die zu Lasten des Grundrechtes auf informationelle Selbstbestimmung gehen. Selbst wenn die öffentlichen Bekanntmachungen regelmäßig durchgeführt werden, ist dies noch kein Beleg dafür, dass den Bürgerinnen und Bürgern die Möglichkeit des Widerspruchs bekannt ist.

Darüber hinaus habe ich alle Meldebehörden darauf hingewiesen, dass sie nicht zur Auskunft verpflichtet sind. Vielmehr handelt es sich um eine Ermessensentscheidung, wobei das Gebot der Gleichbehandlung der Wahlvorschlagsträger beachtet werden muss. 43 Meldebehörden erklärten mir daraufhin, dass sie prinzipiell keine derartigen Melderegisterauskünfte erteilen würden. Dies wurde unter anderem damit begründet, dass der Bekanntmachungszeitraum von mindestens acht Monaten zu lang und vielen Wählern das Widerspruchsrecht nicht bekannt sei. Auch würden es gerade Jungwähler, deren Daten am häufigsten begehrt werden, oft ablehnen, dass derartige Auskünfte erteilt werden.

Parallel zu dieser Umfrage habe ich Hinweise zu einer durch das hiesige Innenministerium zur Kommunalwahl 2009 veröffentlichten Verwaltungsvorschrift gegeben. Diese enthielt den irritierenden Hinweis, wonach für die Entscheidung zwar ein Ermessensspielraum besteht, eine generelle Auskunftsverweigerung aus Gründen des Datenschutzes aber ermessensfehlerhaft und damit rechtswidrig wäre. Ich habe das Innenministerium darauf hingewiesen, dass dies der bestehenden Rechtslage und Rechtssprechung widerspricht. Insbesondere habe ich auf einen Beschluss des Oberverwaltungsgerichtes Greifswald vom 27. August 1998 verwiesen. Das Gericht hatte seinerzeit eine Entscheidung eines Verwaltungsgerichts bestätigt, wonach eine Meldebehörde Gesichtspunkten des Datenschutzes auch gegenüber dem Interesse des Antragstellers aus Artikel 21 Abs. 1 GG Vorrang einräumen darf. Das Innenministerium folgte meinen Empfehlungen und änderte die betreffende Verwaltungsvorschrift (siehe Amtsblatt für Mecklenburg-Vorpommern Nr. 14/2009, S. 230).

2.4.5 Kein Adresshandel mit Meldedaten!

Auch in diesem Berichtszeitraum wurde ich wiederholt mit der Frage konfrontiert, welche Personen und Institutionen einfache Melderegisterauskünfte erhalten und für welche Zwecke sie diese Auskünfte verwenden dürfen.

Nach § 34 Abs. 1 Landesmeldegesetz (LMG) darf eine Meldebehörde anderen Personen Auskunft über den Vor- und Familiennamen, den Doktorgrad und die Anschriften erteilen. Eine derartige Auskunft ist an keine besonderen Voraussetzungen gebunden. Es gilt jedoch hier der Grundsatz des § 7 LMG, dass schutzwürdige Interessen Betroffener nicht beeinträchtigt werden dürfen. Dabei sind insbesondere Auskunftssperren nach § 34 Abs. 5 LMG zu beachten.

Nutzen der einfachen Melderegisterauskünfte durch eine gemeinnützige GmbH
Eine gemeinnützige GmbH, ein Blutspendedienst, nutzte die Möglichkeit der einfachen Melderegisterauskunft unter anderem dazu, eine eigene Datenbank für individuelle Einladungen zur Blutspende anzulegen und zu pflegen. Als Rechtfertigung hierfür wurde neben dem § 19 Abs. 1 Satz 4 Transfusionsgesetz (TFG) auch angeführt, dass alle Blutspender eine Erklärung unterschreiben, mit der sie sich einverstanden erklären, dass ihre Daten unter Beachtung der einschlägigen gesetzlichen Bestimmungen gespeichert werden.

§ 19 Abs. 1 Satz 4 TFG erlaubt dem Blutspendedienst lediglich, eine spendende Person unverzüglich in festgestellten oder begründeten Verdachtsfällen über den anlässlich der Blutspende gesichert festgestellten Infektionsstatus zu unterrichten. Um dieses durchführen zu können, wird die aktuelle Adresse dieser Person benötigt und es kann folglich gegebenenfalls eine einfache Melderegisterauskunft eingeholt werden.

§ 19 Abs. 4 TFG sieht jedoch nicht das Anlegen bzw. Aktualisieren einer Datenbank für Einladungen zum Blutspenden vor. Mangels bestehender Rechtsgrundlage müsste hierfür die Einwilligung des Betroffenen vorliegen. Diese liegt jedoch nicht dadurch vor, dass derjenige eine Erklärung unterschreibt, dass seine Daten unter Beachtung der einschlägigen gesetzlichen Bestimmungen gespeichert werden. Nach § 4 a des Bundesdatenschutzgesetzes (BDSG) ist der Betroffene vielmehr auf den vorgesehenen Zweck der Erhebung, die Verarbeitung oder Nutzung hinzuweisen.

Mit dem Blutspendedienst wurde die betreffende Erklärung einvernehmlich neu formuliert, sodass nunmehr die Bedingungen des § 4 a BDSG erfüllt sind.

Nutzen der einfachen Melderegisterauskünfte durch Adress-Unternehmen
Klarstellungsbedürftig war auch der Umgang mit Melderegisterdaten durch Adress-Unternehmen. Erforderlich war dieses, da nicht ausgeschlossen werden konnte, dass einzelne Unternehmen die über die einfache Melderegisterauskunft eingeholten Daten nach der Weiterleitung an ihren Auftraggeber nicht löschen, sondern in eigenen Datenbanken speichern, um durch Auskünfte hieraus oder durch den listenmäßigen Verkauf von Daten erneut verdienen zu können.

Das hiesige Innenministerium gab im Zusammenwirken mit meiner Behörde mit Schreiben vom 10. Februar 2009 gegenüber den Meldebehörden klarstellende rechtliche Hinweise:

Beim Melderegister handelt es sich nicht um ein öffentliches Register. Deshalb sind stets die schutzwürdigen Interessen der Betroffenen zu berücksichtigen und dürfen nicht beeinträchtigt werden. Aus diesem Grunde erhielten alle Meldebehörden noch einmal den Hinweis, eine einfache Melderegisterauskunft immer nur unter Berücksichtigung des in § 34 Abs. 1 LMG eingeräumten Ermessens zu erteilen. Dazu beitragen kann unter anderem eine schriftliche Erklärung der anfragenden Unternehmen, in der diese versichern, dass die begehrten Meldedaten nur zur Übermittlung an ihren Auftraggeber verwendet und nicht in eigenen Datenbanken gespeichert werden.

2.4.6 Einführung eines neuen Meldescheinsystems in einer Kurverwaltung

Ein Petent informierte mich darüber, dass eine Kurverwaltung plant, ein neues Meldescheinsystem einzuführen. Er sah die Bedingungen, die das Landesmeldegesetz (LMG) hieran stellt, nicht mehr als erfüllt an.

Nach § 26 Abs. 2 LMG haben beherbergte Personen - außer mitreisende minderjährige Kinder und Ehegatten sowie Reisegesellschaften mit mehr als 10 Personen - am Tag der Ankunft einen besonderen Meldeschein handschriftlich auszufüllen und zu unterschreiben. Die Verantwortung, dass die besonderen Meldescheine tatsächlich von jedem Gast ausgefüllt und unterschrieben werden, obliegt nicht der Kurverwaltung beziehungsweise der betreffenden Gemeinde, sondern jedem Inhaber einer Beherbergungsstätte.

Im vorliegenden Fall sollten sämtliche Gästedaten automatisiert erfasst und verarbeitet werden. Lediglich der ausgedruckte besondere Meldeschein hätte hiernach durch den Gast noch unterschrieben werden müssen. Ich habe die betreffende Kurverwaltung darauf hingewiesen, dass § 26 Abs. 2 LMG neben dem Unterschreiben ausdrücklich auch ein handschriftliches Ausfüllen des Meldescheins verlangt.

Die Kurverwaltung informierte mich darüber, dass mit dem automatisierten Verfahren kein neuer besonderer Meldeschein eingeführt werden soll, sondern die Änderung lediglich der Erhebung der Kurabgabe dienen soll. Ich habe die Kurverwaltung darauf hingewiesen, dass dieser Datenverarbeitungsvorgang separat von dem Meldescheinverfahren durchgeführt werden kann. Der Umfang der dabei zu verarbeitenden Daten richtet sich auf die für die Berechnung erforderlichen und in der Meldescheinverordnung aufgeführten meldepflichtigen Daten.

Die Kurverwaltung ist meinen Empfehlungen gefolgt und hat entsprechende Regelungen zu diesem Verfahren in ihrer Kurabgabensatzung getroffen.

2.4.7 Benutzung des Liegenschaftskatasters

Im Berichtszeitraum stand unter anderem auch die Frage zur Diskussion, unter welchen Voraussetzungen einem Windenergie-Unternehmen für einen klar definierten Bereich Eigentümerinformationen aus dem Automatisierten Liegenschaftsbuch (ALB) herausgegeben werden dürfen.

Nach § 12 Abs. 2 Vermessungs- und Katastergesetz (VermKatG) dürfen anderen als den Eigentümern, den Erbbau- und Nutzungsberechtigten sowie deren Beauftragten aus dem ALB Auskünfte erteilt werden, wenn der Auskunftsersuchende ein berechtigtes Interesse an den Daten darlegt und keine öffentlichen Belange dem entgegenstehen. Das berechtigte Interesse ist dabei weiter als das rechtliche Interesse zu fassen. Es genügt, dass ein verständliches, durch die Sachlage gerechtfertigtes Interesse verfolgt wird. Dabei sind die Gründe darzulegen, um die Verfolgung unbefugter Zwecke oder bloßer Neugier auszuschließen.

Im vorliegenden Fall lag ein Kaufinteresse des Windenergie-Unternehmens vor. Das Unternehmen wollte die Eigentümer bestimmter Flächen in Erfahrung bringen, auf denen sich nach einem Entwurf des in Änderung befindlichen Raumentwicklungsprogrammes künftig Eignungsgebiete für die Errichtung von Windparkanlagen befinden sollen. Da diese Eignungsgebiete zu dem Zeitpunkt noch nicht endgültig feststanden, habe ich ein berechtigtes Interesse, wie es der § 12 Abs. 2 VermKatG verlangt, nicht als gegeben angesehen und der betreffenden Behörde für die Übermittlung von Eigentümerdaten ein sogenanntes Adressmittlungsverfahren vorgeschlagen (siehe hierzu auch Erster Tätigkeitsbericht zum IFG M-V, Punkt 3.4).

Ein begründetes wirtschaftliches und damit ein berechtigtes Interesse im Sinne der vorgenannten Vorschrift besteht erst nach Feststehen der Eignungsgebiete im Raumentwicklungsprogramm. Dabei muss allerdings berücksichtigt werden, dass dieses Interesse durch den Auskunftsbegehrenden entsprechend dargelegt werden muss und sich ebenso nur auf die ausgewiesenen Eignungsgebiete beziehen darf. Des Weiteren muss die Verwaltung prüfen, ob möglicherweise öffentliche Belange dem entgegenstehen.

2.4.8 Datenschutz und Datensicherheit in Passbehörden

Im Achten Tätigkeitsbericht habe ich ausführlich über Mängel bei der Einführung des elektronischen Reisepasses berichtet (siehe dort Punkt 2.4.7). Unter anderem hatte ich darauf hingewiesen, dass die Passbehörden erhebliche Anstrengungen unternehmen müssen, um ein ausreichendes IT-Sicherheits- und Datenschutzniveau zu gewährleisten. Zu diesem Zweck hatte ich gemeinsam mit dem Innenministerium detaillierte Hinweise zu den erforderlichen technischen und organisatorischen Maßnahmen erarbeitet.

Bereits im Zusammenhang mit der Modernisierung des Melderechts hatte ich gemeinsam mit der Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH (DVZ M-V GmbH) Empfehlungen zum Datenschutz und zur Datensicherheit in Kommunen erarbeitet (siehe Achter Tätigkeitsbericht, Punkt 2.4.3) und erwartet, dass durch die Umsetzung dieser Maßnahmen zumindest ein IT-Grundschutzniveau in den Kommunen realisiert würde, das auch anderen Bereichen wie etwa den Passbehörden zugute kommen würde.

Diese Erwartung hat sich jedoch nicht erfüllt. Schon sehr bald hat sich gezeigt, dass viele Kommunen mit der Umsetzung der Empfehlungen überfordert sind, da sie offenbar nicht über die erforderlichen finanziellen, zeitlichen und personellen Ressourcen verfügen, um alle empfohlenen Maßnahmen umzusetzen. Insbesondere fehlten oft Sicherheitskonzepte und Verfahrensbeschreibungen. Entsprechende Konsultationen bei meinen Kollegen aus anderen Bundesländern haben gezeigt, dass es sich hierbei keinesfalls um ein Problem unseres Bundeslandes handelt, sondern dass bundesweit vergleichbare Sicherheitslücken in Passbehörden zu konstatieren sind.

Gemeinsam mit meinen Kollegen von Bund und Ländern habe ich mich an das Bundesministerium des Innern (BMI) mit der Bitte um Unterstützung gewandt. Das BMI hat sofort zugesagt, im Rahmen des jährlichen Workshops des AK Technik (siehe Punkt 4.2) die vorhandenen Defizite zu erörtern und gemeinsam mit den Datenschutzbeauftragten nach Lösungsmöglichkeiten zu suchen. Im Ergebnis kamen wir überein, ein Empfehlungspapier zu erarbeiten, das insbesondere die deutschen Passbehörden bei der Auswahl und Umsetzung technischer und organisatorischer Maßnahmen unterstützt und zumindest die Realisierung eines angemessenen IT-Grundschutzniveaus befördern soll.

Das BMI erarbeitete unverzüglich einen ersten Entwurf des Papiers, in dem die erforderlichen grundlegenden Sicherheitsmaßnahmen beschrieben werden. Das BMI verweist dabei auf die Grundschutzmethodik des BSI. Auch wenn im Abstimmungsprozess mit dem AK Technik zahlreiche Verbesserungsvorschläge berücksichtigt wurden, bleiben einige grundsätzliche Kritikpunkte am Passantragsverfahren.

So soll dem Antragsteller die Prüfung der ordnungsgemäßen Erfassung seines Fingerabdrucks durch Anzeige des im Reisepass gespeicherten Fingerabdruckbildes auf einem kleinen Kontrollmonitor des Lesegerätes ermöglicht werden. Ich halte diese Prüfmöglichkeit für völlig untauglich, da die graphische Darstellung des Bildes keinerlei Rückschlüsse auf die Übereinstimmung des gespeicherten mit dem eigenen Fingerabdruck zulässt. Auch auf die bereits in meinem Achten Tätigkeitsbericht beschriebenen Mängel hinsichtlich der Gewährleistung der Vertraulichkeit und Integrität der erfassten Passantragsdaten wird in dem Papier noch nicht ausreichend eingegangen. Hier wären konkrete Empfehlungen sicher hilfreich gewesen. Auch bleibt ungeklärt, wie die Bundesdruckerei die Authentizität der beantragenden Stelle prüft. Die elektronische Signatur der versandten Passantragsdaten gibt lediglich Aufschluss über den Absender. Absender und Ersteller von Antragsdatensätzen müssen aber nicht identisch sein, da nicht alle Passbehörden selbst Antragsdatensätze versenden, sondern mitunter andere Passbehörden damit beauftragen. Schließlich liefert das Papier keine Lösungen, die den Widerspruch zwischen Pflicht zur Löschung der biometrischen Daten in den Passbehörden und der Datensicherungspflicht der Behörden ausräumen. Hier sind die Hersteller der Software gefordert, handhabbare Lösungen anzubieten.

Anfang Oktober 2008 versandte das BMI die weitgehend abgestimmte Schlussversion des Papiers an die Innenministerien der Länder. Das Innenministerium unseres Landes leitete das Papier sofort an die Landkreise und kreisfreien Städte weiter. Die Handreichung des BSI kann auch aus meinem Internetangebot heruntergeladen werden (http://www.datenschutz-mv.de/dschutz/informat/passbehoerden/passbeh.pdf).

Ich empfehle der Landesregierung, die bei der Einführung des elektronischen Reisepasses gewonnenen Erkenntnisse detailliert auszuwerten und die Pass- und Personalausweisbehörden sowohl beim Betrieb des Passantragsverfahrens als auch bei der Einführung der neuen Personalausweise zu unterstützen.

2.4.9 Der neue Personalausweis

Ab dem 1. November 2010 erhalten Bürgerinnen und Bürger auf Antrag den neuen, elektronischen Personalausweis. Zu diesem Zeitpunkt tritt das novellierte Personalausweisgesetz in Kraft, das am 18. Juni 2009 im Bundesgesetzblatt veröffentlicht wurde (BGBl. Jahrgang 2009 Teil I Nr. 33 vom 24. Juni 2009).

Der elektronische Personalausweis im Kreditkartenformat enthält personenbezogene Daten sowohl sichtbar aufgedruckt (etwa Name, Vorname, Tag und Ort der Geburt, Anschrift, Staatsangehörigkeit) als auch elektronisch gespeichert in einem per Funk auslesbaren RFID-Chip. Neben den oben genannten Daten enthält der Chip biometrische Daten des Gesichtsbildes des Inhabers. Massive Proteste - nicht zuletzt von den Datenschutzbeauftragten vom Bund und aus den Ländern - haben bewirkt, dass die biometrischen Daten von zwei Fingerabdrücken nur auf ausdrücklichen Wunsch des Betroffenen erhoben und gespeichert werden. Der neue Personalausweis im Scheckkartenformat vereint den herkömmlichen Ausweis mit den folgenden drei neuen elektronischen Funktionen:

1) Biometrische Identitätsfeststellung von Personen für hoheitliche Anwendungen
Berechtigte Behörden wie Polizei und Grenzkontrolle können zur Identitätsfeststellung künftig auch biometrische Daten des Personalausweises nutzen. Durch elektronischen Vergleich eines aktuell aufgenommenen Gesichtsbildes mit dem im Chip gespeicherten Bild kann mit hoher Wahrscheinlichkeit festgestellt werden, ob der vorgelegte Ausweis tatsächlich der betreffenden Person gehört. Die Verfahren zum Auslesen der Daten per Funk wurden gegenüber den vergleichbaren, aber stark kritisierten Verfahren beim elektronischen Reisepass überarbeitet oder völlig neu entwickelt. Um Daten aus dem Chip auslesen zu können, muss zunächst eine auf dem Ausweis aufgedruckte Zugangsnummer optisch ausgelesen werden. Das trägt dazu bei, dass ein unbemerktes Auslesen von Daten aus der Ferne mit hoher Wahrscheinlichkeit verhindert wird. Das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) neu entwickelte Verschlüsselungsverfahren PACE (Password Authenticated Connection Establishment) sorgt zudem für eine verschlüsselte Übertragung der Daten zwischen Chip und Lesegerät. Zusätzlich muss der RFID-Chip im Personalausweis mit dem sogenannten Chip-Authentication-Verfahren seine Echtheit nachweisen und dem Lesegerät werden mit dem Terminal-Authentication-Verfahren die entsprechenden Leserechte zugewiesen.

Für eine angemessene Sicherheit des gesamten Verfahrens spricht zudem die Tatsache, dass das Betriebssystem des Ausweises und der RFID-Chip nach den international anerkannten Sicherheitskriterien der Common Criteria in der Stufe EAL4+ zertifiziert sind. Die Sicherheit dieser Verfahren wird daher von IT-Fachleuten anerkannt, sodass dem neuen Personalausweis ein höheres Sicherheitsniveau als etwa dem elektronischen Reisepass attestiert und das unberechtigte Auslesen von Ausweisdaten weitgehend ausgeschlossen werden kann.

2) Elektronischer Identitätsnachweis (eID-Funktion)
Der neue Personalausweis bietet mit dem elektronischen Identitätsnachweis eine völlig neue Funktion, mit der Ausweisinhaber sowohl in E-Government- oder E-Business-Anwendungen auf elektronischem Weg - etwa über das Internet - als auch an Automaten und bei Offline-Systemen ihre Identität nachweisen können. Zu diesem Zweck erteilt das Bundesverwaltungsamt Behörden und Unternehmen auf Antrag ein sogenanntes Berechtigungszertifikat, in dem festgelegt ist, welche Daten (bspw. Vor- und Familienname(n), Doktorgrad, Geburtstag und -ort, Angabe, ob ein bestimmtes Alter über- oder unterschritten ist, Anschrift) elektronisch aus dem Ausweis ausgelesen werden dürfen. Das Bundesverwaltungsamt prüft für jeden Antragsteller, welche Daten für welchen Zweck er auslesen möchte. Nur wenn die Zulässigkeit des Abrufs und die Gewährleistung der Zweckbindung bei der abrufenden Stelle nachgewiesen wurden, wird das Zertifikat erteilt.

Um den elektronischen Identitätsnachweis über das Internet nutzen zu können, benötigt der Ausweisinhaber eine spezielle Software, den sogenannten Bürger-Client, und ein zertifiziertes Lesegerät, das an den eigenen Arbeitsplatzcomputer angeschlossen wird und Daten des Personalausweises per Funk auslesen kann. Bevor Ausweisdaten ausgelesen und in verschlüsselter Form an eine Behörde oder an ein Unternehmen übermittelt werden, wird dem Ausweisinhaber das oben beschriebene Berechtigungszertifikat mit allen wichtigen Informationen zum Anbieter des jeweiligen Online-Dienstes angezeigt. In einer weiteren Maske wird detailliert angezeigt, welche Daten ausgelesen werden sollen. Hier hat der Ausweisinhaber die Möglichkeit, das Auslesen einzelner Datenfelder zu unterbinden. Das kann allerdings dazu führen, dass der Online-Dienst nicht erbracht wird. Die freigegebenen Daten werden erst dann ausgelesen und in verschlüsselter Form an den Diensteanbieter übermittelt, wenn der Ausweisinhaber seine sechsstellige PIN eingegeben hat.

Bei der Ausgabe des neuen Personalausweises ist die eID-Funktion standardmäßig freigeschaltet. Möchte jemand diese Funktion jedoch nicht nutzen, kann sie durch die Personalausweisbehörde abgeschaltet werden. Um Missbrauchsmöglichkeiten zu verhindern, besteht zudem jederzeit mit einem Sperrkennwort die Möglichkeit, abhanden gekommene Ausweise durch Eintragung in eine Sperrliste als ungültig erklären zu lassen. Darüber hinaus kann die PIN jederzeit zu Hause oder in der Personalausweisbehörde geändert werden.

Eine wesentliche Voraussetzung für die Sicherheit und Vertrauenswürdigkeit der Eid-Funktion ist eine sehr gute sicherheitstechnische Ausstattung des privaten Personal-computers, auf dem der Bürger-Client installiert wird. Wird die sechsstellige PIN über die Tastatur des PC eingegeben, besteht die Gefahr, dass Kriminelle über eingeschleuste Schadsoftware (Viren oder Trojaner) die PIN mitlesen und in der Folge unbemerkt die eID-Funktion des Ausweises nutzen. Daher ist es unabdingbar, dass auf dem privaten PC aktuelle Antivirensoftware läuft und dass regelmäßig alle Sicherheitsupdates für Betriebs-system, Browser und Anwendungssoftware installiert werden.

Darüber hinaus sollten nur Chipkartenleser mit eigenem Tastaturfeld verwendet werden, damit die PIN nicht über die PC-Tastatur eingeben werden muss. Das Risiko unberechtigten Mitlesens kann dadurch erheblich reduziert werden.

Entscheidend für die datenschutzgerechte Nutzung des elektronischen Identitätsnachweises ist aber auch die sorgfältige Prüfung des Bundesverwaltungsamtes, ob und ggf. welche Ausweisdaten Diensteanbieter auf elektronischem Wege auslesen dürfen. Hier haben die Datenschutzbeauftragten von Bund und Ländern Unterstützung angeboten. In einer gemeinsamen Arbeitsgruppe sollen zusammen mit dem Bundesverwaltungsamt Kriterien festgelegt werden, nach denen die Berechtigungszertifikate erteilt werden.

3) Qualifizierte Signatur

Ich habe in der Vergangenheit mehrfach beklagt, dass elektronische Signaturverfahren und insbesondere die qualifizierte elektronische Signatur zu wenig in Wirtschaft und Verwaltung eingesetzt werden (zuletzt im Achten Tätigkeitsbericht, Punkt 2.15.2). Der neue Personalausweis könnte hier eine Wende bringen, da er die Möglichkeit bietet, qualifizierte elektronische Signaturen zu erzeugen. Die dafür erforderlichen Daten sind auf dem Ausweis im Auslieferungszustand jedoch zunächst nicht enthalten. Möchte ein Ausweisinhaber also künftig mit dem neuen Personalausweis elektronisch unterschreiben können, muss er selbst die Aktivierung der Signaturfunktion bei einem sogenannten Zertifizierungsdiensteanbieter beantragen. Erst dann wird das Signaturschlüsselpaar erzeugt und das entsprechende Zertifikat in den Ausweis übertragen. Durch Eingabe einer zweiten PIN, die sich von der oben genannten sechsstelligen PIN der eID-Funktion unterscheiden muss, können dann qualifizierte Signaturen erzeugt werden, zum Beispiel um Rechtsgeschäfte wie Vertragsunterzeichnungen rechtssicher auch in elektronischer Form abwickeln zu können. Für die Sicherheit des Signaturvorgangs ist jedoch entscheidend, dass dem Nutzer auf dem Bildschirm auch das Dokument angezeigt wird, das er zu unterschreiben beabsichtigt. Komplexe Dokumentenformate wie etwa das PDF-Format bergen die Gefahr von Manipulationen in sich, die dazu führen können, dass das auf dem Bildschirm angezeigte Dokument nicht dem tatsächlich signierten Dokument entspricht. Vor diesem Hintergrund wären klare Vorgaben des Gesetzgebers für einfache und damit weitgehend manipulationssichere Dokumentenformate erforderlich.

Bedauerlich ist zudem die Tatsache, dass allein die Bürger die Kosten tragen sollen, die der Zertifizierungsdiensteanbieter für Zertifikatserteilung und Signaturdienst erhebt. Deshalb wäre es sehr zu wünschen, dass der Staat - etwa durch Fördermittel - Anreize für eine Nutzung dieser Funktion des neuen Ausweises schafft. Ein erster Schritt in diese Richtung könnte getan werden, indem der Bund Bürgerinnen und Bürgern bis zum 31. Dezember 2011 mehr als eine Million Kartenlesegeräte mit den entsprechenden Software-Komponenten zur Verfügung stellen wird. Der Bund beabsichtigt, mit einem „Zuschuss zu einem IT-Sicherheitskit für Bürgerinnen und Bürger“ in Höhe von 24 Mio. Euro die Verbreitung entsprechender Infrastrukturkomponenten zu fördern. Leider wird jedoch die überwiegende Zahl der so bereitgestellten Chipkartenleser über kein eigenes Tastaturfeld verfügen und somit zum Erzeugen qualifizierter Signaturen ungeeignet sein. Damit vergibt der Bund eine weitere Chance zur Verbreitung der qualifizierten Signatur. Darüber hinaus wird mit der Bereitstellung von Chipkartenlesern ohne Tatstaturfeld den oben beschriebenen Sicherheitsrisiken bei der Nutzung der eID-Funktion Vorschub geleistet.

Nicht nur die Bürgerinnen und Bürger werden durch den neuen Personalausweis mit neuen Abläufen und Funktionen konfrontiert. Auch die Personalausweisbehörden erhalten völlig neue Aufgaben. Bei der Beantragung des Ausweises beispielsweise sind das Gesichtsbild und ggf. die Fingerabdrücke zu erfassen und deren biometrische Qualität zu prüfen. Antragstellern ist Informationsmaterial zu den neuen Funktionen zu übergeben. Bei der Ausgabe des Ausweises muss das oben erwähnte Sperrkennwort gespeichert, der PIN-Brief ausgehändigt und ggf. die eID-Funktion im Chip ausgeschaltet werden. Zudem muss dem Antragsteller die Nutzung eines Lesegerätes zum Anzeigen der im Chip gespeicherten Daten ermöglicht werden und schließlich sind die Fingerabdrücke in den Antragsunterlagen zu löschen. Unter dem Stichwort „Änderungsmanagement“ muss die Personalausweisbehörde auf Verlangen die eID-Funktion im Chip ein- und ausschalten, die PIN ändern und nach einem Umzug die Anschrift im Chip ändern können. Bei Verlust eines Personalausweises muss der Sperrdienst bedient werden (Übermittlung der Sperrinformation an den Sperrlistenbetreiber und Speicherung dieser Tatsache im Personalausweis-Register). Dazu gehört auch das Entsperren bei Wiederauffinden des Dokumentes. Erfreulicherweise bietet das Bundesinnenministerium zahlreiche Schulungsmaßnahmen für Mitarbeiter der Personalausweisbehörden und IT-Fachleute der Kommunen an.

Aber auch Bürgerinnen und Bürger sollen sich jederzeit informieren können. Unter der Telefonnummer 0180 - 1 333 333 wird eine Service-Hotline eingerichtet, bei der Fragen zum neuen Personalausweis und den neuen Funktionen beantwortet werden.

Bis zum 1. November 2010 sind zahlreiche Feldtests vorgesehen, mit denen die Integrationsfähigkeit der Module und der Komponenten in die Echtumgebungen sowie die Praxistauglichkeit des gesamten Verfahrens nachgewiesen werden sollen. Zusätzlich sind Anwendungstests geplant, mit denen die Einbindung der Diensteanbieter in E-Business- und E-Government-Verfahren erprobt wird. Der elektronische Identitätsnachweis soll sowohl für E-Business- und E-Government-Dienste als auch an Automaten und bei Offline-Systemen getestet werden. Das Bundesinnenministerium hofft auf eine breite Teilnahme von Diensteanbietern unterschiedlicher Branchen und auf viele Personalausweisinhaber als Probanden, um die erforderlichen Supportstrukturen für das Gesamtverfahren noch optimieren zu können. Die Datenschutzbeauftragten von Bund und Ländern werden diese Tests konstruktiv begleiten.

Ich empfehle der Landesregierung, die Personalausweisbehörden bei der Einführung der neuen elektronischen Personalausweise aktiv zu unterstützen und darauf hinzuwirken, dass ausreichend finanzielle Mittel und genügend qualifiziertes Personal in den Kommunen zur Verfügung steht, damit die zahlreichen neuen Aufgaben auf sichere und datenschutzgerechte Weise bearbeitet werden können.

Die Personalausweisbehörden sollten Bürgerinnen und Bürger bei der Ausgabe des neuen Personalausweises auf die erforderliche Sicherheitsausstattung des privaten Personalcomputers hinweisen und ausdrücklich die Nutzung von Lesegeräten mit eigenem Tastaturfeld empfehlen.

2.4.10 Verlust eines USB-Sticks mit Grundbuchdaten

Anfang 2009 informierte mich der Staatssekretär des Justizministeriums davon, dass bei einem EDV-Dienstleister ein USB-Stick abhanden gekommen war, auf dem Kopien der Daten aller Grundbücher zweier Grundbuchämter aus Mecklenburg-Vorpommern gespeichert waren.

Der Dienstleister betreibt das Verfahren Elektronisches Grundbuch. Eine weitere Firma ist für die Weiterentwicklung und Wartung dieses Verfahrens verantwortlich. Betreiber und Entwickler sind jeweils im Auftrag des Justizministeriums tätig. Der Entwickler sollte die Daten zur Beseitigung einer Störung erhalten. Zu diesem Zweck hatte der Betreiber die vollständigen Datenbanken der beiden Grundbuchämter exportiert und unverschlüsselt auf dem besagten USB-Stick gespeichert. Der USB-Stick ging anschließend im Gebäude des Betreibers verloren. Der genaue Hergang war auch in einem staatsanwaltschaftlichen Ermittlungsverfahren nicht zu klären.

Das Justizministerium war nach Rücksprache mit dem Entwickler davon ausgegangen, dass der Inhalt des USB-Sticks durch Unbefugte nicht gelesen werden kann, obwohl die Daten unverschlüsselt waren. Es nahm an, dass hierzu weitere Informationen über das Format der Daten erforderlich seien, die nur in der Original-Umgebung zur Verfügung stünden, und schloss einen Missbrauch der abhanden gekommenen Daten nahezu aus. Ich wies darauf hin, dass die Exportfunktion üblicher Datenbanken jedoch gerade dazu dient, Daten einschließlich ihrer Struktur so zu speichern, dass sie auf anderen Systemen gelesen und verarbeitet werden können. Außerdem verwies ich auf frei verfügbare Software-Werkzeuge, mit denen jedermann sich solche Daten zugänglich machen kann.

Das Justizministerium hat also gegen die Pflicht verstoßen, technische und organisatorische Maßnahmen zur Sicherung der Vertraulichkeit zu ergreifen (§ 21 Abs. 2 Nr. 1 DSG M-V), indem es für den Transport vorgesehene Daten unverschlüsselt gespeichert hat. Während der datenschutzrechtlichen Prüfung des Vorfalls musste ich zudem feststellen, dass der Vertrag zwischen Justizministerium und Entwickler mangelhaft war. Insbesondere fehlten Vereinbarungen, wie die Grundbuchdaten bei Wartung und gegebenenfalls Fernwartung gegen unbefugten Zugriff zu sichern sind. Hat der Entwickler die Vertraulichkeit der durch den Datenbankexport kopierten Grundbuchdaten tatsächlich falsch eingeschätzt, ist außerdem zu bezweifeln, ob er als Auftragnehmer geeignet ist (§ 4 DSG M-V). Diese Verstöße hat das Justizministerium als Auftraggeber zu verantworten. Ich habe sie förmlich beanstandet.

Daraufhin hat das Justizministerium verschiedene Verbesserungen veranlasst. Benötigt der Entwickler Datenbankexporte, so werden diese künftig verschlüsselt transportiert. Außerdem ist der Vertrag mit dem Entwickler um Klauseln zum Umgang mit personenbezogenen Daten ergänzt worden. In diesem Zusammenhang hat der Betreiber seine Regelungen zum Umgang mit mobilen Datenträgern verbessert. Diese Regelungen sind nunmehr Bestandteil des Vertrages mit dem Justizministerium geworden und inzwischen auch als Empfehlung für die Landesverwaltung veröffentlicht worden. Schließlich hat das Justizministerium eine umfassende Überarbeitung des Sicherheitskonzepts für das Elektronische Grundbuch beauftragt. Diese Arbeiten waren bei Redaktionsschluss noch nicht abgeschlossen.

Neben den oben beschriebenen Mängeln habe ich auch kritisiert, dass für das Elektronische Grundbuch keine Verfahrensbeschreibungen gemäß § 18 DSG M-V existierten und dass das Verfahren nicht gemäß § 19 Abs. 1 DSG M-V freigegeben worden war. Das Justizministerium vertrat jedoch die Auffassung, dass die Regelungen des Landesdatenschutzgesetzes auf den Betrieb des Elektronischen Grundbuchs nicht anwendbar sind und eine Verpflichtung zur Erstellung dieser Dokumente nicht bestünde. Es handele sich hierbei um Rechtspflegeaufgaben, die gemäß § 2 Abs. 4 Satz 2 DSG M-V der Kontrolle durch den Landesdatenschutzbeauftragten entzogen sind. Ich teile diese Auffassung jedoch nicht, da die Umsetzung technischer und organisatorischer Maßnahmen zur Datensicherung bei Gerichten eine reine Verwaltungsangelegenheit ist, die keinesfalls der richterlichen Unabhängigkeit unterliegt.

Ich habe das Justizministerium gebeten, meine Forderung zu unterstützen, die Prüfungs- und Kontrollkompetenz des Landesdatenschutzbeauftragten bei der Umsetzung der technischen und organisatorischen Maßnahmen zur Datensicherheit bei Gerichten klarer als bisher im Landesdatenschutzgesetz festzuschreiben. Der Hamburger Senat hat bereits im Jahr 1993 in seinen Reformüberlegungen zur datenschutzrechtlichen Kontrollkompetenz bei Gerichten festgestellt, dass externe Datenschutzkontrollen im Bereich der äußeren Datensicherheit mit höherrangigem Recht vereinbar sind und die richterliche Unabhängigkeit nicht berühren. Klarstellenden Regelungen wie etwa in Berlin oder in Hamburg (vgl. § 24 Abs. 2 Satz 2 BlnDSG, § 23 Abs. 1 Satz 3 HmbDSG) würde somit nichts im Wege stehen.

Ich empfehle dem Landtag, mit einer Änderung des DSG M-V dem Landesdatenschutzbeauftragten im Bereich der Rechtspflege bei Gerichten eine Prüfungsbefugnis über technische und organisatorische Maßnahmen zur Datensicherheit einzuräumen. Um im Bereich der äußeren Datensicherheit (etwa in Bezug auf die Erforderlichkeit von Sicherheitskonzept, Verfahrensbeschreibung und Freigabe) mehr Rechtsklarheit zu schaffen, sollte der Anwendungsbereich des DSG M-V auf den Bereich der Rechtspflege bei Gerichten ausgeweitet werden. Die Unabhängigkeit der Gerichte bliebe gewahrt, wenn gleichzeitig festgeschrieben wird, dass die §§ 30, 31 und 32 im Bereich der Rechtspflege keine Anwendung finden.

2.4.11 Verlust eines Dienstlaptops

Die Stadtverwaltung Schwerin überlässt seit dem Jahr 2006 den Stadtvertretern Laptops. Die Vorbereitung und der Ablauf der Sitzungen der Stadtvertretung sollen erleichtert werden, indem die Stadtverwaltung Vorlagen und Tagesordnungen für die Sitzungen der Stadtvertretung über das Ratsinformationssystem oder auf CD zur Verfügung stellt. Die Stadtvertreter können die Unterlagen auf den Laptops speichern, mit individuellen Notizen versehen und in der Sitzung der Stadtvertretung unabhängig von einer Verbindung zum Ratsinformationssystem nutzen.

Bereits Ende 2007 informierte die Presse darüber, dass ein hochrangiger Schweriner Stadtvertreter seinen Dienstlaptop samt Passwort sowie einen USB-Stick verpfändet hatte. Die Staatsanwaltschaft eines anderen Bundeslandes beschlagnahmte beide Geräte im Zuge eines Ermittlungsverfahrens gegen eine weitere, unbeteiligte Person.

Vorlagen an die Stadtvertretung enthalten mitunter sensible personenbezogene Daten, so auch Personalangelegenheiten. Da solche Vorlagen auf dem Laptop gespeichert und bearbeitet werden können, ist es nach dem Stand der Technik erforderlich, die Festplatte des Laptops zu verschlüsseln, damit bei Verlust oder Diebstahl des Gerätes die gespeicherten Daten ohne den passenden Schlüssel oder das richtige Passwort nicht gelesen werden können (§ 22 Abs. 3 DSG M-V). Benötigen die Nutzer externe Speichermedien wie USB-Sticks, müssen auch diese verschlüsselt werden. Nicht benötigte USB-Geräte oder Geräteklassen sollten blockiert werden.

Zum damaligen Zeitpunkt waren die Dienstlaptops nicht mit entsprechenden Sicherheitsmechanismen ausgestattet. Die Stadtverwaltung war damals noch mit Auswahl und Test geeigneter Verfahren beschäftigt. Ich habe empfohlen, die Laptops künftig so einzurichten, dass die Nutzer nicht über Administrationsrechte verfügen und somit nicht eigenständig zusätzliche Hard- und Software installieren können. Zudem sollte jeder Laptop mit Verschlüsselungssoftware ausgestattet und der Internetzugang nur über zentral administrierte Firewallsysteme zugelassen werden.

Meine Empfehlungen wurden inzwischen weitgehend umgesetzt. Die Festplatten der Laptops sind nunmehr verschlüsselt, ebenso die Verbindung zum Ratsinformationssystem. Nutzer müssen sich gegenüber dem Laptop authentifizieren und können hierfür auch das biometrische Fingerabdruck-Lesesystem des Laptops nutzen. Alle Laptops wurden mit Virenschutzsoftware ausgestattet, die über den WLAN-Kontakt im Stadthaus regelmäßig aktualisiert wird. Administrative Aufgaben können nur Mitarbeiter des Benutzerservices bearbeiten. Zudem hat die Stadtverwaltung auch die Nutzungsbedingungen überarbeitet und die Verhaltensregeln noch klarer gefasst.

Da mir ein strafbewehrter Verstoß gegen das Landesdatenschutzgesetz möglich erschien (unbefugte Übermittlung personenbezogener Daten gemäß § 42 Abs. 1 Satz 1 DSG M-V), stellte ich bei der Staatsanwaltschaft Strafantrag gegen den Stadtvertreter. Im Zuge der Ermittlungen fand die Staatsanwaltschaft auf dem USB-Stick tatsächlich schutzwürdige personenbezogene Daten. Sie stellte das Strafverfahren trotz dieser Erkenntnisse ein, da sie eine geringe Schuld des Stadtvertreters und mangelndes öffentliches Interesse an der Verfolgung der Tat feststellte.

Fraglich war im Zusammenhang mit dem Strafantrag, ob das unbefugte Überlassen eines Laptops oder USB-Sticks mit nicht offenkundigen, personenbezogenen Daten bereits den Straftatbestand nach § 42 Abs. 1 DSG M-V erfüllt. Als strafbare Handlung wird dort zwar das unbefugte Übermitteln, nicht jedoch das Überlassen mit der Möglichkeit der unbefugten Einsichtnahme benannt. Die Staatsanwaltschaft hat diese Frage nicht erörtert, weil bereits im Vorfeld eine geringe Schuld des Stadtvertreters festgestellt wurde. Aber auch der Landtag befasste sich mit dieser Frage. Mit einer Kleinen Anfrage (LT-Drs. 5/2259) wollte ein Mitglied der FDP-Fraktion klären lassen, ob im DSG M-V möglicherweise eine Gesetzeslücke bestünde. Das Innenministerium stellte klar, dass keinesfalls eine Gesetzeslücke besteht und dass es für die strafbewehrte Übermittlung ausreicht, dass der Empfänger der Daten lediglich die Möglichkeit hat, ungehindert vom Weitergebenden die Informationen zur Kenntnis zu nehmen.

2.4.12 Online-Ticketbestellung bei der BUGA

Kurz nach Eröffnung der Bundesgartenschau (BUGA) 2009 in Schwerin erreichte mich eine Petition zum Online-Kauf von Eintrittskarten. Demnach bot die Stadtmarketinggesellschaft Schwerin mbH auf ihrer Website BUGA-Karten gegen Zahlung per Kreditkarte an, ohne dass die Daten der Besteller verschlüsselt übertragen wurden.

Diesen Vorwurf konnte ich rasch bestätigen. Die Bestelldaten einschließlich der Kreditkartendaten wurden tatsächlich im Klartext übertragen. Damit verstieß die Stadtmarketinggesellschaft sogar gegen ihre eigene Zusicherung, denn auf der Bestellseite hieß es: „Die Datenübertragung erfolgt mit Hilfe einer gesicherten Verbindung.“ Auf diese Weise bestand die Gefahr, dass sich Unbefugte Zugriff auf die Bestelldaten und insbesondere die Kreditkartendaten verschaffen konnten. Dies wäre beispielsweise durch eine nachgebaute oder gefälschte Website durchaus möglich gewesen, da auch wachsame Nutzer kaum Hinweise auf eine Manipulation finden könnten.

Deshalb habe ich die Stadtmarketinggesellschaft noch am selben Tage über diesen Missstand unterrichtet. Ich habe verlangt, das Bestellverfahren durchgängig verschlüsselt abzuwickeln. Insbesondere die Übertragung von Kundendaten bedarf nach heutigem Stand der Technik einer wirksamen kryptographischen Verschlüsselung und einer Möglichkeit, die Identität des Servers überprüfen zu können (Authentifizierung des Servers). Außerdem habe ich empfohlen, das Verfahren bis zur vollständigen Realisierung dieser Anforderungen auszusetzen.

Die Stadtmarketinggesellschaft hatte daraufhin nach einigen Tagen die BUGA-Startseite so umgestaltet, dass bereits diese Seite mit dem Verfahren Transport Layer Security (TLS) verschlüsselt übertragen wird. Forderte ein Nutzer die Seite unverschlüsselt an, so wurde er auf die verschlüsselte Seite umgeleitet. Außerdem wurde die Ticketbestellung auf eine separate, ebenfalls verschlüsselte Seite verlegt. Das TLS-Protokoll bietet außerdem noch die Authentifizierung des Web-Servers: Beim Aufbau einer TLS-Verbindung muss der Web-Server ein Zertifikat übermitteln, welches vom Web-Browser geprüft wird. Nutzer können sich so davon überzeugen, ob sie echte Seiten angezeigt bekommen.

Damit entsprach der Bestellvorgang nunmehr dem Stand der Technik und die BUGA-Interessenten konnten ihre Eintrittskarten nun beruhigt auch über die Website der Stadtmarketinggesellschaft erwerben.

Für bedenklich halte ich jedoch, dass die Gesellschaft das Verfahren nicht vorübergehend abgeschaltet hat. Kunden waren so unnötig einem erhöhten Risiko ausgesetzt, dass ihre Daten missbraucht werden konnten.

2.5 Statistik

2.5.1 Volkszählung 2011

In meinem Achten Tätigkeitsbericht hatte ich unter Punkt 2.7.1 berichtet, dass sich Deutschland an dem von der Europäischen Union für das Jahr 2011 geplanten gemeinschaftsweiten Zensus beteiligt. Trotz der geäußerten datenschutzrechtlichen Bedenken vor dem Innenausschuss des Deutschen Bundestages hatte dieser dem Gesetzesentwurf zugestimmt, sodass das Zensusvorbereitungsgesetz am 13. Dezember 2007 in Kraft getreten ist. Damit war der Weg für die Durchführung des registergestützten Zensus frei.

Das Gesetz über den registergestützten Zensus im Jahre 2011 (ZensG 2011) ist am 16. Juli 2009 in Kraft getreten. Bei einem Berichterstattungsgespräch vor dem Innenausschuss des Deutschen Bundestages am 20. April 2009 zum Entwurf eines Gesetzes zur Anordnung des Zensus 2011 sowie zur Änderung von Statistikgesetzen hatte auch ich als Berichterstatter die Gelegenheit, auf einige datenschutzrechtliche Bedenken hinzuweisen (BT-Drucksache 16/12219).

Zu meinen Kritikpunkten gehörte zum Beispiel auch die Erhebung „der Zugehörigkeit zu einer Religionsgemeinschaft“, auf die erfreulicherweise im Gesetz verzichtet worden ist.

Des Weiteren habe ich darauf hingewiesen, dass in sogenannten Sonderbereichen (Gemeinschafts-, Anstalts- und Notunterkünfte, Wohnheime und ähnliche Unterkünfte) lediglich eine anonyme Datenerhebung zulässig ist, zumal in der Begründung des Zensusvorbereitungsgesetzes 2011 eine solche auch angekündigt worden war. Es ist nicht nachvollziehbar, aus welchem Grund von dieser Aussage abgewichen wird, zumal schon im Volkszählungsurteil für die Bewohner in sensiblen Anstaltsbereichen entsprechende Maßstäbe aufgestellt worden sind und darauf abgestellt wurde, dass die Erhebung Anhaltspunkte über die Belegung der Anstalten liefern soll, also die Mitteilung der zahlenmäßigen Belegung durch den Anstaltsleiter reiche (Bundesverfassungsgerichtsentscheidung 65, 49). Trotz der auch von anderen Datenschutzbeauftragten geübten Kritik sieht das Gesetz dennoch eine personenscharfe Erhebung in Sonderbereichen vor.

Ich habe vor dem Innenausschuss die Möglichkeit genutzt, nochmals meine generellen Bedenken zum Zensus 2011 vorzutragen. Hierzu gehört auch die mangelnde Transparenz des Verfahrens, denn die von der Datenerhebung Betroffenen erfahren regelmäßig nichts von dem Umstand der Erhebung ihrer personenbezogenen Daten, haben damit keine Kontrolle über Inhalt und Empfänger der Übermittlungen und können demzufolge ihre verfassungsrechtliche Befugnis, grundsätzlich selbst zu entscheiden, nicht ausüben.

Außerdem halte ich nach wie vor eine Reidentifizierung auf kommunaler Ebene für wahrscheinlich, denn § 22 Abs. 2 Satz 1 ZensG 2011 sieht vor, dass statistische Einzelangaben „auf Ersuchen“ hin an die kommunalen Statistikstellen übermittelt werden dürfen. Zwar sind in Satz 2 dieser Vorschrift besondere Zulässigkeitsvoraussetzungen hinsichtlich der Einrichtung von kommunalen Statistikstellen formuliert. Ich werde eingehend prüfen, ob die gesetzlich vorgeschriebenen Maßnahmen zur räumlichen, organisatorischen und personellen Trennung der Statistikstellen von den für nichtstatistische Aufgaben zuständigen Stellen der Gemeinden gewährleistet wird.

Zuletzt bleibt auch der Kritikpunkt, dass der Gesetzgeber die Möglichkeit eröffnet, Datenabgleiche für die Bereinigung des Melderegisters zu nutzen. Das „Rückwirkungsverbot“ ist zwar in § 15 Abs. 3 Satz 1 ZensG 2011 gesetzlich normiert, vermag aber auch wegen des Amtsermittlungsgrundsatzes nicht zu überzeugen, zumal nach Aussage des Statistischen Bundesamtes vor dem Innenausschuss gerade der Abgleich von Melderegisterdaten mit erhobenen Daten in sensiblen Bereichen auf der Personenebene das konstituierende Element sei (Dr. Sabine Bechtold, Wortprotokoll der 90. Sitzung des Innenausschusses des Deutschen Bundestages, S. 8, BT-Drucksache 16/12219). Deswegen muss meiner Ansicht nach zumindest verhindert werden, dass solche Rückmeldungen negative Auswirkungen für die betroffenen Bürgerinnen und Bürger haben. Dies könnte nur, wie ursprünglich im Referentenentwurf vorgesehen, mit einer Aussetzung der Bußgeldregelungen geschehen. Auch hier werde ich entsprechende Prüfungen vornehmen müssen.

Auf Landesebene bin ich im Rahmen einer frühzeitigen Verbandskonsultation zum Referentenentwurf eines Gesetzes zur Ausführung des Zensusgesetzes 2011 in Mecklenburg-Vorpommern (Zensusausführungsgesetz-ZensAG M-V) an dem Gesetzesvorhaben beteiligt worden. Daraufhin ist mir im Rahmen der Verbandsanhörung der Entwurf dieses Gesetzes mit der Gelegenheit zur Stellungnahme übersandt worden. Dies habe ich genutzt, um einige datenschutzrechtliche Bedenken zu äußern bzw. Hinweise und Formulierungsvorschläge zu geben, deren Umsetzung vor allem die Einhaltung der allgemeinen und besonderen Maßnahmen zur Datensicherheit, die das Landesdatenschutzgesetz Mecklenburg-Vorpommern festlegt, bei der Durchführung des Zensus gewährleisten soll.

Die Vorbereitung und Durchführung der Volkszählung 2011 werde ich auch weiterhin kritisch aus datenschutzrechtlicher Sicht begleiten.

2.5.2 Einsichtnahme in statistische Einzeldatensätze

Im Zusammenhang mit der Bearbeitung einer Petition zur Befragung beim Mikrozensus habe ich beim Statistischen Amt Mecklenburg-Vorpommern einen Kontroll- und Informationsbesuch durchgeführt, um zu überprüfen, ob die in nicht zulässiger Art und Weise erhobenen Daten im Erhebungsbogen des Petenten gelöscht worden sind. Erfreulicherweise konnte ich feststellen, dass die fraglichen Einzeldatensätze nicht mehr vorhanden waren.

Das Statistische Amt vertritt allerdings die Auffassung, dass der Landesbeauftragte für den Datenschutz generell nicht befugt sei, ohne eine entsprechende Einwilligung des Betroffenen statistische Einzeldatensätze einzusehen, da diese der statistischen Geheimhaltung gemäß § 16 Bundesstatistikgesetz (BStatG) unterliegen würden.

Daraufhin habe ich in meinem Bericht zum Kontroll- und Informationsbesuch auf meine umfassende Kontrollkompetenz auch in Bezug auf Daten, die einem besonderen Amtsgeheimnis wie etwa der beruflichen Schweigepflicht oder dem Steuergeheimnis unterliegen, hingewiesen. Ich habe auch darauf verwiesen, dass gemäß § 10 Abs. 4 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) personenbezogene Daten, die für andere Zwecke erhoben oder erstmalig gespeichert worden sind, zu Zwecken der Ausübung von Aufsichts- und Kontrollbefugnissen in dem dafür erforderlichen Umfang genutzt werden dürfen.

Das Statistische Amt verweist wiederum auf § 16 Abs. 1 Satz 1 BStatG, wonach Einzelangaben über persönliche und sachliche Verhältnisse, die für eine Bundesstatistik gemacht werden, von den Amtsträgern und für den öffentlichen Dienst besonders Verpflichteten, die mit der Durchführung von Bundesstatistiken betraut sind, geheim zu halten sind, soweit durch besondere Rechtsvorschrift nichts anderes bestimmt ist. § 10 Abs. 4 Satz 1 i. V. m. § 30 Abs. 1 DSG M-V sei jedoch keine solche besondere Rechtsvorschrift. Solche Vorschriften würden einer ausdrücklichen Zulassung in einer besonderen Rechtsvorschrift in einem eine Bundesstatistik anordnenden Bundesgesetz bedürfen. Ein Kontrollrecht könne sich aus demselben Grund auch nicht aus § 24 Abs. 6 und Abs. 2 Satz 1 Nr. 2 Bundesdatenschutzgesetz (BDSG) ergeben.

Gemäß § 30 Abs. 1 DSG M-V kontrolliert der Landesbeauftragte für den Datenschutz bei den öffentlichen Stellen die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz. Diese Kontrollkompetenz ist umfassend zu verstehen. Auch personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, können ihm nicht vorenthalten werden. Dies stellt auch die Regelung des § 24 Abs. 6 i. V. m. Abs. 2 Satz 1 Nr. 2 BDSG klar, wonach die Kontrolle der Landesbeauftragten für den Datenschutz auch auf personenbezogene Daten erstreckt wird, die besonderen Geheimhaltungsvorschriften unterliegen.

Ein unbeschränktes Zugangsrecht des Landesbeauftragten für den Datenschutz besteht jedoch auch unabhängig von dieser bundesgesetzlichen Regelung, da die Kontrollkompetenz der Landesdatenschutzbeauftragten von den Ländern als eigene Angelegenheit geregelt wird und diese im Rahmen der Organisationshoheit eingeräumten Informationsrechte des Landesdatenschutzbeauftragten den bundesrechtlichen Geheimhaltungsvorschriften vorgehen.

Außerdem handelt es sich bei einer Kontrolle durch den Landesbeauftragten für den Datenschutz nicht um eine gezielte Datenerhebung bzw. Datenübermittlung von Einzelangaben an eine Stelle außerhalb der amtlichen Statistik. Die Kontrolle wird in der Regel das Ziel haben festzustellen, ob durch die amtliche Statistik mehr Daten erhoben werden, als die die Statistik anordnende Rechtsvorschrift bestimmt. Dass der Gesetzgeber eine solche Kontrolle verhindern wollte, ist meiner Ansicht nach auszuschließen.

Zudem soll § 16 BStatG unter anderem die Trennung von Verwaltungsvollzug und Statistik sicherstellen. Die dem Datenschutzbeauftragten eingeräumte Kontrollfunktion ist jedoch gerade nicht als Teil der „vollziehenden Verwaltung“ zu sehen.

Gegen die Argumentation des Statistischen Amtes spricht außerdem, dass bei einer systematischen Auslegung von § 16 Abs. 1 BStatG der gesetzliche Ausschluss der in Satz 3 dieser Vorschrift genannten abgabenrechtlichen Anzeige- und Mitteilungspflichten überflüssig wäre, wenn unter „besondere Rechtsvorschriften“ im Sinne des § 16 Abs. 1 Satz 1 BStatG nur statistikrechtliche Regelungen fallen würden.

Ich gehe davon aus, dass die bisherige gute Zusammenarbeit mit dem Statistischen Amt, insbesondere im Hinblick auf die Fülle der mit der Volkszählung 2011 zu erwartenden Fragen, ihre Fortsetzung findet und hierzu auch Kontrollen durch den Landesbeauftragten für den Datenschutz ermöglicht werden.

2.6 Wahlen

2.6.1 Veröffentlichung personenbezogener Daten in einer öffentlichen Sitzung des Wahlausschusses

Ein Petent hat sich im April 2009 an mich gewandt, da er als Beisitzer eines Wahlausschusses damit konfrontiert worden ist, dass in der öffentlichen Sitzung bei der Zulassung der Kandidaten für die Bürgermeisterwahl durch die Vertreter des Amtes personenbezogene Daten von Bewerbern bekannt gemacht wurden. Dies betraf auch Angaben über vor Jahren abgeschlossene Strafverfahren und zur Tätigkeit beim ehemaligen Ministerium für Staatssicherheit (MfS) der DDR.

Die gesetzliche Lage gestaltet sich so, dass in der öffentlichen Sitzung des Wahlausschusses die Zulassung der Kandidaten für die Bürgermeisterwahl geprüft wird, das heißt, es wird geprüft, ob die gesetzlich festgelegten Wählbarkeitsvoraussetzungen gemäß §§ 61 Abs. 1 i. V. m. 10 Kommunalwahlgesetz Mecklenburg-Vorpommern (KWG M-V) bei den vorgeschlagenen Kandidaten vorliegen. So war auch eine „Erklärung über eventuelle Straftaten“ gemäß Punkt 10.1 der Verwaltungsvorschrift des Innenministeriums zur Vorbereitung und Durchführung der Europaparlaments- und Kommunalwahlen am 7. Juni 2009 einzureichen. Außerdem war für Ehrenbeamte auch die beamtenrechtliche Geeignetheit gemäß § 8 Abs. 4 Nr. 2 Landesbeamtengesetz Mecklenburg-Vorpommern im Hinblick auf eine Tätigkeit beim MfS zu überprüfen. Hierfür sind die erforderlichen Daten gemäß Punkt 10.1 der oben genannten Verwaltungsvorschrift anhand der „Erklärung aus Anlass der Einstellung in den öffentlichen Dienst“ darzulegen.

Aufgrund dieser gesetzlichen Grundlagen müssen in einer Wahlausschusssitzung also auch Tatsachen ausgewertet und beurteilt werden, die eventuelle Straftaten der Bewerber oder eine Tätigkeit beim MfS der ehemaligen DDR betreffen. Da der Wahlausschuss jedoch in öffentlicher Sitzung tagt, halte ich aus datenschutzrechtlicher Sicht die Preisgabe solcher Daten Dritten gegenüber dennoch für bedenklich, zumal gemäß § 12 Abs. 7 KWG M-V die Mitglieder der Wahlausschüsse, ihre Stellvertreter und ihre Schriftführer über die ihnen bei ihrer amtlichen Tätigkeit bekannt gewordenen Angelegenheiten zur Verschwiegenheit verpflichtet sind. Aus diesem Grunde habe ich dem Petenten empfohlen, mit diesen sehr sensiblen personenbezogenen Daten im Sinne der Interessen der Betroffenen umzugehen, das heißt, wenn möglich keine Namen zu nennen oder die Auswertung hinsichtlich der Wählbarkeitsvoraussetzungen schriftlich vorzunehmen.

Im Rahmen der Bearbeitung dieser Petition bin ich weiterhin auf folgende Problematik gestoßen:

Gemäß § 19 Abs. 1 Satz 2 Stasiunterlagengesetz hat in den dort genannten Fällen eine Mitteilung, Einsichtgewährung und Herausgabe von Unterlagen zu unterbleiben, wenn keine Hinweise vorhanden sind, dass nach dem 31. Dezember 1975 eine inoffizielle Tätigkeit für den Staatssicherheitsdienst oder einen ausländischen Nachrichtendienst vorgelegen hat. Da einer öffentlichen Stelle in einem solchen Fall keine Mitteilung, Einsichtnahme oder Herausgabe seitens der Bundesbeauftragten für die Stasiunterlagen erteilt wird, kann von einem Wahlbewerber die Mitteilung einer entsprechenden Tätigkeit in der „Erklärung aus Anlass der Einstellung in den öffentlichen Dienst“ ebenso nicht verlangt werden, wenn sie Tätigkeiten vor dem 31. Dezember 1975 betreffen.

Diese Frist muss auch für einen Wahlbewerber hinsichtlich der Angabe seiner Daten auf der oben genannten Erklärung gelten, soweit keine Ausnahmeregelung greift. Da dies jedoch für den Wahlbewerber anhand des Textes der Erklärung nicht erkennbar ist, habe ich mich an das Innenministerium Mecklenburg-Vorpommern gewandt und empfohlen, bei künftigen Wahlen die Wahlbewerber auf diese Regelung hinzuweisen.

In der „Erklärung über eventuelle Straftaten“ gemäß der Anlage 5 zu Punkt 10.1 der oben genannten Verwaltungsvorschrift wird darauf hingewiesen, das gemäß § 53 Abs. 2 Bundeszentralregistergesetz (BZRG) alle Verurteilungen anzugeben sind, auch wenn sie nicht in ein Führungszeugnis aufzunehmen sind. Verurteilungen, die nicht in ein Führungszeugnis aufzunehmen sind, sind nach dieser Vorschrift dann zu offenbaren, wenn Gerichte oder Behörden ein Recht auf unbeschränkte Auskunft haben und der Betroffene hierüber belehrt worden ist. Inwieweit sich jedoch ein unbeschränktes Auskunftsrecht im Sinne dieser Vorschrift im Hinblick auf die Tätigkeit des Wahlausschusses gemäß § 41 Abs. 1 BZRG ergibt und ob der Belehrungspflicht gemäß § 53 Abs. 2 BZRG genüge getan wurde, ist nicht ersichtlich. Außerdem ist für die Wahlbewerber nicht erkennbar, dass das Verschwiegenheitsrecht für getilgte oder tilgungsreife Verurteilungen nicht eingeschränkt werden kann und diese Verurteilungen nicht anzugeben sind.

Ich habe das Innenministerium Mecklenburg-Vorpommern gebeten, zu diesen Fragen Stellung zu nehmen und den Petenten hierüber informiert. Daraufhin ist mir mitgeteilt worden, dass die dargelegten Probleme einer eingehenden und abteilungsübergreifenden Prüfung bedürften. Da bereits erste Überlegungen für eine umfassende Änderung des Kommunalwahlrechtes getroffen werden, würden meine Fragen im Zuge der nächsten Novellierung und im Kontext mit den weiteren wahlrechtlichen Änderungen abschließend behandelt und mir ein Formulierungsvorschlag zugeleitet werden.

2.6.2 Fragen zum Wahlhelfereinsatz

Eine Petentin hat mir mitgeteilt, dass die Abteilung Personalmanagement der Hansestadt Rostock zur Vorbereitung der Europa- und Kommunalwahlen am 7. Juni 2009 die Daten sämtlicher Bediensteter (Familienname, Vorname, Geburtsdatum, Anschrift) - sowohl innerhalb als auch außerhalb des Zuständigkeitsbereiches der ersuchenden Gemeindewahlbehörde wohnend - an den Bereich Grundsatz und Wahlen (als ersuchende Stelle) weitergeleitet habe.

Daraufhin habe ich der Hansestadt Rostock meine Auffassung mitgeteilt und zunächst auf den Wortlaut des § 74 Abs. 5 Kommunalwahlgesetz Mecklenburg-Vorpommern (KWG M-V) verwiesen. Dort heißt es, dass aus dem Kreis der Bediensteten einer Dienststelle lediglich die Personen zu benennen sind, die ihre Wohnung innerhalb des Zuständigkeitsbereiches der ersuchenden Gemeindewahlbehörde haben. Es dürfen daher keine personenbezogenen Daten von Bediensteten, die ihren Wohnsitz nicht im Zuständigkeitsbereich der ersuchenden Gemeindewahlbehörde haben, an diese übermittelt werden. In § 74 Abs. 5 S. 3 KWG M-V ist lediglich festgelegt, dass Bedienstete die entsprechenden Ehrenämter wahrnehmen können, wenn sie nicht im Gebiet der ersuchenden Gemeindewahlbehörde wohnen. Daher besteht für diese Bediensteten meiner Auffassung nach jedoch keine Pflicht zur Ausübung dieser Ehrenämter.

Da die Hansestadt Rostock jedoch weiterhin davon ausgegangen ist, dass solche Verpflichtungen nach § 74 KWG M-V grundsätzlich möglich seien, habe ich das Innenministerium Mecklenburg-Vorpommern gebeten, zu dieser Problematik Stellung zu nehmen. Das Innenministerium hat meine Auffassung zu § 74 Abs. 5 KWG M-V geteilt und bestätigt, dass die Wahlbehörde ihr Datenübermittlungsverlangen an die Abteilung Personalmanagement auf diejenigen Beschäftigten hätte beschränken müssen, die im Bereich der Hansestadt Rostock wohnen.

Die Hansestadt Rostock will künftig bei Wahlen meiner Empfehlung entsprechend verfahren. Sie sei für diese Thematik besonders sensibilisiert worden, sodass in Vorbereitung der Bundestagswahl 2009 eine Wahlteamberatung des Kreiswahlleiters dazu genutzt worden sei, meine Auffassung der Gemeindewahlbehörde, dem Wahlleiter und der behördlichen Datenschutzbeauftragten mitzuteilen und entsprechende Schlussfolgerungen daraus zu ziehen. Im Ergebnis aller Betrachtungen zum Thema Wahlehrenamt sei außerdem beabsichtigt, die Erfahrungsberichte über die Europa- und Kommunalwahlen und der Bundestagswahl zu nutzen, um die Problematik der Wahlhelfergewinnung nochmals ausführlich zu beleuchten und gemäß der praktischen Erkenntnisse eine Novelle der Wahlgesetze anzuregen.

2.7 Finanzwesen

2.7.1 Überwachung auch bei Fahrschulen - Auskunftsersuchen eines Finanzamtes an die DEKRA

Die DEKRA hat sich an mich gewandt, da sie von der Steuerfahndungsstelle eines Finanzamtes aufgefordert worden ist, personenbezogene Daten für sämtliche Fahrschulen in Mecklenburg-Vorpommern für die Jahre 2004 - 2007 zu übermitteln. Die zu übermittelnden Daten sollten mindestens folgende Daten je Fahrschule enthalten:

1. Name, Anschrift, Geburtsdatum der Fahrschüler,
2. Datum der praktischen Prüfung und geprüfte Führerscheinklasse,
3. Angaben zu Wiederholungsprüfungen.

Die Steuerfahndungsstelle hat ihr Auskunftsbegehren auf § 208 Abs. 1 Nr. 3 Abgabenordnung (AO) gestützt, wonach Aufgabe der Steuerfahndung die Aufdeckung und Ermittlung unbekannter Steuerfälle ist. Nach ihrer Aussage sollen die erbetenen Auskünfte den für die Besteuerung der Fahrschulen zuständigen Finanzämtern die Kontrolle ermöglichen, ob die Einnahmen aus Fahrschultätigkeit, insbesondere im Hinblick auf die Erfassung aller Fahrschüler, ordnungsgemäß versteuert wurden. Im Rahmen von Außenprüfungen sei bei Fahrschulen festgestellt worden, dass diese ihre steuerlichen Pflichten nicht immer ordnungsgemäß erfüllten. So seien in den geprüften Fällen die Einnahmen aus Fahrschultätigkeit ganz oder teilweise nicht erklärt worden. Mehrfach hätten sich die Namen von Fahrschülern gar nicht aus der Buchführung ergeben.

Vor dem Hintergrund, dass die Steuerfahndung nach dieser Vorschrift nur bei hinreichendem Anlass tätig werden darf - das heißt, wenn aufgrund konkreter Momente oder aufgrund allgemeiner Erfahrung eine Überprüfung angezeigt erscheint -, habe ich das Finanzamt um Stellungnahme gebeten und bin daraufhin zu dem Ergebnis gekommen, dass das Auskunftsbegehren zwar grundsätzlich von § 208 Abs. 1 Nr. 3 AO gedeckt sein kann.

Allerdings hatte ich nach wie vor Bedenken, was die Verhältnismäßigkeit bzw. den Umfang der angeforderten Daten betraf. Für mich war nicht nachvollziehbar, warum der Name und das Geburtsdatum jedes Fahrschülers erforderlich sein sollte. Hierzu habe ich die Ansicht vertreten, dass ein unbekannter Steuerfall schon dann aufgedeckt wird, wenn die von der DEKRA übermittelten Zahlen über absolvierte Prüfungen und Wiederholungsprüfungen nicht mit der Anzahl der Fahrschüler, die sich aus der Buchführung bzw. den Angaben der Steuererklärung des Fahrschullehrers ergibt, übereinstimmen. Daher habe ich der DEKRA mitgeteilt, dass es zunächst ausreiche, wenn sie die Datenbestände der einzelnen Fahrschulen pseudonymisiert zur Verfügung stelle, da es der Steuerfahndungsstelle anhand dieses Datenmaterials durch den Abgleich mit den internen Daten möglich sei, eventuelle Differenzen festzustellen. Erst wenn Differenzen tatsächlich bei bestimmten Fahrschulen auftreten, kann es in einem zweiten Schritt erforderlich sein, die entsprechenden Namen der Fahrschüler anzufordern, um diese Differenzen zu konkretisieren.

Die DEKRA hat dem wiederholten Auskunftsverlangen des Finanzamtes diese Argumentation entgegengehalten und die Daten lediglich in pseudonymisierter Form übermittelt. Sie hat mich anschließend darüber informiert, dass die Steuerfahndungsstelle dies so akzeptiert habe und gegebenenfalls erst in einem zweiten Schritt die Namen von Fahrschülern abfragen werde.

2.7.2 Auskunftsrecht für Betroffene im Steuerverfahren wieder unterlaufen

Das Bundesverfassungsgericht hat in einem Beschluss (Beschluss vom 10. März 2008, 1 BvR 2388/0) festgelegt, dass § 19 Bundesdatenschutzgesetz (BDSG) auch gegenüber der Finanzverwaltung gilt. Das Gericht hat den Auskunftsanspruch unmittelbar für anwendbar erklärt, indem es das grundsätzlich grundrechtsgeschützte Interesse Betroffener, Kenntnisse von den sie betreffenden Datensammlungen zu erlangen, festgestellt hat. Das Bundesverfassungsgericht stellt außerdem klar, dass einer Finanzbehörde bei der Entscheidung über die Auskunftsgewährung kein Ermessen zukomme.

In Reaktion auf diesen Beschluss ist in den Entwurf eines Jahressteuergesetzes 2009 der Auskunftsanspruch derart aufgenommen worden, dass dem Betroffenen nach Maßgabe des § 19 BDSG Auskunft zu erteilen sei. Diese Regelung ist anschließend wieder aus dem Gesetzentwurf herausgenommen worden. Nach Aussage des Bundesministeriums der Finanzen seien sich die obersten Finanzbehörden des Bundes und der Länder zwar einig, bereichsspezifische Datenschutzregelungen zu schaffen, hinsichtlich der Ausgestaltung der Regelung bestehe jedoch noch Abstimmungsbedarf.

Das Finanzministerium Mecklenburg-Vorpommern hat mir gegenüber in Bezug auf den Beschluss des Bundesverfassungsgerichts und zum aktuellen Stand bezüglich der Schaffung einer Regelung zum Auskunftsanspruch die Auffassung vertreten, dass das Argument, der Gesetzgeber der Abgabenordnung habe bewusst auf ein Auskunfts- bzw. Akteneinsichtsrecht verzichtet und der absichtsvolle Regelungsverzicht gehe als bereichsspezifische Regelung den Datenschutzgesetzen des Bundes und der Länder vor, nach der Entscheidung des Bundesverfassungsgerichts nicht mehr tragfähig sei. Soweit die Abgabenordnung keine bereichsspezifischen Regelungen der sogenannten Betroffenen-Rechte enthalte, würden damit die allgemeinen Datenschutzgesetze des Bundes oder der Länder gelten.

Das Finanzministerium hat weiter mitgeteilt, dass sich die Mehrheit der Länder jedoch dafür ausgesprochen habe, vor Schaffung einer gesetzlichen Grundlage in der Abgabenordnung das Auskunftsrecht zunächst im Wege einer bundeseinheitlichen Verwaltungsanweisung zu regeln.

Diese Verwaltungsanweisung ist am 17. Dezember 2008 erlassen worden. Sie regelt, dass den Beteiligten auf Antrag Auskunft über die zu ihrer Person gespeicherten Daten erteilt werden soll, jedoch nur, wenn sie ein berechtigtes Interesse darlegen.

Der Bundesbeauftragte und die Landesbeauftragten für den Datenschutz sind sich darüber einig, dass diese weitgehende Einschränkung des Auskunftsanspruchs des Betroffenen den datenschutzrechtlichen Grundsätzen widerspricht. Die Verwaltung darf weder eine Begründung für die Geltendmachung des Anspruchs verlangen noch weitere Bedingungen aufstellen, die über den gesetzlichen Rahmen hinausgehen. Es ist daher unzulässig, wenn in einer untergesetzlichen Regelung der Finanzverwaltung die Erfüllung des Anspruchs von einem „berechtigten Interesse“ abhängig gemacht wird, welches die Gesetze selbst, auf die sich der Betroffene berufen könnte, nicht vorsehen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher in einer Entschließung vom 26./27. März 2009 gefordert, dass das Bundesministerium der Finanzen die Verwaltungsanweisung vom 17. Dezember 2008 unverzüglich aufhebt und der Bundesgesetzgeber den Auskunftsanspruch der Steuerpflichtigen durch eine eindeutige Regelung in der Abgabenordnung klarstellt, die dem § 19 BDSG entspricht.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat das Schreiben des Bundesministeriums der Finanzen (BMF) vom 17. Dezember 2008 beanstandet, da auf diese Forderungen nicht reagiert worden ist. Da sich auch das Finanzministerium Mecklenburg-Vorpommern im Hinblick auf die Bundeseinheitlichkeit des Besteuerungsverfahrens an die Rechtsauffassung und den Erlass des BMF vom 17. Dezember 2008 gebunden fühlt, habe ich dies bereits als Grund für eine Beanstandung der Verwaltungsanweisung gesehen und diese unmittelbar gegenüber der Finanzministerin unseres Landes beanstandet. Ich habe gefordert, dass das Landesdatenschutzgesetz nicht durch kritiklose Übernahme einer Weisung des Bundesministeriums der Finanzen unterlaufen werden darf.

2.7.3 Kontenabrufverfahren nehmen zu

In meinem letzten Tätigkeitsbericht (Achter Tätigkeitsbericht, Punkt 2.5.2) hatte ich über die Entscheidung des Bundesverfassungsgerichtes zur Rechtmäßigkeit der Kontenabrufverfahren berichtet. Aufgrund der Feststellung des Gerichtes zu § 93 Abs. 8 Abgabenordnung (AO), dass diese Norm nicht hinreichend bestimmt festlege, welche Behörden ein Ersuchen zum Abruf der Kontostammdaten stellen können sowie welchen Aufgaben ein solches Ersuchen dienen könne, hat der Bundesgesetzgeber eine Neuregelung des § 93 Abs. 8 AO beschlossen. In dieser Regelung ist genau festgelegt, welche Verwaltungsbehörden die Möglichkeit eines automatisierten Kontenabrufes beim Bundeszentralamt für Steuern nutzen können (BGBl. I 2007 S. 1912).

Zu diesen Verwaltungsbehörden gehören Behörden, die zuständig sind für:

1. die Grundsicherung für Arbeitssuchende nach dem Zweiten Buch Sozialgesetzbuch,
2. Sozialhilfe nach dem Zwölften Buch Sozialgesetzbuch,
3. Ausbildungsförderung nach dem Bundesausbildungsförderungsgesetz,
4. Aufstiegsfortbildung nach dem Aufstiegsfortbildungsförderungsgesetz und
5. Wohngeld nach dem Wohngeldgesetz.

Weiterhin ist geregelt worden, dass ein Abrufersuchen für andere Zwecke nur zulässig ist, soweit dies durch ein Bundesgesetz ausdrücklich zugelassen ist.

Ich informiere mich mit Hilfe monatlicher Übersichten des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit regelmäßig darüber, in welchem Umfang Finanzämter und andere Behörden des Landes Mecklenburg-Vorpommern von der Möglichkeit des Kontenabrufes Gebrauch machen.

Nach § 93 Abs. 8 AO sind im Jahr 2008 in unserem Bundesland insgesamt 55 Abrufe von Sozialbehörden erfolgt, im Jahr 2009 waren es 129 Kontenabrufe. Nach Mitteilung der Landesregierung auf eine Kleine Anfrage (Landtagsdrucksache 5/2725) haben die in Mecklenburg-Vorpommern für das ALG II (SGB II) zuständigen Behörden in den Jahren 2007, 2008 und bis einschließlich Juli 2009 bisher 137 Kontenabrufe gem. § 93 Abs. 8 AO durchgeführt. Ein Kontenabruf wurde im Januar 2008 von der für die Sozialhilfe nach dem SGB XII zuständigen Behörde veranlasst.

Im September 2007 hatte mir das Finanzministerium mitgeteilt, dass seit April 2005 484 Kontenabrufe gem. § 93 Abs. 7 AO und 8 Kontenabrufe gem. § 93 Abs. 8 AO durchgeführt worden seien. Hierbei hätten 201 Kontenabrufe zur Feststellung bisher unbekannter Konten und Depots geführt, wobei die Höhe der Steuern, die durch einen Kontenabruf zusätzlich festgesetzt bzw. vollstreckt werden konnten, 1,5 Millionen Euro betragen würde.

Allein im Jahr 2009 sind nach den mir zur Verfügung gestellten Angaben des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit 430 Kontenabrufe gemäß § 93 Abs. 7 AO durchgeführt worden. Statistische Angaben darüber, wie viele Konten und Depots in Bezug auf Abfragen nach dieser Vorschrift im Einzelnen (Bankkontenstammdaten) ermittelt wurden, liegen der Landesregierung nicht vor (siehe o. g. Landtagsdrucksache).

Die oben genannten Zahlen lassen erkennen, dass die Zahl der Kontenabrufe insgesamt deutlich steigt. Ich werde beobachten, wie sich diese Entwicklung fortsetzt, und gegebenenfalls nochmals stichprobenartig prüfen, ob die durchgeführten Kontenabrufe tatsächlich erforderlich waren bzw. die Kontenabfragen unter Einhaltung datenschutzrechtlicher Grundsätze erfolgen.

Da nach Aussage der Landesregierung keine statistischen Angaben darüber vorliegen, wie viele Konten und Depots aufgrund von Kontenabfragen ermittelt werden konnten, empfehle ich der Landesregierung, statistische Angaben über die ermittelten Konten und Depots zur Verfügung zu stellen, um Feststellungen darüber zu ermöglichen, ob die diesbezüglich zu verzeichnenden Erfolge in einem angemessenen Verhältnis zu der Anzahl der durchgeführten Kontenabrufe stehen.

2.7.4 Einführung der Steueridentifikationsnummer

In meinem letzten Tätigkeitsbericht (Achter Tätigkeitsbericht, Punkt 2.5.1) hatte ich über die datenschutzrechtlichen Bedenken im Hinblick auf die geplante Einführung der Steueridentifikationsnummer berichtet. Trotz der von den Datenschutzbeauftragten des Bundes und der Länder geäußerten Kritik an der Einführung der Steueridentifikationsnummer ist am 1. August 2008 mit dem Versand der Mitteilungsschreiben über die zugeteilten Steueridentifikationsnummern durch das Bundeszentralamt für Steuern begonnen worden. Bundesweit kam es hierbei zu nicht unerheblichen Pannen, die auch datenschutzrechtliche Aspekte betrafen. So erreichten mich im Zusammenhang mit der Vergabe der Steueridentifikationsnummer einige Petitionen, aufgrund derer eine rechtswidrige Nutzung des Melderegisters aufgedeckt worden ist. Übergeordnete Fragen hierzu habe ich an den Bundesbeauftragten für den Datenschutz weitergeleitet, sodass dieser entsprechende Stellungnahmen zur Rechts- und Sachlage vom Bundesministerium der Finanzen und vom Bundesministerium des Innern einholen konnte.

2.7.5 Rechtswidrige Nutzung des Melderegisters in Zusammenhang mit der Vergabe der Steueridentifikationsnummer

Ein Petent hat mich darüber informiert, dass in einem Mitteilungsschreiben an seine minderjährige Tochter im Adressfeld unter dem Namen die Abkürzung „EFH1“ stehe. Da die gleiche Abkürzung auch unter den gespeicherten Daten aufgetaucht sei, ist er davon ausgegangen, dass damit gemeint sei „Einfamilienhaus, Anzahl 1“. Beim Petenten hat dies den Eindruck erweckt, dass so jedem Briefträger mitgeteilt werde, wer wie viele Immobilien besitze.

Die entsprechende Stadt hat mir hierzu mitgeteilt, dass die Aufnahme des Merkmals „EFH“ zusammen mit einer entsprechenden Wohnungsnummer in das Melderegister mit dem sogenannten integrierten Stadtentwicklungskonzept der Stadt zusammenhänge, welches eine der Grundlagen der Stadtentwicklung und als solches maßgebend für die Städtebauförderung sei. Die Registrierung im Melderegister hänge mit der Software zusammen, die aufgrund der Einführung dieses Konzeptes eingesetzt werde.

Hierzu habe ich der Stadt mitgeteilt, dass für die Speicherung des oben genannten Merkmals im Melderegister im Landesmeldegesetz Mecklenburg-Vorpommern keine Rechtsgrundlage besteht und auch die Übermittlung dieses Merkmals zum Zwecke der erstmaligen Zuteilung der Identifikationsnummer an das Bundeszentralamt für Steuern von keiner Rechtsvorschrift gedeckt ist. Daraufhin ist die Stadt meiner Forderung, das Merkmal in allen relevanten Fällen umgehend aus dem Melderegister zu entfernen, nachgekommen.

Zu meiner Frage, aus welchem Grund trotz fehlender Rechtsgrundlage für die Speicherung und Übermittlung des Merkmals „EFH1“ das Bundeszentralamt für Steuern dieses im Adressfeld der Mitteilungsschreiben aufführt, hat das Bundesministerium der Finanzen dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit mitgeteilt, dass die 2. Bundesmeldedatenübermittlungsverordnung und Steueridentifikationsnummernverordnung anhand genau benannter Felder des DSMeld- Standards den Umfang der zu speichernden und entgegenzunehmenden Daten bestimme.

Danach sei die Übermittlung des DSMeld-Feldes 1211 vorgesehen, welches die Übermittlung von Zusatzangaben zur Anschrift unter Verwendung sinnvoller Abkürzungen erlaube. Das Bundeszentralamt für Steuern habe dann ausgehend von den gesetzlichen Rahmenbedingungen diese zusätzliche Information als Teil der Anschrift mitgespeichert, da es sachfremde Erwägungen nicht feststellen könne und somit von der Erforderlichkeit dieser Angabe für die Adressierung ausgegangen sei.

Auch aufgrund anderer Petitionen ist mir bekannt geworden, dass die jeweiligen Kommunen aus Gründen der Städtebauförderung oder der regelmäßigen Auswertungen zur Entwicklung des Wohnungsmarktes dieses Feld genutzt haben, um weitere Informationen über die gegenwärtige Anschrift abzulegen, was jedoch nicht dem DSMeld- Standard entspricht.

Da für die Richtigkeit der im Melderegister gespeicherten Daten ausschließlich die Meldebehörden zuständig sind, sind die Länder durch das Bundesministerium des Innern zur Übermittlung bereinigter Datensätze aufgefordert worden. Hierzu seien in der Datenbank des Bundeszentralamtes für Steuern ca. 350.000 Datensätze, in denen zusätzliche Angaben gespeichert worden seien, identifiziert und den zuständigen Behörden mit der Bitte um Korrektur übermittelt und zunächst zu diesem Zweck vom Druck und der Übersendung an die Bürger zurückgestellt worden.

Ein weiteres Problem war die Mitteilung des Geburtslandes. Einige Petenten haben mir geschildert, dass in ihrem Mitteilungsschreiben in das Feld Geburtsland „ungeklärt“ eingetragen wurde. Auch verlangten einige Petenten richtige Angaben, da zum Beispiel als Geburtsland „Polen“ in dieses Feld eingetragen wurde. Auch hier fand sich der Ursprung des Problems bei den Meldebehörden, die den Geburtsstaat in Form eines Gebietsschlüssels erfassen, welcher auf dem Länderverzeichnis für den amtlichen Gebrauch in der Bundesrepublik Deutschland beruht. Dieses Länderverzeichnis wird ständig überarbeitet und entspricht dem jeweils aktuellen Gebietsstand. So hätten nach Aussage des Bundesministeriums des Innern viele Gemeinden in der Annahme, dass mit dem Gebietsschlüssel nur eine aktuelle geografische Zuordnung beabsichtigt gewesen sei, Geburtsorte, die zur Zeit der Geburt zum Deutschen Reich gehört hätten, mit dem aktuellen Gebietsschlüssel versehen. Dies habe in einer gewissen Zahl von Fällen dazu geführt, dass bei Vertriebenen ein ausländischer Geburtsstaat eingetragen worden sei, obwohl der Geburtsort im Zeitpunkt der Geburt innerhalb der Grenzen des damaligen Deutschen Reiches gelegen habe.

Auf die Empfehlung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, dass ein historisch zutreffender Gebietsschlüssel anzuwenden sei, ist eine Änderung des entsprechenden Datenblattes vorgesehen, in dem künftig der Gebietsschlüssel (und nicht der Staatsangehörigkeitsschlüssel) des Gebietsstaates des Geburtsstaates angeben werden soll. Nach Aussage des Bundesbeauftragten habe das Bundesministerium des Innern empfohlen, dass Personen, die bis zum 2. August 1945 jenseits von Oder und Neiße im Deutschen Reich in den Grenzen vom 31. Dezember 1937 geboren seien, melderechtlich nicht als im Ausland erfasst werden sollten.

Danach wird also zukünftig in solchen Fällen kein Geburtsstaat mehr in das Melderegister eingetragen bzw. ein eingetragener Geburtsstaat gelöscht. Betroffene Personen können sich somit zur Korrektur ihrer Daten an ihr Meldeamt wenden oder aber auch unmittelbar auf Antrag den Datensatz beim Bundeszentralamt für Steuern korrigieren lassen.

2.7.6 Offenlegung von wirtschaftlichen Verhältnissen bei Stundungsanträgen

Immer wieder erreichen mich Anfragen und Beschwerden im Zusammenhang mit beantragten Stundungen oder Erlassen von Gebühren oder Beiträgen öffentlicher Stellen und insbesondere von Zweckverbänden. Häufig beschweren sich Bürgerinnen und Bürger darüber, dass sie auf den Antragsformularen zu einer umfassenden Offenlegung ihrer wirtschaftlichen Verhältnisse (Einkommen, Verbindlichkeiten) aufgefordert werden.

Die Voraussetzungen für eine Stundung gemäß § 12 Kommunalabgabengesetz (KAG) i. V. m. § 222 Abgabenordnung (AO) können nur anhand bestimmter Angaben geprüft werden. So kommt eine Stundung von Forderungen nur in Betracht, wenn die Einziehung der Forderung bei Fälligkeit eine erhebliche Härte für den Schuldner bedeuten würde und der Anspruch durch die Stundung nicht gefährdet erscheint. Dies ergibt sich aus § 222 AO, der in solchen Fällen entsprechend anzuwenden ist. Danach ist zu prüfen, ob die Einziehung der Forderung eine erhebliche Härte darstellt. Von einer erheblichen Härte ist auszugehen, wenn sich aus den vom Betroffenen dargelegten sachlichen und persönlichen Gründen ergibt, dass er sich aufgrund der Umstände des Einzelfalls auf die Erfüllung der Forderung nicht rechtzeitig vorbereiten konnte oder dass er sich augenblicklich in ungünstigen wirtschaftlichen Verhältnissen befindet, z. B. ernsthafte Zahlungsschwierigkeiten hat.

Damit also die prüfende Stelle über einen Antrag auf Stundung entscheiden kann, muss der Antragsteller die hierfür erforderlichen Daten offenbaren. Die Stelle muss sich ein Bild über seine wirtschaftlichen Verhältnisse machen können, das heißt, der Antragsteller muss ein zeitnahes Bild seiner wirtschaftlichen Verhältnisse schaffen. Zweckmäßig ist daher eine Gegenüberstellung der flüssigen bzw. kurzfristig realisierbaren Vermögenswerte und der rückständigen bzw. kurzfristig fällig werdenden Verpflichtungen. Gegebenenfalls hat der Antragsteller Angaben in seinem Stundungsantrag unter Beweis zu stellen.

Im Ergebnis sind für die Bescheidung eines Stundungsantrages also sehr sensible personenbezogene Daten zu offenbaren. Es kommt jedoch immer wieder vor, dass auch Daten erhoben werden, die für eine Entscheidung der Stelle nicht erforderlich sind. Hierzu gehören zum Beispiel Angaben zum Beruf/Gewerbe des Schuldners, zum Namen und zur Anschrift des Arbeitgebers des Schuldners oder der Beruf der Kinder. In den meisten Fällen nehmen die Verwaltungen bzw. Zweckverbände meine datenschutzrechtlichen Hinweise zum Anlass, die Fragebögen und Merkblätter zur Stundung, Ratenzahlung, Niederschlagung oder zum Erlass von Forderungen entsprechend zu überarbeiten.

Im Sinne einer bürgerfreundlichen Bearbeitung solcher Anträge sollte öffentlichen Stellen und Zweckverbänden daran gelegen sein, jeden Antrag individuell und einzelfallbezogen zu bearbeiten, um offene Fragen und Unverständnis zu vermeiden. Dies sollte auch schon im Anschreiben an den Antragsteller zum Ausdruck kommen, der eine hinreichende Aufklärung über die im jeweiligen Fall notwendigen Voraussetzungen für die Bewilligung eines Stundungsantrages erhalten sollte, sodass er sich hiervon ein Bild und Überlegungen zu seinen Erfolgsaussichten machen kann.

2.7.7 Beauftragung eines Inkasso-Unternehmens durch eine öffentliche Verwaltung

Ein Petent hat mir ein Mahnschreiben des Inkasso-Unternehmens Creditreform übersandt, welches sich auf eine offene Rechnung bezog, die er gegenüber der Sozialagentur Ostvorpommern hatte (ALG II, Miet- und Heizkosten, Zuschüsse). Der Petent wollte wissen, ob die Übermittlung so sensibler Daten durch die Sozialagentur an das Inkasso-Unternehmen rechtmäßig sei.

Ich habe den Sachverhalt geprüft. Im Ergebnis meiner Prüfung habe ich gegenüber dem Landkreis Ostvorpommern eine Beanstandung ausgesprochen, da ich die Übertragung eines Teils des Mahnwesens und damit die Übermittlung von sensiblen personenbezogenen Daten an ein Privatunternehmen wegen fehlender Rechtsgrundlage für diese Beauftragung für unzulässig halte.

Der Auffassung des Landkreises, wonach § 120 Abs. 1 Kommunalverfassung Mecklenburg-Vorpommern (KV M-V) i. V. m. § 59 Abs. 1 KV M-V eine hinreichende Rechtsgrundlage für diese Datenverarbeitung sei, und der Aussage des Innenministeriums, dass zur Unterstützung der Kommunen bei der Forderungseinziehung eine Zusammenarbeit im Rahmen des § 59 KV M-V im Sinne der Einbeziehung Dritter als Verwaltungshelfer rechtlich zulässig sei, kann ich mich nicht anschließen. Hierzu habe ich ausführlich in meiner Beanstandung vom 24. Juli 2009, welche auf meiner Internetseite veröffentlicht ist, Stellung genommen. Ich habe unter anderem darauf verwiesen, dass die Einschaltung Privater bei der Vorbereitung und dem Erlass von Verwaltungsakten, die im Namen einer Behörde ergehen, rechtswidrig ist, wenn die Maßnahme nur noch der Form nach im Namen einer Behörde ergeht, alle wesentlichen Entscheidungen aber von dem Privaten getroffen werden.

Im vorliegenden Fall geht die Auslagerung eines Teils des Mahnwesens im Hinblick auf die Tätigkeit von Creditreform über die reine Verwaltungshilfe hinaus, da Creditreform die Daten selbständig mit Hilfe ihrer Datenbank abgleicht bzw. mit neuen Informationen anreichert und diese Kenntnisse für die weitere Bearbeitung der Mahnungen mit einfließen lässt. Gerade dies ist Sinn und Zweck dieser Aufgabenverlagerung. Dieser Zweck wird jedoch von den Regelungen der Datenverarbeitung im Auftrag gemäß § 4 Datenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) nicht umfasst, da die Auftragsvergabe nach dem DSG M-V die Datenverarbeitung lediglich im technischen Sinne meint. Hierfür ist Voraussetzung, dass die Daten schon in zulässiger Art und Weise an den Auftragnehmer übermittelt worden sind. Selbst wenn für die inhaltliche Aufgabenverlagerung eine gesetzliche Grundlage erkennbar wäre, sind die Anforderungen an eine Datenverarbeitung im Auftrag im Sinne des DSG M-V nicht erfüllt. Dies habe ich ebenfalls in meiner Beanstandung anhand einiger gesetzlicher Kriterien (Verantwortlichkeit, Vertraulichkeit, Transparenz, Verfahrensverzeichnis/Sicherheitskonzept) ausführlich erläutert. Vor allem konnte bisher anhand der hergereichten Unterlagen keine Prüfung der technisch-organisatorischen Maßnahmen zur Gewährleistung der Vertraulichkeit, insbesondere innerhalb der betrieblichen Datenverarbeitung, durch den Landkreis festgestellt werden. Im Gegenteil wird zum Beispiel in der Verfahrensbeschreibung nicht zwischen Daten differenziert, die zu unterschiedlichen Zwecken erhoben und gespeichert werden, das heißt, es wird nicht zwischen den Daten aus dem Bereich der Auskunftei und des Inkassos unterschieden. Danach ist es zweifelsfrei weder geregelt noch vereinbart, dass die Daten aus dem Inkassobereich nicht auch für andere Unternehmenszwecke genutzt werden könnten.

Nach meinem bisherigen Kenntnisstand stellt sich die Situation bislang so dar, dass nicht mit der notwendigen Sicherheit gewährleistet werden kann, dass die übermittelten Daten nicht auch für andere Zwecke verwendet werden können. Ich gehe davon aus, dass Inkassounternehmen, welche gleichzeitig auch Auskunftsdienste anbieten, grundsätzlich ungeeignet sind, im Wege der Auftragsdatenverarbeitung für die öffentliche Hand einen Teil des Mahnwesens zu übernehmen.

Aus diesen Gründen bin ich zu dem Ergebnis gekommen, dass neben einer entsprechenden Rechtsgrundlage für die Datenübermittlung an Creditreform ebenfalls technisch und organisatorisch gewährleistet bzw. nachgewiesen werden muss, dass Daten, die zu unterschiedlichen Zwecken gespeichert werden, nicht für andere Zwecke verwendet werden können.

2.8 Medien

2.8.1 Vorratsdatenspeicherung

In meinem letzten Tätigkeitsbericht (siehe Achter Tätigkeitsbericht, Punkt 2.1.2) hatte ich über die datenschutzrechtlichen Bedenken gegen die geplante Vorratsdatenspeicherung informiert. Im Januar 2008 ist das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Übermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG in Kraft getreten (Gesetz vom 9. November 2007, BGBL. I S. 3198). Trotz zahlreicher kritischer Äußerungen, auch von den Datenschutzbeauftragten des Bundes und der Länder, sind mit dem Gesetz umfangreiche Änderungen des Telekommunikationsgesetzes vorgenommen worden. So verpflichtet das Gesetz die Anbieter öffentlich zugänglicher Telekommunikationsdienste, umfangreiche Verkehrsdaten für sechs Monate auf Vorrat für die Strafverfolgungsbehörden zu speichern (§§ 113 a, b TKG), sodass das gesamte Telekommunikationsverhalten der Bürger erfasst wird, ohne dass ein konkreter Verdacht vorliegt. Seit dem 1. Januar 2009 müssen im Fall von Internettelefondiensten auch die Internetprotokoll-Adresse (IP-Adresse) des anrufenden und des angerufenen Anschlusses gespeichert werden. Ebenfalls müssen Anbieter von Diensten der elektronischen Post (E-Mail) sowie von Internetzugangsdiensten bestimmte Verkehrsdaten speichern.

Gegen die §§ 113 a und 113 b des Telekommunikationsgesetzes sind Ende 2007 bzw. Anfang 2008 mehrere Verfassungsbeschwerden eingelegt worden, weil eine systematische, verdachtslose Speicherung personenbezogener Daten auf Vorrat mit den Grundrechten offensichtlich nicht vereinbar sei.

Mit Beschluss vom 11. März 2008 (1 BvR 256/08, MMR 2008, 303) erließ daraufhin das Bundesverfassungsgericht eine einstweilige Anordnung, die festlegt, dass Anbieter von Kommunikationsdiensten die verlangten Daten zwar erheben und speichern müssen. Allerdings sind die Daten nur dann an die Strafverfolgungsbehörden zu übermitteln, wenn Gegenstand des Ermittlungsverfahrens eine schwere Straftat im Sinne des § 110 a Abs. 2 Strafprozessordnung (StPO) ist, die auch im Einzelfall schwer wiegt, der Verdacht durch bestimmte Tatsachen begründet ist und die Erforschung des Sachverhalts auf andere Weise wesentlich erschwert oder aussichtslos wäre (§ 100 a Abs. 1 StPO).

In den übrigen Fällen des § 100 g Abs. 1 StPO ist nach Aussage des Gerichts von einer Übermittlung der Daten einstweilen abzusehen. Eine Aussetzung des Vollzuges von § 113 a TKG, der die Speicherungspflicht für die Verkehrsdaten regelt, hat das Bundesverfassungsgericht abgelehnt, da es in der Vorratsdatenspeicherung keinen so schwerwiegenden und irreparablen Nachteil gesehen hat, der eine solche Aussetzung rechtfertigen könnte.

Die einstweilige Anordnung vom 11. März 2008 ist für die Dauer von sechs Monaten, längstens jedoch bis zur Entscheidung über die Verfassungsbeschwerde, vom Bundesverfassungsgericht wiederholt worden. Hinzu kommt ein weiterer Beschluss des Bundesverfassungsgerichts vom 28. Oktober 2008 (1 BvR 256/08). Das Bundesverfassungsgericht hat mit einstweiliger Verfügung entsprechende Einschränkungen für die Gefahrenabwehr und den Verfassungsschutz bzw. Nachrichtendienst angeordnet.

Bisher dürfen der Inhalt der Kommunikation und Daten über abgerufene Internetseiten nicht gespeichert werden. Jedoch ist zu befürchten, dass bei nächster Gelegenheit die Forderung nach einer präventiven anlasslosen Speicherung von Kommunikationsinhalten erhoben und beschlossen wird, wenn das Bundesverfassungsgericht die jetzt anhängigen Verfassungsbeschwerden nicht dazu nutzt, eine absolute Grenze der Überwachung von Kommunikation und ihrer näheren Umstände zu ziehen.

2.9 Soziales

2.9.1 Änderung des Kindertagesförderungsgesetzes

Der Entwurf eines Dritten Gesetzes zur Änderung des Kindertagesförderungsgesetzes (KiföGÄndG) wurde mir von der Landesregierung im Rahmen der Ressortanhörung mit der Bitte um datenschutzrechtliche Stellungnahme übersandt.

Der Gesetzentwurf sah unter anderem in § 1 Abs. 5 E-3. KiföGÄndG vor, dass der kindliche Entwicklungsprozess beobachtet und dokumentiert werden soll und dass dazu die Ergebnisse der Vorsorgeuntersuchungen zu berücksichtigen sind.

In Bezug auf die Beobachtung und die Dokumentation der kindlichen Entwicklungsprozesse war in § 10 Abs. 2 Satz 1, 2 des Entwurfs nicht geregelt, wie mit den Unterlagen umzugehen ist, wenn das Kind die Kindertageseinrichtung verlässt. Ich habe empfohlen klarzustellen, ob die Dokumentation den Personensorgeberechtigten dann mitgegeben wird oder ob, wie lange und wo sie aufzubewahren ist sowie für welche Zwecke sie genutzt werden darf.

Aus dem Entwurf ging nicht hervor, ob Personensorgeberechtigte die Daten, die der ärztlichen Schweigepflicht unterliegen, auf der Grundlage einer Auskunftspflicht der Kindertageseinrichtung zur Verfügung stellen sollten oder ob die Kindertageseinrichtung diese Daten bei den Personensorgeberechtigten auf freiwilliger Basis erheben soll. Der Begründung zum Gesetzestext war jedoch zu entnehmen, dass eine datenschutzrechtliche Einwilligung der Personensorgeberechtigten eingeholt werden sollte. Eine Einwilligung ist freiwillig und kann daher verweigert sowie später mit Wirkung auf die Zukunft jederzeit widerrufen werden (siehe § 8 Landesdatenschutzgesetz - DSG M-V).

Sind hingegen, was ich nachvollziehen kann, bestimmte Gesundheitsdaten des Kindes für die Betreuung in einer Kindertageseinrichtung erforderlich, wie beispielsweise der Impfstatus, habe ich empfohlen, im Gesetz zu regeln, dass und welche Gesundheitsdaten die Personensorgeberechtigten bei Aufnahme ihres Kindes in der Einrichtung mitzuteilen haben. Alternativ besteht die Möglichkeit, dass die Personensorgeberechtigten gebeten werden, Gesundheitsdaten auf freiwilliger Basis (datenschutzrechtliche Einwilligung) anzugeben.

Eine schriftliche Information, inwieweit meine Hinweise im Rahmen der Gesetzgebung berücksichtigt werden, liegt mir bisher noch nicht vor.

2.9.2 Dauerthema Hartz IV

Die Zahl der Eingaben von Arbeitslosengeld-II-Empfängern ist im Berichtszeitraum wieder sehr groß gewesen. Im Folgenden berichte ich über die häufigsten Fragen:

Welche datenschutzrechtlichen Anforderungen müssen bei der Durchführung von Hausbesuchen berücksichtigt werden?
Ein Petent schilderte, dass er bei einer Arbeitsgemeinschaft nach dem SGB II (ARGE) einen Antrag auf Sozialleistungen gestellt hatte. Sein Antrag wurde mit der Begründung abgelehnt, dass er in einer eheähnlichen Gemeinschaft mit seiner Nachbarin lebe. Er teilte mir auch mit, dass aufgrund einer anonymen Anzeige bei ihm mehrfach unangekündigt Hausbesuche durchgeführt werden sollten, ohne dass er darüber entsprechend aufgeklärt wurde. Der Petent wollte wissen, ob das Vorgehen der ARGE mit den datenschutzrechtlichen Bestimmungen vereinbar sei.

Hausbesuche sind als besondere Form der Datenerhebung nicht grundsätzlich unzulässig, oft aber auch nicht erforderlich. Häufigster Grund für Hausbesuche scheint der Verdacht zu sein, dass der Hilfesuchende in einer sogenannten Einstands- und Verantwortungsgemeinschaft (eheähnlichen Gemeinschaft) lebe, dieses jedoch, aus welchen Gründen auch immer, nicht angegeben hat. Sofern eine solche Bedarfsgemeinschaft vorliegt, hat die ARGE bei der Berechnung des Arbeitslosengeldes II auch das Einkommen und das Vermögen des Lebenspartners zu berücksichtigen. Da ein Hausbesuch für den Betroffenen einen besonders belastenden Charakter hat, muss der Außendienst in jedem Fall besondere Regeln beachten. Um für alle Beteiligten Rechtssicherheit bei der Durchführung von Hausbesuchen zu schaffen, hat die Bundesagentur für Arbeit fachliche Anweisungen erarbeitet. Danach hat die ARGE die konkreten Gründe für den Hausbesuch in einer Akte zu vermerken. Des Weiteren müssen dem Betroffenen vorher oder zu Beginn des Besuches diese Gründe erläutert werden.

Auf diese Anweisungen habe ich die betreffende ARGE hingewiesen und empfohlen, diese bei der Durchführung von Hausbesuchen zu beachten und in einem ersten Schritt zunächst die für die Entscheidung erforderlichen Daten beim Betroffenen zu erheben (§ 67 a Abs. 2 Satz 1 Sozialgesetzbuch Zehntes Buch (SGB X)). Die ARGE ist meiner Empfehlung gefolgt.
Die „Fachlichen Hinweise Außendienst“ der Bundesagentur für Arbeit können auf der Internetseite www.arbeitsagentur.de über den Pfad -für Bürgerinnen und Bürger- über die lokale Suchfunktion aufgerufen werden.

Für welchen Zeitraum darf die ARGE Kontoauszüge verlangen und darf sie diese für die Leistungsakte kopieren?
Auch zu diesem Thema haben mich wieder viele Anfragen von Hilfesuchenden erreicht, die unsicher waren, ob die Forderung der ARGE, Kontoauszüge vorzulegen, zulässig ist und ob die Mitarbeiter berechtigt sind, diese zu kopieren und in die Leistungsakte zu übernehmen.

Da Einkommen und Vermögen des Hilfesuchenden für das Arbeitslosengeld II relevant sind, kann der Sozialleistungsträger auch verlangen, dass Kontoauszüge vorgelegt werden. Klare gesetzliche Vorgaben, ob und in welchem Umfang der Leistungsträger bei der Beantragung von Sozialleistungen die Vorlage der Kontoauszüge verlangen darf und welche Angaben ggf. vom Antragsteller geschwärzt werden können, gibt es jedoch nicht. Daher haben die Landesbeauftragten für den Datenschutz der Länder Berlin, Brandenburg, Hamburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und Schleswig-Holstein Hinweise zur datenschutzgerechten Ausgestaltung der Anforderungen von Kontoauszügen bei der Beantragung von Sozialleistungen herausgegeben. Diese sind unter anderem in meinem Internetangebot unter www.datenschutz-mv.de über den Pfad -für Bürgerinnen und Bürger-, Informationsmaterial, Soziales veröffentlicht.

In diesen Hinweisen ist auch ein aktuelles Urteil des Bundessozialgerichts berücksichtigt worden, das die Vorlage von Kontoauszügen als erforderlich und damit zulässig beurteilt. Vorlage bedeutet jedoch nicht, dass Kopien der Auszüge regelmäßig in die Leistungsakte übernommen werden dürfen. Im Regelfall genügt ein Vermerk in der Akte, aus welchem Zeitraum Kontoauszüge eingesehen wurden und dass keine für den Leistungsanspruch relevanten Daten ermittelt wurden. Nur wenn leistungsentscheidende Angaben (Nachweis von Versicherungsbeiträgen, Angaben zur Vermögensbildung oder zu Unterhaltszahlungen) aus den Auszügen feststellbar sind, können sie im Einzelfall zur Leistungsakte genommen werden. Werden Kopien der Kontoauszüge zur Akte genommen, sind alle nicht erforderlichen Daten zu schwärzen. Zu der Übernahme von Kopien der Kontoauszüge in die Leistungsakte hat sich das Bundessozialgericht zwar nicht geäußert, es hat aber bei der Vorlage den Leistungsempfängern zugestanden, nicht erforderliche Daten unkenntlich zu machen. Übrigens bedeutet „Vorlage“ nach meiner Auffassung nicht, dass die Auszüge der betroffenen Person unmittelbar zurückgegeben werden müssen, sondern dass sie für den Zeitraum der Prüfung bei der ARGE verbleiben können.

Vor diesem Hintergrund ist gegen die Vorlage der Kontoauszüge der letzten drei Monate bei der Beantragung von Sozialleistungen aus datenschutzrechtlicher Sicht grundsätzlich nichts einzuwenden. Die vielen Anfragen zu diesem Thema zeigen jedoch, dass der Umgang mit Kontoauszügen bei den ARGEn häufig noch nicht den datenschutzrechtlichen Grundsätzen entspricht.

Muss der Arbeitslosengeld-II-Bescheid bei der Gebühreneinzugszentrale (GEZ) für die Befreiung von der Rundfunkgebühr vorgelegt werden?
Mehrere Petenten informierten mich, dass sie von der ARGE den Bescheid über das Arbeitslosengeld II mit dem Hinweis erhalten haben, diesen auch für den Antrag auf Befreiung von der Rundfunkgebührenpflicht zu nutzen. Da auf dem Bescheid auch Angaben enthalten sind, die für den Antrag bei der GEZ nicht erforderlich sind, haben sie mich um Unterstützung gebeten.

Ich habe mich daraufhin an die ARGEn gewandt und gefragt, ob es nicht möglich wäre, den Betroffenen einen gesonderten Leistungsnachweis auszustellen, den sie dem Antrag auf Befreiung von der Rundfunkgebührenpflicht beifügen können und der nur die zu diesem Zweck erforderlichen Daten enthält. Die ARGEn haben mir jedoch mitgeteilt, dass dies nicht möglich sei und dass die Hilfesuchenden die Möglichkeit hätten, die Angaben unkenntlich zu machen, die für die Aufgabe der GEZ nicht erforderlich sind.

Da diese Lösung aus datenschutzrechtlicher Sicht nicht zufriedenstellend war, wurde dieses Thema vom Arbeitskreis Medien der Landesbeauftragten für den Datenschutz und des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit aufgegriffen und in Zusammenarbeit mit der Bundesanstalt für Arbeit eine sogenannte Drittbescheinigung, welche nur die Personalien des Leistungsempfängers und den Zeitraum der Leistungsbewilligung enthält, erarbeitet. Eine solche Bescheinigung wird seit Juli 2009 an die Leistungsempfänger versandt, wenn sie einen Antrag auf Befreiung von der Rundfunkgebührenpflicht stellen möchten.

2.9.3 Im Notfall steht Kinderschutz vor Datenschutz?

Aufgrund von Vernachlässigung durch die Eltern hat es in Schwerin am Ende des Jahres 2007 den tragischen Tod eines Mädchens gegeben. Es ist öffentlich die berechtigte Frage an die Stadtverwaltung gestellt worden, ob durch anderes behördliches Handeln das Kind hätte gerettet werden können. Hierzu hat es eine Untersuchungskommission gegeben, die sich mit den näheren Umständen des Falles befasst und unter anderem vorgeschlagen hat, wie Gespräche und Hinweise im Jugendamt dokumentiert werden können, um Gefahren für das Kindeswohl rechtzeitig zu erkennen. In einem Pressebericht wurde das Ergebnis der Kommission kurz gefasst mit den Worten wiedergegeben: Im Notfall steht Kinderschutz vor Datenschutz. Diese Aussage suggeriert, dass der Datenschutz ein Hemmnis hinsichtlich des Kinderschutzes war. Sie verwundert insbesondere vor dem Hintergrund, dass die Kommission im vorliegenden Fall keine datenschutzrechtlichen Hürden erkannt hat, die durch gesetzliche Maßnahmen beseitigt werden müssten.

Mit dem Jugendamt der Stadt Schwerin und mit weiteren Jugendämtern habe ich das Thema Datenschutz und Kinderschutz diskutiert. Das gesetzliche Instrumentarium ist jedenfalls vorhanden, um Gefährdungen für das Wohl von Kindern rechtzeitig erkennen zu können, sodass geeignete Maßnahmen zur Abwehr dieser Gefahr eingeleitet werden können (§ 8a Sozialgesetzbuch Achtes Buch - SGB VIII). Während der Diskussionen zeigte sich jedoch, dass - trotz guter Hinweise und Empfehlungen des Landesamtes für Gesundheit und Soziales (LAGuS) zur Umsetzung dieser Rechtsvorschrift - in vielen Detailfragen Unsicherheit bei den Mitarbeitern öffentlicher und freier Träger der Jugendhilfe sowie bei Bürgerinnen und Bürgern hinsichtlich der Zulässigkeit und des Zeitpunktes der Übermittlung von personenbezogenen Daten bzw. Sozialdaten besteht.

Vor diesem Hintergrund habe ich dem Ministerium für Soziales und Gesundheit Mecklenburg-Vorpommern empfohlen, einen Handlungsleitfaden zur Verarbeitung von personenbezogenen Daten in der Kinder- und Jugendhilfe herauszugeben. Das Ministerium hat diesen Vorschlag aufgegriffen und die Aufgabe dem Deutschen Kinderschutzbund, Landesverband Mecklenburg-Vorpommern e. V., übertragen.

Der Kinderschutzbund hat regelmäßige Beratungen zum Inhalt dieses Handlungsleitfadens mit Vertretern des Ministeriums, von Jugendämtern und meiner Behörde durchgeführt. Die Arbeiten an dem Leitfaden haben sich durch das in der 16. Wahlperiode des Deutschen Bundestages angekündigte Bundeskinderschutzgesetz, das dann aber nicht in Kraft gesetzt worden ist, verzögert. Ich gehe jedoch davon aus, dass der Handlungsleitfaden bald herausgegeben wird, und bin sicher, dass er eine gute praktische Hilfe sein wird.

2.9.4 Elektronischer Entgeltnachweis ELENA

Seit mehreren Jahren begleite ich gemeinsam mit meinen Kollegen von Bund und Ländern die Entwicklung und Einführung des automatisierten Verfahrens zum Elektronischen Entgeltnachweis ELENA (ehemals JobCard). Kern des Verfahrens ist eine bundesweite Zentraldatei (die sogenannte Zentrale Speicherstelle - ZSS), in der Einkommensdaten der über 30 Millionen abhängig Beschäftigten, Beamten, Richter und Soldaten gespeichert werden sollen. Welche Daten gespeichert werden sollen, ist in § 97 Abs. 1 Sozialgesetzbuch Viertes Buch (SGB IV) festgelegt *(siehe Kasten)*. Diese Regelung lässt jedoch kaum erahnen, wie umfangreich der Datenbestand tatsächlich ist und wie lückenlos und detailliert das Berufsleben Einzelner abgebildet sein wird. Der sogenannte multifunktionale Verdienstdatensatz (MVDS), den jeder Arbeitgeber monatlich für jeden Beschäftigten an die ZSS übermitteln muss, umfasst nämlich mehrere hundert Datenfelder. Ein Ausdruck der vollständigen Liste (abrufbar von der ELENA-Homepage unter http://www.das-elena-verfahren.de) ist mehr als 40 DIN-A4-Seiten lang und beinhaltet neben den reinen Einkommensdaten eine Vielzahl weiterer, teilweise äußerst sensibler Informationen. In der Version vom August 2009 sind beispielsweise Informationen zu Fehlzeiten (z. B. unrechtmäßiger Streik, rechtmäßiger Streik, Aussperrung, unentschuldigtes Fehlen, Arbeitsbummelei) oder zu Kündigungen bzw. Entlassungen gespeichert. Dort wird beispielsweise registriert, ob der Arbeitnehmer Kündigungsschutzklage eingereicht hat, ob und wann er abgemahnt wurde, ob er sich vertragswidrig verhalten hat oder ob der Kündigung eine Sozialauswahl vorausging.

Die datenschutzrechtlichen Kritikpunkte habe ich im Siebten (siehe dort Punkt A.VIII.2) und im Achten Tätigkeitsbericht (siehe dort Punkt 2.8.1) bereits ausführlich erläutert. Meine datenschutzrechtliche Bewertung des ELENA-Verfahrens hat sich seitdem nicht grundlegend geändert. Angesichts der oben beschriebenen Menge der gespeicherten Daten steht nach wie vor fest, dass ein großer Teil der erhobenen Daten nie gebraucht wird, weil viele Betroffene keine der fraglichen Sozialleistungen beantragen werden. Damit werden Daten in unzulässiger Weise auf Vorrat gespeichert und der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit wird missachtet. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher zum wiederholten Male verfassungsrechtliche Bedenken geäußert und zugleich Verbesserungen im technischen und organisatorischen Bereich des Verfahrens gefordert (siehe Anlage 1.14, Entschließung vom 7. November 2008).

Die Konferenz hat unter anderem gefordert, dass Schlüssel zur Ver- und Entschlüsselung der bei der Zentralen Speicherstelle gespeicherten Daten nicht in der Verfügungsgewalt der Zentralen Speicherstelle liegen dürfen, sondern von einer unabhängigen Treuhänderstelle verantwortet werden. Dieser Forderung ist der Bundestag letztendlich nachgekommen. Das ELENA-Verfahrensgesetz (siehe unten) legt fest, dass die Verwaltung des sogenannten Datenbank-Hauptschlüssels dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit übertragen wird.

Die Bundesregierung hat am 25. Juni 2008 den Gesetzentwurf über das Verfahren des elektronischen Entgeltnachweises (ELENA-Verfahrensgesetz) beschlossen (BT-Drs. 16/10492). Das Gesetz wurde am 1. April 2009 verkündet. Somit werden voraussichtlich ab dem Jahr 2012 die bisherigen Bescheinigungen des Arbeitgebers bei der Beantragung von Arbeitslosengeld, Bundeserziehungsgeld und Wohngeld durch den elektronischen Entgeltnachweis ersetzt.

Schon vor Beginn der Einmeldepflicht am 1. Januar 2010 erreichte mich eine Vielzahl von Beschwerden betroffener, vor allem klein- und mittelständischer Unternehmen. Ich werde das Projekt deshalb auch weiterhin beratend begleiten. Sowohl als Vorsitzender des AK Technik (siehe Punkt 5) als auch durch meine Mitarbeit in der Arbeitsgruppe Informationssicherheit und Datenschutz des ELENA-Projektes werde ich mich dafür einsetzen, die immer noch vorhandenen Verfahrensmängel zu beseitigen. So muss beispielsweise das im Rahmen des ELENA-Modellvorhabens erarbeitete differenzierte Löschungskonzept weiterentwickelt und umgesetzt werden. Für abrufende Stellen sind starke Authentisierungsverfahren erforderlich, die dem Stand der Technik entsprechen und den Forderungen der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Oktober 2006 zur sachgemäßen Nutzung von Authentisierungs- und Signaturverfahren genügen. Und mittelfristig ist ein Verfahren anzustreben, das die technische Verfügungsmöglichkeit über die individuellen Daten den Betroffenen überträgt.

§ 97 Abs. 1 Satz 1 - 4 SGB IV
(1) Der Arbeitgeber hat der Zentralen Speicherstelle für jeden Beschäftigten, Beamten, Richter oder Soldaten monatlich gleichzeitig mit der Entgeltabrechnung eine Meldung zu erstatten, welche die Daten enthält, die in die erfassten Nachweise (§ 95 Absatz 1) aufzunehmen sind. Das sind insbesondere

1. die Versicherungsnummer (§ 147 des Sechsten Buches) oder Verfahrensnummer (Absatz 4), Familienname, Vornamen, Tag der Geburt und Anschrift des Beschäftigten, Beamten, Richters oder Soldaten,
2. das erfasste Einkommen in Euro, Beginn und Ende des Zeitraums, für den das erfasste Einkommen erzielt worden ist, die Art des Einkommens, die Beitragsgruppen, falls vorhanden, und die laufende Nummer der Meldung sowie
3. Name und Anschrift des Arbeitgebers sowie die Betriebsnummer des Beschäftigungsbetriebs.

Sonstige personenbezogene Daten darf die Meldung nicht enthalten. Zusätzlich zur monatlichen Meldung nach Satz 1 hat der Arbeitgeber der Zentralen Speicherstelle die Meldung zu den erfassten Nachweisen zu dem Zeitpunkt und mit dem Inhalt zu übermitteln, den das für den jeweiligen Nachweis geltende Gesetz bestimmt.

2.10 Gesundheitswesen

2.10.1 Datenabgleich bei Kinderuntersuchungen

Der Gesetzgeber hat den von mir in meinem Achten Tätigkeitsbericht (Punkt 2.8.4) kritisierten Datenabgleich von Meldungen über die Teilnahme an Kinderuntersuchungen (§ 26 Sozialgesetzbuch Fünftes Buch - SGB V) mit den Daten des Einwohnermelderegisters ab 23. Oktober 2008 bis zum 30. September 2013 (§ 15b Gesetz über den Öffentlichen Gesundheitsdienst - ÖGDG M-V) in Kraft gesetzt. Meine Kritik richtete sich im Wesentlichen dagegen, dass eine freiwillige medizinische Untersuchung nunmehr staatlich überwacht wird und dass, um die an der Untersuchung nicht-teilnehmenden Kinder zu finden, die Daten der Teilnehmer mit dem Melderegister abgeglichen werden. Ungeachtet meiner Kritik an der gesetzlichen Regelung in § 15b ÖGDG M-V habe ich das Landesamt für Gesundheit und Soziales (LAGuS) bei der Umsetzung der Rechtsvorschrift beraten.

Nach § 15b ÖGDG M-V ist ein Arzt verpflichtet, die Teilnahme an einer Untersuchung dem LAGuS zu melden. Die Ärzte sollen dafür die Daten der Krankenversichertenkarten der Kinder nutzen. Allerdings sind diese Karten für die ersten Stufen der Kinderuntersuchungen (U2 und U3) in den Krankenhäusern noch nicht verfügbar. Ein Arzt aus einer Geburtsklinik hat deswegen empfohlen, für die Teilnahmemeldung an der zweiten und gegebenenfalls dritten Kinderuntersuchung (U2 und U3) die Daten des freiwilligen Neugeborenenscreenings auf Stoffwechselkrankheiten zu nutzen (siehe Siebter Tätigkeitsbericht, Punkt IX 1). Andere Möglichkeiten, beispielsweise ein entsprechender Datenexport aus dem jeweiligen Krankenhausinformationssystem (KIS), sind aus Zeitmangel vom LAGuS und den Krankenhausvertretern nicht weiter verfolgt worden. Die Verwaltung hat sich schnell darauf verständigt, die Screening-Identitätsnummer (Screening-ID) für diesen Zweck zu nutzen. Die Screening-ID ist allerdings nicht in dem Datenkatalog des § 15b ÖGDG M-V enthalten. Dadurch ist nun die paradoxe Situation entstanden, dass die Ärzte des Krankenhauses, um ihrer Meldepflicht nachkommen zu können, die Eltern um eine Einwilligung zur Übermittlung der Screening-ID an das LAGuS ersuchen müssen. Diese Einwilligung habe ich gefordert, weil eine Rechtsgrundlage zur Übermittlung der Screening-ID nicht besteht. Erteilen die Eltern diese spezielle Einwilligung neben der Einwilligung für das freiwillige Screening auf Stoffwechselkrankheiten, wird diese Nummer an die Medizinische Fakultät der Universität Greifswald übermittelt. Von dort werden dann die erforderlichen personenbezogenen Daten an das LAGuS weitergeleitet. Die Eltern werden über das Verfahren aufgeklärt und darauf hingewiesen, dass sie die Einwilligung verweigern können, ohne dass ihnen daraus Nachteile entstehen. Wird die Einwilligung verweigert, haben die Ärzte ein Meldeformular mit den personenbezogenen Daten auszufüllen und per Post an das LAGuS zu senden.

Ich hoffe, dass nach dem Auslaufen dieser gesetzlichen Regelung am 30. September 2013 eine Lösung gefunden wird, die es zumindest ermöglicht, zielgerichtet die nicht-teilnehmenden Kinder zu ermitteln. Dies könnte beispielsweise anhand des Datenbestandes der Krankenkassen realisiert werden, denn dort werden die Abrechnungsdaten erfasst, aus denen abgeleitet werden kann, welches Kind die entsprechende Stufe der Untersuchung versäumt hat.

Am 28. Mai 2009 hat übrigens der Verfassungsgerichtshof Rheinland-Pfalz (VGH B 45/08) zu einer mit der oben dargestellten vergleichbaren Regelung geurteilt, dass der rheinland-pfälzische Landesgesetzgeber befugt ist, durch ein behördliches Einladungs- und Erinnerungsverfahren Eltern zur Wahrnehmung der Früherkennungsuntersuchungen anzuhalten, um so Gefährdungen der Kindergesundheit entgegenzuwirken. Er hat in dem Urteil unter anderem ausgeführt, dass die Einschränkungen des Grundrechts der Eltern auf informationelle Selbstbestimmung bei Beachtung der verfahrensmäßigen Sicherungen und vorbehaltlich der Ergebnisse einer im Jahr 2010 vorgesehenen Evaluation gerechtfertigt sind.

2.10.2 Wer hat Zugriff auf Patientendaten in einem Krankenhaus?

Im September 2008 hat sich ein Petent bei mir beschwert über die nach seiner Auffassung zu weitgehenden Zugriffsrechte von Krankenhausmitarbeitern auf Patientendaten. Er schilderte, dass das ärztliche Personal sowie das Pflegepersonal jederzeit unbeschränkt auf Patientendaten zugreifen könnten. Auch wenn die Behandlung eines Patienten abgeschlossen sei, bestehe weiterhin die Möglichkeit, auf diese Daten zuzugreifen. Es sei nicht sichergestellt, dass Ärzte, die einen Patienten nicht behandelt haben, auf dessen Daten auch nicht zugreifen könnten.

Der Ärztliche Direktor hat auf meine Bitte um Stellungnahme mitgeteilt, dass alle Mitarbeiter bei ihrer Einstellung über die Bestimmungen zum Datenschutz aufgeklärt und zur Wahrung des Datengeheimnisses verpflichtet werden. Im Krankenhausinformationssystem seien Rollenkonzepte umgesetzt worden, die einen Zugriff auf Patientendaten des jeweiligen klinischen Fachbereiches gestatten. So gäbe es beispielsweise für einen Arzt einer bestimmten Fachrichtung die Rollen

- Laborviewer (zur Einsicht in Laborbefunde sowie zum Arbeitsstand eines Laborauftrages),
- Arzt im Fachbereich,
- Notfall,
- Medizinischer Dienst der Krankenversicherung (MDK, kann Patientendaten zur Prüfung anfordern) sowie
- Abrechnung der Fallpauschalen (Diagnosis Related Groups - DRG).

Für Krankenschwestern und Krankenpfleger bestünden die Rollen Laborviewer und Pflegedokumentation im Fachbereich. Darüber hinaus seien Rollen für Verwaltungsmitarbeiter und für die Operationspflege eingerichtet. Verwaltungsmitarbeiter stellen den Krankenkassen und gegebenenfalls den Patienten Rechnungen über die Behandlung im Krankenhaus. In der Operationspflege gäbe es während dieser Behandlung fachbereichsübergreifende Zugriffsrechte, weil diese Leistung bereichsübergreifend erbracht wird. Notfallzugriffe von Ärzten würden außerdem genau protokolliert, um nachvollziehen zu können, wer wann auf welche Patientendaten zugegriffen hat.

Den Petenten habe ich entsprechend informiert.

Dass die Gewährung und die Begrenzung von Zugriffsrechten auf Patientendaten in vielen Krankenhäusern nach wie vor eine datenschutzrechtliche Aufgabe ist, zeigen die Entscheidung des Europäischen Gerichtshofes für Menschenrechte (EGMR) in dem Fall I v. Finland (Case I v. Finland) vom 17. Juli 2008 (http://echr.coe.int/echr/en/hudoc) und die „Normativen Eckpunkte für Zugriffe auf elektronische Patientendaten im Krankenhaus“ meines hamburgischen Kollegen (www.hamburg.de/datenschutz/).

Der EGMR hatte einer Krankenschwester mit der Diagnose HIV-positiv, die sich in dem Krankenhaus behandeln ließ, in dem sie tätig war, eine Entschädigung zugesprochen, weil das Krankenhaus nicht nachweisen konnte, welche Mitarbeiter auf ihre Daten zugegriffen und sie missbräuchlich zur Kenntnis genommen hatten. Das Krankenhaus hatte die Datenzugriffe nicht protokolliert. Die Nachricht über ihre Erkrankung hatte sich unter den Mitarbeitern verbreitet, wodurch ihr befristeter Arbeitsvertrag nicht verlängert wurde.

Die Eckpunkte zum Zugriff auf Patientendaten stehen nun zur Diskussion. Ich werde mich auch über den Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder dafür einsetzen, dass diese Fragen mit den Entwicklern und Nutzern von Krankenhausinformationssystemen beraten und datenschutzrechtlich akzeptable Ergebnisse erzielt werden.

2.10.3 Rahmenkonzept für Datenschutz und IT-Sicherheit des Instituts für Community Medicine an der Universität Greifswald

Das Institut für Community Medicine (ICM) an der Universität Greifswald führt umfangreiche Studien durch, in denen es um die Analyse, Verbesserung und Evaluation der medizinischen Versorgung der Bevölkerung geht. Es verarbeitet dazu medizinische Daten in großem Umfang. Bekannte Projekte des ICM sind zum Beispiel die Regionale Basisstudie Vorpommern und AGnES (siehe Zweiter Tätigkeitsbericht, Punkt 2.14.5 und Achter Tätigkeitsbericht, Punkt 2.9.8). Damit die betroffenen Bürgerinnen und Bürger den Forschungsvorhaben offen gegenüberstehen, ist ein hohes Datenschutzniveau unabdingbar. Im Jahr 2008 entschloss sich das ICM daher, IT-Sicherheit und Datenschutz bei all seinen Projekten auf eine solide Basis zu stellen und ein Rahmenkonzept für Datenschutz und IT-Sicherheit zu schaffen. Ich habe das ICM hierbei beraten.

Dabei konnten insbesondere folgende Verbesserungen erzielt werden:

Die Daten der Forschungsvorhaben werden wenn möglich pseudonymisiert verarbeitet, sodass die Forscherinnen und Forscher Probanden nur dann identifizieren können, wenn dies unerlässlich ist. Die identifizierenden Daten und die Pseudonyme werden in einer Treuhandstelle im ICM verarbeitet. Diese Treuhandstelle ist jetzt so gestaltet, dass der zuständige Mitarbeiter in Ausübung seiner Funktion weisungsfrei ist und dass außer ihm niemand mehr Zugriff auf die Daten hat, auch der Leiter des ICM nicht.

Die für alle Bereiche und Projekte des ICM gültigen Sicherheitsmaßnahmen werden nun mit der bewährten Methode des BSI-Standards 100-2 aus den Grundschutzkatalogen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ausgewählt. Die Entsorgung von Biomaterialien wird in einem besonderen Konzept geregelt.

Defekte und ausgesonderte PC, Drucker und andere Geräte enthalten oft Festplatten und andere Datenspeicher, auf denen sensible personenbezogene Daten gespeichert sein können. Im Konzept ist nun vermerkt, dass diese Bauteile zuverlässig gelöscht oder zerstört werden müssen. Auch zur Entsorgung von CD-ROMs und DVDs sind bessere vertragliche Regelungen mit den beauftragten Unternehmen vorgesehen.

Für die einzelnen Projekte des ICM werden darüber hinaus spezielle Datenschutz- und IT-Sicherheitskonzepte erstellt, um zu dokumentieren, welche über das Rahmenkonzept hinausgehenden Anforderungen bestehen und welche Maßnahmen hierzu ergriffen werden. Insgesamt konnte ich feststellen, dass das Rahmenkonzept des ICM derzeit dem in § 21 Abs. 1 DSG M-V geforderten Stand der Technik entspricht.

2.10.4 Das OnkoNET Wismar

Ein Forschungsteam der Hochschule Wismar hat mich darüber informiert, dass es gemeinsam mit Ärzten der Region und einem Krankenhaus eine telemedizinische Anwendung - das OnkoNET Wismar - gründen und nach der Entwicklung in Betrieb nehmen will. Den teilnehmenden Ärzten und Gesundheitseinrichtungen soll damit die Möglichkeit geboten werden, über das Internet zu kommunizieren und Daten von an Krebs erkrankten Patienten zu dokumentieren und zu nutzen. Die Anwendung soll dazu beitragen, die Versorgungsqualität zu verbessern. Dieses Ziel soll in erster Linie dadurch erreicht werden, dass die an der Behandlung eines Patienten beteiligten Ärzte ihre Maßnahmen abstimmen und Erfahrungen austauschen. Rechtliche Grundlage für die Teilnahme sowohl der Ärzte und der medizinischen Einrichtungen als auchder Patienten sollten Freiwilligkeit und Einwilligung sein. Das Forschungsteam hat mich um datenschutzrechtliche Beratung gebeten.

Es war geplant, die Patientendaten pseudonymisiert in einer Datenbank auf einem Server bei einem Dienstleister zu speichern. Durch Artikel 30 des Gesetzes zur Modernisierung der Gesetzlichen Krankenversicherung aus dem Jahr 2003 ist der Beschlagnahmeschutz auf medizinische Daten bei einem Dienstleister erweitert worden, § 97 Abs. 2 Satz 2 Strafprozessordnung (StPO). Als wesentliches Merkmal zum Schutz vor unberechtigten Datenzugriffen sollten das aus dem Homebanking bekannte PIN/TAN-Verfahren (Persönliche Identifikationsnummer und Transaktionsnummer) und sichere Übertragungskanäle eingesetzt werden.

Ich habe mehrere datenschutzrechtliche Beratungen mit den Entwicklern des OnkoNET Wismar durchgeführt. So habe ich empfohlen, bereits bei der Entwicklung des Telemedizinnetzes den Einsatz der elektronischen Gesundheitskarte und des Heilberufsausweises vorzusehen, weil sich beides zu dieser Zeit in der Entwicklung befand und damit nach meiner Auffassung ein wesentlicher telemedizinischer Standard für die Übermittlung personenbezogener medizinischer Daten geschaffen wird.

Des Weiteren waren aus datenschutzrechtlicher Sicht folgende Hinweise bei der Projektentwicklung zu berücksichtigen:

- Aufgrund der freiwilligen Teilnahme der Patienten muss die Möglichkeit bestehen, dass bei einem schriftlichen Widerruf die Daten unverzüglich gelöscht werden.
- Für den Fall, dass ein Arzt an dem OnkoNET nicht mehr teilnimmt oder ein Patient wünscht, von einem anderen Arzt betreut zu werden, sollten die Patienten die Möglichkeit haben, sich für einen anderen Arzt im Netzwerk zu entscheiden, der dann die entsprechenden Zugriffsrechte auf die Daten erhält.
- Die Patienten sollten entscheiden können, welcher Arzt auf ihre Daten zugreifen darf.
- Die Ärzte sollten umfassend über die Arbeitsweise des Systems sowie über den Umfang, den Inhalt und die Auswertungsmöglichkeiten der protokollierten Daten informiert werden, damit sie wiederum die Patienten aufklären können. Zu diesem Zweck wird ein Handbuch erstellt.
- Die Nutzer sollten umfassend über notwendige Schutzmaßnahmen ihrer Praxisräume informiert und bei deren Realisierung unterstützt werden.
- Datensicherungsmaßnahmen sollten festgelegt und auf ihre Wirksamkeit regelmäßig überprüft werden. Dazu ist ein Datenschutz- und Datensicherheitskonzept zu erstellen.

Meine datenschutzrechtlichen Empfehlungen sind umgesetzt worden. Das OnkoNET Wismar bildet die Grundlage für eine palliativonkologische Versorgung nach § 140a Sozialgesetzbuch Fünftes Buch (SGB V).

2.10.5 Auditierung einer Diabetes-Simulationssoftware

Der Hersteller einer Diabetes-Simulationssoftware hat sich 2009 an mich gewandt. Er suchte nach einer Möglichkeit, die Datenschutzkonformität seines Produktes zertifizieren zu lassen.

Das Landesdatenschutzgesetz von Mecklenburg-Vorpommern (DSG M-V) sieht tatsächlich eine solche Zertifizierungsmöglichkeit vor. In § 5 Abs. 2 Satz 1 DSG M-V heißt es: „Informationstechnische Produkte, deren Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit in einem Prüfverfahren festgestellt wurde, sollen vorrangig eingesetzt werden.“ Damit sind prinzipiell die Voraussetzungen gegeben, um ein Datenschutzgütesiegel für entsprechend geprüfte Produkte zu vergeben. Allerdings lautet der Satz 2 dieser Vorschrift: „Die Landesregierung regelt durch Rechtsverordnung Inhalt, Ausgestaltung und die Berechtigung zur Durchführung des Verfahrens.“

Die Landesregierung, insbesondere der Innenminister unseres Landes, sieht jedoch keinen Bedarf für ein solches Gütesiegel. Entgegen meinen Erfahrungen - bei mir gehen regelmäßig Anfragen zu Zertifizierungsmöglichkeiten ein - ist der Innenminister der Auffassung, dass ein Auditverfahren den Unternehmen des Landes mehr schaden als nützen würde, und hat deshalb noch keine Rechtsverordnung erlassen. Und dass, obwohl ich bereits vor Jahren einen eigenen Entwurf der Verordnung und der Kriterienkataloge sowohl für die Zertifizierung von Produkten als auch für die Akkreditierung von Gutachtern vorgelegt habe (siehe Sechster Tätigkeitsbericht, Punkt 2.18.1, Siebter Tätigkeitsbericht, Punkt A.I.4.1.3 und Achter Tätigkeitsbericht, Punkt 2.15.1).

Unabhängig von den Aktivitäten des Landesgesetzgebers hatte ich gehofft, dass auf Bundesebene eine Auditierungsmöglichkeit geschaffen wird. Das BDSG sieht diese Möglichkeit in § 9a vor, ebenso § 78c Zehntes Buch Sozialgesetzbuch (SGB X). Jedoch waren auch die Bemühungen der Bundesregierung bisher wenig Erfolg versprechend, sodass mit einem Audit auf Bundesebene in absehbarer Zeit ebenfalls kaum zu rechnen ist (siehe Punkt 3.3).

So musste ich den Hersteller der Diabetes-Simulationssoftware an das Unabhängige Landeszentrum für Datenschutz in Kiel (ULD) verweisen. In Schleswig-Holstein vergibt man bereits seit mehreren Jahren Datenschutz-Gütesiegel. Es wäre sicher ein Gewinn für das Gesundheitsland Mecklenburg-Vorpommern gewesen, wenn ich dem Unternehmen ein vergleichbares Verfahren hätte anbieten können.

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

2.11 Personalwesen

2.11.1 Beamtenrechtsneuordnungsgesetz

Die Landesregierung übersandte mir im Juli 2008 den Entwurf eines Gesetzes zur Neuordnung des Beamtenrechts für das Land Mecklenburg-Vorpommern (Beamtenrechtsneuordnungsgesetz - BRNG M-V) zur datenschutzrechtlichen Stellungnahme. Die Neuordnung des Beamtenrechts ist nach Aussage der Landesregierung notwendig, weil durch die Föderalismusreform das Beamtenrecht mit Ausnahme des Laufbahn-, Besoldungs- und Versorgungsrechts in die konkurrierende Gesetzgebung überführt worden ist. Die rechtlichen Kernbereiche werden künftig im bundeseinheitlichen Beamtenstatusgesetz (BeamtStG) geregelt.

Die datenschutzrechtlich relevanten Regelungen über die Personalakten und die Verarbeitung von Personalaktendaten sind im BRNG M-V gegenüber dem Landesbeamtengesetz nicht wesentlich geändert worden. Es war allerdings eine neue Bestimmung enthalten, die es gestatten sollte, dass die Personalakte in Teilen oder vollständig elektronisch geführt werden kann.

Bei der elektronischen Verarbeitung personenbezogener Daten ist zu beachten, dass die Daten jederzeit ihrem Ursprung zugeordnet werden können (Authentizität). Außerdem muss diese Verarbeitung protokolliert werden, um feststellen zu können, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit). Authentizität und Revisionsfähigkeit müssen, wenn eine Personalakte ausschließlich elektronisch geführt wird, durch zusätzliche Maßnahmen sichergestellt werden. Deshalb habe ich hierzu folgende Ergänzung empfohlen, die in den Gesetzentwurf aufgenommen worden ist:

„Wird bei einer vollständig elektronisch geführten Personalakte auf die Papierform verzichtet, ist jedes gespeicherte elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 26. Februar 2007 (BGBl. I S. 179), zu versehen. Die Signierung mit einem Pseudonym, das die Identifizierung der Person des Signaturschlüsselinhabers nicht ermöglicht, ist nicht zulässig."

Die sonst nach dem Signaturgesetz allgemein eröffnete Möglichkeit, ein elektronisches Dokument mit einem Pseudonym zu unterzeichnen, ist im Dienstverkehr nicht sinnvoll. Denn derjenige Mitarbeiter, der ein solches Dokument signiert, muss sowohl für den Betroffenen als auch für Personalsachbearbeiter und Dienstvorgesetzte erkennbar sein. Deshalb habe ich empfohlen, dass die Signierung mit einem Pseudonym nicht zulässig sein soll.

Meine Empfehlung hat die Landesregierung in den Gesetzentwurf eingefügt, der dem Landtag zur Abstimmung vorgelegt worden ist.

Von einer Interessenvertretung von Arbeitnehmern und Beamten bin ich ebenfalls um eine datenschutzrechtliche Stellungnahme zu dem Entwurf des BRNG M-V gebeten worden. Die Interessenvertretung hatte sich unter anderem zu § 44 des Gesetzentwurfs geäußert, der ärztliche Untersuchungen regelt, insbesondere im Zusammenhang mit der Feststellung der Dienstfähigkeit. Ärztliche Untersuchungen haben immer auch einen mittelbaren datenschutzrechtlichen Bezug, denn es werden in diesem Zusammenhang medizinische Daten einer Person verarbeitet. Ich habe der Interessenvertretung empfohlen, sich dafür einzusetzen, dass bei ärztlichen Untersuchungen zum Zweck der Feststellung der Dienstfähigkeit einer Beamtin oder eines Beamten die Möglichkeit geboten wird, aus mehreren Gutachtern eine Auswahl zu treffen. Dieses Gutachterwahlrecht ist beispielsweise in der Gesetzlichen Unfallversicherung vorgesehen - § 200 Abs. 2 Satz 1 Sozialgesetzbuch Siebtes Buch (SGB VII). Eine Begutachtung der Dienstfähigkeit ist für jede Beamtin oder jeden Beamten eine einschneidende Maßnahme, bei der die betroffene Person dieses Wahlrecht haben sollte. In dem oben genannten Gesetzentwurf der Landesregierung ist das Gutachterwahlrecht bei ärztlichen Untersuchungen noch nicht enthalten. Dies ist jedoch auch keine Forderung, die sich originär aus datenschutzrechtlichen Grundsätzen ergibt. Vor diesem Hintergrund habe ich die Aufnahme einer entsprechenden Regelung von der Landesregierung nicht verlangt.

2.11.2 Personalübergang im Zuge der Landkreisneuordnung

Die Landesregierung plant eine Neuordnung der Landkreise auf der Grundlage eines entsprechenden Gesetzes. Mit dieser Neuordnung ist verbunden, dass Personal von aufgelösten Landkreisen und jetzt noch kreisfreien, künftig aber eingekreisten Städten an die neuen Landkreise übergeht.

Mit den Vorarbeiten für diesen Personalübergang war das zentrale Personalmanagement (siehe Siebter Tätigkeitsbericht, Punkt IV 3) beim Finanzministerium Mecklenburg-Vorpommern betraut worden, das mich bereits vor dem Gesetzgebungsverfahren um eine datenschutzrechtliche Beratung gebeten hat. Es war geplant, nicht nur Personalstellen den neuen Landkreisen zu übertragen, sondern es sollte auch das Personal auf der Basis von Überleitungsverträgen auf die neuen Landkreise übergehen.

Um neue Verträge vorbereiten zu können, sollten bestimmte Personalaktendaten an die neuen Landkreise als künftige Dienstherren übermittelt werden. Nach dem Landesbeamtengesetz wäre eine solche Datenübermittlung nur zulässig, wenn die Beschäftigten eingewilligt hätten. Da eine Einwilligung im Einzelfall nicht zweifelsfrei freiwillig gewesen wäre, die Daten aber zur Erfüllung der Aufgabe erforderlich sind, habe ich vorgeschlagen, eine Rechtsgrundlage für die Übermittlung zu schaffen. Es sollte für alle Beteiligten klar zu erkennen sein, welche Daten an wen übermittelt werden. Mein Vorschlag wurde aufgegriffen und in den Gesetzentwurf der Landesregierung aufgenommen, der vom Landtag Mecklenburg-Vorpommern noch beraten wird. Nach der Vorschrift des Entwurfes sollen nunmehr folgende Daten ohne Einwilligung eines Beamten an die jeweiligen Verhandlungspartner übermittelt werden dürfen: Name, Vorname, Geburtsdatum, Familienstand, Anzahl der Kinder unter 18 Jahren im Haushalt, Wohnort, Dienstort, Bildungsabschluss und sonstige Qualifikationen, Laufbahn- und Besoldungsgruppe, bisherige berufliche Tätigkeiten, Umfang der regelmäßigen wöchentlichen Arbeitszeit, Vorliegen einer Schwerbehinderung oder einer gleichgestellten Behinderung sowie Vorliegen einer Altersteilzeitvereinbarung. Diese Regelung soll für Arbeitnehmer und Auszubildende entsprechend gelten.

Die vorgesehene gesetzliche Regelung ist nach meiner Auffassung für die Personalüberleitung erforderlich und verhältnismäßig.

2.11.3 Personenbezogene Daten von Mitarbeitern im Internet?

Immer wieder werde ich gefragt, ob und welche personenbezogenen Daten von Mitarbeitern im Internet veröffentlicht werden dürfen und welche Rechtsgrundlagen in diesem Zusammenhang zu beachten sind.

Eine Veröffentlichung personenbezogener Daten von Mitarbeitern im Internet ist datenschutzrechtlich eine Übermittlung an Stellen und Personen außerhalb des öffentlichen Bereiches. Für Mitarbeiterdaten ist hier die Rechtsvorschrift des § 35 Abs. 2 DSG M-V maßgeblich. Danach ist es zulässig, Mitarbeiterdaten an Personen oder Stellen außerhalb des öffentlichen Bereiches zu übermitteln, wenn

1. die betroffene Person eingewilligt hat,
2. eine Rechtsvorschrift dies vorsieht,
3. Art oder Zielsetzung der einem Beschäftigten übertragenen Aufgabe oder der Dienstverkehr es erfordern oder
4. der Empfänger ein rechtliches Interesse glaubhaft macht und der Betroffene vor der Übermittlung unterrichtet wurde und dieser nicht widersprochen hat.

Um die Vielfältigkeit der in diesem Zusammenhang bei mir eingegangenen Anfragen zu zeigen, hier nun zwei Beispiele:

Im Falle einer Hochschule war zu prüfen, ob es zulässig ist, die Stundenpläne und dazu personenbezogene Daten der Lehrenden im Internet zu veröffentlichen. Zu klären war, ob ohne Einwilligung der Betroffenen zum Beispiel eine Übermittlung/Veröffentlichung im Internet nach der oben genannten Nummer 3 in Betracht kommen würde. Nach Auskunft der Hochschule waren diese Voraussetzungen erfüllt. Mit einer solchen Veröffentlichung wolle man Fern- und Gaststudenten sowie Studieninteressierte besser und schneller informieren können, zum Beispiel über (zusätzliche) Lehrangebote, über Stundenausfälle oder Stundenverlegungen bzw. Vertretungen.

Meine Empfehlung, solche Stundenpläne nur in einem Intranet oder mit Zugriffsbeschränkungen im Internet zu veröffentlichen, wurde mit dem Hinweis abgelehnt, dass durch eine Veröffentlichung der Stundenpläne im Intranet nicht sichergestellt werden könne, dass Fern- und Gaststudenten sowie Studieninteressierte auf die für sie relevanten Informationen zugreifen können. Außerdem sei durch die namentliche Nennung der Lehrenden im Stundenplan kein Rückschluss auf die Arbeitsverteilung der betroffenen Personen möglich. Dies wäre nur dann gegeben, wenn genaue Kenntnisse sämtlicher Lehr- und Forschungsaktivitäten der Einzelperson unter besonderer Berücksichtigung individueller Umstände wie Forschungsfreisemester, Tätigkeiten in den Selbstverwaltungskörperschaften oder ähnliches vorhanden wären.

Aus meiner Sicht war diese Argumentation schlüssig, sodass die Veröffentlichung nicht zu beanstanden war. Dennoch sollte stets geprüft werden, ob Angaben so veröffentlicht werden können, dass nur die Personen darauf zugreifen können, für die diese Kenntnisse notwendig sind. Bei der Veröffentlichung von Stunden- und Vertretungsplänen von Lehreinrichtungen im Internet sollten daher beispielsweise geschlossene Benutzergruppen eingerichtet werden.

In einem anderen Fall haben Mitarbeiter einer Stadtverwaltung Bedenken an mich herangetragen gegen eine geplante Veröffentlichung von Mitarbeiterdaten im Internet. Zu diesem Zweck sollten die Daten (Name, Vorname, Dienstbezeichnung, Stelle, konkrete Aufgabe, Telefonnummer und E-Mail-Adresse) aller Beschäftigten, die in irgendeiner Weise Bürgerkontakt haben, ins Internet gestellt werden.

Als Handlungsempfehlung für die Stadtverwaltung habe ich die „Orientierungshilfe zur Präsentation öffentlicher Stellen im Internet“ empfohlen. Danach können Personen einer öffentlichen Stelle, die Außenkontakte haben, also beispielsweise Schreiben unterzeichnen, Kontrollen oder Prüfungen durchführen und dergleichen, mit ihren Kontaktdaten und Aufgabenbezeichnungen auf der Internetseite der öffentlichen Stelle veröffentlicht werden. Die Orientierungshilfe ist auf meiner Internetseite unter www.datenschutz-mv.de zu finden.

2.11.4 Mitarbeiterüberwachung in einer Stadtverwaltung

Ein Abgeordneter einer Stadtvertretung schilderte mir, dass der Bürgermeister Mitarbeitern der Stadtverwaltung vorwerfe, sie hätten ihre Verschwiegenheitspflicht verletzt. Zur Feststellung des „Informationslecks“ habe er die Verbindungsdaten der in einem definierten Zeitraum geführten dienstlichen Telefonate nach bestimmten Zielrufnummern durchsuchen lassen. Dabei soll insbesondere ausgeforscht worden sein, von welchen Apparaten der Stadtverwaltung bestimmte Abgeordnete der Stadtvertretung und Journalisten angewählt worden sind.

Hintergrund dieser Maßnahme, so teilte der Abgeordnete mit, seien Berichte in der regionalen Presse über die Einführung einer leistungsorientierten Vergütung für die Mitarbeiter der Stadtverwaltung gewesen sowie die dagegen gerichtete Kritik. Einem Pressebericht war mit Hinweis auf einen nicht namentlich genannten Mitarbeiter zu entnehmen, dass Leistungsentgelte willkürlich und planlos gezahlt worden seien.

In meinem Schreiben an den Bürgermeister mit der Bitte, zu der Angelegenheit Stellung zu nehmen, habe ich bereits deutlich gemacht, dass eine öffentliche Kritik über die Praxis der Leistungsvergütung aus meiner Sicht keine Verletzung der Verschwiegenheitspflicht darstelle. Die Einführung einer Leistungsvergütung sei kein Aspekt, der eine besondere Geheimhaltung erfordere, sofern damit keine personenbezogenen Daten offenbart werden. Hinsichtlich der Kritik über die Leistungsvergütung habe die Verwaltung im Übrigen die Möglichkeit, ihre Sicht der Dinge der Öffentlichkeit darzulegen.

Der Bürgermeister ging in seiner Stellungnahme nicht darauf ein, in welcher rechtlich relevanten Weise hier gegen die Verschwiegenheitspflicht verstoßen worden sein soll. Er brachte jedoch einen anderen Gesichtspunkt in die Diskussion ein und legte dar, ein Mitarbeiter habe auf Kosten der Stadt ein bzw. mehrere Telefongespräche mit einem Abgeordneten der Stadtvertretung geführt. Dies habe die Auswertung der Telefonlisten und die daran anschließende Befragung der Mitarbeiter ergeben. Der betroffene Mitarbeiter habe eine außerordentliche fristlose Kündigung erhalten.

Da der Bürgermeister auch nach längerem Schriftverkehr und einem Gespräch in meiner Dienststelle nicht zur Einsicht kam, dass seine Vorgehensweise unverhältnismäßig und unzulässig gewesen war, habe ich eine Beanstandung ausgesprochen. Darin habe ich ausgeführt, dass die Voraussetzungen zur Nutzung der Telefonverbindungsdaten für einen anderen Zweck hier nicht vorlagen (§ 10 Abs. 3 DSG M-V). Nach weiterem Schriftwechsel sowie einer Kontrolle der Verarbeitung der Telefonverbindungsdaten hat der Bürgermeister mir schließlich mündlich zugesichert, künftig nicht mehr in der beanstandeten Art und Weise vorzugehen.

Als Fazit bleibt festzuhalten: Auch Telefonverbindungsdaten unterliegen wie alle anderen personenbezogenen Daten der Zweckbindung. Diese Zweckbindung kann nur unter engen Voraussetzungen aufgehoben werden. Diese Voraussetzungen lagen hier nicht vor. Die außerordentliche fristlose Kündigung des Mitarbeiters aus vorstehenden Gründen musste nach Prozessen vor dem Arbeitsgericht und dem Landesarbeitsgericht zurückgenommen werden.

2.11.5 Kontrolle im Ministerium für Bildung, Wissenschaft und Kultur

Im Berichtszeitraum hat sich der beim Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern eingerichtete Lehrerhauptpersonalrat an mich gewandt. Er hat mich gebeten zu prüfen, ob die ihm zur Verfügung gestellte Informations- und Kommunikationstechnik so eingerichtet ist, dass er die ihm anvertrauten Angelegenheiten so vertraulich bearbeiten kann, wie dies im Personalvertretungsgesetz des Landes Mecklenburg-Vorpommern vorgesehen ist. Ich habe hierzu im Bildungsministerium einen Kontroll- und Informationsbesuch durchgeführt und bin dabei unter anderem zu folgenden Ergebnissen gekommen:

Das Ministerium für Bildung, Wissenschaft und Kultur nimmt am Verfahren IP-Telefonie (siehe auch Punkt 2.14.1) teil. Es ist dabei gegenüber dem Innenministerium als Auftraggeber gemäß § 4 DSG M-V anzusehen. Nach dieser Vorschrift muss es einen Vertrag mit dem Innenministerium schließen. Darüber hinaus müssen eine Verfahrensbeschreibung (§ 18), ein Sicherheitskonzept (§ 22 Abs. 5) und eine Freigabeerklärung durch den Behördenleiter (§ 19 Abs. 1) vorliegen. Alle diese Dokumente lagen nicht vor, da sich das Bildungsministerium für unzuständig hielt.

Bei der IP-Telefonie werden - wie auch bei herkömmlichen Telefonanlagen - Verkehrsdaten gehender Gespräche erfasst. Bestimmte Personen wie behördliche Datenschutzbeauftragte und freigestellte Mitglieder von Personalvertretungen müssen jedoch von der Speicherung der Zielrufnummern ausgenommen werden. So regelt es die Dienstvereinbarung des Innenministeriums vom 16. April 2007 zur IP-Telefonie, welche auch im Bildungsministerium gilt. Dennoch konnte das Bildungsministerium den Mitgliedern des Lehrerhauptpersonalrates nicht mitteilen, ob diese Vereinbarung umgesetzt war. Die Funktionsweise des entsprechenden technischen Verfahrens hätte das Bildungsministerium aus den oben beschriebenen Unterlagen entnehmen können. Um festzustellen, ob eine bestimmte Rufnummer von der Rufnummernerfassung ausgeschlossen ist, hätte es nur eines kurzen Blickes in den Elektronischen Geschäftsverteilungsplan (EGVP) bedurft. An diesem Verbundverfahren nimmt das Bildungsministerium ebenfalls teil. Es dient der Pflege von Stammdaten der Beschäftigten und liefert unter anderem die Bestandsdaten für die IP-Telefonie. Im EGVP wird für jeden Beschäftigten gespeichert, ob er der Rufnummernerfassung unterliegt.

Das Ministerium für Bildung, Wissenschaft und Kultur erlaubt seinen Beschäftigten, Internetdienste am Arbeitsplatz auch privat zu nutzen. Dies gilt auch für die elektronische Post. Protokolliert wird hierbei erfreulich sparsam: Der Proxy, der einen Teil der Internetkommunikation zwischenspeichert, um häufig gefragte Inhalte schneller ausliefern zu können, speichert keine IP-Adressen der anfordernden Rechner. Daten über die laufenden Zugriffe können nur an der Konsole des Proxys beobachtet werden. Dies dient ausschließlich der Klärung von Fehlern. Darüber hinaus speichert das Mail-System alle Versuche von Mail-Übertragungen für drei Wochen. Dies dient ebenfalls ausschließlich der Fehlersuche und dem Nachweis, ob eine bestimmte Sendung das Ministerium für Bildung, Wissenschaft und Kultur ordnungsgemäß verlassen hat. Trotz dieser sehr datensparsamen Betriebsweise waren datenschutzrechtliche Defizite festzustellen. Erstens gilt das Bildungsministerium gegenüber den Beschäftigten, die den Internetzugang privat nutzen, als Provider im Sinne des Telemediengesetzes. Ohne Einwilligung der Nutzer ist daher auch die beschriebene Protokollierung von Mails und die Beobachtungsmöglichkeit am Proxy unzulässig. Zweitens treffen die einschlägigen Dienstvereinbarungen und Dienstanweisungen für die dienstliche Nutzung des Internetzugangs Regelungen, die eine detailliertere Protokollierung zunächst möglich erscheinen lassen. Da aber weder der genaue Umfang der Protokollierung noch das Auswertungsverfahren festgelegt sind, sind die genannten Regelungen zu unbestimmt, um als ausreichende rechtliche Grundlage dienen zu können. Außerdem ist die Weisungslage für die Beschäftigten intransparent.

Ferner setzt das Ministerium für Bildung, Wissenschaft und Kultur moderne Druck- und Kopiertechnik ein. Sie ist grundsätzlich ebenfalls datenschutzfreundlich eingerichtet. Die Beschäftigten erzeugen einen Druckauftrag, gehen dann zu einem Drucker ihrer Wahl und starten dort die Ausführung ihres Auftrags mit einer PIN. Auf diese Weise können sie die Druckausgabe überwachen und verhindern, dass Unbefugte ihre Ausdrucke einsehen können. Jedoch hat es das Ministerium für Bildung, Wissenschaft und Kultur bisher versäumt, sich ausreichend um die ordnungsgemäße Reparatur und Rückgabe dieser Drucktechnik zu kümmern. Die Druck- und Kopieraufträge werden nämlich auch auf internen Festplatten dieser Geräte gespeichert. Nach Bearbeitung des Auftrags wird der Speicher nur freigegeben, aber nicht überschrieben. Mit entsprechenden Werkzeugen können diese Inhalte oft noch nach langer Zeit zugänglich gemacht werden. Damit verhalten sich die Drucker nicht anders als übliche PC-Betriebssysteme. Aus diesem Grund müssen Festplatten ausgesonderter und defekter Geräte ordnungsgemäß gelöscht oder zerstört werden. Das Ministerium für Bildung, Wissenschaft und Kultur hat jedoch bereits zugesagt, diesen Punkt künftig mit dem Leasinggeber und anderen Servicepartnern vertraglich zu regeln.

Die Stellungnahme des Ministeriums für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern zu meinem Bericht steht derzeit noch aus.

2.11.6 Personaldatenverarbeitung in der Landesverwaltung

Bereits am 27. Januar 2004 hatte das Kabinett beschlossen, das Elektronische Personal-, Organisations- und Stellenmanagementsystem EPOS 2.0 landesweit als zentrale Lösung einzuführen. Das vom Bundesverwaltungsamt entwickelte Produkt soll Personalsachbearbeiter bei der Stellenplanverwaltung, der Mittelkalkulation, der Materialverwaltung sowie der Darstellung von Organisationsstrukturen entlasten und unterstützen. Im E-Government-Masterplan der Landesregierung (siehe Sechster Tätigkeitsbericht Punkt 2.16.4) wird die Zentralisierung von Datenhaltung und Administration von EPOS als wichtiges ressortübergreifendes Projekt beschrieben. Im Frühjahr 2007 startete ein Pilotprojekt im Justizministerium, mit dem die Migration von der bisherigen dezentralen Lösung auf den zentralen Betrieb getestet werden sollte. Das Justizministerium arbeitet nach erfolgter Datenmigration aus der Vorgängerversion EPOS 1.5 und umfassenden Testphasen seit Juli 2008 mit EPOS 2.0 im Wirkbetrieb. Im Jahr 2009 wurde der gesamte Geschäftsbereich an EPOS 2.0 angeschlossen. Auch das Finanzministerium nutzt inzwischen die neue Version. Seit Mai 2009 läuft dort der Wirkbetrieb EPOS 2.0.

Von Beginn an bestand Einigkeit bei allen Beteiligten, dass die Umstellung auf eine zentrale Datenhaltung für alle am Projekt beteiligten Dienststellen völlig neue Anforderungen an den Datenschutz und die Datensicherheit mit sich bringen würde. Deshalb begannen frühzeitig die Planungen für ein zentrales Sicherheitskonzept. Da alle Sicherheitskonzepte der Landesverwaltung nach der Grundschutzmethodik des Bundesamtes für Sicherheit in der Informationstechnik erstellt werden, war der erste Schritt für das EPOS-Sicherheitskonzept eine detaillierte Schutzbedarfsanalyse. Im Ergebnis wurde in Bezug auf die Vertraulichkeit und die Integrität der verarbeiteten Personaldaten ein sehr hoher Schutzbedarf konstatiert, insbesondere vor dem Hintergrund, dass auch besonders schutzbedürftige Daten beispielsweise der Mitarbeiter der Verfassungsschutzabteilung des Innenministeriums verarbeitet werden sollten.

Für das gesamte Verfahren wurde ein Sicherheitskonzept erarbeitet. Durch eine ergänzende Sicherheitsanalyse wurden zudem Maßnahmen gesucht, die dem sehr hohen Schutzbedarf genügen würden. Sehr bald zeigte sich jedoch, dass mit finanziell vertretbarem Aufwand kein sehr hoher Schutzbedarf für das gesamte Verfahren zu realisieren sein würde. Daher wurde von den ursprünglichen Planungen Abstand genommen, die sehr sensiblen Daten der oben genannten besonders schutzbedürftigen Mitarbeiter im EPOS-Gesamtsystem zu speichern. Das Innenministerium plant nunmehr, für die Verwaltung besonders sensibler Personaldaten, etwa für den Bereich des Verfassungsschutzes, eine separate EPOS-Serverumgebung einzurichten. Angesichts der Menge und der Sensibilität der an zentraler Stelle gespeicherten Daten verblieb dennoch ein – gemäß den BSI-Bewertungskriterien - hoher Schutzbedarf. Im Ergebnis einer detaillierten Risikoanalyse entstand dann ein Sicherheitskonzept, dessen Umsetzung diesen Schutzbedarf in angemessener Weise abdecken würde.

Erwähnenswert ist die Tatsache, dass zusätzlich zum Sicherheitskonzept ein Katalog mit Sicherheitsmaßnahmen formuliert wurde, die von den am EPOS-Verfahren beteiligten Behörden vor Ort umzusetzen sind. Dort wird beispielsweise gefordert, ergänzend zum zentralen Konzept ein behördenspezifisches Sicherheitskonzept zu erstellen und das Verfahren formell gemäß § 19 Landesdatenschutzgesetz freizugeben. Zudem werden die Protokollierungsregeln detailliert beschrieben und Sicherheits-Vorgaben für die EPOS-Arbeitsplätze gemacht. Auch wird genau festgelegt, dass für Schulungs-, Wartungs- und Reparaturzwecke grundsätzlich keine Echtdaten verwendet werden dürfen. Unterstützt wird diese Forderung durch das Vorhalten von drei verschiedenen EPOS-Umgebungen:

Die zentrale Schulungsumgebung dient zur Ausbildung der Mitarbeiter und wird ausschließlich mit Testdaten betrieben. Daneben wurde ein zentrales Referenzsystem eingerichtet, in dem Softwarekomponenten und Software-Updates getestet sowie Softwarefehler analysiert werden. In dieser Umgebung können Echtdaten nur unter genau definierten Randbedingungen und nur nach Einzelfall bezogener Sondergenehmigung verwendet werden. Die dritte Umgebung ist die Produktionsumgebung mit Echtdaten. Die Nutzung dieses Datenbestandes für Fehleranalysen ist auf absolute Ausnahmefälle beschränkt und nur zulässig, wenn nachgewiesen wurde, dass weder im Schulungs- noch im Referenzsystem eine Fehleranalyse möglich war. Der Umgang mit Echtdaten genügt somit weitgehend den Vorgaben, die die Datenschutzbeauftragten von Bund und Ländern in der entsprechenden Orientierungshilfe „Datenschutz im Projekt- und Produktivbetrieb“ (siehe Punkt 2.14.8) empfohlen haben.

Gleichzeitig mit dem Sicherheitskonzept wurden weitere datenschutzrelevante Unterlagen erarbeitet, die Voraussetzung für den Start des Produktivbetriebes sind. So wurde eine Dienstvereinbarung über den zentralen Einsatz von EPOS 2.0 in der Landesverwaltung formuliert, die meine Empfehlungen etwa zu Fragen der Nutzung der gespeicherten Daten, der Speicherdauer und der Protokollierung auch lesender Zugriffe in vollem Umfang berücksichtigt. Der Produktivbetrieb von EPOS 2.0 wurde für das Justizministerium bereits Ende Dezember 2008 formell freigegeben und läuft dort zunächst als Pilotbetrieb für die gesamte Landesverwaltung. Zur Freigabe lagen die Verfahrensbeschreibung nach § 18 Landesdatenschutzgesetz und ein detailliertes Systemeinführungskonzept vor. Das schon damals vorliegende Sicherheitskonzept ist seitdem mehrfach überarbeitet worden, um künftig die Anforderungen an den Einsatz von EPOS in der gesamten Landesverwaltung zu erfüllen.

Bisher sind jedoch noch nicht alle Maßnahmen vollständig umgesetzt. Einige Maßnahmen werden erst relevant, wenn EPOS im besonders sensiblen Bereich der Landespolizei zum Einsatz kommt. Wegen der besonderen Sicherheitsanforderungen an IT-Systeme der Landespolizei werden hier Sicherheitsvorkehrungen gefordert, die für andere Dienststellen der Landesverwaltung nicht relevant sind. Von besonderer Bedeutung für alle EPOS-Nutzer sind jedoch Fragen der kryptographischen Verschlüsselung der übertragenen und gespeicherten Daten. Schon jetzt wird beispielsweise der gesamte Datenverkehr zwischen EPOS-nutzenden Behörden und Daten- bzw. Applikationsservern beim Dienstleister DVZ M-V GmbH verschlüsselt. Auch die Übertragung aller Protokollierungsinformationen auf einen zentralen Log-Server und die Datensicherungen ist durch kryptographische Verschlüsselung wirksam gegen die Kenntnisnahme Unbefugter geschützt. Das Sicherheitskonzept fordert darüber hinaus jedoch auch die Verschlüsselung der EPOS-Datenbank, um dem hohen Schutzbedarf der dort gespeicherten, zahlreichen Personaldaten gerecht zu werden. Diese Maßnahme wurde bisher nicht umgesetzt, weil nach Aussagen des Innenministeriums wesentliche konzeptionelle Fragen und mögliche Auswirkungen auf die Implementierung und den Betrieb von EPOS ungeklärt sind. Das EPOS-Sicherheitsteam ist jedoch beauftragt, das Thema im Zusammenhang mit der Bewertung vorhandener Restrisiken zu bearbeiten.

Ich empfehle der Landesregierung, vor dem Einsatz von EPOS in jeder Dienststelle das behördenspezifische Sicherheitskonzept zu erarbeiten und das Verfahren vor der Inbetriebnahme formell freizugeben. Das Innenministerium sollte zudem gemeinsam mit dem Software-Hersteller unverzüglich die im Sicherheitskonzept geforderte Datenbankverschlüsselung realisieren.

2.11.7 Elektronische Arbeitszeiterfassung in der Landesverwaltung

Die Landesregierung hat beschlossen, die organisatorischen und formellen Voraussetzungen zu schaffen, um ein zentrales Arbeitszeiterfassungssystem in der Verwaltung der Landesregierung einzuführen.

Vor diesem Hintergrund habe ich dem Innenministerium, das diese Aufgabe koordiniert und die entsprechenden Rechtsvorschriften erarbeitet, empfohlen, die Verordnung über die Arbeitszeit der Beamten im Land Mecklenburg-Vorpommern (AZVO) den technischen Gegebenheiten anzupassen. Insbesondere sind Zugriffsberechtigungen auf die elektronisch gespeicherten Daten über Arbeitszeiten festzulegen. Es ist zu regeln, welche Daten in welcher Form zu welchen Zwecken verarbeitet werden dürfen. Darüber hinaus ist zu klären, ob und in welcher Form Schnittstellen zwischen dem Zeiterfassungssystem und dem eingesetzten bzw. künftig in den Ministerien einzusetzenden Personalverwaltungssystem EPOS 2.0 geschaffen werden sollen. Das Innenministerium hat im März 2009 mitgeteilt, dass die AZVO derzeit überarbeitet wird und dass sich mit der elektronischen Arbeitszeiterfassung erneuter Anpassungsbedarf ergeben werde. Die Schnittstelle zwischen den beiden Systemen werde offline geplant und mit meiner Behörde eng abgestimmt. Bis zum Ende dieses Berichtszeitraumes lagen jedoch keine weiteren Novellierungsvorschläge für die AZVO vor.

Im Mai 2009 lud das Innenministerium zu einer Workshopreihe ein, um die Einführung der elektronischen Arbeitszeiterfassung vorzubereiten. Das Ministerium hatte zuvor Kontakt zum Bundesverwaltungsamt aufgenommen, das das Arbeitszeiterfassungssystem FAZIT (die Abkürzung steht für Flexible Arbeitszeit im Team) einsetzt und bei anderen Anwendern betreut. Es besteht die Absicht, dieses System auch in der Landesverwaltung einzusetzen. In den bis Dezember 2009 insgesamt fünf durchgeführten Workshops spielte die datenschutzgerechte Gestaltung des Systems eine zentrale Rolle. Ein wesentlicher Punkt war, welche Kontrollrechte der Dienstvorgesetzte bei Einführung des Systems hat. Bei den bisher eingesetzten Arbeitszeiterfassungssystemen war es nach Aussage von Workshop-Teilnehmern üblich, dass jeder Beschäftigte sein Monatsjournal, welches das Datum und die Zeit des Kommens und Gehens sowie das entsprechende Zeitguthaben enthielt, dem Dienstvorgesetzten zur Kontrolle vorlegen musste. Mit Einführung der elektronischen Arbeitszeiterfassung bei gleichzeitiger Vorgabe der Gleitzeitbedingungen sehe ich diese Praxis als nicht zulässig an, sofern die Beschäftigten die Vorgaben einhalten. In diesen Fällen ist es nicht erforderlich, dass der Dienstvorgesetzte das Journal zur Kenntnis erhält. Dagegen wurde eingewandt, dass Dienstvorgesetzte dann nicht mehr kontrollieren könnten, ob und wann Mitarbeiter anwesend seien. Solange sich Mitarbeiter an die Gleitzeitregelung halten und kein hinreichender Verdacht auf Missbrauch des Systems besteht, ist in der Tat keine Kontrolle erforderlich und wäre damit auch unzulässig. Weicht jedoch ein Mitarbeiter von den Gleitzeitregelungen ab, so wird dies durch das System erfasst und kann selbstverständlich ausgewertet werden. Gegebenenfalls kann dann auch der Dienstvorgesetzte darüber informiert werden, welcher Mitarbeiter in welcher Weise die Gleitzeitregelung verletzt hat. Der Dienstvorgesetzte kann damit seine Fürsorgepflicht wahrnehmen oder auch, wenn dies notwendig erscheint, personalrechtliche Konsequenzen einleiten. Außerdem habe ich empfohlen zu regeln, wie bei einem Verdacht auf Missbrauch des Systems zu verfahren ist. Beispielsweise könnte dann, um den Sachverhalt zu klären, der Dienstvorgesetzte bei der Gleitzeitstelle beantragen, die Anzahl der Mitarbeiter seines Bereiches mitzuteilen, die aktuell im System als anwesend registriert sind. Dies ist ausreichend, um Verstöße gegen die Gleitzeitregelung oder Manipulationen feststellen zu können.

Außerdem habe ich empfohlen, dass die elektronisch erfassten Gleitzeitdaten gegebenenfalls von zwei Personen ausgewertet werden. Eine Person sollte der Stelle angehören, die für die Datenverarbeitung verantwortlich ist, und die zweite Person sollte ein von der Personalvertretung gewählter Gleitzeitbeauftragter bzw. Mitarbeiter sein. Dadurch könnten die Interessen der Mitarbeiter wahrgenommen werden.

In den Workshops ist eine Musterdienstvereinbarung beschlossen worden, die wesentliche datenschutzrechtliche Aspekte enthält. Darüber hinaus wird ein Datenschutz- und Datensicherheitskonzept erstellt, durch das datenschutzrechtliche Vorgaben weiter untersetzt werden. Ich gehe davon aus, dass damit gute Grundlagen zur Einführung einer elektronischen Arbeitszeiterfassung bestehen.

2.12 Bildung, Kultur, Wissenschaft und Forschung

2.12.1 Missgeschick beim E-Mail-Versand

Ein Student hat mich darauf aufmerksam gemacht, dass ein Professor zu Zwecken der Kursplanung und der Verteilung von Vorträgen und Hausarbeiten eine Liste mit Namen, Matrikelnummern, Geburtsdaten, Geburtsorten und E-Mail-Adressen von Studenten per E-Mail an Studenten dieses Studienganges verschickt hat. Der Student hatte den Professor bereits auf die datenschutzrechtlich fragwürdige Übermittlung der Daten aufmerksam gemacht, aber von ihm keine Antwort erhalten. Deshalb hat er mich um Unterstützung gebeten.

Ich habe mich an den Datenschutzbeauftragten der Universität gewandt, der meine Anfrage zum Anlass genommen hat, den Sachverhalt im Hause zu prüfen. Es stellte sich heraus, dass der Professor sich über die Brisanz des Sachverhaltes nicht im Klaren war und nicht wusste, welche Gefährdung des Rechts auf informationelle Selbstbestimmung aus der Kombination von einer Matrikelnummer mit dem dazugehörigen Namen resultieren kann. Zum Beispiel kann man mit diesem Wissen die Prüfungsergebnisse von Studenten erfahren, da die Ergebnisse über die Matrikelnummer an der Studieneinrichtung öffentlich zugänglich sind.

Die Matrikelnummer ist ein hochschulinternes personenbezogenes Datum, das in der Regel wie ein Pseudonym zur (öffentlichen) Bekanntgabe der Ergebnisse von Leistungstests und Prüfungen genutzt wird. Diese Nutzung setzt aber voraus, dass Dritte nicht erkennen können, welchem Studierenden welche Matrikelnummer zugeordnet ist. Die einem Studierenden zugeordnete Matrikelnummer darf deshalb nur für hochschulinterne Anwendungen und in diesem Rahmen nur berechtigten Mitarbeitern zugänglich sein.

Ich habe die Universität auf diesen Verstoß gegen datenschutzrechtliche Bestimmungen hingewiesen und empfohlen, das Verfahren zur Veröffentlichung von Studienergebnissen zu ändern. Mit dem Bekanntwerden der Matrikelnummer zusammen mit dem Namen und dem Vornamen war sie als Pseudonym nicht mehr zu verwenden. Um die Vertraulichkeit der Prüfungsergebnisse zu wahren, konnten die Studenten die Ergebnisse nur noch über den Evaluationscode abrufen.

Der Datenschutzbeauftragte der Universität hat mitgeteilt, dass künftig ein anderes Verfahren zur Veröffentlichung der Studienergebnisse (ohne Matrikelnummer) genutzt werden wird. Über dieses Ergebnis habe ich den Studenten informiert.

2.12.2 Forschungsvorhaben zum Krankenstand bei Lehrern

Eine Universität in Mecklenburg-Vorpommern hat die in der Vergangenheit verstärkten Diskussionen um die Lehrerbelastungen aufgegriffen und wollte im Rahmen eines Forschungsprojektes die Krankheitsursachen von Lehrern ermitteln und im Ergebnis Vorschläge unterbreiten, wie man die Belastungen möglicherweise abbauen oder mindern könnte. Im Rahmen des erforderlichen Genehmigungsverfahrens durch das Bildungsministerium Mecklenburg-Vorpommern erhielt ich die Unterlagen mit der Bitte um datenschutzrechtliche Prüfung. Dieses Forschungsvorhaben lag auch im Interesse des Ministeriums, da so auch Erkenntnisse darüber gewonnen werden können, ob sich die Eröffnung von Freiräumen und die Stärkung der Eigenverantwortung von Schulen auf den Krankenstand der Lehrkräfte auswirken.

Nach dem Konzept der Universität sollten die Staatlichen Schulämter gebeten werden, folgende Daten der Lehrer an die Universität zu übermitteln:

- Geschlecht,
- Alter,
- Art der Erkrankung,
- Zeitraum der Krankheit,
- Zuordnung zum Schultyp,
- Zeitraum der Beschäftigung, Beschäftigungsverhältnis.

Es bestand mit dem Ministerium Einigkeit darüber, dass die Art der Erkrankung der Lehrkräfte nicht an die Universität übermittelt werden sollte. Angaben zum Gesundheitszustand der Lehrer liegen den Schulämtern nur in Einzelfällen vor, zum Beispiel im Ergebnis einer amtsärztlichen Begutachtung. Außerdem ist dieses Datum für das Forschungsziel nicht erforderlich, da es keine repräsentative Aussagekraft besitzt.

Das Bildungsministerium ging des Weiteren davon aus, dass der oben erwähnte Datenkatalog keinen Personenbezug zulässt und es sich damit um eine anonyme Datenerhebung handelt. Sofern die Anonymität der Betroffenen bereits bei der Datenbeschaffung gesichert ist, unterliegt die weitere Verarbeitung und Nutzung keinen datenschutzrechtlichen Vorschriften. Diese Voraussetzung war nach meiner Auffassung hier jedoch nicht erfüllt. Aus dem gewünschten Datenkatalog besteht bei einer relativ kleinen Schule die theoretische Möglichkeit, aus der Kombination der Erhebungsmerkmale (z. B. Alter 62 Jahre, krank vom 1. April bis zum 30. Juni, Beamter) einen Personenbezug herzustellen.

Daher habe ich dem Bildungsministerium vorgeschlagen, der Universität zu empfehlen, verschiedene Altersklassen zu bilden oder den Zeitraum der Erkrankung in Wochen sowie den Zeitraum der Beschäftigung in Jahren oder in Monaten anzugeben. Zumal es bei Forschungsvorhaben in der Regel nicht auf die einzelne Person ankommt. Damit wären die Daten dann nicht mehr personenbezogen bzw. personenbeziehbar und würden auch keinen datenschutzrechtlichen Bestimmungen unterliegen (§ 3 Abs. 1 DSG M-V).

2.12.3 Uneingeschränkter Zugriff auf Patientendaten für ein Forschungsprojekt?

Eine Universitätsklinik hat mich über ein Forschungsvorhaben informiert. In den Kliniken für Innere Medizin sollten Daten aller Patienten mit unerwünschten Arzneimittelwirkungen erfasst und bewertet werden. Darüber hinaus war vorgesehen, diese Daten gegebenenfalls für eine Therapieberatung zu nutzen. Der überwiegende Teil der Befunddaten war elektronisch gespeichert. Damit unerwünschte Arzneimittelwirkungen zeitnah an das Bundesinstitut für Arzneimittel und Medizinprodukte gemeldet werden können, wurde ein Zugriff auf die elektronischen Patientenakten beim Administrator beantragt. Die Universität hat mich gebeten, diesen Sachverhalt datenschutzrechtlich zu bewerten.

Der Zugriff auf Patientendaten zu Forschungszwecken ist in § 20 Landeskrankenhausgesetz (LKHG M-V) geregelt. Danach ist es zulässig, Patientendaten für Forschungszwecke zu nutzen, wenn der Patient eingewilligt hat. Dies sollte der Regelfall sein. Zu beachten ist, dass die Einwilligung immer nur für ein konkretes Forschungsvorhaben gelten kann. Dabei müssen die gesetzlichen Voraussetzungen, beispielsweise Schriftform, Aufklärung des Patienten, Empfänger der Daten bei Übermittlungen, Widerrufsrecht, erfüllt sein (§ 15 Abs. 2 LKHG M-V). Abweichend vom Regelfall dürfen Patientendaten nur unter ganz bestimmten Voraussetzungen auch ohne Einwilligung verarbeitet werden (§ 20 Abs. 2 LKHG M-V).

Bei dem geplanten Vorhaben war es offensichtlich schwierig, die Einwilligungen einzuholen, denn die Behandlungen waren abgeschlossen und die Patienten hielten sich nicht mehr in der Klinik auf. Folglich kam als rechtliche Grundlage nur eine Genehmigung durch die zuständige oberste Aufsichtsbehörde in Frage. Genehmigungsbehörde war in diesem Fall das Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern.

Ein Zweck dieser Verarbeitung von Patientendaten sollte es unter anderem sein, dass die gesetzlichen Meldefristen bei unerwünschten Arzneimittelwirkungen eingehalten werden. Für diesen Zweck dürfen allerdings nur pseudonymisierte Daten übermittelt werden. Auf der Grundlage einer Genehmigung könnten sie dann zwar personenbezogen erfasst, müssten dann jedoch entsprechend pseudonymisiert werden.

Ein weiterer Grund für den Zugriff auf Patientendaten sollte gegebenenfalls eine nachträgliche Therapieberatung sein. Hier wäre dann ein Zugriff auf Patientendaten auf der Grundlage des Behandlungsvertrages zulässig (§ 15 Abs. 1 Nr. 1 LKHG M-V). Ob im vorliegenden Fall die den Zugriff auf Patientendaten beantragende Ärztin als Behandlerin einzuordnen ist, muss der ärztliche Leiter/Direktor der Klinik beurteilen. Er trägt die Verantwortung dafür, dass nur behandelnde Ärzte Zugriff auf Patientendaten haben.

Ich habe daher empfohlen, diese Punkte zu klären, bevor das Forschungsvorhaben gestartet werden kann, und war bereit, die Universität dabei aus datenschutzrechtlicher Sicht weiterhin zu beraten.

2.12.4 Studie zur Erreichbarkeit niedergelassener Ärzte für über 60-Jährige

Eine Universität in Mecklenburg-Vorpommern beabsichtigte, in einem Projekt den demographischen Wandel der Bevölkerung in Mecklenburg-Vorpommern und die danach erforderlichen medizinischen Versorgungskapazitäten zu untersuchen. Zu diesem Zweck wollte die Universität Daten aus dem Melderegister nutzen. Ich wurde um eine datenschutzrechtliche Beratung gebeten.

Bei der Universität handelt es sich um eine öffentliche Stelle im Sinne des § 31 Abs. 1 Landesmeldegesetz (LMG). Für die öffentlichen Stellen kann nach § 3 a Abs. 1 LMG eine automatisierte Übermittlung von Meldedaten aus dem zentralen Informationsregister (ZIR) erfolgen. Dieser Zugang muss beim Innenministerium Mecklenburg-Vorpommern beantragt werden. Der Zugang zum ZIR erfolgt, gesehen auf die einzelnen Forschungsvorhaben, immer für einen zeitlich eindeutig definierten Abschnitt. Aus diesem Grunde habe ich auch empfohlen, dass die Universität einen eigenen behördlichen Datenschutzbeauftragten bestellt. Dieser sollte in die Prüfung der Rechtmäßigkeit der betreffenden Datenübermittlung aus dem ZIR eingebunden werden.

Bei jedem Forschungsvorhaben sollte er folgende Punkte prüfen (Vorabkontrolle):

1. öffentliches Interesse des Vorhabens,
2. erforderlicher Datenumfang aus dem ZIR,
3. Datenherkunft (Meldebehörde) und
4. zu treffende Maßnahmen zum Datenschutz und zur Datensicherheit (§§ 21, 22 DSG M-V).

Für diese Studie sollten die Meldeämter Namen und Adressen aller Personen ab einem Alter von 60 Jahren mit Hauptwohnsitz in den Landkreisen Ostvorpommern und Uecker-Randow sowie in der kreisfreien Stadt Greifswald automatisiert übermitteln. Eine solche sogenannte Gruppenauskunft ist unter den Voraussetzungen des § 31 Abs. 1 Satz 3 LMG möglich. Aus dieser Gruppe sollten dann 800 Probanden durch ein Zufallsprinzip bestimmt werden. Hinsichtlich der Probandenziehung hatte ich empfohlen festzulegen, wann die überzähligen Daten zu löschen sind und wer dies kontrolliert. Die Ergebnisse sollten schriftlich dokumentiert und in einem Datenschutzkonzept zusammengefasst werden.

Ein weiterer Aspekt war, dass in dem vorbereiteten Anschreiben an die betroffenen Personen versichert wurde, dass ihre Daten anonym ausgewertet werden. Dies traf zumindest nicht für die gesamte Projektphase zu. Es war vorgesehen, eine Zuordnungsliste mit den identifizierenden Daten (Name, Adresse) und dem Pseudonym (Probanden-ID) zu führen, da die Teilnehmer zu einem späteren Zeitpunkt erneut kontaktiert werden sollten. Ich habe hierzu empfohlen, dass diese Liste von einem Mitarbeiter verwaltet werden sollte, der nicht direkt an der Studie mitarbeitet. Dadurch könnte auf einem höheren Niveau gewährleistet werden, dass die Reglungen des Datenschutzes eingehalten werden. Des Weiteren sollten die Probanden auf diesen wesentlichen Datenverarbeitungsvorgang - erneute Kontaktaufnahme - bereits im ersten Anschreiben hingewiesen werden, ebenso wie auf die Möglichkeit, die Teilnahme schon nach dem ersten Schreiben abzulehnen.

Die Daten selbst sollten von den Teilnehmern per Fragebogen erhoben werden. Ich habe hier zu bedenken gegeben, dass aus den Angaben Straße, Ort und Postleitzahl im Zusammenhang mit den Angaben Alter, Geschlecht, Familienstand, Anzahl der Personen im Haushalt gerade bei den in den ausgewählten Landkreisen vorhandenen kleinen Ortschaften mit wenigen Einwohnern es unter Umständen leicht möglich ist, eine Person zu bestimmen. Aus diesem Grund habe ich vorgeschlagen, nicht die vollständige, sondern eine um die letzten beiden Ziffern verkürzte Postleitzahl zu verwenden, wenn ein Ortsbezug notwendig ist. Ich habe auch empfohlen, frühzeitig Orts- und Stadtteilmittelpunkte aus den Adressdaten zu bilden und dann nur noch diese zu speichern und die Adressdaten zu löschen.

Nicht zuletzt sollte vor einer Veröffentlichung der Daten oder ihrer Weitergabe an Dritte sorgfältig geprüft werden, dass keine Zuordnung der Angaben zu Personen möglich ist. Im Anschreiben könnte den Teilnehmern versichert werden, dass nach Auswertung der Daten diese in einer Form dargestellt werden, die keinen Rückschluss auf ihre Person ermöglicht.

Meine Empfehlungen wurden umgesetzt.

2.13 Wirtschaft und Gewerbe/Landwirtschaft

2.13.1 Das Kehrbuch der Schornsteinfeger - eine begehrte Datenquelle

Aufgabe der Schornsteinfeger ist es, in regelmäßigen Abständen Heizungsanlagen zu kontrollieren. Grundlage für diese Kontrollen sind unter anderem die Daten der Kunden, die in einem Kehrbuch, das auch elektronisch geführt werden kann, zu dokumentieren sind. In einem Kehrbuch werden beispielsweise folgende Angaben erfasst: Name des Grundstückseigentümers oder Verwalters sowie gegebenenfalls des Betreibers der Anlage, Anzahl und Bezeichnung der kehr- und überprüfungspflichtigen Anlagen etc.

Dass diese Daten des Kehrbuches begehrt sind, habe ich schon in meinem Siebten Tätigkeitsbericht, Punkt V 2, dargestellt. In diesem Bericht ging es darum, dass Zollbehörden von den Schornsteinfegern wissen wollten, welche Personen eine Ölfeuerungsanlage haben. Die Zollbehörden wollten offensichtlich mit dieser Kenntnis bei den Betroffenen gezielte Kontrollen des verwendeten Kraftstoffs in den Fahrzeugen durchführen, um so gegebenenfalls den Missbrauch des Heizöls als Dieselkraftstoff feststellen zu können. Diese Datenübermittlung ohne konkreten Anlass und mangels Rechtsgrundlage war unzulässig.

Der gleiche Bürger, der mich damals zu den Datenübermittlungen der Schornsteinfeger an die Zollbehörden befragte, hat sich in diesem Berichtszeitraum wieder an mich gewandt und mir mitgeteilt, dass ein Umweltamt bei einem Schornsteinfeger Name und Adresse der Besitzer von Ölfeuerungsanlagen erheben wollte.

Auf meine Bitte um Stellungnahme hat mir das Umweltamt mitgeteilt, dass das Landeswassergesetz (LWaG M-V) die Anzeige von Anlagen vorschreibt, die wassergefährdende Stoffe enthalten (§ 20 Abs. 1 LWaG M-V). Das Umweltamt hatte die begründete Annahme, dass in einem bestimmten Bereich nicht alle Betreiber von Anlagen ihre Anzeigepflicht erfüllt hatten. Es hat deshalb den für den fraglichen Bereich zuständigen Schornsteinfeger gebeten, aus seinen Aufzeichnungen mitzuteilen, unter welcher Adresse (Ort, Ortsteil, Straße, Hausnummer) und in welcher Art von Gebäuden Ölfeuerungsanlagen betrieben werden.

Das Umweltamt nimmt die Aufgabe einer Wasserbehörde wahr. Deshalb darf es auch personenbezogene Daten erheben und verarbeiten sowie entsprechende Auskünfte verlangen (§ 118 Abs. 3 und Abs. 1 LWaG M-V). Eine Erhebung bei den Betroffenen war nicht möglich, denn das Umweltamt wusste nicht, wer seiner Anzeigepflicht nicht nachgekommen ist; es bestand jedoch die begründete Vermutung, dass es mehrere Personen sein könnten. Aus diesem Grunde durfte das Amt die Daten bei dem Schornsteinfeger mit Hinweis auf die Auskunftspflicht erheben und der Schornsteinfeger durfte die Daten an das Umweltamt nach dem Schornsteinfeger-Handwerksgesetz (SchfHwG) übermitteln (§ 19 Abs. 5 Satz 2 SchfHwG).

Der Bürger hat mich anschließend darum gebeten, ihm zu erläutern, weshalb ich - bei seiner Meinung nach gleichem Sachverhalt - zu diesen unterschiedlichen datenschutzrechtlichen Bewertungen gekommen bin. Dies stellt sich wie folgt dar: Für die Datenerhebung bei den Schornsteinfegern und die Datenübermittlung an den Zoll lag weder eine Rechtsgrundlage noch eine hinreichend begründete Vermutung für rechtswidriges Verhalten vor. Somit war diese Datenübermittlung unzulässig. Bei der Datenübermittlung an das Umweltamt jedoch beruhte die Übermittlung auf einer begründeten Vermutung sowie einer Rechtsgrundlage und war somit zulässig.

Zu Beginn des Jahres 2009 erhielt ich zwei weitere Anfragen zur Nutzung der Daten des Kehrbuches. In einem Fall wollte ein Student im Rahmen seiner Diplomarbeit den Wärmebedarf analysieren, und in dem anderen Fall sollten Studenten die Daten des Kehrbuches als Grundlage für ein Klimaschutzkonzept erfassen und verarbeiten. In beiden Fällen waren dazu aber keine personenbezogenen Daten erforderlich, sondern nur die Anzahl von Öl-, Gas-, Kohle- oder Holzfeuerungsanlagen in den verschiedenen Ortsteilen.

Weil möglicherweise auch andere Gemeinden Interesse daran haben, Daten des Kehrbuches für ein Klimakonzept zu erheben und zu verarbeiten, habe ich mit dem Ministerium für Wirtschaft, Arbeit und Tourismus das Verfahren zur Datenübermittlung abgestimmt. Das Ministerium hat die Landesinnung der Schornsteinfegermeister darüber informiert. Im Ergebnis dürfen die Schornsteinfeger anonymisierte Daten für den genannten Zweck an die Gemeinden übermitteln. In kleineren Städten sollen die Zahlen nur für das gesamte Stadtgebiet herausgegeben werden, um eine Bestimmbarkeit von Personen auszuschließen. Dabei sollte auch darauf geachtet werden, dass die Anzahl der Anlagen nicht kleiner als drei ist, weil dies zu einer Bestimmbarkeit beitragen könnte. Anlagen, die weniger als dreimal vorhanden sind, müssten dann in einer anderen, größeren Gruppe aufgehen.

2.13.2 Personenbezogene Gefahrgutkontrollen?

Der Datenschutzbeauftragte eines Landkreises hat mich darüber informiert, dass die Ordnungsbehörden von einer Landesbehörde aufgefordert worden sind, regelmäßig Daten über bearbeitete Bußgelder im gewerblichen Güterverkehr zu übermitteln. Dazu zählten folgende Angaben: Name und Anschrift des Unternehmens, Art und Datum des Verstoßes, Kennzeichen des kontrollierten Fahrzeuges sowie Name des Fahrers. Der Datenschutzbeauftragte hat mich gebeten zu prüfen, ob dieses Ersuchen mit den datenschutzrechtlichen Bestimmungen vereinbar ist.

Bei den von der Landesbehörde erwünschten Angaben handelt es sich um personenbezogene Daten. Deshalb müssen für die Verarbeitung dieser Daten auch die datenschutzrechtlichen Vorschriften beachtet werden, das heißt, eine Übermittlung personenbezogener Daten ist nur zulässig, wenn eine Rechtsvorschrift dies ausdrücklich zulässt. Eine entsprechende Rechtsvorschrift war in dem Übermittlungsersuchen jedoch nicht aufgeführt.

Auf meine Anfrage hin hat mir die Landesbehörde mitgeteilt, dass sie für die Kontrolle der Einhaltung der Gefahrgutvorschriften in den Unternehmen Mecklenburg-Vorpommerns zuständig sei. Die Daten aus den Bußgeldverfahren wegen Verstoßes gegen die Gefahrgutvorschriften seien erforderlich, um die Kontrollen zu planen. Als Rechtsgrundlage für die Datenübermittlung wurde § 4 Abs. 1 Gefahrgutkontrollverordnung i. V. m. § 14 Abs. 1 und § 10 Abs. 3 Nr. 6 Landesdatenschutzgesetz (DSG M-V) genannt.

Ich habe die Rechtsgrundlagen geprüft und bin zu dem Ergebnis gekommen, dass § 4 Abs. 1 Gefahrgutkontrollverordnung zwar die Rechtsgrundlage für die Gefahrgutkontrolle ist, darauf jedoch nicht die Übermittlung der geforderten Daten gestützt werden kann. Rechtsgrundlage für die Datenübermittlung durch die Ordnungsbehörden an die Kontrollbehörde könnte § 41 Abs. 1 Satz 1 Sicherheits- und Ordnungsgesetz (SOG M-V) sein. Danach können anderen Behörden, unter anderem anderen öffentlichen Stellen, personenbezogene Daten übermittelt werden, wenn sie an der Abwehr von Gefahren beteiligt sind und soweit die Kenntnis dieser Daten zur Gefahrenabwehr erforderlich ist.

Dies habe ich der Landesbehörde mitgeteilt. Zur Planung von Kontrollen schienen mir allerdings die Namen der Fahrer, gegen die ein Bußgeld wegen Verstoßes gegen Gefahrgutvorschriften verhängt worden ist, sowie die Kennzeichen der kontrollierten Kraftfahrzeuge nicht erforderlich zu sein. Ich habe daher empfohlen, den Datenkatalog um diese Daten zu reduzieren.

Die Landesbehörde hat meine Empfehlungen umgesetzt und hat überarbeitete Anschreiben an die Ordnungsämter mit einem geänderten Datenkatalog sowie mit dem Hinweis auf die Rechtsgrundlage für die Datenübermittlung gesandt.

2.13.3 Unzulässige Datenübermittlung durch einen regionalen Wasserversorger

Ein Rechtsanwalt hat mich darüber informiert, dass ein Wasserversorger Verbrauchsdaten seines Mandanten an eine Stadtverwaltung übermittelt hat. Hintergrund hierfür war ein Rechtsstreit zwischen seinem Mandanten und der Stadt, bei dem anhand der Wasserverbrauchsdaten belegt werden sollte, dass der Betroffene zu einem maßgeblichen Stichtag seinen Lebensmittelpunkt nicht in dem von ihm bewohnten Haus gehabt hatte. Dies wäre aber entscheidend für ein besonderes Kaufrecht, das der Mandant des Anwalts beantragt hat. Der Rechtsanwalt hatte sich bereits an den Wasserversorger gewandt und darauf hingewiesen, dass eine Übermittlung der Verbrauchsdaten an die Stadt aufgrund der fehlenden Einwilligung seines Mandanten nicht zulässig war, da es sich hier um dessen personenbezogene Daten handelte. Diese Auffassung wurde vom Wasserversorger nicht geteilt. Er war der Meinung, dass Verbrauchsdaten keine personenbezogenen Daten seien, weil nicht bestimmt werden kann, welche Person Wasser entnommen hat. Der Rechtsanwalt bat mich daher um Unterstützung.

Die Lesart des Wasserversorgers, dass Wasserverbrauchsdaten keine personenbezogenen Daten seien, entspricht nicht der Rechtslage. § 3 Abs. 1 Landesdatenschutzgesetz (DSG M-V) definiert den Begriff personenbezogene Daten. Hierunter werden demnach Einzelangaben über persönliche (Name, Anschrift, Geburtsdatum) oder sachliche Verhältnisse (Verbrauchsdaten) einer bestimmten und bestimmbaren Person verstanden. Der Begriff Einzelangaben umfasst somit jede Information, die einer einzelnen Person zugeordnet werden kann. Diese gesetzlichen Voraussetzungen waren hier erfüllt, sodass die personenbezogenen Daten des Kunden nur unter Berücksichtigung der Grundsätze des DSG M-V hätten verarbeitet werden dürfen. Es kommt nicht darauf an, welche Person eines Haushaltes Wasser entnimmt, die Verbrauchsdaten sind vielmehr der Person zuzuordnen, die die Kosten des Wasserverbrauchs zu tragen hat. Demnach liegt eine zulässige Datenverarbeitung nur vor, wenn die Vorschriften des DSG M-V sie zulassen, eine andere Rechtsvorschrift sie erlaubt oder zwingend voraussetzt oder der Betroffene eingewilligt hat.

Auch nachdem ich mehrfach versucht habe, dem Wasserversorger die Grundlagen des Datenschutzes zu erklären und verschiedene Kommentare zur Definition des Begriffes „personenbezogene Daten“ empfohlen habe, ist er nicht von seiner oben vertretenen Position abgerückt. Ich habe die Datenübermittlung daher gemäß § 32 Abs. 1 Satz 1 Nr. 4 DSG M-V beanstandet und ihn aufgefordert, unrechtmäßige Datenübermittlungen künftig zu unterlassen. In seiner Stellungnahme zu der Beanstandung hat mir der Wasserversorger dann versichert, eine Übermittlung von Kundendaten in ähnlichen Fällen zu unterlassen.

Hinsichtlich der Rechtmäßigkeit der Datenübermittlung habe ich mich auch an die Stadt gewandt und auf die bei der Übermittlung von personenbezogenen Daten zu beachtenden datenschutzrechtlichen Vorschriften hingewiesen und gebeten, mir den Zweck des Übermittlungsersuchens mitzuteilen.

Die mir daraufhin übermittelten Argumente für die Nützlichkeit der Wasserverbrauchsdaten im Rahmen des Rechtsstreites waren zwar schlüssig, allerdings fehlte in dem Schreiben die Rechtsgrundlage, nach der die Erhebung zulässig gewesen wäre. Sofern die Stadt die Angaben des Petenten zum Lebensmittelpunkt und damit die Voraussetzungen für das besondere Kaufrecht bezweifelt, hätte sie zunächst den Petenten auffordern müssen, seine Behauptung zu belegen. Kommt er dieser Aufforderung nicht nach bzw. kann er seine Behauptung nicht belegen, hätte sein Antrag auf Kauf des Grundstückes abgelehnt werden können.

Vor diesem Hintergrund habe ich dem Amt empfohlen, für derartige Zwecke künftig keine Daten mehr bei dem Wasserversorger zu erheben.

2.13.4 Zweckbindung bei Datennutzung nach dem Landpachtverkehrsgesetz?

Ein Käufer von Ackerland hat sich bei mir darüber beschwert, dass das Amt für Landwirtschaft bei Förderanträgen auf EU-Beihilfen die kompletten Pachtverträge, einschließlich der Pachthöhe, verlange. Darüber hinaus habe das Amt für Landwirtschaft beim zuständigen Grundbuchamt Daten ohne sein Wissen erhoben. Seiner Auffassung nach sei dies eine rechtswidrige Datenausspähung des Amtes.

Ich habe das Amt für Landwirtschaft um eine schriftliche Stellungnahme zu diesem Sachverhalt gebeten. Dazu hatte der Petent dann noch weitere Nachfragen; deshalb habe ich bei dem Amt für Landwirtschaft eine datenschutzrechtliche Kontrolle angekündigt und darum gebeten, mir im Vorfeld der Kontrolle die Verfahrensverzeichnisse für die Datenverarbeitungen zuzusenden (§ 18 DSG M-V). Der Justiziar des Amtes teilte mir mit, dass diese Verzeichnisse bis zum Kontrolltermin nicht vorgelegt werden können.

Während der Kontrolle habe ich die entsprechende Verwaltungsakte sowie einen Ausdruck der automatisiert verarbeiteten Daten eingesehen. Es stellte sich Folgendes heraus:

Der Beschwerdeführer hatte im Jahr 2008 bei dem Amt für Landwirtschaft die Kaufabsicht landwirtschaftlicher Flächen angezeigt, um den Kauf genehmigen zu lassen. Die Rechtsgrundlage für diese Anzeige ergibt sich aus dem Grundstücksverkehrsgesetz (GrdstVG, § 2 Abs. 1 Satz 1). Er führte in seiner Anzeige aus, dass er einen Land- bzw. Forstwirtschaftsbetrieb im Nebenerwerb betreibe, was die Genehmigung positiv beeinflussen kann. Das Amt hatte jedoch Zweifel, ob der Erwerb tatsächlich für landwirtschaftliche Zwecke angestrebt wird, und hat dem Betroffenen mitgeteilt, dass es ein Verfahren zur Ausübung des Vorkaufsrechts einleite. Sofern sich nämlich ein Landwirt findet, der Interesse an den zum Verkauf stehenden Flächen hat, diese zu landwirtschaftlichen Zwecken nutzen will und sie in seinen Landwirtschaftsbetrieb sinnvoll eingliedern kann, wäre er zu bevorzugen. Aus dieser Mitteilung konnte der Beschwerdeführer erkennen, dass seine Kaufabsicht wohl nicht genehmigt wird. Er hat deshalb seinen Antrag auf Genehmigung des Grundstückskaufs zurückgezogen.

Im weiteren Verlauf zeigte im Mai 2009 eine Agrar GmbH dem Amt für Landwirtschaft an, dass sie einen Pachtvertrag verlängert und neue Flächen gepachtet hat. Rechtsgrundlage für diese Anzeige ist das Landpachtverkehrsgesetz (LPachtVG). Es handelte sich dabei nicht, wie von dem Petenten vermutet, um einen Antrag auf EU-Beihilfen.

Die erforderlichen Daten nach dem Grundstücksverkehrsgesetz und nach dem Landpachtverkehrsgesetz werden durch die Mitarbeiter des Amtes in einer gemeinsamen Datei, der BSFlur, verarbeitet. Dadurch ist es aufgefallen, dass Teile der von der Agrar GmbH angezeigten neu gepachteten Flächen identisch mit den Flächen waren, für die der Kauf im Jahr 2008 vom Amt nach dem Grundstücksverkehrsgesetz genehmigt werden sollte. Das Amt für Landwirtschaft vermutete, dass die Genehmigung umgangen worden ist oder umgangen werden sollte. Es hat deshalb bei dem zuständigen Grundbuchamt nachgefragt, ob für die fragliche Liegenschaft ein anderer als der bisher bekannte Eigentümer eingetragen sei. Das Grundbuchamt bestätigte dies, und es stellte sich heraus, dass der Beschwerdeführer aufgrund eines Erbteilkaufvertrages Eigentümer des Grundstücks geworden ist.

Ich habe das Vorgehen des Amtes für Landwirtschaft als zulässig bewertet. Beide Gesetze verfolgen das Ziel, eine der Landwirtschaft dienliche Agrarstruktur aufrechtzuerhalten und weiterzuentwickeln, kurz gesagt, Bodenspekulationen weitgehend auszuschließen. Die Verarbeitung der Daten nach dem Grundstücksverkehrsgesetz und nach dem Landpachtverkehrsgesetz dient also nicht unterschiedlichen, sondern den gleichen Zwecken. Gegen die Zweckbindung der Daten ist daher nicht verstoßen worden.

Die von dem Beschwerdeführer vermutete unrechtmäßige Datenverarbeitung habe ich nicht festgestellt, dennoch hatte seine Beschwerde einen datenschutzrechtlichen Nutzen. Denn bisher lagen in dem Amt für Landwirtschaft die gesetzlich vorgeschriebenen Verfahrensbeschreibungen für die Datenverarbeitungen nicht vor, was ich in meinem Bericht vom November 2009 kritisiert habe. Dieser Vorwurf richtet sich in erster Linie nicht an das Amt selbst, sondern an das Ministerium für Landwirtschaft, Umwelt und Verbraucherschutz, da es sich bei dem Verfahren BSFlur offensichtlich um ein Verbundverfahren (§ 17 DSG M-V) handelt und die Ämter für Landwirtschaft die Software nicht selbst beschafft haben. Ich gehe davon aus, dass das Ministerium zügig die Verfahrensverzeichnisse für die Software sowie das Sicherheitskonzept erstellt und somit die gesetzlichen Vorgaben umsetzt.

2.14 Technik und Organisation

2.14.1 Einführung der Internet-Telefonie in der Landesverwaltung

Die Landesregierung Mecklenburg-Vorpommern führt seit dem Kabinettsbeschluss vom 18. April 2006 die Internet-Telefonie in den obersten Landesbehörden ein. Künftig werden keine konventionellen ISDN-Telefonanlagen mehr betrieben. Die Landesbehörden nutzen ihre vorhandenen lokalen Netze sowie das Landesverwaltungsnetz CN-LAVINE nicht nur für die Datenkommunikation, sondern auch für die Übertragung von Sprache. Erste Planungen hierfür gab es bereits im Jahr 2004 und so konnte ich schon seit längerer Zeit das Projekt begleiten (siehe Siebter Tätigkeitsbericht, Punkt A.II.1.10 und Achter Tätigkeitsbericht, Punkt 2.15.3). Vorgesehen ist eine Versorgung von etwa 25.000 Teilnehmern.

In einem umfassenden Sicherheitskonzept wurde schon frühzeitig dokumentiert, mit welchen technischen und organisatorischen Maßnahmen der geforderte hohe Grad an Datenschutz und Informationssicherheit gewährleistet werden soll. So wird durch Sicherheitsgateways an den Übergängen zu lokalen Netzwerken und durch die logische Trennung der Sprach- und Datenkommunikation auf der Basis separater virtueller privater Netze (VPN) im CN-LAVINE und separater virtueller lokaler Netze (VLAN) in den lokalen Netzen der Behörde der Schutz hochsensibler Daten innerhalb des CN-LAVINE sichergestellt. Mit Hilfe von VPN bzw. VLAN werden geschlossene Bereiche mit definierten Sicherheitsanforderungen bzw. definierten dienst- und anwendungsabhängigen Anforderungen an die Netzstruktur geschaffen. Durch den Aufbau redundanter Server, die Mehrstufigkeit der Dienstleistungserbringung (zentral/dezentral), den Einsatz von unterbrechungsfreien Stromversorgungen (USV) für zentrale Komponenten und die Nutzung alternativer Leitungswege und Netzübergänge wird eine hohe Verfügbarkeit der IP-Telefonie erreicht. Besonders positiv bewerte ich den Einsatz von kryptographischen Verfahren, welche die Vertraulichkeit und Integrität der Kommunikation sicherstellen. So garantiert der Einsatz der Transport Layer Security (TLS) zur Übertragung verschlüsselter Signalisierungsinformationen (Secure SCCP) und des Secure Real-Time Protocol (SRTP) für eine verschlüsselte Übertragung der Sprachdaten, dass sowohl der Gesprächsaufbau als auch das Gespräch selbst abhörsicher ablaufen können. Zusätzlich sorgt eine gestaffelte Public Key Infrastructure (PKI) dafür, dass nur Endgeräte mit einem gültigen Zertifikat benutzt werden können. Eine digitale Signierung der Softwareimages für die Endgeräte stellt zudem sicher, dass nur authentisierte und vom Betreiber freigegebene Endgerätesoftware eingesetzt werden kann. Einer Manipulation der Endgeräte durch das Einspielen schadhafter Software wird so wirkungsvoll vorgebeugt. Zusätzliche Absicherung erfährt die IP-Telefonie durch mehrere Firewallsysteme und Access-Listen, die auf den beteiligten Switchen hinterlegt sind. Ein detailliertes Notfallkonzept stellt durch ein redundant ausgelegtes zentrales Vermittlungssystem und durch dezentrale Voicegateways in den jeweiligen Dienststellen sicher, dass auch beim Ausfall des CN-LAVINE telefoniert werden kann, wenn auch mit eingeschränktem Komfort. Bemerkenswert ist, dass die Verschlüsselung bei solch einem Notfall nicht verlorengeht und weiterhin eine sichere Kommunikation gewährleistet werden kann.

Nach Beginn des Echtbetriebes im Innenministerium am 31. März 2008 habe ich die Umsetzung der datenschutzrechtlichen und -technischen Vorschriften kontrolliert. Im Mittelpunkt meiner Kontrolle stand neben Details der technischen Umsetzung der Umgang mit den anfallenden Verkehrsdaten. Um die entstehenden Telefonkosten auf die einzelnen Ressorts umlegen zu können, kommt eine spezielle Auswertesoftware zum Einsatz. Da es sich bei dieser Software um ein sehr mächtiges Werkzeug handelt und mit ihrer Hilfe eine Auswertung des Telefonverhaltens sämtlicher Mitarbeiter aller beteiligten Behörden nicht ausgeschlossen werden kann, sind besonders hohe Datenschutzanforderungen unabdingbar. Zu diesem Zweck wird unter anderem ein sogenannter Hardwaredongle verwendet, ohne den ein Zugriff auf die verschlüsselten Gesprächsdaten unmöglich ist und der ein unberechtigtes Kopieren der Daten verhindert. Zudem wurden verschiedene Nutzerrollen im System eingerichtet, sodass ich einen angemessenen Schutz der Verkehrsdaten bestätigen konnte. Auch die Mitbestimmungsrechte der Personalvertretung sind gewahrt. So erfordert das Erstellen von Einzelverbindungsnachweisen grundsätzlich das Anmelden mit zwei verschiedenen Passwörtern, wobei eines bei der Personalvertretung hinterlegt wurde.

Durch solch eine technische Umsetzung des Vier-Augen-Prinzips, durch automatisches Protokollieren von Zugriffen und durch regelmäßige Auswertungen durch ein Revisionsteam wird einem Missbrauch wirksam vorgebeugt. Zudem bewirkt eine klare Mandantentrennung innerhalb des Systems, dass eine Behörde nicht auf die Verkehrsdaten einer anderen zugreifen kann.

Im Ergebnis meiner Kontrolle konnte ich mich von einer in allen Bereichen technisch sehr gelungenen Umsetzung überzeugen und dem Verfahren zu Recht ein angemessenes, dem Stand der Technik entsprechendes Datenschutz- und IT-Sicherheitsniveau bescheinigen. Im organisatorischen Bereich musste ich jedoch erhebliche Datenschutzmängel feststellen. So existierte zum Zeitpunkt der Kontrolle kein gültiger Vertrag zwischen dem Innenministerium als Auftraggeber und der DVZ M-V GmbH als Auftragnehmer. Die Anforderungen des § 4 DSG M-V zur Verarbeitung personenbezogener Daten im Auftrag waren somit nicht umgesetzt. Zudem hatte das Innenministerium weder die gemäß § 18 Abs. 1 DSG M-V erforderliche Verfahrensbeschreibung erstellt noch das Verfahren IP-Telefonie formell gemäß § 19 DSG M-V freigegeben. Auch die Frage der datenschutzrechtlichen Verantwortung für alle Teile des Verfahrens konnte nicht abschließend geklärt werden. Mit welchen Problemen diese Frage grundsätzlich verbunden ist, habe ich unter Punkt 2.1.6 ausführlich erläutert.

Die für die Landesverwaltung aufgebaute technische Infrastruktur der IP-Telefonie nutzen inzwischen auch kommunale Behörden. Im Laufe des Jahres 2009 ist mit dem Landkreis Ludwigslust die erste Kommune dem Projekt IP-Telefonie beigetreten. Da ich davon ausgehe, dass auch weitere Landkreise dem Beispiel Ludwigslust folgen werden, war es mir besonders wichtig, die Nutzung der IP-Telefonie dort zeitnah zu kontrollieren und mögliche Empfehlungen auszusprechen. Da die Implementierung der IP-Telefonie im Landkreis Ludwigslust auf Basis der Lösung für die Landesverwaltungen aufsetzte, überraschte es nicht, dass auch hier die sicherheitstechnischen Aspekte nicht zu bemängeln waren. Aber auch hier zeigten sich einige organisatorische Defizite. So fehlten neben dem Verfahrensverzeichnis eine formelle Freigabe und das von § 22 Abs. 5 DSG M-V geforderte vollständige Sicherheitskonzept. Zudem war versäumt worden, die Dienstvereinbarung der neuen Kommunikationstechnik anzupassen, da sich die vorhandene auf die alte Telefonanlage bezog. Hervorzuheben ist die besonders datenschutzfreundliche Lösung zum Umgang mit Verkehrsdaten. Zum Zeitpunkt meiner Kontrolle sah der Landkreis keine Veranlassung dafür, anfallende Gesprächsdaten länger als technisch unvermeidbar aufzubewahren. Auf den Einsatz der in der Landesverwaltung genutzten Auswertungssoftware wurde ganz verzichtet. So wird vorbildlich die in § 5 Abs. 1 DSG M-V geforderte Datensparsamkeit umgesetzt.

Ich werde die Einführung der IP-Telefonie in der Landesverwaltung und in weiteren Kommunen auch weiterhin begleiten und auf den datenschutzgerechten Umgang mit allen in diesem Verfahren anfallenden personenbezogenen Daten drängen. Nachdem ich mich von dem hohen technischen Sicherheitsniveau überzeugen konnte und festgestellt habe, dass durch die Einrichtung von Mandanten die Möglichkeit der strikten Trennung der Verkehrsdaten verschiedener Mandanten gegeben ist, wird voraussichtlich auch meine Behörde dem Projekt IP-Telefonie beitreten und die in der DVZ M-V GmbH aufgebaute technische Infrastruktur nutzen.

2.14.2 Elektronisches Dokumentenmanagement in der Landesverwaltung

Das Kabinett hat in seiner Sitzung am 29. April 2008 beschlossen, das elektronische Dokumentenmanagement- und Vorgangsbearbeitungssystem DOMEA® bis Ende 2013 in den Ministerien und in der Staatskanzlei einzuführen. Betroffen sind von diesem Projekt etwa 2.400 Arbeitsplätze. Die Federführung des Projektes wurde dabei dem Finanzministerium übertragen. Die zentralen IT-Komponenten des Verfahrens soll die DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH (DVZ M-V GmbH) im Auftrag der Landesregierung betreiben.

Da mit dem DOMEA® System auch zahlreiche personenbezogene Daten verarbeitet werden, ist bei der Vorbereitung der Pilotierung und der Einführung eine Vielzahl von datenschutzrechtlichen Aspekten zu berücksichtigen. Daher habe ich das Projekt von Beginn an beratend begleitet. Detaillierte Empfehlungen für eine datenschutzgerechte Umsetzung des Verfahrens konnte das Finanzministerium zudem der Orientierungshilfe „Datenschutz bei Dokumentenmanagementsystemen“ (abrufbar unter http://www.datenschutz-mv.de/dschutz/informat/dms/oh_dms.html) entnehmen, die unter meiner Mitarbeit im Arbeitskreis „E-Government“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeitet wurde.

Im Rahmen meiner beratenden Tätigkeit begleite ich auch die Erstellung des Sicherheitskonzeptes, das wie alle Sicherheitskonzepte der Landesverwaltung auf der Basis der Grundschutzmethodik des Bundesamtes für Sicherheit in der Informationstechnik (BSI) erarbeitet wurde. Die in diesem Kontext erforderliche Schutzbedarfsfeststellung ergab in den Kategorien Vertraulichkeit und Verfügbarkeit einen hohen Schutzbedarf. Daraus resultiert eine ergänzende Sicherheitsanalyse, um festzustellen, ob über das Grundschutzniveau hinausreichende zusätzliche Schutzmaßnahmen erforderlich sind. Auch diesen Schritt werde ich beratend begleiten.

Von besonderer Bedeutung für das Projekt ist eine datenschutzgerechte Protokollierung des Verfahrens (siehe dazu auch Punkt 2.14.8). Das Protokollierungsverfahren hat zum einen die Vorgaben des § 21 Abs. 2 Nr. 5 DSG M-V (Revisionsfähigkeit) umzusetzen, damit festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat. Darüber hinaus ist aber auch § 22 DSG M-V zu berücksichtigen. Hier wird in Abs. 2 verlangt, dass es nur berechtigten Personen - in der Regel den Administratoren - möglich sein darf, Änderungen an einem automatisierten Verfahren durchzuführen, und dass diese Änderungen protokolliert und kontrolliert werden müssen. Die Protokollierung dient dabei nicht nur einer Kontrolle der Einhaltung der Datenschutzvorschriften durch die Administratoren, vielmehr sollte sie auch als ein Schutzmechanismus angesehen werden, denn nur mit einer angemessenen Protokollierung können sich Administratoren vor unberechtigten Vorwürfen hinsichtlich eines Missbrauches ihrer administrativen Rechte schützen.

Für ein Dokumentenmanagementsystem, das perspektivisch ausschließlich elektronisch gespeicherte Akten verwalten soll, ist insbesondere die Anforderung des § 22 Abs. 4 DSG M-V relevant. Demnach ist bei einer ausschließlich automatischen Speicherung von personenbezogenen Daten zu protokollieren, wer wann und in welcher Weise die Daten gespeichert hat und ob sie verändert oder übermittelt wurden. Als Speicherdauer wird hierbei ein Jahr vorgesehen. Zudem ist auch bei der Protokollierung das Prinzip der Datensparsamkeit und Datenvermeidung umzusetzen. Ich berate das Finanzministerium auch zu diesen Aspekten, um eine ausgewogene und angemessene Protokollierungsmöglichkeit zu finden.

Erwähnenswert ist die Tatsache, dass vollständig darauf verzichtet wurde, dem Softwarehersteller einen Remotezugriff für Wartungs- und Reparaturzwecke zu gewähren. Ich habe im Rahmen meiner Kontroll- und Beratungstätigkeit wiederholt festgestellt, dass die Softwarehersteller in der Lage sind, per Fernwartung frei und oft auch ohne Kontrolle der verantwortlichen Stelle Wartungszugänge auf dem System zu benutzen. Dies hat zur Folge, dass sämtliche Echtdaten - darunter in der Regel auch personenbezogene Daten - einsehbar sind. Darüber hinaus besteht mit einem solchen Fernwartungstunnel das Risiko, dass nicht nur die Herstellerfirma Zugang zu IT-Systemen erhält *(siehe Kasten)*. Deshalb sollte auf die Nutzung von Echtdaten zur Fehlersuche grundsätzlich verzichtet werden und ein Verfahren gewählt werden, das sich an den Empfehlungen der Orientierungshilfe „Datenschutz und Datensicherheit in Projekten“ orientiert (siehe Punkt 2.14.8).

Unter einem Remotezugriff versteht man die Möglichkeit, auf einen entfernten Rechner zugreifen zu können, um diesen zu steuern oder seine Daten abzugreifen. Ein Remotezugriff kann entweder über ein lokales Netzwerk erfolgen oder einen weltweiten Zugriff über das Internet ermöglichen. Prinzipiell ist diese Möglichkeit des Zugriffs für eine Fernwartung gedacht, bei der technisches Personal aus der Distanz Wartungs- und Reparaturarbeiten an technischen Systemen durchführen kann. In der Regel findet diese Fernwartung über eine getunnelte Verbindung (Fernwartungstunnel) mit dem Ziel statt, dass nur der Ausgangs- und der Zielrechner auf die dazwischen übertragenen Daten zugreifen können.

2.14.3 Infrastruktur für elektronische Unterschriften (Landes-PKI)

Bereits mehrfach habe ich der Landesregierung nahegelegt, verstärkt elektronische Signaturen einzusetzen, zuletzt im Achten Tätigkeitsbericht, Punkt 2.15.2. Besonders interessant für E-Government-Verfahren und verwaltungsinterne Anwendungen sind hierbei die sogenannten qualifizierten Signaturen, denn Dokumente mit solchen Signaturen sind klassischen, handschriftlich unterschriebenen Dokumenten weitestgehend rechtlich gleichgestellt.

Sowohl Signatur als auch die Verschlüsselung von Daten erfordern in jeder größeren Anwendung eine Einrichtung, die das Erstellen, Beglaubigen, Verteilen und notfalls auch das Sperren von Schlüsselmaterial übernimmt. Diese Einrichtung heißt Public Key Infrastructure (PKI). Die Landesregierung hat grundsätzlich erkannt, wie wichtig PKIs sind, und sie deshalb in ihren E-Government-Masterplan (siehe Sechster Tätigkeitsbericht, Punkt 2.16.4) aufgenommen. Für einzelne Verfahren, wie das zentrale Melderegister (siehe Achter Tätigkeitsbericht, Punkt 2.4.2, und Siebter Tätigkeitsbericht, A.II.1.4), sind solche Strukturen auch schon vorhanden, jedoch kann der vorhandene Bedarf damit noch nicht gedeckt werden.

Beispielsweise setzt die neue EU-Dienstleistungsrichtlinie (siehe auch Punkt 2.1.8) ein sicheres elektronisches Antragswesen voraus. Die Richtlinie verlangt, dass alle Formalitäten für die Aufnahme und Ausübung von Dienstleistungstätigkeiten mit einem Einheitlichen Ansprechpartner abgewickelt werden können, und zwar auch auf elektronischem Wege. Hierbei müssen immer wieder sensible personenbezogene Daten kommuniziert werden. Daher sind ausreichende Vorkehrungen zum Schutz der Vertraulichkeit und Integrität zu schaffen. Dies ist aber ohne Signatur und Verschlüsselung praktisch undenkbar.

Auch das vom Finanzministerium betriebene Travel Management System (TMS, siehe zuletzt Achter Tätigkeitsbericht, Punkt 2.10.1) unterstützt immer noch keine qualifizierten elektronischen Signaturen. Landesbedienstete können Dokumente wie Dienstreiseanträge, Genehmigungen von Dienstreisen und Anträge auf Reisekostenerstattung nicht qualifiziert signieren. Rechtssicherheit ist deshalb nur gegeben, wenn die genannten Dokumente ausgedruckt, handschriftlich unterschrieben und in Papierform versandt und aufbewahrt werden.

Im Berichtszeitraum hat das Innenministerium die landeseigene DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH (DVZ M-V GmbH) mit dem Aufbau weiterer PKI-Dienste beauftragt. Diese werden jedoch vorrangig die sogenannten fortgeschrittenen elektronischen Signaturen unterstützen. Ich sehe dies als wichtigen Zwischenschritt an, erwarte aber, dass auch die qualifizierten Signaturen stärker berücksichtigt werden, da deren hoher Beweiswert für viele Verfahren unabdingbar ist.

Ich empfehle der Landesregierung erneut, ihre Beschlüsse zur Basiskomponente Signatur entschlossen umzusetzen und sich für eine stärkere Verbreitung der qualifizierten elektronischen Signatur einzusetzen. In Mecklenburg-Vorpommern sollte sie Anwendungen der qualifizierten elektronischen Signatur sowohl in der Verwaltung als auch in der Wirtschaft fördern.

2.14.4 IT-Management-System für die Landesverwaltung

E-Government und Verwaltungsmodernisierung führen zu einem stetig zunehmenden Einsatz von Informations- und Kommunikationstechnik in der Verwaltung des Landes. Die damit verbundene Abhängigkeit der Verwaltung vom reibungslosen Funktionieren dieser Technik erfordert ein wirksames Managementsystem für Fragen der IT-Sicherheit. Um die IT-Infrastruktur effizient verwalten und administrieren zu können, beschreibt der E-Government-Masterplan der Landesregierung (siehe Sechster Tätigkeitsbericht, Punkt 2.16.4) daher als ein wichtiges Handlungsfeld die Einrichtung einer einheitlichen gemeinsamen Managementumgebung mit den Komponenten Desktopmanagement, Netzwerkmanagement, Systemmanagement, Problemmanagement und Konfigurationsmanagement. Den engen Zusammenhang von IT-Sicherheits- und Datenschutzmanagement habe ich in meinem Achten Tätigkeitsbericht (siehe dort Punkt 2.15.5) ausführlich erläutert.

Vor diesem Hintergrund begrüße ich ausdrücklich die Bestrebungen der Landesregierung, gemeinsam mit dem IT-Landesdienstleister DVZ M-V GmbH eine umfassende Managementlösung zu schaffen.

Zu diesem Zweck wurde bereits im Jahr 2006 ein Projekt gestartet, mit dem unter Federführung des Innenministeriums eine landeseinheitliche Managementlösung entwickelt werden soll. Im November 2008 lag ein erstes, umfassendes Konzept vor, das die im IT-Service-Management zu betrachtenden Prozesse in folgende Kernbereiche unterteilt:

- operativer Bereich der Unterstützung von IT-Dienstleistungen (genannt „Service Support“) mit den Managementprozessen Störungs-, Problem-, Konfigurations-, Veränderungs- und Versionsmanagement,
- taktischer Bereich der Planung und Steuerung von IT-Dienstleistungen (genannt „Service Delivery“) mit den Managementprozessen Dienstgüte-, Finanz-, Kapazitäts-, Notfall- und Verfügbarkeitsmanagement.

Maßgeblich für die Optimierung und serviceorientierte Gestaltung von IT-Prozessen sollen die international anerkannten Richtlinien der sogenannten IT Infrastructure Library (ITIL) sein. Dass diese Richtlinien auch der Durchsetzung grundlegender Datenschutzstandards dienen und somit von den Datenschutzbeauftragten von Bund und Ländern ausdrücklich unterstützt werden, habe ich bereits im Achten Tätigkeitsbericht (siehe dort Punkt 5) im Zusammenhang mit den Aktivitäten des AK Technik erläutert.

Der E-Government-Masterplan führt das IT-Management-System zu Recht nicht als einzelnes E-Government-Projekt auf. Das Vorhaben ist tatsächlich von grundlegender Bedeutung für alle anderen Einzelprojekte. Ohne ordnungsgemäßes IT-Management ist der sichere Betrieb jedes einzelnen E-Government-Verfahrens gefährdet. Deshalb wäre es erforderlich, dieses Vorhaben vorrangig zu bearbeiten. Leider ist dies nicht der Fall.

Im September 2009 informierte das Innenministerium ausführlich über den Stand des Projektes „IT-Management-System“. Demnach konnte der Zeitplan des Projektes nicht eingehalten werden, da es erhebliche Probleme bei der Definition der Schnittstellen zwischen verschiedenen Systemkomponenten gab. Zudem waren zum damaligen Zeitpunkt noch nicht alle Anforderungen formuliert, die aus dem erforderlichen Zusammenspiel mit anderen Projekten wie der IP-Telefonie oder dem Corporate Network der Landesverwaltung resultieren. Damit konnten weder der geplante Pilotbetrieb im Innenministerium noch die Vorbereitung und Einführung weiterer Mandanten realisiert werden.

Ich begrüße daher insbesondere die Bemühungen der DVZ M-V GmbH, gemeinsam mit dem Innenministerium die Einrichtung eines einheitlichen IT-Management-Systems voranzutreiben, und biete auch weiterhin meine Unterstützung an.

Ich empfehle der Landesregierung, dem Projekt „IT-Management-System“ den erforderlichen Stellenwert beizumessen. Um die sichere und datenschutzgerechte Funktion der Informations- und Kommunikationstechnik gewährleisten zu können, muss unverzüglich ein IT-Management-System mit den oben beschriebenen Komponenten realisiert werden.

2.14.5 Datenschutzförderndes Identitätsmanagement

Die Menge personenbezogener Daten in öffentlichen und privaten Datenbanken steigt ständig. Moderne Informations- und Kommunikationstechnologie macht es immer einfacher, diese verteilt gespeicherten Daten miteinander zu verknüpfen und somit aussagekräftige Persönlichkeitsprofile Einzelner zu erstellen. Für die Verknüpfung verschiedener Datenbestände eignen sich Identifizierungsnummern, mit denen einzelne Datenbestände erschlossen werden. Derartige Nummern werden daher potenziell zu allgemeingültigen Personenkennzeichen. Ein solches Merkmal ist beispielsweise die Steuer-Identifikationsnummer (siehe Punkt 2.7.4 und Achter Tätigkeitsbericht, Punkt 2.5.1). Wenn Daten ohne entsprechende Rechtsgrundlage und ohne Wissen Betroffener verknüpft werden, ist das Recht auf informationelle Selbstbestimmung potenziell gefährdet. Deshalb sind Technologien erforderlich, die Betroffenen die Möglichkeit geben, in unterschiedlichen Umgebungen mit verschiedenen Identitäten (Pseudonymen) zu agieren. Bereits in ihrer Entschließung vom April 2008 (siehe Anlage 1.4) hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder auf diese Risiken hingewiesen und die Bundesregierung aufgefordert, den Einsatz datenschutzfördernder Identitätsmanagementsysteme voranzutreiben.

Mit der bundesweiten Einführung des neuen elektronischen Personalausweises (siehe Punkt 2.4.9) gewinnt das Thema Identitätsmanagement weiter an Bedeutung. Mit diesem Ausweis erhält jeder Bürger auch eine „elektronische Identität“. Damit ist nicht nur die Authentisierung jedes Ausweisinhabers gegenüber elektronischen Portalen der Verwaltung und der Wirtschaft möglich, sondern auch die Nutzung von E-Government- und E-Commerce-Verfahren unter verschiedenen Pseudonymen. Elektronische Identitäten sind mittlerweile der Schlüssel zur Teilnahme an der digitalen Welt. Die Möglichkeiten der pseudonymen Nutzung, die Gewährleistung von Datensparsamkeit und Datensicherheit sowie der Schutz vor Identitätsdiebstahl und Profilbildung sind wichtige Grundpfeiler moderner Informations- und Kommunikationstechnologien. Daher wird es immer wichtiger, Bürgerinnen und Bürgern Möglichkeiten zu einem selbstgesteuerten Identitätsmanagement anzubieten, das einfach bedienbar ist, dessen Funktionsweise für alle Beteiligten transparent ist, dessen Komponenten möglichst weitgehend standardisiert sind und dessen Technik von unabhängigen Dritten jederzeit vollständig nachprüfbar ist.

Anonymisierte oder pseudonymisierte Nutzung von elektronischen Verfahren und die dezentrale Haltung von Identifikationsdaten ist unter einer möglichst weitgehenden Kontrolle der Betroffenen möglich. Das zeigt das Arbeitspapier „Datenschutzförderndes Identitätsmanagement“, das von Mitgliedern des AK Technik (siehe Punkt 4) erarbeitet wurde und das die Auffassung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum Thema Identitätsmanagement widerspiegelt (abrufbar unter http://www.datenschutz-mv.de/dschutz/informat/idmgt/id-mgt.pdf). Das Papier beschreibt, wie man sich durch datenschutzförderndes Identitätsmanagement vor unangemessener Überwachung und Verknüpfung seiner Daten schützen kann, ohne dabei eine moderne und effektive Datenverarbeitung zu verhindern. Datenschutzfördernde Identitätsmanagementsysteme verhindern, dass unkontrolliert der Bezug zwischen einer elektronischen Identität und einer Person hergestellt werden kann.

Unter bestimmten, klar definierten Bedingungen kann mit Hilfe von Identitätsmanagementsystemen sichergestellt werden, dass ein Pseudonym bei Bedarf bezogen auf einen bestimmten Zweck (z. B. Besteuerung) einer Person zugeordnet werden kann.

Ich empfehle der Landesregierung, insbesondere bei der Entwicklung und beim Betrieb moderner E-Government-Verfahren, die Grundsätze der Datensparsamkeit und der Datenvermeidung zu beachten und den Einsatz datenschutzfördernder Identitätsmanagementsysteme voranzutreiben.

2.14.6 Umgang mit IP-Adressen, IP-Anonymisierung

Grundsätzlich gilt, dass der beste Datenschutz erreicht wird, wenn möglichst wenig oder im Idealfall keine personenbezogenen Daten erhoben, verarbeitet oder genutzt werden. Dieser Grundsatz spiegelt sich im Landesdatenschutzgesetz wieder, das in § 5 Absatz 1 größtmögliche Datenvermeidung bei der Gestaltung von Verfahren und bei der Auswahl von informationstechnischen Produkten zum Einsatz in automatisierten Verfahren fordert. Denn wo keine personenbezogenen Daten vorhanden sind, ist auch kein Missbrauch zu befürchten.

Regelmäßig erreichen mich Anfragen von Kommunen, Behörden oder Bürgern bezüglich der Speicherung der IP-Adresse im Zusammenhang mit dem Webseitenauftritt. Prinzipiell steht jeder Webseitenbetreiber vor dem Problem, dass sein Webserver in Abhängigkeit von der Konfiguration eine Vielzahl unterschiedlichster Protokolle erzeugen kann. Diese Protokolle erhalten Informationen wie die aufgerufenen Webseiten oder den Browsertyp und das Betriebssystem, das für den Besuch verwendet wurde, und in der Regel auch die IP-Adresse, mit welcher der Nutzer die entsprechende Seite aufgerufen hat. Gemäß § 15 Telemediengesetz (TMG) ist die Protokollierung personenbezogener Daten des Nutzers jedoch nur zulässig, sofern dies für eine Abrechnung notwendig ist. Weitergehende Nutzungsprofile dürfen nur unter Verwendung von Pseudonymen erstellt werden. Die Aufsichtsbehörden für den nichtöffentlichen Bereich haben in ihrem Beschluss vom November 2009 ausdrücklich darauf hingewiesen, dass IP-Adressen keine Pseudonyme im Sinne des TMG sind (siehe Anlage 2.12). Da die Protokoll-Dateien jedoch tatsächlich für viele nützliche Zwecke, wie statistische Auswertungen oder für Fehlerdiagnosen eingesetzt werden können, ist also eine Anonymisierung in der Form notwendig, dass der Personenbezug schon vor dem Ablegen im Protokoll entfernt wird.

Im Auftrag des Sächsischen Datenschutzbeauftragten entwickelte ein Dresdener IT-Systemhaus ein Softwaremodul (abrufbar unter: http://www.saechsdsb.de/ipmask) für die beiden gängigsten Webserver, den Apache und Microsoft Internet Information Server, welches automatisch eine solche Anonymisierung der IP-Adresse vornimmt. Standardmäßig wird hierbei die letzte Zahl der vierteiligen IP-Adresse durch eine 0 ersetzt. So bleibt die IP-Adresse anonymisiert im Protokoll erhalten und kann weiterhin von den gängigen Statistik Programmen für eine Auswertung des Webangebots herangezogen werden.

Ich empfehle der Landesregierung, die öffentlichen Stellen des Landes für eine datenschutzgerechte Ausgestaltung der Webseitenprotokollierung mit entsprechender Anonymisierung zu sensibilisieren.

2.14.7 Das Bürgerportalgesetz

E-Mails sind zu einem Massenkommunikationsmittel geworden, das sowohl im privaten Umfeld als auch bei der Kommunikation mit Behörden und Unternehmen immer mehr genutzt wird. Ohne zusätzliche Sicherungsmaßnahmen gleicht eine E-Mail jedoch einer mit Bleistift geschriebenen Postkarte, die problemlos von Unbefugten lesbar ist und bei der sehr leicht Absenderangaben gefälscht werden können. Sender und Empfänger können daher nie sicher sein, mit wem sie tatsächlich kommunizieren.

Vor diesem Hintergrund hat das Bundeskabinett im Februar 2009 den Entwurf eines Bürgerportalgesetzes verabschiedet. Er sah vor, dass private Anbieter Portale betreiben sollen, über die der von der Bundesregierung als sicher bezeichnete E-Mail-Verkehr „De-Mail“ und zusätzlich eine sichere Dokumentenablage „De-Safe“ sowie ein Identitätsbescheinigungsdienst abgewickelt werden sollen. Ziel war es, die elektronische Kommunikation im Rechts- und Geschäftsverkehr voranzubringen und die Funktionsfähigkeit und Akzeptanz der elektronischen Kommunikation trotz steigender Internetkriminalität und wachsender Datenschutzprobleme zu erhalten und auszubauen.

Den hohen Datenschutzanforderungen an ein solches Vorhaben wurde der Gesetzentwurf jedoch nicht gerecht. In ihrer Entschließung vom 16. April 2009 (siehe Anlage 1.24) verlangten die Datenschutzbeauftragten von Bund und Ländern daher grundlegende Korrekturen. Beispielsweise forderten sie, die Kommunikation zwischen Absender und Empfänger standardmäßig durch eine Ende-zu-Ende-Verschlüsselung nach dem Stand der Technik zu sichern und im Gesetz nicht nur als Option anzubieten. Förmliche Zustellungen auf elektronischem Wege mit den entsprechenden Rechtsfolgen dürften zudem nur auf Basis einer sicheren Anmeldung erfolgen. Die nach der Gesetzesbegründung ebenfalls mögliche unsichere Anmeldung mit Passwort lehnten sie ab. Zudem forderten die Datenschutzbeauftragten, Nutzerinnen und Nutzer bei der Eröffnung des Bürgerportalkontos auf mögliche Rechtsfolgen - etwa zur verbindlichen Kommunikation mit staatlichen Stellen - hinzuweisen. Die Aufklärungs- und Informationspflichten müssten im Gesetzestext klarer gefasst werden. Da nur akkreditierte Anbieter Portale betreiben dürfen, wurde zudem gefordert, dass die Akkreditierung nicht allein vom Nachweis der technischen und administrativen Sicherheit, sondern auch von der Einhaltung datenschutzrechtlicher Standards abhängig gemacht werden muss. Die dabei zu erfüllenden Mindestanforderungen müssten verbindlich im Gesetz vorgegeben werden.

Der Bundesrat schloss sich der Kritik der Datenschutzbeauftragten an und hielt den Gesetzentwurf für so unzureichend, dass er ihn vollständig ablehnte (BR-Drs. 174/1/09 vom 23. März 2009).

Nicht zuletzt wegen der vielen ungeklärten Fragen hat die Bundesregierung den Gesetzentwurf in der 16. Wahlperiode bis zu den Neuwahlen im September 2009 nicht mehr verabschiedet. Die neugewählte Bundesregierung hat sich jedoch im Koalitionsvertrag vom 25. Oktober 2009 wie folgt positioniert: „Wir werden ein De-Mail-Gesetz verabschieden und dabei die Erfahrungen aus dem Pilotprojekt und die Stellungnahmen der Datenschutzbeauftragten des Bundes und der Länder berücksichtigen.“

Ich empfehle der Landesregierung, sich dafür einzusetzen, dass die Kritikpunkte der Datenschutzbeauftragten von Bund und Ländern am Entwurf des Bürgerportalgesetzes bei der Ausgestaltung des De-Mail-Gesetzes berücksichtigt werden.

2.14.8 Empfehlungen zur datenschutzgerechten Modernisierung der öffentlichen Verwaltung

Die Modernisierung der öffentlichen Verwaltung ist ein zentrales Ziel der Landesregierung Mecklenburg-Vorpommerns. Die Strategie hierfür hat die Landesregierung im E-Government-Masterplan veröffentlicht, welcher bereits im Jahr 2004 vom Kabinett beschlossen wurde. Für alle der 75 potentiellen E-Government-Projekte besteht ein erheblicher Beratungsbedarf zu Fragen der IT-Sicherheit und des Datenschutzes (siehe Sechster Tätigkeitsbericht, Punkt 2.16.4).

In allen Bundesländern gibt es vergleichbare E-Government-Vorhaben mit sehr ähnlichen Anforderungen an Datenschutz und Datensicherheit. Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ (AK Technik), der unter meinem Vorsitz als Gremium der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zweimal im Jahr tagt (siehe Punkt 4), hat es sich zu einer zentralen Aufgabe gemacht, bundesweit einheitliche Empfehlungen zu solchen E-Government-Projekten auszusprechen, um in allen Bundesländern ein vergleichbar hohes Datenschutz- und IT-Sicherheitsniveau zu gewährleisten. Zu diesem Zweck erarbeitet und veröffentlicht der AK Technik regelmäßig sogenannte Orientierungshilfen zu verschiedenen Themen aus der Praxis bzw. aktualisiert vorhandene Unterlagen. Die folgenden Punkte zeigen beispielhaft, welche Themen im Berichtszeitraum bearbeitet wurden.

Datenschutz im Projekt- und Produktivbetrieb

Im Rahmen der Einführung neuer IT-Systeme zeigen sich regelmäßig Unklarheiten, wie unterschiedliche Phasen der Entwicklung und Einführung von IT-Verfahren bezeichnet werden sollten (etwa Testbetrieb, Pilotbetrieb, Projektbetrieb, Echtbetrieb) und ob bzw. unter welchen Voraussetzungen personenbezogene Daten verarbeitet werden dürfen. Zu welchen Problemen die unterschiedliche Interpretation solcher Begriffe führen kann, habe ich beispielsweise im Achten Tätigkeitsbericht, Punkt 2.3.1 (Papierloses Arbeiten beim Verfassungsschutz) beschrieben.

In der Orientierungshilfe „Datenschutz und Datensicherheit in Projekten: Projekt- und Produktivbetrieb“ (abrufbar unter http://www.datenschutz-mv.de/dschutz/informat/projekt/oh_projekt.pdf) werden die verschiedenen Phasen der Verfahrensentwicklung aus datenschutzrechtlicher Sicht beschrieben. Der Begriff **Projektbetrieb** beschreibt die erste Phase, die aus Funktions-, Integrations- und Abnahmetest besteht. Die zweite Phase wird als **Produktivbetrieb** bezeichnet und umfasst den Pilotbetrieb und den anschließenden Regelbetrieb. Die Orientierungshilfe stellt klar, dass personenbezogene Daten, die möglicherweise schon während der Verfahrenseinführung verarbeitet werden, nicht weniger schutzbedürftig sind als bei der Verarbeitung im Regelbetrieb. Die Regelungen der Datenschutzgesetze von Bund und Ländern gelten für die Verarbeitung personenbezogener Daten ungeachtet der Frage, ob die Daten bereits im Regelbetrieb oder noch in einer früheren Projektphase verarbeitet werden.

In der Orientierungshilfe wird für jede der Phasen erläutert, ob bzw. unter welchen Umständen personenbezogene Daten verarbeitet werden dürfen. Die jeweils erforderlichen organisatorischen und technischen Maßnahmen werden ausführlich beschrieben. Zu nennen sind etwa eine ausreichende Protokollierung von Zugriffen, ggf. auch die Anonymisierung von Echtdaten, beschränkter Zugang zu den verwendeten Daten sowie eine revisionssichere Dokumentation.

Schließlich wird darauf hingewiesen, dass ein Sicherheitskonzept und die schriftliche Freigabe des Verfahrens für alle Phasen der Verfahrensentwicklung und -einführung erforderlich sind, in denen personenbezogene Daten verarbeitet werden.

Datenschutzgerechte Protokollierung

Schon bei der Planung und der Einführung neuer IT-Systeme taucht regelmäßig die Frage auf, welche Aktivitäten von Nutzern und Administratoren in welchem Umfang zu protokollieren sind, um den Anforderungen insbesondere der Datenschutzgesetze von Bund und Ländern an die sogenannte Revisionsfähigkeit (siehe Kasten 1) zu genügen.

Sowohl das Landes- als auch das Bundesdatenschutzgesetz enthalten Regelungen, aus denen sich eine Pflicht zur Protokollierung ergibt oder zumindest ableiten lässt. Zudem gelten für eine Reihe von Verwaltungsverfahren oft wesentlich konkretere, bereichsspezifische Protokollierungsvorschriften, die vom Datenschutzrecht des Bundes und des Landes abweichen (etwa in Meldegesetzen, Polizeigesetzen, Verfassungsschutzgesetzen). Dennoch gibt es nur wenige Vorgaben für die konkrete Ausgestaltung der Protokollierung. Gleichwohl haben sich auf Basis der Anforderungen inzwischen erprobte, datenschutzgerechte Vorgehensweisen entwickelt. Diese Vorgehensweisen werden in der Orientierungshilfe Protokollierung (abrufbar unter: http://www.datenschutz-mv.de/dschutz/informat/protokol/oh-proto.pdf) aufgegriffen und zur Umsetzung empfohlen.

Die Orientierungshilfe erläutert zunächst einige Datenschutzgrundsätze der Protokollierung. Der Zweck der Protokollierung besteht darin, ein Verfahren zur Verarbeitung personenbezogener Daten so transparent zu machen, dass die Ordnungsmäßigkeit bzw. ein Verstoß gegen die Ordnungsmäßigkeit einer Verarbeitung personenbezogener Daten nachweisbar ist. Die Protokolldaten müssen darüber Auskunft geben können, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat. Allerdings muss schon bei der Konzeption von Protokollierungsverfahren und insbesondere bei der Nutzung von Protokolldaten der Grundsatz der Zweckbindung beachtet werden (vgl. § 31 BDSG, § 10 Abs. 6 DSG M-V). Die Protokollierung dient allein dem Zweck der Aufrechterhaltung von Datenschutz und Datensicherheit und darf daher nicht für eine Verhaltens- und Leistungskontrolle der Beschäftigten genutzt werden. Für die Gestaltung der Protokollierungsverfahren gilt zudem der Grundsatz der Erforderlichkeit. Art und Umfang der Protokollierung sowie die Dauer der Speicherung sind auf das zur Erfüllung des Protokollierungszwecks erforderliche Maß zu beschränken. Für die technische Ausgestaltung und Auswahl der Verfahren der Protokollierung ist das Gebot der Datensparsamkeit und Datenvermeidung zu befolgen. Erfahrungsgemäß besteht jedoch immer ein Zielwiderspruch zwischen der Vollständigkeit und der Datensparsamkeit. Zur Lösung dieses Konfliktes gibt es kein Patentrezept. Vor dem Hintergrund der verfahrensspezifischen Bedingungen muss in jedem Einzelfall versucht werden, den Konflikt so weit aufzulösen, dass ein bestmöglicher Ausgleich der Ziele erreicht wird.

Die Orientierungshilfe erläutert ausführlich die datenschutzrelevanten Unterschiede der Protokollierung von administrativen Tätigkeiten und Nutzeraktivitäten und beschreibt die aus datenschutzrechtlicher Sicht erforderlichen Inhalte und Formate. Abschließend werden technische und organisatorische Aspekte bei der Erzeugung, Übertragung, Speicherung, Auswertung und Löschung von Protokolldaten beleuchtet.

Biometrische Authentisierung

Regelmäßig erreichen mich Fragen zur Zulässigkeit von biometrischen Verfahren zur Authentisierung von Personen (siehe Kasten 2). Mitunter soll beispielsweise eine biometrische Authentisierung herkömmliche Zugangskontrollen oder konventionelle Anmeldeverfahren an IT-Systemen ersetzen. In der Orientierungshilfe zum Thema „Biometrische Authentisierung - Möglichkeiten und Grenzen“ (abrufbar unter: http://www.datenschutz-mv.de/dschutz/informat/biometrie/oh-biometrie.pdf) werden zunächst einige Grundprinzipien biometrischer Verfahren sowie die Unterschiede zwischen der biometrischen Authentisierung und der Authentisierung, die nach dem Prinzip „Besitz und/oder Wissen“ funktioniert, erläutert.

Besonders wird darauf hingewiesen, dass biometrische Daten im Gegensatz zu einer UserID eindeutig und potenziell lebenslang mit dem Betroffenen verbunden sind. Deshalb müssen biometrische Daten besonders geschützt werden und deren Zusammenführung mit anderen Identitätsdaten darf nur unter genau definierten Bedingungen möglich sein. Der Schutz des Speichersystems der biometrischen Referenzdaten ist für Datensicherheit und Datenschutz des Verfahrens deshalb von grundlegender Bedeutung. Es wird empfohlen, die für den Vergleich erforderlichen Referenzdaten keinesfalls zentral zu speichern, sondern eine dezentrale Speicherung, z. B. auf einer Chipkarte, vorzuziehen. Speicherung und Übertragung der biometrischen Daten müssen gegen Abhören, unbefugte Offenbarung und Modifikation geschützt werden. Dies erfordert den Einsatz kryptographischer Verfahren. Es ist zudem ratsam, biometrische Daten nicht allein zur Authentisierung heranzuziehen, sondern sie mit sperr- und veränderbaren Daten wie Besitz und Wissen wirksam zu koppeln.

Nutzung des Internet am Arbeitsplatz

Seit vielen Jahren stellen die Datenschutzbeauftragten des Bundes und der Länder mit der „Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet“ (abrufbar unter: http://www.datenschutz-mv.de/dschutz/informat/internet/oh-internet.pdf) ein Hilfsmittel für die datenschutzgerechte Konzeption und den Betrieb von Netzen der öffentlichen Verwaltung, die an das Internet angeschlossen werden sollen, zur Verfügung. Den Verantwortlichen soll deutlich gemacht werden, mit welchen Risiken für die Sicherheit der „internen“ Netze bei einem Anschluss an das Internet zu rechnen ist und wie diese Risiken begrenzt werden können.

Ein PC-Arbeitsplatz der öffentlichen Verwaltung ohne Internetzugang ist kaum noch vorstellbar. Das Internet wird von der öffentlichen Verwaltung nicht mehr nur als Plattform für die Präsentation von Informationen und Dienstleistungen genutzt, sondern in zunehmendem Maße auch als Informationsmedium und Kommunikationsplattform für eigene Zwecke. Dabei hat sich nichts an der Grundaussage geändert, dass der Anschluss an das Internet nach wie vor mit erheblichen Gefährdungen des Datenschutzes und der Datensicherheit verbunden ist. Die Rechner und Übertragungswege dieses weltweiten Computernetzes sind nicht kontrollierbar. Welchen Weg eine Nachricht nimmt oder in welchem Vermittlungsrechner die Nachricht bearbeitet wird, ist für den Endnutzer nicht transparent, geschweige denn beeinflussbar.

Vor diesem Hintergrund und mit Blick auf die rasante technische Entwicklung in diesem Bereich wurde die Orientierungshilfe im AK Technik umfassend überarbeitet und aktualisiert. In der Orientierungshilfe wurden die Empfehlungen zum Einsatz von sogenannten Sicherheitsgateways vollständig überarbeitet und detaillierte Hinweise zu virtuellen privaten Netzen (VPN) und zum Virenschutz eingearbeitet. Zudem werden verschiedene Anti-Spam-Strategien vorgestellt und empfehlenswerte Zusatzmaßnahmen für die Verarbeitung sensibler Daten erläutert. Sehr detailliert befasst sich die Orientierungshilfe nun auch mit Fragen der Zulässigkeit von Protokollierung und Inhaltskontrolle mittels einer Firewall. Dabei wird insbesondere auf die Bestimmungen des Telekommunikationsgesetzes (TKG) und des Telemediengesetzes (TMG) bzw. des Rundfunkstaatsvertrages (RStV) eingegangen. Schließlich wird erläutert, welche zusätzlichen Regelungen der Arbeitgeber oder Dienstherr beachten muss, wenn er auch die private Nutzung des Internet-Zuganges oder des E-Mail-Dienstes zulässt.

Ich empfehle der Landesregierung, die Kernaussagen der Orientierungshilfen des AK Technik in ihre entsprechenden Planungsgrundsätze, etwa das IT-Sicherheitsrahmen-Konzept der Landesverwaltung, zu übernehmen und somit verbindlich einzuführen.

Regelungen des Landesdatenschutzgesetzes zur Revisionsfähigkeit:

§ 21 Allgemeine Maßnahmen zur Datensicherheit
(1) Die Ausführung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz ist durch technische und organisatorische Maßnahmen sicherzustellen, die nach dem Stand der Technik und nach der Schutzbedürftigkeit der zu verarbeitenden Daten erforderlich und angemessen sind.
(2) Dabei ist insbesondere zu gewährleisten, dass
...
5. unter Beteiligung der Personal- oder Arbeitnehmervertretung von der Daten verarbeitenden Stelle ein Protokollierungsverfahren festgelegt wird, das die Feststellung erlaubt, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit) ...

§ 22 Besondere Maßnahmen zur Datensicherheit beim Einsatz automatisierter Verfahren
(2) Zugriffe, mit denen Änderungen an automatisierten Verfahren bewirkt werden können, dürfen nur den dazu ausdrücklich berechtigten Personen möglich sein. Die Zugriffe dieser Personen sind zu protokollieren und zu kontrollieren.
(4) Sollen personenbezogene Daten ausschließlich automatisiert gespeichert werden, ist zu protokollieren, wann, durch wen und in welcher Weise die Daten gespeichert wurden. Entsprechendes gilt für die Veränderung und Übermittlung der Daten. Die Protokollbestände sind ein Jahr zu speichern. Es ist sicherzustellen, dass die Verfahren und Geräte, mit denen die gespeicherten Daten lesbar gemacht werden können, verfügbar sind.

Authentisierung
Die Authentifizierung ist die Prüfung, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Sie ist in jedem informationstechnischen System, mit dem schutzbedürftige Daten verarbeitet werden, unerlässlich. Die Authentisierung ist dabei der Teilschritt, den der Kommunikationspartner durchführt, nämlich die Vorlage eines Nachweises, in dem seine Identität bestätigt wird. Beispiele hierfür sind die Eingabe eines Passworts oder das Auflegen eines Fingers auf einen Fingerabdruckleser.

Authentisierung durch Besitz und Wissen
Die Authentisierung durch Besitz und Wissen ist eine Zwei-Faktor-Authentisierung. Sie verlangt vom Kommunikationspartner die Kenntnis eines Geheimnisses (z. B. Passwort oder PIN) und den Besitz eines Gegenstandes (z. B. Chipkarte oder TAN-Liste). Die Kombination beider Authentisierungsmethoden erhöht die Sicherheit, da Unbefugte sowohl das Geheimnis erfahren als auch den Gegenstand finden oder stehlen müssen, um eine erfolgreiche Authentifikation durchführen zu können.

Biometrische Authentisierung
Die biometrische Authentisierung ist die Authentisierung mit einem unverwechselbaren körperlichen Merkmal. Geeignete Merkmale sind beispielsweise Fingerabdrücke, die Unterschrift, das Gesichtsbild oder die Stimme. Die Merkmale eines Menschen werden mit einem passenden Sensor erfasst (wie Fingerabdruckleser, berührungsempfindliches Display, Kamera, Mikrofon). Im weiteren Verlauf werden die so gewonnenen Daten mit einem bereits gespeicherten Referenzmuster verglichen. Das Ergebnis ist nie die vollständige Übereinstimmung, sondern immer ein Wahrscheinlichkeitswert.

2.14.9 Broschüre der GDD: „Datenschutzgerechte Datenträgerentsorgung nach dem Stand der Technik“

Die Gesellschaft für Datenschutz und Datensicherung e. V. (GDD) ist einer der großen Datenschutz-Fachverbände in Deutschland, in dem sich Personen und Unternehmen zusammengeschlossen haben, die sich mit Fragen des Datenschutzes beschäftigen. Mitglieder der GDD sind unter anderem betriebliche Datenschutzbeauftragte, freiberufliche Datenschutzexperten und Fachbetriebe. Im Rahmen der 50. Sitzung des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ (siehe Punkt 4) hatte die GDD eine intensivere Zusammenarbeit mit dem Arbeitskreis angeregt.

Im Jahr 2008 trat die GDD an mich heran mit der Bitte um Unterstützung bei der Überarbeitung ihrer Broschüre zur Datenträgerentsorgung. Diesem Ansinnen bin ich gern nachgekommen, denn auch mich erreichen immer wieder Anfragen zu diesem Thema (siehe Achter Tätigkeitsbericht, Punkt 2.8.10).

Die Broschüre „Datenschutzgerechte Datenträgerentsorgung nach dem Stand der Technik“ richtet sich an Entscheidungsträger und Datenschutzbeauftragte in Wirtschaft und Verwaltung. Die Datenträgerentsorgung wird als Prozess beschrieben und anhand von Schutzklassen differenziert. Anhand umfangreicher Checklisten können die Nutzer der Broschüre Maßnahmekataloge und Bausteine für Sicherheitskonzepte erstellen, die jeweils auf die Bedürfnisse ihrer Organisation zugeschnitten sind.

Neben vielen Verbesserungen im Detail enthält die neue Auflage erstmals spezielle Kapitel zur Zertifizierung und zur Datenträgerentsorgung im Ausland. Außerdem gibt es einen neuen Abschnitt für Berufsgruppen und Institutionen, die besonderen Berufs- und Amtsgeheimnissen unterliegen, beispielsweise Angehörige von Heilberufen, Rechtsanwälte, Notare und Steuerberater sowie Bedienstete der Steuer- und der Sozialverwaltung.

Im Jahr 2009 hat die GDD die neu bearbeitete und erweiterte zweite Auflage der Broschüre „Datenschutzgerechte Datenträgerentsorgung nach dem Stand der Technik“ herausgegeben. Die Broschüre ist inzwischen im Datakontext-Verlag erschienen.

3. Nichtöffentlicher Bereich

3.1 Einführung zum 4. Tätigkeitsbericht nicht-öffentlicher Bereich gem. § 38 Abs. 1 BDSG

Im Rahmen meiner Zuständigkeit als Aufsichtsbehörde für den nicht-öffentlichen Bereich lege ich dem Landtag und der Landesregierung den Bericht über die Tätigkeit der Aufsichtsbehörde vor, der den Zeitraum vom 1. Januar 2008 bis zum 31. Dezember 2009 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 Abs. 1 BDSG in nationales Recht übernommen.

Im Rahmen ihrer Prüfungstätigkeit kann die Aufsichtsbehörde nach § 38 BDSG Auskünfte verlangen, Geschäftsräume zur Prüfung betreten, Einsicht in Unterlagen nehmen und Maßnahmen zur Beseitigung festgestellter Verstöße bei der Verarbeitung personenbezogener Daten oder bei technischen und organisatorischen Mängeln anordnen. Bei schwerwiegenden Verstößen oder Mängeln, die trotz Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden, kann sie die Erhebung, Verarbeitung und Nutzung beziehungsweise den Einsatz einzelner Verfahren untersagen. Die Aufsichtsbehörde klärt im Rahmen ihrer Möglichkeiten den Sachverhalt auf und nimmt eine rechtliche Bewertung vor, aufgrund derer die betroffenen Unternehmen und Betriebe in einem Großteil der Fälle die jeweils beanstandete Datenerhebung bzw. -verarbeitung so umgestalten, dass sie den rechtlichen Vorgaben des Bundesdatenschutzgesetzes gerecht werden. Gleichzeitig kann die Stellungnahme der Aufsichtsbehörde vom Petenten gegebenenfalls auch in gerichtlichen Verfahren - ähnlich wie ein Gutachten - verwendet werden. Falls eine unzulässige Datenverarbeitung vorliegt, besteht die Möglichkeit, ein Ordnungswidrigkeitsverfahren einzuleiten (§ 43 BDSG) oder - in besonders schwerwiegenden Fällen - Strafantrag zu stellen (§ 44 Abs. 2 BDSG).

Nach § 38 Abs. 1 i. V. m. § 21 Abs. 1 Satz 1 BDSG besteht für jedermann die Möglichkeit, sich an mich zu wenden, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch nicht-öffentliche Stellen (Unternehmen und Betriebe) in seinen Rechten verletzt worden zu sein. Die Anfragen und Petitionen im Berichtszeitraum umfassten das gesamte Spektrum der datenschutzrechtlichen Fragen der Unternehmen einschließlich arbeitnehmerdatenschutzrechtlicher Fragen. Dabei zeichnete sich - neben dem Bereich Auskunfteien - ein gewisser Schwerpunkt bei den Bereichen Adresshandel/Werbung und Videoüberwachung ab.

Dies stand auch im Zusammenhang mit der Kette von Skandalfällen des illegalen Handels mit Adress- und Bankverbindungsdaten, die seit Herbst 2008 aufgedeckt wurden und zu umfangreichen Ermittlungen u. a. auch der Staatsanwaltschaften geführt haben. Bedauerlicher Weise wurde eine seitens des ehemaligen Bundesinnenministers angekündigte Änderung des Bundesdatenschutzgesetzes während des Gesetzgebungsverfahrens durch eine Vielzahl von Ausnahmeregelungen zugunsten der Werbewirtschaft in ihrem Schutzzweck gegenüber den betroffenen Bürgern stark aufgeweicht (siehe auch Punkt 3.2).

Einen Schwerpunkt im Jahre 2008 bildete die Aufklärung und Sanktionierung im Fall eines großen Discounters, der bundesweit seine Mitarbeiter systematisch durch Detekteien und andere Sicherheitsunternehmen - teilweise unter Einsatz von Videotechnik - überwachen ließ. Da diese Überwachungsmaßnahmen durch rechtlich selbständige Vertriebsgesellschaften der Discounterkette in den jeweiligen Bundesländern in Auftrag gegeben worden waren, habe ich - wie auch die Aufsichtsbehörden der übrigen betroffenen Bundesländer - gegen die in Mecklenburg-Vorpommern ansässige Vertriebsgesellschaft des Unternehmens ein umfassendes Überprüfungsverfahren eingeleitet und nach umfangreichen Ermittlungen mit dem Erlass eines Bußgeldbescheides in beträchtlicher Höhe abgeschlossen (siehe auch Punkt 3.8).

Schwerpunkt war auch die Übernahme des Vorsitzes im sogenannten Düsseldorfer Kreis durch Mecklenburg-Vorpommern für das Jahr 2009. Der Düsseldorfer Kreis bildet das Koordinations- und Beschlussgremium der obersten Datenschutzaufsichtsbehörden der Länder und des Bundes zur länderübergreifenden Abstimmung der wichtigsten Fachfragen der Datenschutzaufsicht im Unternehmensbereich. Die in diesem Zeitraum gefassten Beschlüsse des Düsseldorfer Kreises sind unter Punkt 7 zu finden.

Einen weiteren Schwerpunkt bildete im Frühjahr 2009 die seitens der Firma Google beabsichtigte Einführung des Systems „Google Streetview“ (siehe auch Punkt 3.11).

Im Berichtszeitraum verstärkt wurde der Bereich der Datenschutz-Schulung, insbesondere für betriebliche Datenschutzbeauftragte von Unternehmen im Lande. In diesem Zusammenhang haben Mitarbeiter meiner Behörde zahlreiche datenschutzrechtliche und datensicherheitstechnische Seminare und Schulungsveranstaltungen (u. a. in Zusammenarbeit mit der Industrie- und Handelskammer zu Schwerin), aber auch Blockseminare an verschiedenen Hochschulen und Universitäten des Landes durchgeführt. Zum laufenden Tagesgeschäft zählen Einzelberatungen von Betrieben und Unternehmen zur gesamten Palette datenschutzrechtlicher und datensicherheitstechnischer Fragen im Unternehmensbereich.

Zusammenfassend lässt sich für den Berichtszeitraum 2008/2009 eine erhebliche Zunahme an Datenschutzskandalen im Unternehmensbereich verzeichnen. Im Gegensatz zu früheren Jahren, in denen der Datenschutz in Unternehmen auch bei den Medien eher eine Randposition einnahm, vergeht nunmehr kaum ein Quartal ohne umfangreiche Medienberichte über illegale Überwachung von Unternehmensmitarbeitern, millionenfachen illegalen Handel von Bankverbindungsdaten, unrechtmäßiges Ausspionieren von E-Mail-Kontakten eigener Mitarbeiter, illegalen Einsatz von Videoüberwachung etc.

Die wachsende Aufmerksamkeit für den Datenschutz in Unternehmen spiegelt sich wider im ansteigenden Beratungs- und Kontrollbedarf durch die Datenschutzaufsichtsbehörden. Die beschriebene Entwicklung hat deshalb konsequenterweise in einigen Bundesländern bereits zu einer erheblichen personellen Aufstockung der Datenschutzaufsichtsbehörden geführt. Mecklenburg-Vorpommern hat sich bisher dieser Entwicklung nicht angeschlossen. Ich appelliere daher an die Landesregierung, den begrüßenswerten Plädoyers und Appellen für die Verhinderung von Datenschutzskandalen Taten folgen zu lassen und das Stellenkonzept meiner Behörde dem rasch steigenden Kontroll- und Beratungsbedarf zügig anzupassen.

3.2 Gesetz zur Änderung des Bundesdatenschutzgesetzes - BDSG-Novelle II

Nachsicht bei Werbung, Stärkung der betrieblichen Datenschutzbeauftragten

Seit Herbst 2008 häuften sich Presseberichte über Fälle des illegalen Handels mit sensiblen personenbezogenen Daten - insbesondere Kontoverbindungsdaten (über 1 Mio. Datensätze). Es kam in diesem Zusammenhang zu zahlreichen Betrugsfällen, bei denen von den Konten der Betroffenen (meist unter Vorspiegelung angeblich telefonisch abgeschlossener Lottoteilnahmeverträge) Beträge ohne Rechtsgrundlage abgebucht worden waren.

Daraufhin kündigte der damalige Bundesinnenminister in einem Spitzengespräch am 4. September 2008 (sog. „Datenschutzgipfel“) Änderungen im Bundesdatenschutzgesetz mit dem Ziel an, die Weitergabe von personenbezogenen Daten für Werbezwecke ausschließlich von der Einwilligung der jeweiligen Betroffenen abhängig machen zu wollen.

Die dann am 1. September 2009 in Kraft getretene Änderung des Bundesdatenschutzgesetzes („BDSG-Novelle II“) wurde dieser Ankündigung allerdings nicht gerecht. Die Regelung in § 28 Abs. 3 BDSG ist vielmehr nach intensiver Lobbyarbeit, insbesondere der Werbewirtschaft, durch zahlreiche Ausnahmeregelungen zugunsten des Adresshandels erheblich aufgeweicht und zusätzlich durch eine Übergangsregelung abgeschwächt worden.

Personenbezogene Daten dürfen nunmehr zwar im Grundsatz nur mit Einwilligung der Betroffenen genutzt werden - die Ausnahmen, das sogenannte Listenprivileg (Verwendung von Name, Berufs-, Branchen- oder Geschäftsbezeichnung, Titel, Geburtsjahr, akademischer Grad sowie eines Merkmales zu einer Gruppenzugehörigkeit), gelten jedoch nach § 28 Abs. 3 BDSG weiter in den Bereichen der Werbung für eigene Zwecke, der Werbung im Hinblick auf die berufliche Tätigkeit des Betroffenen, bei Werbung für steuerbegünstigte Spenden, Beipackwerbung etc. Zusätzlich wurde mit § 47 BDSG eine für die Werbebranche großzügige Übergangsregelung eingeführt, nach der personenbezogene Werbedaten, die vor dem 1. September 2009 erhoben oder gespeichert wurden, für Zwecke der Werbung noch bis zum 31. August 2012 weiter nach der alten gesetzlichen Regelung behandelt werden. Diese rechtliche Privilegierung setzt allerdings voraus, dass der Zeitpunkt der erstmaligen Speicherung nachgewiesen werden kann.

Begrüßenswert sind demgegenüber die Neuregelungen zur Stärkung der Rechtsstellung des betrieblichen Datenschutzbeauftragten, die detaillierteren Anforderungen an die Auftragsdatenverarbeitung (§ 11 BDSG), eine Regelung für die Erhebung und Verarbeitung von Arbeitnehmerdaten (§ 32 BDSG) sowie eine Informationspflicht bei Datenschutzpannen, insbesondere hinsichtlich sensibler personenbezogener Daten, Bankverbindungsdaten und Daten, die einem Berufsgeheimnis unterliegen (§ 42 a BDSG). Begrüßenswert ist auch die Stärkung der Befugnisse der Aufsichtsbehörden, die nun nach § 38 Abs. 5 BDSG auch die Möglichkeit haben, Maßnahmen zur Beseitigung von Verstößen anzuordnen, sowie der erhöhte Bußgeldrahmen bei Ordnungswidrigkeitsverfahren (§ 43 BDSG).

3.3 Bundesdatenschutzauditgesetz

Im Jahr 2001 war mit § 9 a Bundesdatenschutzgesetz (BDSG) eine Regelung zur Schaffung eines Datenschutzaudits in das Bundesdatenschutzgesetz aufgenommen worden. Für Anbieter von Datenverarbeitungssystemen und -programmen sowie für datenverarbeitende Stellen sollte die Möglichkeit geschaffen werden, ihr Datenschutzkonzept und ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten zu lassen. Nach § 9 a Satz 2 BDSG sollen die näheren Anforderungen an die Prüfung sowie das Verfahren und die Auswahl und Zulassung der Gutachter durch besonderes Gesetz geregelt werden. Von den Datenschutzbehörden wird seitdem die Schaffung dieses Gesetzes gefordert.

Im Dezember 2008 hat die Bundesregierung - als Teil der Novellierung des Bundesdatenschutzgesetzes - den Referentenentwurf eines „Datenschutzauditgesetzes“ vorgelegt. Nicht nur auf Seiten der Datenschützer stieß dieser Entwurf auf starke Kritik, da er weder die Unabhängigkeit der Bewertung eines solchen Datenschutzaudits noch dessen Qualität, Transparenz bzw. Rechtssicherheit des Verfahrens gewährleistete.

Eine Prüfung der Zertifizierung durch unabhängige Dritte war im Gesetzentwurf nicht vorgesehen. Da am Auditierungsverfahren nur zwei Parteien beteiligt sein sollten, die beide ein wirtschaftliches Interesse an der schnellen Durchführung gehabt hätten, würde die Gefahr von Gefälligkeitsgutachten bestehen (der Antragsteller hat Interesse am Gütesiegel, der Prüfer ein wirtschaftliches Interesse an der Vergütung). Insbesondere fehlte im Gesetzentwurf die vertrauenswürdige Qualitätssicherung und Beurkundung eines Siegels durch eine unabhängige staatliche Stelle.

Der Bundesrat hatte daraufhin die Bundesregierung im Frühjahr 2009 aufgefordert, den Gesetzentwurf grundlegend zu überarbeiten. Das vorgesehene Verfahren sei zu bürokratisch, kostenträchtig und nicht transparent genug. Im Juli 2009 entschied der Innenausschuss des Deutschen Bundestages, das Auditgesetz aus dem Novellierungspaket des BDSG herauszunehmen.

3.4 Videoüberwachung in einem großen Einkaufszentrum

Gegenstand einer länderübergreifenden Kontrolle von Videoüberwachungseinrichtungen war ein großes Einkaufszentrum einer bundesweit vertretenen Unternehmenskette. In der Filiale in Mecklenburg-Vorpommern wurden u. a. die Ein- und Ausfahrten des Parkhauses, die Parkplatzticketautomaten, die Notrufsäulen innerhalb des Parkhauses und die Vorräume zu den Aufzügen per Videokamera überwacht. Begründet wurde diese Maßnahme überwiegend mit Sachbeschädigung und Vandalismus (insbes. Graffiti) bzw. Missbrauch der Notrufsäulen. Zum überwiegenden Teil erfolgte keine Aufzeichnung, sondern eine reine Beobachtung.

Eine weitere Kamera befand sich in der unteren Ladenpassage. Sie erfasste den Bereich einer Espressobar. Diese Kamera war nach einem entsprechenden Hinweis der Aufsichtsbehörde zum Zeitpunkt des Kontrollbesuches bereits abgebaut worden. Bei der Videoüberwachung von Sitz- und Ruhebereichen von Cafés und Restaurants überwiegen in der Regel die schutzwürdigen Interessen der sich dort aufhaltenden Besucher gegenüber den mit der Videoüberwachung verfolgten Sicherheitsinteressen.

Durch eine Überprüfung der auf den beiden Monitoren durchlaufend angezeigten Kameraübertragungsperspektiven während des Kontrollbesuches konnte eine weitere - zuvor nicht angegebene - Videokamera festgestellt werden. Diese Kamera überwachte den Eingangsbereich zu den Toilettenanlagen. Als Überwachungszweck wurde seitens des Center-Managements angegeben, man beabsichtige das Fernhalten von Drogenkonsumenten. Die Installation dieser Videokamera wurde als unzulässig beanstandet. In intimen Schutzbereichen, zu denen Toilettenbereiche gehören, überwiegen durch den starken Eingriff in das allgemeine Persönlichkeitsrecht der Betroffenen eindeutig deren schutzwürdige Interessen gegenüber einem etwaigen berechtigten Interesse oder dem Hausrecht der verantwortlichen Stelle. Unabhängig davon war die Kamera in diesem Bereich ungeeignet, den vom Center-Management genannten Überwachungszweck zu erreichen. Die Kamera ist daraufhin kurzfristig entfernt worden.

Das Einkaufszentrum hat inzwischen einen betrieblichen Datenschutzbeauftragten bestellt. Die endgültige datenschutzrechtliche Bewertung der übrigen Videokameras wird zurzeit zwischen den Länderaufsichtsbehörden abgestimmt, in deren Bundesländer das Unternehmen Einkaufszentren betreibt.

3.5 Videoüberwachung beim Nachbarn

Zu den zahlreichen Anfragen und Petitionen im Zusammenhang mit Videoüberwachungsanlagen zählten auch Fälle, in denen Videokameras zur Überwachung des eigenen Grundstücks installiert worden waren. Diese Fälle sind differenziert zu beurteilen.

Werden durch die Videoüberwachung auch öffentlich-zugängliche Räume (Straßen, Gehwege, öffentlich-zugängliche Gemeinschaftsflächen etc.) erfasst, sind die Voraussetzungen des § 6 b BDSG einzuhalten. Danach ist die Beobachtung öffentlich-zugänglicher Räume mit Videoanlagen nur zulässig, soweit sie etwa zur Wahrnehmung des Hausrechts oder berechtigter Interessen für konkrete Zwecke erforderlich ist und zusätzlich keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der von der Videoüberwachung Betroffenen überwiegen.

Erforderlich ist die Videoüberwachung nur dann, wenn zur Erreichung des angestrebten Zweckes kein weniger einschneidendes Mittel existiert (z. B. zusätzliche Beleuchtung durch Scheinwerfer mit Bewegungssensoren, Alarmaufschaltung etc.). Darüber hinaus sind die in § 6 b Abs. 2 bis 5 BDSG genannten Anforderungen - insbesondere die Hinweispflicht (Beschilderung) - zu erfüllen. Die zur Überwachung und zum Schutz des eigenen Grundstücks eingesetzte Videoüberwachungsanlage darf insbesondere nicht dazu führen, dass - quasi nebenbei - auch anliegende öffentliche Wege oder Nachbargrundstücke und die sich dort aufhaltenden Personen mitüberwacht werden.

Wenn die Videoüberwachung außerhalb von öffentlich-zugänglichen Räumen erfolgt, ist § 6 b BDSG nicht anwendbar. In der Regel bestehen jedoch zivilrechtliche Unterlassungs- und Abwehransprüche aus den §§ 1004 und 823 BGB sowie gegebenenfalls entsprechende Schadensersatzansprüche. Auch kann ein Verstoß gegen das Kunsturhebergesetz bzw. eine Verletzung des allgemeinen Persönlichkeitsrechts im Sinne des § 823 Abs. 1 BGB vorliegen.

Die Gerichte gehen bei der Bewertung eines zielgerichteten, ständigen Beobachtens von Nachbarn per Kamera ohne dessen ausdrückliche Einwilligung regelmäßig von einem unzulässigen Eingriff in dessen Persönlichkeitssphäre aus, was entsprechende Schadensersatzansprüche nach sich ziehen kann.

3.6. Datenerhebung durch Verkehrsbetriebe

Gegenstand von Anfragen war auch in diesem Berichtszeitraum die Datenerhebung durch Verkehrsbetriebe insbesondere durch entsprechende Formulare, wenn Personen bei Fahrausweiskontrollen ohne Fahrschein angetroffen wurden.

Eines dieser Formulare, das durch eine im Wege der Funktionsübertragung von einem Verkehrsbetrieb mit Kontrollen beauftragten Firma verwendet wurde, ist von diesem Unternehmen inzwischen überarbeitet worden. So waren insbesondere die zuvor vorgesehene Erfassung der Personalausweisnummer sowie weitere pauschale Rubriken („Fahrgast war aggressiv / nicht kooperativ...“ etc.) entnommen worden.

Falls sich ein zunächst festgestellter Vertragsverstoß im Nachhinein als unberechtigt bzw. der zunächst beanstandete Fahrausweis als gültig herausstellen sollte, werden die personenbezogenen Daten des Betroffenen gelöscht. Bei nachgewiesener Schwarzfahrt wird der Fahrgast darauf hingewiesen, dass seine personenbezogenen Daten bis zu zwei Jahre gespeichert werden können, wenn im Rahmen einer Kulanzregelung auf eine Strafanzeige wegen Fahrens ohne gültigen Fahrausweis verzichtet wird, sofern innerhalb dieses Zeitraumes keine weitere Schwarzfahrt festgestellt wird. Der betroffene Fahrgast kann unabhängig davon der Speicherung seiner personenbezogenen Daten widersprechen - jedoch dabei nicht gleichzeitig die Kulanzregelung in Anspruch nehmen, die sich auf eine Wiederholung innerhalb des oben genannten Zeitraumes bezieht.

Allerdings erfordert diese Speicherung personenbezogener Daten für zwei Jahre eine Rechtsgrundlage, die derzeit innerhalb der zugrunde liegenden „Besonderen Beförderungsbedingungen“ des Verkehrsbetriebes fehlt. Eine Bezugnahme auf den zugrunde liegenden Beförderungsvertrag scheidet hier ebenso aus wie eine Einwilligung des Fahrgastes. In Anbetracht der drohenden Strafanzeige gemäß § 265a StGB für den Fahrgast wäre seine Einwilligung mangels Freiwilligkeit unwirksam.

Ich empfehle der Landesregierung, die „Besonderen Beförderungsbedingungen“ um eine entsprechende Regelung zu ergänzen und dabei eine Löschungsfrist von einem Jahr vorzusehen.

3.7 Unaufgeforderte Werbung

Eine Vielzahl von Anfragen im Berichtszeitraum bezog sich auf die Zusendung unerwünschter Werbung. Quelle für die Adressen bei der Werbung von Unternehmen sind häufig Rabattsysteme oder Kundenbindungsprogramme („Bonuspunkte“ etc.). Vielfach bedienen sich auch Betriebe der Adressbestände anderer Unternehmen oder führen Preisausschreiben mit dem einzigen Ziel durch, hiermit an Anschriften zu kommen, die dann für Werbung genutzt werden können. Adresshandelsunternehmen verkaufen oder vermieten Datenbestände, die speziell auf Zielgruppen zugeschnitten sind (Senioren, Akademiker etc.). Hierfür werden in großem Umfang öffentlich-zugängliche Quellen ausgewertet (Adress- und Telefonbücher, Handels- und Vereinsregister, Internetseiten und Anzeigen in Zeitungen, E-Mail- und Branchenverzeichnisse etc.). Unternehmen sind daran interessiert, in ihre Werbekonzepte möglichst viele Informationen über den jeweiligen Kundenkreis einzubeziehen, um ihre Werbung „maßgeschneidert“ gegenüber potenziellen Abnehmern lancieren zu können.

Nach der Novellierung des Bundesdatenschutzgesetzes dürfen ab dem 1. September 2009 personenbezogene Daten zu Zwecken der Werbung und des Adresshandels grundsätzlich nur mit Einwilligung der Betroffenen verarbeitet werden (siehe auch Punkt 3.2). Die Novelle enthält allerdings eine Reihe von Ausnahmen. Ohne Einwilligung dürfen Unternehmen gemäß § 28 Abs. 3 Satz 2 BDSG sogenannte Listendaten (insbesondere Name, Titel, Anschrift und Geburtsjahr sowie Berufs-, Branchen- oder Geschäftsbezeichnung) für die Werbung für eigene Angebote weiter nutzen. Gleiches gilt für Zwecke der Werbung in Bezug auf die berufliche Tätigkeit des Betroffenen und an die berufliche Anschrift sowie für Spendenwerbung gemeinnütziger Organisationen. Nach § 28 Abs. 3 Satz 5 BDSG dürfen personenbezogene Daten auch für Zwecke der Werbung für fremde Angebote genutzt werden, wenn die Betroffenen anhand der Werbung die für die Nutzung verantwortliche Stelle erkennen können. Zusätzlich gilt für Daten, die vor dem 1. September 2009 erhoben worden sind, eine großzügige Übergangsfrist, nach der die neue Rechtslage für Werbedaten erst ab dem 1. September 2012 wirksam wird.

Schutz vor Zusendung weiterer Werbung bietet ein Werbewiderspruch nach § 28 Abs. 4 BDSG („Ich widerspreche der Verarbeitung oder Nutzung meiner Daten für Werbezwecke und für die Markt- und Meinungsforschung.“). Ein solcher Widerspruch kann auch schon beim Abschluss von Verträgen eingelegt werden, indem auf Vertragsformularen ein entsprechender Hinweis ergänzt wird.

Auf die Möglichkeit dieses Widerspruchs muss durch das Unternehmen im Werbeschreiben bzw. bei Abschluss eines Vertrages hingewiesen werden, wenn eine Datenverarbeitung zu Werbezwecken beabsichtigt ist. Gegenüber den werbenden Unternehmen besteht nach § 34 Abs. 1 BDSG ein Auskunftsrecht über die personenbezogenen Daten des Betroffenen, ihre Herkunft, den Zweck der Speicherung und den Empfänger oder die Empfängerkategorien, an die die Daten weitergegeben werden.

Schutz vor unadressierter Werbung und vor kostenlosen Werbepostillen bieten entsprechende Briefkastenaufkleber („Bitte keine Werbung und keine Zeitungs-Freiexemplare!“). Wird dieser Wunsch ignoriert, liegt ein Verstoß gegen das Gesetz gegen den unlauteren Wettbewerb vor. Hilfreich ist es auch, sich in die sogenannte „Robinsonliste“ des Deutschen Direkt-Marketing-Verbands (DDV) eintragen zu lassen. Diejenigen Unternehmen, die dem DDV angeschlossen sind, werden benachrichtigt, dass die Person auf der Liste keine Werbung wünscht. Das Formular ist erhältlich bei: DDV, Robinsonliste, Postfach 14 01, 71243 Ditzingen, Telefon 07156/951010 oder unter www.direktmarketing-info.de.

3.8 Mitarbeiterüberwachung durch Lebensmitteldiscounter-Unternehmen

Im März 2008 füllten Medienberichte die Schlagzeilen, wonach ein großer, bundesweit vertretener Lebensmitteldiscounter seine Mitarbeiter systematisch durch Sicherheitsunternehmen bzw. Detekteien überwacht hat. Da es sich bei den Auftraggebern dieser Maßnahmen um rechtlich selbstständige Vertriebsgesellschaften der Discounter-Kette handelte, haben die für die Unternehmenssitze zuständigen Datenschutzaufsichtsbehörden - auch in Mecklenburg-Vorpommern - umfangreiche Ermittlungen und Überprüfungsverfahren durchgeführt.

Im Untersuchungszeitraum 1. Januar 2006 bis Ende März 2008 waren auch in den Filialen des Discounters in Mecklenburg-Vorpommern Sicherheitsdienste und Detekteien mit teilweise heimlichen Beobachtungsmaßnahmen von Mitarbeitern (in der Regel kombiniert mit dem Einsatz von Videokameras) beauftragt worden. Dabei erfolgte der Einsatz der Detektive teils mit Wissen der Filialmitarbeiter; er richtete sich jedoch nicht - wie diesen gegenüber behauptet - in erster Linie gegen Ladendiebe, sondern auf die Überwachung der Beschäftigten in den Filialen. Teilweise wurden ohne Wissen der Mitarbeiter heimlich Mikrokameras installiert, mit denen der Detektiv das Geschehen von einem externen Kontrollmonitor verfolgte. Die Einsätze der Detektive wurden gegenüber den Mitarbeitern des Discounters mit der Aufdeckung von Kundendiebstählen bzw. der Aufklärung von „hohen Inventurverlusten“ begründet. Sie richteten sich jedoch zumindest zu einem Teil auch auf die Beobachtung des Verhaltens der Mitarbeiter.

Während ihres Aufenthaltes in den Filialen notierten die Detektive mitgehörte Gespräche und (teilweise private) Telefonate sowie Unterhaltungen in Pausenräumen etc. und legten entsprechende Informationen in Einsatzberichten nieder, die dann an die Vertriebsgesellschaft übersandt wurden. In den Detektivprotokollen („Revisionsberichten“) der Detekteien finden sich - neben Angaben zur Anzahl der im jeweiligen Zeitraum ermittelten Ladendiebe - auch personenbezogene Daten über Mitarbeiter und Mitarbeiterinnen der Filialen, die keinerlei Bezug zu der Ermittlung von Diebstählen oder zur Diebstahlsprävention haben, sondern persönliche Eigenheiten und Verhaltensweisen der jeweiligen Beschäftigten wiedergeben („Mit Ausnahme von Frau Y scheinen auch alle beliebt. Frau X wird als zickig bezeichnet.“).

Nach Abschluss der umfangreichen Ermittlungen haben die zuständigen Datenschutzaufsichtsbehörden der Länder gegen 35 Vertriebsgesellschaften des Discounter-Unternehmens Bußgelder in einer Gesamthöhe von 1.462.000 Euro festgesetzt. In Mecklenburg-Vorpommern wurden am 10. September 2008 zwei Bußgeldbescheide in einer Gesamthöhe von 22.000 Euro gegen die Regionalgesellschaft des Discounters in Mecklenburg-Vorpommern erlassen.

Das Discounter-Unternehmen hat mittlerweile in allen Filialen ein datenschutzgerechtes Gesamtkonzept für den Einsatz von Videoüberwachung und Ladendetektiven eingeführt.

3.9 Führung von Krankenakten durch Unternehmenskette

Im Frühjahr des Jahres 2009 wurden in einem Mülleimer eines Betriebes in Nordrhein-Westfalen Listen mit Gesundheitsdaten von Mitarbeitern eines großen, bundesweit tätigen Lebensmitteldiscounters gefunden. Den nachfolgenden Medienberichten war zu entnehmen, dass in Filialen dieses Unternehmens Mitarbeiter nach Erkrankungen systematisch von ihren Vorgesetzten nach der Art der Erkrankung befragt würden. Die entsprechenden Angaben, die von „Grippe“ über „Rückenleiden“ bis hin zu „will schwanger (werden), Befruchtung nicht funktioniert“ reichten, seien in Listen erfasst worden. In diese Listen seien auch beabsichtigte weitergehende Maßnahmen eingetragen worden (zum Beispiel „Kündigung zum 31.07.08“). Bundesweit werde für die Erfassung ein einheitlicher Vordruck verwendet.

Die für die Dienstleistungsgesellschaft des Unternehmens in Baden-Württemberg zuständige Aufsichtsbehörde und die Aufsichtsbehörden in den betroffenen Ländern - auch in Mecklenburg-Vorpommern - haben daraufhin Ermittlungen durchgeführt, die ergaben, dass sieben der bundesweit 35 Regionalgesellschaften Krankheitsdaten ihrer Mitarbeiter erhoben hatten. Für die Erhebung hatten die Regionalgesellschaften von ihnen selbst entworfene Vordrucke eingesetzt. Die Erfassung der genannten Daten war von den einzelnen Regionalgesellschaften bereits bis zum Ende des Jahres 2008 beendet worden, nachdem die Dienstleistungsgesellschaft in Baden-Württemberg davon Kenntnis erhalten und die Erfassung wegen datenschutzrechtlicher Bedenken gestoppt hatte. Die fraglichen Listen waren in allen Bundesländern (auch in Mecklenburg-Vorpommern) - bis auf die später in Nordrhein-Westfalen gefundenen - spätestens im Januar 2009 vernichtet worden. Die Überprüfungen wurden mit folgendem Ergebnis abgeschlossen:

In Nordrhein-Westfalen (wo die entsprechenden Unterlagen noch nicht vernichtet worden waren) wurde gegen eine Vertriebsgesellschaft des Unternehmens ein Bußgeld in Höhe von 36.000 Euro verhängt. In den anderen fünf Bundesländern (auch in Mecklenburg-Vorpommern) hatten die Ermittlungen der Datenschutzaufsichtsbehörden zwar den Verdacht erhärtet, dass die jeweiligen Vertriebsgesellschaften bis 2008 zumindest teilweise Mitarbeiter in unzulässiger Weise befragt und in Listen erfasst hatten. Eindeutige Feststellungen ließen sich jedoch nicht mehr treffen, da - wie oben erwähnt - sämtliche Unterlagen bereits vernichtet worden waren. Daher kam in diesen Fällen der Erlass eines Bußgeldbescheides nicht in Betracht.

Die baden-württembergische Aufsichtsbehörde hat den Vorgang zum Anlass genommen, sich bei der Dienstleistungsgesellschaft des Unternehmens eingehend über den Stand und die Inhalte der von dem Unternehmen durchgeführten Überprüfungen aller datenschutzrechtlich relevanten Verfahren informieren zu lassen.

3.10 Datenerhebung durch Rechtsanwälte – kein kontrollfreier Raum

Im Rahmen einer Petition erreichte mich die Bitte um Unterstützung wegen der unrechtmäßigen Speicherung von personenbezogenen Daten durch eine Rechtsanwaltskanzlei. Dabei handelte es sich um sensible Daten aus einem persönlichen Tagebuch, das nach Angabe der Petentin durch deren Ex-Ehemann hinterzogen worden war und in ein laufendes Scheidungs-/Sorgerechtsverfahren eingeführt werden sollte. Die Einführung dieses Tagebuches in das Verfahren war durch den Anwalt der Petentin verhindert worden, der gleichzeitig ein Beweisverwertungsverbot durch das Gericht und die Herausgabeverfügung des Originals hatte erreichen können. Seitens der Petentin bestand dennoch die begründete Besorgnis, dass bei der Rechtsanwaltskanzlei Kopien existierten bzw. elektronisch gespeichert waren.

Auf mein Stellungnahmeersuchen hin hat die Kanzlei die datenschutzrechtliche Kontrollzuständigkeit des Landesdatenschutzbeauftragten nach § 38 BDSG bestritten.
Hintergrund ist die bereits seit vielen Jahren bestehende Kontroverse zwischen Aufsichtsbehörden und Rechtsanwälten bzw. Rechtsanwaltskammern über die datenschutzrechtliche Aufsichts- und Kontrollkompetenz. Seitens der Rechtsanwälte wird regelmäßig die Auffassung vertreten, dass die Vorschriften der Bundesrechtsanwaltsordnung denen des Bundesdatenschutzgesetzes als speziellere Regelung vorgingen, wodurch sie nach ihrer Ansicht nicht der Aufsicht der Datenschutzaufsichtsbehörden, sondern der der Rechtsanwaltskammern unterliegen würden.

Im vorliegenden Fall hatte sich die Petentin parallel an die Rechtsanwaltskammer Mecklenburg-Vorpommern gewandt - war jedoch nach Prüfung des Falles von dort zunächst auf den Zivilrechtsweg verwiesen worden.

Mit Blick sowohl auf dieses unbefriedigende Ergebnis für die Petentin als auch auf die Klärung der Grundsatzfrage der datenschutzrechtlichen Kontrollzuständigkeit für Rechtsanwälte im Lande habe ich beide Fragen mit der Rechtsanwaltskammer Mecklenburg-Vorpommern erörtert. Im Rahmen der sehr konstruktiven Gespräche konnte erreicht werden, dass die Rechtsanwaltskammer den Fall der Petentin gegenüber dem beteiligten Rechtsanwalt unter den oben genannten datenschutzrechtlichen Aspekten weitergeführt hat. Zur Grundsatzfrage der datenschutzrechtlichen Aufsichtszuständigkeit nach dem Bundesdatenschutzgesetz (BDSG) hat sich die Kammer in den Gesprächen zurückhaltend geäußert. Im Ergebnis des Falles ist jedoch inzwischen sichergestellt, dass bei der betreffenden Kanzlei alle oben genannten Daten der Petentin vernichtet bzw. gelöscht worden sind.

Unabhängig von der gegenteiligen Auslegung der Rechtsanwaltskammer umfasst die Zuständigkeit der Datenschutzaufsicht gemäß § 38 BDSG jedoch auch die Tätigkeit von Rechtsanwaltskanzleien und Notariaten.

3.11 Google Street View

Street View ist stärker als andere Internetdienste von Google in die öffentliche Diskussion geraten. Dies hängt auch damit zusammen, dass dieser Dienst erstmals die Persönlichkeitsrechte der Betroffenen nicht nur in der virtuellen Welt, sondern auch im realen Leben berührt. Street View ermöglicht jedem Internetnutzer virtuelle Rundfahrten und Spaziergänge aus dem Blickwinkel des Autofahrers oder Fußgängers, wobei es sich nicht um Livebilder handelt, sondern um Fotos, die im Zweisekundentakt von neun Kameras aus ca. 2,5 Meter Höhe von speziell ausgerüsteten Pkws aus aufgenommen werden, die öffentliche Straßen, z. T. auch Wege, Parks etc. abfahren. Für den Nutzer ist es so möglich, eine Strecke virtuell zu „fahren“, anzuhalten, sich umzudrehen und die Richtung zu wechseln, ganz so, als befände man sich wirklich in der betreffenden Straße. Vor Urlaubsbeginn lässt sich recherchieren, wie weit das gebuchte Hotel vom Strand entfernt ist oder wo sich die nächste Einkaufsmöglichkeit befindet. Man kann für sein Unternehmen werben oder potentiellen Käufern Bilder von Immobilien zur Verfügung stellen.

Den Vorteilen stehen jedoch erhebliche Nachteile und Risiken gegenüber. Es ist denkbar, dass einzelne Personen an Orten wiedererkannt werden, an denen sie nicht gesehen werden möchten, oder sich in Situationen wiederfinden, die ihnen unangenehm sind. Dies gilt auch für die Erkennbarkeit von Kfz-Nummernschildern, die Rückschlüsse auf die Aufenthaltsorte von Fahrern oder Haltern zulassen. Vor allem ermöglicht es Street View, in Gärten und Höfe, ggf. auch in geöffnete Fenster hineinzuschauen. Kritiker befürchten zudem, dass Hauseigentümer mit einer Werbeflut von Renovierungsunternehmen rechnen müssten, sobald diese in der Lage seien, den Zustand von Häusern im Internet zu begutachten. Auch wird auf die Gefahr hingewiesen, dass über Street View Haus- und Wohnungseinbrüche oder andere Straftaten vorbereitet werden könnten.

Seit 2007 ist Street View in mittlerweile 19 Staaten eingeführt worden und z. B. in den USA, in Frankreich, in Italien und in Großbritannien verfügbar. In der Bundesrepublik Deutschland steht der Einsatz von Street View noch bevor. Die notwendigen Fotos wurden in den beiden vergangenen Jahren bereits gemacht. Zwar sind immer noch Google-Fahrzeuge unterwegs. Doch werden - Google zufolge - nur noch Lücken geschlossen und Fahrten dort wiederholt, wo es technische Probleme mit dem Bildmaterial gab.

In Deutschland hatte bereits im November 2008 der Düsseldorfer Kreis, das Gremium der obersten Datenschutzaufsichtsbehörden, festgestellt, dass „die Veröffentlichung von georeferenzierten und systematisch bereitgestellten Bilddaten unzulässig ist, wenn hierauf Gesichter, Kraftfahrzeugkennzeichen oder Hausnummern erkennbar sind. Den betroffenen Bewohnern und Grundstückseigentümern ist zudem die Möglichkeit einzuräumen, der Veröffentlichung der sie betreffenden Bilder zu widersprechen und dadurch die Bereitstellung der Klarbilder zu verhindern. Keine schutzwürdigen Interessen bestehen, wenn die Darstellung der Gebäude und Grundstücke so verschleiert bzw. abstrakt erfolgt, dass keine individuellen Eigenschaften mehr erkennbar sind“. Damit wurden entsprechende Internetveröffentlichungen zwar grundsätzlich akzeptiert, aber unter den Vorbehalt begleitender Datenschutzmaßnahmen gestellt.

Datenschutzrechtlich ist die Problematik nicht unkompliziert, wie eine Reihe von inzwischen vorliegenden Rechtsgutachten zeigt, die teilweise zu unterschiedlichen Ergebnissen kommen. Grundsätzlich ist nach den Vorschriften des Bundesdatenschutzgesetzes das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn die Daten allgemein zugänglich sind, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt. Daraus ergibt sich angesichts der Tatsache, dass die Aufnahmen ausschließlich auf öffentlichen Straßen gefertigt werden und damit grundsätzlich allgemein zugänglich sind, die Notwendigkeit einer spezifischen Abwägung zwischen den Interessen des Unternehmens und den schutzwürdigen Interessen der Betroffenen. Ein offensichtliches Überwiegen aller Betroffeneninteressen konnte nicht von vornherein angenommen werden, weil das Produkt durchaus auch Befürworter hat.

Die - wegen der deutschen Niederlassung in Hamburg für die deutschen Datenschutzaufsichtsbehörden federführende - Datenschutzaufsichtsbehörde Hamburg hatte damit die schwierige Aufgabe, in Verhandlungen mit dem Unternehmen ein Ergebnis zu erzielen, das den schutzwürdigen Interessen aller Betroffenen gerecht wird. Ein erster Durchbruch konnte im Vorfeld der Sitzung des Düsseldorfer Kreises im April 2009 erreicht werden. Google zeigte - neben den bereits vorgesehenen Verpixelungen der Gesichter und Kfz-Kennzeichen - erstmals Kompromissbereitschaft insbesondere in Bezug auf die Einräumung von Widerspruchsrechten. Darüber hinaus wurde zugesichert, die jeweils aktuell befahrenen Gebiete auf der Seite von Google zu veröffentlichen. Auf das Widerspruchsrecht weist Google seither auf seiner Homepage hin. Somit kann jeder Betroffene direkt gegenüber Google Widerspruch einlegen unter http://maps.google.de/intl/de/help/maps/streetview/ oder schriftlich bei der Google Germany GmbH, betr.: Street View, ABC-Straße 19, 20354 Hamburg. Betroffen sein kann nahezu jeder Bundesbürger, sei es als Bewohner oder Eigentümer eines der aufgenommenen Häuser oder als Kfz-Besitzer bzw. Fußgänger.

Die Einräumung dieser Widerspruchsmöglichkeit wurde dann Teil eines Zusicherungskataloges, den der Hamburgische Landesbeauftragte für den Datenschutz mit Google erzielen konnte. Darin hat Google insbesondere verbindlich zugesichert:

eine Technologie zur Verschleierung von Gesichtern und Kfz-Kennzeichen vor der Veröffentlichung von derartigen Aufnahmen einzusetzen.
Widerspruchsmöglichkeiten zur Entfernung bzw. Unkenntlichmachung eines Gebäudes durch einen Bewohner oder Eigentümer vorzuhalten und derartige Widersprüche zu bearbeiten.
Widersprüche zu Personen, Kennzeichen und Gebäuden bzw. Grundstücken bereits vor der Veröffentlichung von Bildern in einer einfachen Form zu berücksichtigen mit der Folge, dass die entsprechenden Bilder vor der Veröffentlichung unkenntlich gemacht werden. Voraussetzung ist eine Identifizierung des Grundstücks, der Person oder des Fahrzeugs.
die geplanten Befahrungen mit einem Hinweis auf die Widerspruchsmöglichkeit im Internet rechtzeitig vorher bekannt zu geben. Die vorhandenen Befahrungspläne werden bis zu 2 Monate im Voraus veröffentlicht und ständig aktualisiert. Google hat die verbindliche Zusage gemacht, die Liste genauer zu gestalten und auf Landkreise und kreisfreie Städte zu erstrecken. Ferner gibt es die Zusage, dass die Widerspruchsmöglichkeit auch nach der Veröffentlichung noch besteht.

Die bei Google eingelegten Widersprüche werden zeitnah bestätigt. E-Mails mit Widersprüchen werden bereits bestätigt, alle entsprechenden Briefe werden fortlaufend beantwortet.

Der vollständige Zusicherungskatalog ist unter http://www.hamburg.de/datenschutz/ zu finden.
Skepsis ist deshalb angebracht, weil das Unternehmen bereits im vergangenen Jahr zum Teil nur sehr zögerlich bei der Umsetzung von Zusagen war. Der Hamburgische Datenschutzbeauftragte beobachtet und kontrolliert deshalb laufend die Einhaltung der Zusagen durch das Unternehmen. Er hat insbesondere darauf hingewiesen, dass Street View erst online gehen dürfe, wenn sämtliche Widersprüche berücksichtigt worden seien.

Insgesamt zeigt sich, dass sich die Generalklauseln des Bundesdatenschutzgesetzes für die Beurteilung von Projekten zur Erhebung von Geodaten als wenig taugliche Regulierungsgrundlage erweisen. Auch im Internet muss der Einzelne sein Recht auf informationelle Selbstbestimmung durchsetzen können. Ein modernes Datenschutzrecht muss internetfähig sein. Eine spezialgesetzliche Normierung der Erhebung und Nutzung von Geodaten würde einen einheitlichen und rechtssicheren Rahmen gerade für private Anbieter bereitstellen. Solange der Bundesgesetzgeber die notwendige Modernisierung des Bundesdatenschutzgesetzes nicht vornimmt, kann es jedoch mit Blick auf Street View nur darum gehen, im Rahmen der vorhandenen Gesetze und der bestehenden Internetstruktur den Persönlichkeitsinteressen der Bürgerinnen und Bürger soweit wie möglich Geltung zu verschaffen, gleichzeitig aber auch mit gegenläufigen Grundrechtspositionen zum Ausgleich zu bringen.

Positiv zu bewerten ist deshalb die vorliegende Hamburger Bundesratsinitiative für eine entsprechende gesetzliche Regelung der Erfassung von Straßenpanoramen durch eine entsprechende Novellierung des Bundesdatenschutzgesetzes, die auch von den Justizministern des Bundes und der Länder am 24. Juni 2010 ausdrücklich begrüßt worden ist. Es bleibt zu hoffen, dass der Gesetzentwurf Auftakt zu einer umfassenden Modernisierung des Datenschutzrechts sein wird.

Ende April dieses Jahres hat Google außerdem auf eine entsprechende Veröffentlichung des Hamburgischen Datenschutzbeauftragten und des Bundesbeauftragten für den Datenschutz hin eingeräumt, bei seinen Fahrten für Street View nicht nur zu fotografieren, sondern auch Daten von WLAN-Netzen zu scannen. Der Hamburgische Datenschutzbeauftragte kontrolliert diesen neuen, von Google bisher zurückgehaltenen Sachverhalt und hat wegen des Verstoßes des Unternehmens Strafantrag gestellt. Die Staatsanwaltschaft Hamburg hat (koordinierend über Hamburg hinaus auch für die übrigen Länder) entsprechende Ermittlungen aufgenommen. Aktuelle Informationen dazu unter http://www.hamburg.de/datenschutz/.

3.12 Bildergalerien von öffentlichen Veranstaltungen im Internet

Zunehmend stellen sowohl Unternehmen als auch Private zu verschiedenen Zwecken Fotos von Personen ins Internet. Oft handelt es sich um Fotogalerien mit Bildern von Veranstaltungen und Partys, die von den veranstaltenden Clubs, Discos oder auch von Teilnehmern der jeweiligen Veranstaltung im Internet veröffentlicht werden. Damit sind die Fotos weltweit zugänglich und können darüber hinaus kopiert oder weiterbearbeitet werden.

Bei der beabsichtigten Veröffentlichung im Internet ist das Recht der Fotografierten am eigenen Bild zu beachten. Die datenschutzrechtliche Zulässigkeit der Veröffentlichung im Internet ist in den §§ 22 und 23 Kunsturhebergesetz (KUG) geregelt. Ausnahmen sind nach § 23 Abs. 1 i. V. m. Abs. 2 KUG möglich.

Grundsätzlich ist gemäß § 22 KUG zur Veröffentlichung die Einwilligung der fotografierten Person erforderlich. In diesem Falle ist nicht nur eine Einwilligung für das Fotografieren erforderlich, sondern zusätzlich auch die Einwilligung dazu, dass das Foto danach im Internet veröffentlicht werden darf.

Ausnahmen wären zum Beispiel, wenn es sich um eine Person „aus dem Bereich der Zeitgeschichte“ handelt oder um Fotos, auf denen die Person nur als „Beiwerk“, z. B. neben einer Landschaft, erscheint, beziehungsweise um Bilder von Versammlungen etc. Auch in diesen Ausnahmefällen darf jedoch nach § 23 Abs. 2 KUG ein Personenfoto nur dann veröffentlicht werden, wenn hierdurch kein berechtigtes Interesse des Abgebildeten verletzt wird.

Die Verbreitung und Vervielfältigungsmöglichkeit „klassischer“ analoger Fotos war für den Fotografierten einschätzbar und überschaubar. Die Entwicklung der digitalen Fotografie und die Verbreitungsmöglichkeiten über das Internet eröffnen demgegenüber zwar neue fotografische Möglichkeiten, aber auch vielfältige Missbrauchsszenarien. Moderne Kameras enthalten zunehmend eine Zusatzfunktion, mit der die Kamera bereits beim Fotografieren über GPS einen Ortsbezug zu der fotografierten Person herstellt, der als Dateiinformation zu dem digitalen Foto zugespeichert werden kann („Geo-Tagging“).

Auch sind digitale Fotos zunehmend über biometrische Merkmale im Internet suchfähig. Durch die Verbreitung solcher Personenfotos steigt das Risiko, dass im Internet über das Foto als „digitales Suchmerkmal“ Verknüpfungen zu vielfältigen anderen personenbezogenen Informationen zur gleichen Person hergestellt werden können.

Vor dem Hintergrund dieser technischen Möglichkeiten ist die Einhaltung der oben genannten rechtlichen Voraussetzung bei der Veröffentlichung von Personenfotos im Internet von besonderer Bedeutung.

3.13 Smart Metering durch Energieversorgungsunternehmen und Mieterdatenschutz

Nach § 21 b Energiewirtschaftsgesetz (EnWG) sind ab dem 1. Januar 2010 in Neubauten und bei größeren Renovierungen Energiezähler einzubauen, die den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit anzeigen. Bis Ende 2010 sollen dann Energieversorgungsunternehmen den Verbrauchern Tarife anbieten, bei denen Anreize zur Energieeinsparung und zur Steuerung des Energieverbrauchs gegeben werden sollen. Durch die Zähler sollen die Verbrauchsdaten abgebildet werden können, die für die neuen Tarife relevant sind.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) haben sich in ihrer Sitzung im November 2009 mit dem Thema Smart Metering befasst. Sie haben gegenüber der Bundesnetzagentur insbesondere darauf hingewiesen, dass mit den künftig erhobenen Verbrauchsdaten von Privathaushalten detaillierte Nutzungsprofile der Bewohner gebildet werden können, die Rückschlüsse auf deren Lebensgewohnheiten ermöglichen.

Verbrauchsdaten von Privathaushalten sind in der Regel personenbezogene Daten im Sinne von § 3 Abs. 1 BDSG. Daher sind Energieversorger, Netzbetreiber und Messstellenbetreiber aufgefordert, solchen Messverfahren den Vorzug zu geben, die das Prinzip der Datenvermeidung und Datensparsamkeit nach § 3 a BDSG umsetzen. Der Anschlussinhaber muss auch beim Einsatz intelligenter Zähler weiterhin die Hoheit über seine Verbrauchsdaten haben. Die Messverfahren und die Datenübermittlungen müssen transparent für ihn sein.
Ablesezeitpunkte, Intervalle, Übertragungswege und die datenschutzrechtlichen Regelungen müssen daher mit den Betroffenen vertraglich vereinbart werden.

Weitergehende Angebote zur Verfolgung von Energieverbrauch und Nutzungszeit durch die Verbraucher, z. B. die Erstellung und Wiedergabe von Lastprofilen über das Internet auf der Grundlage von Messungen in kurzen Intervallen und Übertragung aus der Wohnung auf zentrale Server erfordern das Einverständnis der Betroffenen und sind daher gesondert vertraglich zu regeln.

Beim Einbau intelligenter Messeinrichtungen sind technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit der Verbrauchsdaten gewährleisten. Dazu gehören Maßnahmen der Zugangskontrolle nach § 9 BDSG, die in angemessener Weise sicherstellen, dass Unbefugte die Daten aus Zählern nicht auslesen können. Von besonderer Bedeutung sind derartige Maßnahmen bei Messeinrichtungen, die außerhalb der Wohnung angebracht sind, etwa zusammengefasst in Fluren oder Kellerräumen. Allein die Tatsache, dass dort oft eine größere Anzahl von Messeinrichtungen gemeinsam untergebracht ist, verhindert nicht die Zuordnung von Verbrauchsdaten zu einzelnen Haushalten und ist deshalb keine geeignete Maßnahme zur Zugangskontrolle. Messeinrichtungen außerhalb der Wohnungen bedürfen daher weiterer Schutzvorkehrungen. Geeignet wären mechanische Vorrichtungen, wie verschließbare Klappen vor den Displays einzelner Zähler oder abschließbare Zählerschränke. Denkbar wären auch elektronische Schutzvorkehrungen, wie das passwortgeschützte Auslesen oder chipkartenbasierte Zugangskontrollen.

Neben Schutzvorkehrungen gegen unberechtigtes Auslesen der Messeinrichtung selbst sind auch Vorkehrungen zu treffen, die die Datensicherheit bei der Übermittlung der Verbrauchsdaten gewährleisten. Maßnahmen zur Weitergabekontrolle gemäß § 9 BDSG sind sowohl bei der Übertragung der Messdaten per Funk als auch bei der kabelgebundenen Übertragung über vorhandene Stromleitungen (Powerline Communication) erforderlich. Dies betrifft sowohl Datenübermittlung an Dienstleister (Energieversorger, Netzbetreiber und Messstellenbetreiber) als auch die Übertragung von Messdaten an Anschlussinhaber etwa auf ein Anzeigedisplay in der Wohnung oder die Bereitstellung der Daten in einem Webportal. Hier ist solchen Verfahren der Vorzug zu geben, die Daten in anonymisierter oder ggf. pseudonymisierter Form übertragen. Sofern eine Anonymisierung der Daten vor der Übermittlung nicht möglich ist, sind kryptografische Verschlüsselungsverfahren nach dem Stand der Technik erforderlich.

Auch bei der Findung von lastvariablen oder tageszeitabhängigen Tarifen nach § 40 Abs. 3 EnWG ist von den Energieunternehmen das Prinzip der Datenvermeidung und der Datensparsamkeit nach § 3 a BDSG zu beachten. Dabei ist Verfahren der Vorzug zu geben, die ohne die Erhebung von Messdaten aus einzelnen Wohnungen auskommen.

Den obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich ist bewusst, dass die intelligenten Zähler sowohl abrechnungsrelevante als auch steuerungsrelevante Daten erfassen. Somit liegen nicht nur Daten über entnommene Energiemengen, sondern auch Daten darüber vor, wann in welcher Menge Energie durch den Abnehmer verbraucht wird, sodass individuelle Lastprofile erstellt werden können. Bereits im Gesetzgebungsverfahren zum Gesetz zur Öffnung des Messwesens bei Strom und Gas für den Wettbewerb hatte der Bundesrat Bedenken hinsichtlich der Wahrung des Verbraucher- und Datenschutzes geäußert.

Diese Bedenken teilen die Datenschutzaufsichtsbehörden. Sie unterstreichen ausdrücklich, dass durch Smart Meter erhobene Verbrauchsinformationen von Privathaushalten Auskunft geben über die persönlichen und sachlichen Lebensverhältnisse der Anschlussnutzer. Die menschliche Existenz in einer modernen Gesellschaft ist geprägt durch eine hochtechnisierte und automatisierte Lebensweise. Diese ist eng mit dem Verbrauch von Energie verbunden. Es gibt kaum noch Handlungen, die nicht unmittelbar oder zumindest mittelbar zu einem Verbrauch von Energie führen. So ist z. B. ein Großteil des heutigen Kommunikations- und Freizeitverhaltens ohne Elektrizität nicht denkbar. Tagesabläufe spiegeln sich in der Nutzung von Energie wieder. Die gerätegenaue Erfassung verbrauchter Energie kann daher zu einer Ausforschung der Lebensgewohnheiten der Betroffenen führen.

Die Aspekte und die Tatsache, dass das Ablesen vor Ort jedenfalls aus technischer Sicht nicht mehr erforderlich und durch den Anschlussnutzer daher nicht kontrollierbar ist, erfordern eine grundsätzliche datenschutzrechtliche Bewertung von Smart Metern. Unterschiede zwischen der datenschutzrechtlichen Bewertung intelligenter Zähler zu den konventionellen Ferraris-Zählern ergeben sich aufgrund der technischen Potenziale der Smart Meter, der Vielzahl der beteiligten Marktakteure und aus den daraus resultierenden, möglichen Vertragskonstellationen und Datenflüssen.

Die intelligenten Stromzähler sind lediglich der Auftakt einer wesentlich umfassenderen Konzeption von intelligenten Stromnetzen (Smart Grids), die mittlerweile weltweit diskutiert und auch in der Bundesrepublik mit mehreren Modellprojekten bereits getestet werden. Falls, wie beabsichtigt, Stromverbrauchswerte in einzelnen Haushalten in Zeitintervallen von 15 Minuten oder einem geringeren Zeitintervall erfasst werden, so entstehen zwangsläufig detaillierte Verhaltensprofile von Menschen, ihren Gewohnheiten beim Gebrauch ihrer Wohnung, ihrer An- und Abwesenheit, ihres Heizverhaltens, Wasserverbrauchs etc.
Bei aller derzeitigen Begeisterung für die Entwicklung dieser neuen Art von Energienetzen ist es daher besonders wichtig, die Entwicklung der Smart Grids insbesondere im Hinblick auf das Prinzip einer strikten Datensparsamkeit zu begleiten und den Schutz der personenbezogenen Daten, die in diesem Zusammenhang erfasst und übermittelt werden, zu gewährleisten.

3.14 Datenschutzkonforme Gestaltung sozialer Netzwerke im Internet

Soziale Netzwerke im Internet haben in den letzten Jahren einen Boom erlebt. Der überwiegende Teil aller Schüler und Studenten ist bei Netzwerken wie StudiVZ oder SchülerVZ registriert; Netzwerke wie „Xing“ werden für berufliche Kontakte genutzt ebenso wie „Facebook“ für die private Nutzung und den Kontakt im (digitalen) Freundeskreis.

Durch diese Internetnetzwerke werden häufig in großem Umfang persönliche Daten erfasst (insbesondere bei der Erstellung des jeweiligen Profils) und für die teilweise millionenfachen Nutzer der großen sozialen Netzwerke zugänglich gemacht. Neben der persönlichen Sorgfalt bei der Verwendung der eigenen personenbezogenen Daten ist es deshalb von besonderer Bedeutung, dass die Anbieter der Internetnetzwerke diese Netzwerke datenschutzgerecht gestalten.

Die obersten Datenschutzaufsichtsbehörden im nicht-öffentlichen Bereich haben deshalb am 3./4. April 2008 einen Beschluss zur „Datenschutzkonformen Gestaltung sozialer Netzwerke“ gefasst (siehe Anlage 2.2). Sie haben dabei insbesondere darauf hingewiesen, dass die Anbieter sozialer Netzwerke ihre Nutzer umfassend über die Verarbeitung der jeweiligen personenbezogenen Daten, über ihre Wahl- und Gestaltungsmöglichkeiten, über Risiken für die Privatsphäre und über den Umgang mit personenbezogenen Daten Dritter unterrichten müssen. Ferner ist nach den Bestimmungen des Telemediengesetzes eine Verwendung von personenbezogenen Nutzungsdaten für Werbezwecke nur mit wirksamer Einwilligung der Betroffenen zulässig. Bei Werbemaßnahmen aufgrund von Profildaten müssen die Betroffenen mindestens eine Widerspruchsmöglichkeit haben. Eine Speicherung von personenbezogenen Nutzungsdaten über das Ende der Verbindung hinaus ist ohne Einwilligung der Nutzer nur gestattet, soweit die Daten zu Abrechnungszwecken ihnen gegenüber erforderlich sind. Die Aufsichtsbehörden haben betont, dass das Telemediengesetz die Anbieter dazu verpflichtet, das Handeln in sozialen Netzwerken anonym oder unter Pseudonym zu ermöglichen, und die Anbieter dazu aufgefordert, für ihre Dienste datenschutzfreundliche Standardeinstellungen zu wählen, durch die die Privatsphäre der Nutzer möglichst umfassend geschützt wird. Diese Standardeinstellungen sind besonders restriktiv zu fassen, wenn sich das Portal an Kinder richtet. Der Zugriff durch Suchmaschinen darf nur vorgesehen werden, wenn der Nutzer eingewilligt hat. Dieser muss zudem die Möglichkeit haben, sein Profil auf einfache Weise wieder selbst zu löschen.

3.15 Internetportale zur Bewertung von Einzelpersonen

Die obersten Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich haben mit ihrem Beschluss vom 3./4. April 2008 „Internet-Portale zur Bewertung von Einzelpersonen“ (siehe Anlage 1.7) darauf hingewiesen, dass es sich bei Bewertungen und Beurteilungen von Einzelpersonen (z. B. Lehrerinnen und Lehrern) in Internetportalen vielfach um sensible Informationen und subjektive Werturteile über Betroffene handelt, die in das Portal eingestellt werden, ohne dass die Urheber erkennbar sind, und die jederzeit von jedermann abgerufen werden können. Die Datenschutzaufsichtsbehörden weisen darauf hin, dass die Vorschriften des Bundesdatenschutzgesetzes einzuhalten sind und bei der vorgeschriebenen Abwägung den schutzwürdigen Interessen der bewerteten Personen Rechnung getragen werden muss. Das Recht auf freie Meinungsäußerung rechtfertigt es nicht, das Recht der Bewerteten auf informationelle Selbstbestimmung generell als nachrangig einzustufen.

Der Bundesgerichtshof (BGH) hat sich mit seinem Urteil vom 23. Juni 2009 („spickmich.de“) mit der Klage einer Lehrerin gegen ihre „Bewertung“ im Internet mittels eines Schulnotensystems befasst. In seinem Urteil hat der BGH zwar die Klage unter Berücksichtigung des Einzelfalls der klagenden Lehrerin abgewiesen, jedoch gleichzeitig die Anwendbarkeit der Vorschriften des Bundesdatenschutzgesetzes und die Notwendigkeit einer Prüfung des schutzwürdigen Interesses, hier in Form einer Abwägung zwischen dem Schutz des Rechtes auf informationelle Selbstbestimmung des Betroffenen nach Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG gegenüber dem Recht auf Kommunikationsfreiheit nach Art. 5 Abs. 1 GG hervorgehoben. Wesentliches Bewertungskriterium war auch die Frage, ob die Bewertungen im Internet die Schwelle der Formalbeleidigung oder einer „unsachlichen Schmähkritik“ überschreiten. Dies war beim vorliegenden Sachverhalt nicht der Fall - dürfte andernfalls jedoch zu einer Bestätigung des Schutzes des informationellen Selbstbestimmungsrechtes der Klägerin geführt haben. Gegen das Urteil ist eine Verfassungsbeschwerde beim Bundesverfassungsgericht anhängig.

3.16 Arbeitsweise von Auskunfteien und Rechte der Betroffenen

Zur datenschutzrechtlichen Zulässigkeit der Tätigkeit von Handels- und Wirtschafts-Auskunfteien haben mich auch in diesem Berichtszeitraum wieder zahlreiche Anfragen erreicht. Vorangegangen war meist die gesetzlich vorgesehene Mitteilung einer Auskunftei gemäß § 33 Abs. 1 Satz 2 BDSG an einen Betroffenen darüber, dass sie personenbezogene Daten über ihn gespeichert und weitergeleitet hätte. Diese Mitteilungen der Auskunfteien führten bei den Betroffenen zu Irritationen und zu der Besorgnis, in Dateien von Auskunftei-Unternehmen gespeichert zu sein, ohne dies bisher gewusst zu haben. Die Betroffenen hatten vor allem Fragen nach der rechtlichen Zulässigkeit und nach persönlichen Abwehrrechten.

Das Tätigkeitsfeld von Handels- und Wirtschaftsauskunfteien besteht in der Sammlung von Informationen über die Kreditwürdigkeit, die Bonität und die wirtschaftliche Betätigung von Unternehmen und Privatpersonen. Die Tätigkeit der Auskunfteien ist zulässig, sofern sie sich im Rahmen der besonderen gesetzlichen Zulassungsbedingungen und der Regelungen des Bundesdatenschutzgesetzes (BDSG) bewegt.

Die Form der Benachrichtigung war jeweils nicht zu beanstanden. Die Auskunfteien kamen damit ihrer Verpflichtung aus § 33 Abs. 1 Satz 2 BDSG nach. Die Kenntnis über die Speicherung von Daten ist Voraussetzung für die Ausübung der eigenen weiteren Rechte durch den Betroffenen - insbesondere des Rechtes auf Auskunft gemäß § 34 BDSG über die zu seiner Person gespeicherten Daten, den Speicherungszweck und die Kategorien von Empfängern, an die die Daten weitergegeben werden. Ferner besteht gemäß § 35 BDSG das Recht auf Berichtigung bzw. Sperrung, falls die Daten unrichtig sind, oder - bei Unzulässigkeit der Speicherung - das Recht auf Löschung der Daten.

Die Zulässigkeit der Weiterübermittlung der Daten an Dritte regelt sich nach § 29 Abs. 2 BDSG. Danach ist die Übermittlung von personenbezogenen Daten durch Auskunfteien an Dritte nur dann zulässig, wenn der Dritte ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat und insbesondere kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung hat. Dabei muss das berechtigte Interesse des Anfragenden jeweils begründet werden. Anfragen werden überwiegend durch Geschäftsleute gestellt und betreffen zum großen Teil Firmen, die sich über andere Unternehmen erkundigen. Anfragen über Privatpersonen erfolgen oft seitens des Versandhandels, aber auch durch Banken, Kaufhäuser oder andere Firmen, die Kontakte mit dem jeweiligen Privatkunden haben. Eine Auskunft ist zulässig, sofern ein konkretes berechtigtes Interesse besteht. In vielen Fällen begründet sich dieses berechtigte Interesse durch einen Kauf, für den die Rechnung erst später erstellt oder in Ratenzahlungen beglichen wird.

Der Übermittlung der gespeicherten Daten stehen schutzwürdige Interessen der Betroffenen entgegen, falls die personenbezogenen Angaben nicht zur Beurteilung der Zahlungsfähigkeit bzw. der Kreditwürdigkeit der Betroffenen dienen - insbesondere im Falle unrichtiger Daten. Eine Verletzung des schutzwürdigen Interesses eines Betroffenen läge auch vor bei Angaben zu dessen Gesundheitszustand, da es sich hierbei um sensible personenbezogene Daten gemäß § 3 Abs. 9 BDSG handelt.

Der Düsseldorfer Kreis hat in den Sitzungen am 17./18. April 2008 und am 22. Oktober 2009 im Zusammenhang mit der Tätigkeit von Auskunfteien zwei Beschlüsse gefasst. Diese beschäftigen sich zum einen mit der Zulässigkeit von Bonitätsanfragen durch Vermieter über (künftige) Mieter und zum anderen mit der Erteilung von Bonitätsauskünften speziell beim Versandhandel und bei Dauerschuldverhältnissen (siehe Anlagen 2.4 und 2.9).

4. Arbeitskreis „Technische und organisatorische Datenschutzfragen“

4.1 Turnusmäßige Sitzungen

Auch in diesem Berichtszeitraum fanden unter meiner Federführung wieder vier turnusmäßige Sitzungen des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ (AK Technik) der Konferenz der Datenschutzbeauftragten des Bundes und der Länder statt.

In einem besonders festlichen Rahmen fand im Februar 2008 die **50. Sitzung des AK Technik** statt. Aus Anlass dieses Jubiläums hatte ich zu einer Festsitzung in die Aula der Ernst-Moritz-Arndt-Universität der Hansestadt Greifswald eingeladen. Zu den über 100 Gästen aus Deutschland und der Schweiz zählten viele Kolleginnen und Kollegen, betriebliche und behördliche Datenschutzbeauftragte, Landtagsabgeordnete, führende Vertreter der Wirtschaft des Landes sowie zahlreiche Mitarbeiterinnen und Mitarbeiter aus Behörden, Unternehmen und Universitäten. Mit der Übernahme der Schirmherrschaft über die Veranstaltung verdeutlichte die Präsidentin des Landtages Mecklenburg-Vorpommern, welch hohen Stellenwert der Datenschutz in Mecklenburg-Vorpommern genießt.

Als Motto der Festsitzung diente ein Zitat von Heinrich Heine, das auch Hermann Kant seinem Roman „Die Aula“ - dem Ort der Festsitzung - voranstellte: „Der heutige Tag ist ein Resultat des gestrigen. Was dieser gewollt hat, müssen wir erforschen, wenn wir zu wissen wünschen, was jener will.“ Ich hatte meine Gäste eingeladen, einen Blick zurück auf die Entwicklung des technischen Datenschutzes zu werfen, um einen Blick in die (wahrscheinliche) Zukunft zu ermöglichen und damit bei der Bewältigung der aktuellen Aufgaben Unterstützung zu finden.

Dr. Peter Münch, Technikvorstand der Gesellschaft für Datenschutz und Datensicherung e. V. (GDD), eröffnete die Festsitzung mit einem Grußwort. Mit Blick auf die zunehmende Verflechtung von Wirtschaft und Verwaltung appellierte er an die Mitglieder des AK Technik, künftig noch enger mit der Wirtschaft zusammenzuarbeiten. Er begrüßte jedoch ausdrücklich, dass die Arbeitsergebnisse des AK Technik auch in der Wirtschaft zunehmend genutzt werden.

Die Festrede hielt Professor Dr. Friedemann Mattern von der Eidgenössischen Technischen Hochschule Zürich. Als ausgewiesenen Experten auf den Gebieten „Verteilte Systeme“, „Ubiquitous Computing“ und Infrastrukturmechanismen für das „Internet der Dinge“ hatte ich Professor Mattern gebeten, die Herausforderungen der technischen Entwicklungen zu beschreiben und einen Ausblick auf die mögliche Tagesordnung der 100. Sitzung des AK Technik zu geben.

In einem äußerst unterhaltsamen und sehr informativen Vortrag beschrieb er zunächst die Zukunftsvisionen der Forscher des angehenden 20. Jahrhunderts und zeigte, dass deren Prognosen nur zu einem geringen Teil Realität geworden sind. Selbst die Vorhersagen der 50er und 60er Jahre des vergangenen Jahrhunderts waren noch zu optimistisch. Einen direkten Bezug zu aktuellen Datenschutzthemen stellte Professor Mattern mit der Prognose von Kahn und Wiener her, die 1967 vorausgesagt hatten, dass es „eine einzige, nationale Informationsspeicheranlage mit allen Daten über Steuern, Gesetze, nationale Sicherheit, Kredite, Bildung, medizinische, berufliche und andere Informationen über alle Staatsbürger“ geben würde.

Wie schwer seine Aufgabe sei, die Tagesordnung der 100. Sitzung vorherzusagen, verdeutlichte Mattern dann mit den nicht vorhergesehenen Technikentwicklungen. Niemand hatte zur damaligen Zeit etwa Desktop Publishing, GPS-Lokalisierung oder eingebettete Systeme vorausgesehen, und völlig unvorstellbar waren damals YouTube, Wikipedia, Google oder Amazon.

Dennoch wagte Mattern - zum Teil mit einem Augenzwinkern - den Blick in die Zukunft. Es könnte sein, dass in 25 Jahren Themen wie SmartDust, Fernwartung von Implantaten oder Datenschutz bei implantierten Bodyservices auf der Tagesordnung stehen. Auch E-Pass-Viren, Avatar-Mining bei MySpace oder Herzschrittmacher-Hacking wären nicht auszuschließen. So fanden es die Zuhörer auch gar nicht abwegig, dass RFID in Geldscheinen, ein Archivgesetz für IP-Adressen oder die elektronische Steuererfassung die Datenschützer künftig beschäftigen. Ernsthaft müsse man sich allerdings Gedanken darüber machen, ob der Begriff „Datenschutz“ künftig nicht wesentlich umfassender interpretiert werden sollte und vielleicht sogar durch „Menschenwürdeschutz“ ersetzt werden muss.

Peter Schaar, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, sprach in seinem Vortrag über die Modernisierung des Datenschutzrechtes und die Ethik der Informationsgesellschaft. Mit seinen Hinweisen auf die verschiedenen aktuellen Vorschläge deutscher und internationaler Politiker zur weiteren Einschränkung von Persönlichkeitsrechten verdeutlichte Schaar den Teilnehmern der Festsitzung auf eindrucksvolle Weise, welchen Stellenwert technische Aspekte beim Schutz der Privatsphäre Einzelner schon immer hatten und künftig in verstärktem Maße haben werden.

Schließlich kam mit Uwe Jürgens auch ein Gründungsmitglied des AK Technik zu Wort. Sein Rückblick auf 27 Jahre AK Technik zeigte, dass Themen von 1981 teilweise noch heute aktuell sind. Jürgens plauderte natürlich auch etwas aus dem Nähkästchen. Dass neben intensiven fachlichen Diskussionen die Weiterentwicklung der kulturell/kulinarischen Kompetenz nie zu kurz kam, verschwieg er genauso wenig wie die Tatsache, dass es die Techniker als Exoten in den Datenschutzdienststellen oftmals nicht so leicht hatten.

Den Abschluss der gelungenen Veranstaltung bildete ein festlicher Empfang, zu dem die Landtagspräsidentin mit Unterstützung der GDD und der Energiewerke Nord GmbH eingeladen hatte.

Neben der Festsitzung hatten die Mitglieder des Arbeitskreises aber auch wieder ein umfangreiches Fachprogramm abzuarbeiten. So wurde die Orientierungshilfe „Datenschutzförderndes Identitätsmanagement“ verabschiedet und ein begleitender Entschließungsentwurf für die Datenschutzkonferenz erarbeitet (siehe Punkt 2.14.5). Weiterhin wurde vor dem Hintergrund der Mängel beim Antragsverfahren für elektronische Reisepässe (siehe Achter Tätigkeitsbericht, Punkt 2.4.7) über Verbesserungen des Verfahrens und über mögliche Formen der Zusammenarbeit mit dem Bundesinnenministerium und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) beraten.

Die **51. Sitzung des AK Technik** fand im Oktober 2008 in Mainz statt. Bei der Organisation der Sitzung konnte ich die tatkräftige Unterstützung meiner Kollegen aus Rheinland-Pfalz in Anspruch nehmen. Das Schwerpunktthema dieser Sitzung war das Verfahren zum elektronischen Entgeltnachweis ELENA (siehe Punkt 2.9.4). Ich hatte Vertreter der Informationstechnischen Servicestelle der gesetzlichen Krankenversicherung (ITSG) eingeladen, die maßgeblich an der Entwicklung des Verfahrens und der Durchführung mehrerer Pilotprojekte zum Test des Verfahrens beteiligt waren. Die ITSG stellte den damals aktuellen Verfahrensstand vor. Im Ergebnis formulierte der Arbeitskreis eine Reihe von Anforderungen etwa in Bezug auf Schlüsselverwaltung, Daten-Löschkonzept, Signaturkarten der Sachbearbeiter oder personeller, organisatorischer und infrastrukturell/technischer Trennung der Zentralen Speicherstelle, die im damaligen Entwurf des ELENA-Verfahrensgesetzes berücksichtigt werden müssten. Während der 51. Sitzung des AK Technik wurden zudem die vollständig überarbeitete Orientierungshilfe Internet verabschiedet (siehe Punkt 2.14.8) und Datenschutzaspekte des Grobkonzeptes zur Einführung des neuen (elektronischen) Personalausweises beraten (siehe Punkt 2.4.9).

Mit der **52. Sitzung des AK Technik** im Februar 2009 betrat ich insofern Neuland, als dass wir uns auf Einladung des Datenschutzbeauftragten des Kantons Zürich erstmals im Ausland trafen. Damit wurde der zunehmenden Bedeutung der Länder übergreifenden Zusammenarbeit im Datenschutz noch mehr Rechnung getragen als bisher. Denn bereits seit einigen Jahren nehmen regelmäßig Vertreter von Datenschutzbehörden aus der Schweiz, aus Österreich und aus Liechtenstein an den Sitzungen des AK Technik teil.

Während der Sitzung informierte der Gastgeber, Herr Dr. Bruno Baeriswyl, Datenschutzbeauftragter des Kantons Zürich, die Mitglieder des AK Technik sowohl über die Arbeitsschwerpunkte als auch über die Strategien und Methoden seiner Behörde insbesondere bei der Kontrolle des technischen Datenschutzes. Besonders hob er hervor, dass die Ergebnisse der IT-Revision ebenso wie die der anderen Tätigkeitsfelder des DSB Zürich mit einem Qualitätsmanagementsystem nach ISO 9001 gemessen werden. Neben diesen sehr interessanten Einblicken in das Tätigkeitsfeld der Schweizer Kollegen konnten sich die Mitglieder des Arbeitskreises zudem über Schwachstellen in Web Applikationen informieren. Professor Rennhard von der Zürcher Hochschule für Angewandte Wissenschaften erläuterte und klassifizierte derartige Schwachstellen, demonstrierte entsprechende Angriffsszenarien wie SQL-Injection oder Cross Site Scripting und beschrieb mögliche Gegenmaßnahmen und deren Wirksamkeit.

Während dieser Sitzung beriet der Arbeitskreis zudem über den Entwurf des BSI-Gesetzes (siehe Punkt 2.1.4) und entwarf eine Entschließung mit Forderungen an den Bundesgesetzgeber, befasste sich erneut mit aktuellen Datenschutzfragen des ELENA-Verfahrens und beriet über Möglichkeiten der Novellierung von Technikregelungen in den Datenschutzgesetzen.

Zur **53. Sitzung des AK Technik** im Oktober 2009 lud ich die Arbeitskreismitglieder nach Schwerin ein. Erneut stand das ELENA-Verfahren im Mittelpunkt der Beratungen. Gemeinsam mit dem Bundesdatenschutzbeauftragten, der ITSG und der Deutschen Rentenversicherung Bund als Betreiber der Zentralen Speicherstelle (ZSS) wurde über Datenschutz- und IT-Sicherheitsaspekte beim Betrieb der ZSS beraten.

Um den Einblick in ein vergleichbares Projekt zu bekommen, hatte ich einen Vertreter der Österreichischen Datenschutzkommission (DSK) eingeladen. Er beschrieb, wie in Österreich aus der sogenannten Stammzahl einer Person bereichsspezifische Personenkennzeichen für verschiedene Verwaltungszwecke gebildet werden, und erläuterte die Rolle der DSK beim Einsatz des Krypto-Moduls, das zur Bildung der Kennzeichen verwendet wird.

Während dieser Sitzung nahm die Diskussion zur Neuformulierung der Schutzziele in den Landesdatenschutzgesetzen einen breiten Raum ein (Details dazu siehe unten). Darüber hinaus wurde über die technische Umsetzung von Zugriffsregelungen in Krankenhausinformationssystemen beraten und eine Arbeitsgruppe zur Formulierung detaillierter Anforderungen in diesem Bereich gebildet.

4.2 Jährliche Workshops

Die im letzten Berichtszeitraum erstmalig durchgeführten Workshops des AK Technik haben sich bewährt. Die gemeinsame Weiterbildung von Juristen und Technikern der Datenschutzdienststellen von Bund und Ländern hat dazu beigetragen, fachübergreifende Kenntnisse zu gewinnen und Datenschutzberatung auf hohem Niveau anbieten zu können.

Auch in diesem Berichtszeitraum habe ich wieder zwei Workshops organisiert. Im Mai 2008 veranstaltete ich gemeinsam mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit einen Workshop zum Antragsverfahren für elektronische Reisepässe. Eingeladen waren neben Juristen und Technikern der Datenschutzbeauftragten Vertreter des Bundesinnenministeriums (BMI), des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und der Bundesdruckerei sowie Hersteller von Software für Passbehörden. Gemeinsam wurde beraten, wie die in Kontrollen festgestellten Mängel des Antragsverfahrens (siehe Achter Tätigkeitsbericht, Punkt 2.4.7) abgestellt und die detaillierten Sicherheitsempfehlungen des BSI (die sogenannten Technischen Richtlinien) insbesondere in den Passbehörden umgesetzt werden können. Im Ergebnis sagte das BMI zu, eine Handreichung für die Passbehörden zu erstellen, die einen Überblick über Standard-Sicherheitsmaßnahmen gibt, mit denen Passbehörden das gesetzlich geforderte Schutzniveau einhalten können. Nach intensiver Abstimmung mit dem AK Technik lag die erste Version des Papiers im Oktober 2008 vor. Eine überarbeitete Version der Handreichung erhielten die Passbehörden im Dezember 2008.

Der Workshop im September 2009 befasste sich mit dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, das das Bundesverfassungsgericht im Februar 2008 im Zusammenhang mit seinem Urteil zur sogenannten Online-Durchsuchung abgeleitet hatte. Ich hatte Kolleginnen und Kollegen von Bund und Ländern in die Landesvertretung Mecklenburg-Vorpommerns beim Bund nach Berlin eingeladen, um gemeinsam mit renommierten Wissenschaftlern über die Auswirkungen des Urteils auf den Datenschutz in Deutschland zu beraten. Professor Dr. Matthias Bäcker von der Universität Mannheim erläuterte zunächst die Grundzüge des Urteils des Bundesverfassungsgerichts zur „Online-Durchsuchung“ und die Ableitung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Mögliche Auswirkungen des Urteils des Bundesverfassungsgerichts auf die zu erwartende Entwicklung des Datenschutzrechts beschrieb sodann Professor Dr. Martin Kutscha von der FHVR Berlin.

Schließlich befasste sich Professor Dr. Andreas Pfitzmann (TU Berlin) mit den zu erwartenden Konsequenzen für die Entwicklungen im datenschutztechnischen Bereich. Alle Teilnehmer konnten wertvolle Anregungen für die tägliche Arbeit in den Datenschutzdienststellen mitnehmen und erste Ideen entwickeln, welche Änderungen im Datenschutzrecht erforderlich sind, um die Anforderungen des neuen Grundrechts umzusetzen.

4.3 Gemeinsame Weiterbildung

Die tägliche Kontroll- und Beratungspraxis hat gezeigt, dass insbesondere im Technikbereich ein permanenter Fortbildungsbedarf vorhanden ist. Dieser Bedarf besteht in vergleichbarer Weise in allen Datenschutzaufsichtsbehörden von Bund und Ländern. Vor diesem Hintergrund habe ich angeboten, unter dem Dach des AK Technik gemeinsame Schulungsveranstaltungen zu organisieren. Auf diese Weise können Schulungsinhalte genau auf unsere Tätigkeit zugeschnitten und nicht zuletzt auch erhebliche Kosten eingespart werden.

Eine Bedarfsabfrage unter meinen Kollegen ergab vordringlichen Schulungsbedarf für die Themen Virtualisierung, Grundschutzmethodik des BSI und Datenschutzfragen beim Einsatz von SAP-Software. Im Berichtszeitraum habe ich daher zunächst zu diesen drei Themenblöcken jeweils eine Weiterbildungsveranstaltung organisiert. Die Seminare waren sehr gut besucht, sodass schon jetzt absehbar ist, dass weitere Veranstaltungen dieser Art folgen werden.

4.4 Modernisierung der Technikregeln

Der AK Technik hat in seiner 51. Sitzung eine Arbeitsgruppe eingerichtet, die Vorschläge für eine Novellierung des Bundesdatenschutzgesetzes und der Landesdatenschutzgesetze im Technikbereich erarbeiten sollte. Anlass hierfür war das Urteil des Bundesverfassungsgerichts zur „Online-Durchsuchung“ und die Ableitung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Bereits vor etwa 10 Jahren waren Novellierungsvorschläge einer ähnlichen Arbeitsgruppe des AK Technik im Zusammenhang mit der Umsetzung der EU-Datenschutzrichtlinie in zahlreiche Landesdatenschutzgesetze, unter anderem in das DSG M-V, eingeflossen.

Die Arbeitsgruppe hatte sich die Aufgabe gestellt, elementare und Technik unabhängige Schutzziele zu definieren, aus denen sich weitere Schutzziele systematisch herleiten lassen. Die Schutzziele sollten einfach, verständlich und praxistauglich sein. Sie sollten soweit wie möglich den elementaren Schutzzielen der IT-Sicherheit (Verfügbarkeit, Unversehrtheit, Vertraulichkeit) entsprechen und/oder zumindest mit ihnen korrespondieren. Gleichzeitig sollte aber die spezielle Sichtweise des Datenschutzes zum Tragen kommen. Auf der Basis der Schutzziele sollte sich ein Katalog von Datenschutzmaßnahmen ableiten lassen, die - ähnlich dem IT-Grundschutzkatalog des BSI - in ein flexibles, einfaches, praxistaugliches und durch Software unterstütztes Verfahren umgesetzt und als Kriterien-Katalog eines Datenschutzaudits herangezogen werden können.

Der im Dezember 2009 vorgelegte Formulierungsvorschlag der Arbeitsgruppe umfasste dann die bereits im DSG M-V festgelegten Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Transparenz (vgl. § 21 Abs. 2). Als neue Schutzziele wurden Zweckbindung (Verfahren sind so einzurichten, dass deren Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können) und Intervenierbarkeit (Verfahren sind so zu gestalten, dass sie dem Betroffenen die Ausübung der ihm zustehenden Rechte wirksam ermöglichen) vorgeschlagen. Die Novellierungsvorschläge sind in die Eckpunkte zur Modernisierung des Datenschutzrechts aufgenommen worden, die eine Arbeitsgruppe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder entwickelt hat und die als Richtschnur für die Novellierung des deutschen Datenschutzrechts dienen soll.

5. Öffentlichkeitsarbeit

5.1 Datenschutz-Fachtagung 2008: Datenschutz im Tourismusland – Zwischen Marketing und Kundenvertrauen

Am 17. Juli 2008 fand die jährliche Datenschutz-Fachtagung zum Thema „Datenschutz im Tourismusland - Zwischen Marketing und Kundenvertrauen“ im kurz zuvor eröffneten Ozeaneum in Stralsund statt. Der Einladung waren rund 140 Vertreter vor allem aus der Tourismuswirtschaft, der Politik und der Wissenschaft gefolgt. Sie konnten sich anhand etlicher Beispiele von der Attraktivität Mecklenburg-Vorpommerns als Tourismusland im Allgemeinen und Stralsunds im Besonderen überzeugen.

Der Chef der Staatskanzlei Mecklenburg-Vorpommern und Präsident des Deutschen Tourismusverbandes e. V., Herr Staatssekretär Reinhard Meyer, sprach zu Beginn der Fachtagung das Grußwort. Er betonte - insbesondere auch aus den Erfahrungen aus seiner Tätigkeit als Präsident des Tourismusverbandes -, dass es für das Kundenvertrauen einerseits unerlässlich ist, die Rechte der Urlauber, unter anderem das Recht auf informationelle Selbstbestimmung, zu wahren. Andererseits wünschen viele Urlauber eine besondere persönliche Beratung und Betreuung, die nur geleistet werden kann, wenn personenbezogene Daten verarbeitet werden. Die Datenverarbeitung muss dabei für jeden Urlauber transparent sein, um Kundenvertrauen zu erreichen.

Die Vorträge der Datenschutz-Fachtagung stehen unter folgender Adresse zur Verfügung: www.datenschutz-mv.de/dschutz/veransta/touri/index-touri.html.

Das Schlusswort der Fachtagung sprach Herr Alexander Alvaro, Mitglied des Europäischen Parlaments. Herr Alvaro schilderte sehr anschaulich das Bemühen der Parlamentarier, in das Fluggastabkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika datenschutzrechtliche Leitlinien einzufügen. Das Schlusswort ermutigte die Teilnehmer der Fachtagung, sich für das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger - also den Datenschutz - einzusetzen.

5.2 Datenschutz-Fachtagung 2009: Privatsphäre – gefangen im Netz der Koordinaten

Die jährliche Fachtagung habe ich im Jahr 2009 gemeinsam mit dem Deutschen Zentrum für Luft- und Raumfahrt e. V. Neustrelitz unter dem Motto „Privatsphäre - gefangen im Netz der Koordinaten“ veranstaltet. In der Aula des Neustrelitzer Gymnasiums Carolinum diskutierten rund 130 Fachleute aus Politik, Wirtschaft, Forschung und Verwaltung über Datenschutzaspekte beim Umgang mit Geodaten in Wirtschaft und Verwaltung.

In seinem Grußwort gab Dr. Stefan Rudolph, Staatssekretär im Ministerium für Wirtschaft, Arbeit und Tourismus des Landes Mecklenburg-Vorpommern, seiner Hoffnung Ausdruck, dass die Tagung mit dazu beitragen wird, eine Datenschutzstrategie zu entwickeln, die den Gedanken berücksichtigt, dass ein präventiver Datenschutz wirtschaftlicher ist als ein repressiver Datenschutz. Er erinnerte daran, dass Geo-Informationen die Grundlage für etwa 80% aller Entscheidungen im privaten und im wirtschaftlichen Leben sind. Beim Schutz der Privatsphäre müsse gelten: Agieren ist vernünftiger als reagieren!

Im ersten Fachvortrag vermittelte Holger Maass vom Deutschen Zentrum für Luft- und Raumfahrt e. V. einen Eindruck davon, welche Möglichkeiten von Informationsprodukten und -diensten bereits heute auf der Grundlage von Satellitensystemen existieren. Er beschrieb den Informationsweg von Satellitendaten von der Bestellung über die Satellitenaufnahme bis hin zur Auslieferung an den Kunden am Beispiel von TerraSAR-X Daten und stellte den unmittelbaren Zusammenhang zwischen Sicherheits- und Datenschutzanforderungen dar.

Professorin Lesley Jane Smith, Spezialistin für Fragen des Weltraumrechts, betrachtete das Thema Geodaten zunächst aus der Sicht der Informationsfreiheit und stellte die Frage, ob es in der Informationsgesellschaft auch ein grundsätzliches Recht auf Zugang zu Geodaten gäbe. Sie geht davon aus, dass in absehbarer Zeit auf europäischer Ebene Geo-Portale mit öffentlichen Informationen dieses Quasi-Recht verstärkt unterstützen werden. In ihrem Vortrag erörterte Professorin Smith Regulierungsansätze für den Umgang mit Geo-Daten. Diese könnten von einer Mithaftung des Geodaten-Betreibers für verarbeitete Erdbeobachtungsinformationen bis hin zur Genehmigungspflicht zur Weitergabe von Geodaten durch die betroffenen Staaten reichen. Neue Lösungen können nicht allein in Händen des nationalen Gesetzgebers liegen, sondern müssen auf der zuständigen europäischen und internationalen Regulierungsebene systematisch angegangen und diskutiert werden.

Dr. Martin Fornefeld, Geschäftsführer der MICUS Management Consulting GmbH, beschrieb den Umsetzungsstand der Richtlinie 2007/2/EG zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (INSPIRE-Richtlinie). Er erläuterte den Zusammenhang der Richtlinie und des daraus folgenden Geodatenzugangsgesetzes mit dem Informationsweiterverwendungsgesetz (IWG), dem Umweltinformationsgesetz (UIG) und dem Informationsfreiheitsgesetz (IFG).

Dr. Hartmut Streuff aus dem Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit war innerhalb der Bundesregierung federführend verantwortlich für die Erarbeitung der INSPIRE-Richtlinie sowie deren Umsetzung auf Bundesebene mittels des Geodatenzugangsgesetzes.

In seinem Vortrag erläuterte er seine Sicht auf die Datenschutzaspekte dieses neuen Bundesgesetzes. Er setzte sich detailliert mit der Kritik der Konferenz der Datenschutzbeauftragten von Bund und Ländern am Geodatenzugangsgesetz auseinander (siehe Punkt 2.1.2) und kam zu dem Ergebnis, dass - entgegen der Auffassung der Datenschützer - beim Zugang der Öffentlichkeit zu Geodaten und Geodatendiensten der Schutz personenbezogener Daten schon jetzt angemessen berücksichtigt sei. Dr. Streuff warb für einen - im Rahmen des unabweisbar notwendigen Schutzes personenbezogener Daten - möglichst offenen Umgang mit Geodaten und Geodatendiensten, um die Ziele der INSPIRE-Richtlinie (Transparenz, Teilhabe, Verwaltungsvereinfachung, Aktivierung des Wertschöpfungspotenzials) nicht zu gefährden.

Marco Klisch, Leiter des Fachbereiches „Landeskoordinierungsstelle für Geoinformationssysteme“ im Landesamt für innere Verwaltung Mecklenburg-Vorpommern, stellte das GeoPortal.MV vor, das als zentraler Zugangsknoten zur Geodateninfrastruktur Mecklenburg-Vorpommerns den Zugang zu einer Vielzahl von raumbezogenen Informationen aus verschiedenen Bereichen der öffentlichen Verwaltung in Mecklenburg-Vorpommern ermöglicht. Er erläuterte die unterschiedlichen Sicherungsmechanismen auf Portal-, Netz- und Diensteebene für zugangsbeschränkte Geodatenangebote und zeigte damit, dass zumindest aus technischer Sicht Zugangsberechtigungen mit klassischen Rechte- und Rollenmanagementsystemen steuerbar sind.

Die Wünsche der Geodatenwirtschaft Deutschlands erläuterte Dr. Jörg Reichling, Leiter der Geschäftsstelle der Kommission für Geoinformationswirtschaft. Er zitierte ein Memorandum der GIW-Kommission vom April 2005, in dem Geoinformation als „Digitaler Rohstoff“ und somit als Beitrag zur Förderung und Sicherung des Wirtschaftsstandortes Deutschland charakterisiert wird. Dr. Reichling geht davon aus, dass nicht nur gute Qualität, hohe Verfügbarkeit, einfacher Zugang und wirtschaftliche Preismodelle, sondern auch vernünftiger Datenschutz zu optimierten Geschäftsprozessen und neuen Geschäftsmodellen führen werden.

Im letzten Fachbeitrag des Tages arbeitete Dr. Thilo Weichert, Landesbeauftragter für den Datenschutz Schleswig-Holstein, heraus, dass trotz unterschiedlicher Erscheinungsformen und Zwecke der Verarbeitung von Geodaten immer wieder die gleichen rechtlichen Fragestellungen diskutiert werden. Wann kann und muss ein Personenbezug von Geodaten angenommen werden? Welche Konsequenzen hat es, dass Geodaten allgemein zugänglich sind? Bestehen generelle Informationsinteressen, welche die Veröffentlichung besonderer Geodaten rechtfertigen? Nach welchen Kriterien und über welche Verfahren kann eine pauschalierte Interessenabwägung zwischen Persönlichkeitsschutz und Informationsinteresse vorgenommen werden? Bei der Beantwortung dieser Fragen wäre die Besonderheit von Geodaten zu berücksichtigen, dass diesen praktisch immer ein latenter Personenbezug anhaftet, ohne dass es gerechtfertigt wäre, in jedem Fall die strengen Regeln des allgemeinen Datenschutzrechtes anzuwenden. Jedenfalls handele es sich bei der Feststellung des Personenbezugs um einen objektiven Vorgang, der bei globaler Verfügbarkeit von Verkettungsdaten völlig unabhängig ist von der Identität und von den Intentionen der Daten haltenden Stelle. Dr. Weichert distanzierte sich von der Auffassung des Instituts für Rechtsinformatik (IRI) an der Leibniz-Universität Hannover, das bei der Feststellung des Personenbezugs auf die Zielsetzung der Verarbeitung abstellt. Vielmehr könne die Frage der Anwendung des Datenschutzrechtes nur davon abhängig sein, ob objektiv eine persönlichkeitsrechtliche Gefährdung besteht und nicht davon, ob die verarbeitende Stelle eine solche Gefährdung bejaht.

Der Vortrag schloss mit dem Appell an die Gesetzgeber, dem auf nationaler wie auf europäischer Ebene bestehenden Regelungsbedarf nachzukommen.

Mein besonderer Dank gilt der Gesellschaft für Datenschutz und Datensicherung e. V., die auf ihre Kosten gemeinsam mit dem Datakontext Verlag alle Tagungsbeiträge in einem Tagungsband veröffentlicht hat. Der Tagungsband kann über meine Dienststelle angefordert werden.

5.3 Zweiter Europäischer Datenschutztag: „Datenschutz macht Schule“

Am 28. Januar 2008 wurde der Zweite Europäische Datenschutztag begangen. Gemeinsam mit dem Deutsch-Polnischen Gymnasium in Löcknitz haben wir einen Projekttag unter dem Titel „Datenschutz macht Schule“ durchgeführt. Der europäische Charakter konnte durch die Veranstaltung an diesem Gymnasium sehr gut dargestellt werden. Die gemeinsame Vorbereitung des Zweiten Europäischen Datenschutztages begann im September 2007. Wir verabredeten folgendes Programm: Nach einem kurzen Einführungsvortrag sollten vier Arbeitsgruppen von Schülern verschiedene Themen am Vormittag weitgehend selbständig bearbeiten und am Nachmittag ihre Ergebnisse präsentieren. In den Arbeitsgruppen wurden folgende Themen bearbeitet: „Würde des Menschen und personenbezogene Daten“, „Wer sammelt Daten und was kann man damit machen?“, „Datensammlung durch Internet-Foren, Fotohandy und Co.“ und „Technische Möglichkeiten des Schutzes der Privatsphäre“. Meine Mitarbeiter standen den Schülern bei der Themenbearbeitung hilfreich zur Seite. Die von den Schülern vorgestellten Ergebnisse belegten ihre große Kreativität und zeugten von einer guten Kenntnis der allgemeinen Fragen und Aufgaben des Datenschutzes. Zwei Firmen aus Schwerin haben die Veranstaltung finanziell und mit Sachpreisen für die Schüler unterstützt, was wesentlich zum Gelingen beigetragen hat.

Am Zweiten Europäischen Datenschutztag nahmen als Gäste Mitglieder des Landtages und des Bundestages sowie Mitarbeiter des Ministeriums für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern teil. Die Veranstaltung wurde von einem NDR-Fernsehteam begleitet. In einer Regionalsendung wurde der Bericht ausgestrahlt. Auch andere Medien haben über diesen erfolgreichen Tag berichtet.

Nach der Auswertung des Zweiten Europäischen Datenschutztages habe ich in einem Schreiben an den Staatssekretär des Ministeriums für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern empfohlen, dass Pädagogen gemeinsam mit Mitarbeitern meiner Dienststelle Materialien zum Datenschutz erarbeiten sollten, die dann in geeigneten Unterrichtsveranstaltungen eingesetzt werden könnten. Daraufhin teilte mir der Referent für Informatik und Medienerziehung des Ministeriums im Auftrag des Staatssekretärs unter anderem mit, dass das Thema in der Klasse 11 behandelt werde und darüber hinaus umfangreiche Fortbildungsmaßnahmen zu den Aspekten Jugendmedienschutz und Persönlichkeitsrechte für Lehrerinnen und Lehrer durchgeführt werden. Bei einem Gespräch mit dem Referenten im Bildungsministerium hat er die verschiedenen Aktivitäten vorgestellt. Wir vereinbarten, dass wir anlässlich der Fachtagung Jugendmedienschutz im Schulamtsbereich Schwerin den Workshop „Datenschutz - geht mich das was an?“ gestalten werden. Die Veranstaltung hat am 16. September 2009 stattgefunden.

Meine Hoffnung auf eine intensive und für das Datenschutzwissen der Schülerinnen und Schüler fruchtbringende Zusammenarbeit mit Pädagogen hat sich damit nur teilweise erfüllt. Es wäre daher zu begrüßen, wenn mein Angebot künftig umfassend in Anspruch genommen würde.

6. Projekt „Elektronische Verwaltung und Datenschutz“

Untersuchungen auf kommunaler Ebene am Beispiel des elektronisch zu führenden Melderegisters - Durchführung 2009 - Mecklenburg-Vorpommern

6.1 Vorbemerkungen

In der zweiten Jahreshälfte 2009 hat der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern auf kommunaler Ebene Untersuchungen zum Stand der Umsetzung der Regelungen zum Datenschutz am Beispiel des elektronisch zu führenden Melderegisters durchgeführt. Dazu wurden nach Durchführung einer Erhebung mittels Fragebogen bei allen Kommunen des Landes in rund zwanzig Kommunen unterschiedlicher Art und Größe Besuche durchgeführt, bei denen die Situation vor Ort besprochen wurde und Empfehlungen zur Verbesserung des Datenschutzes abgegeben wurden. Bei den Untersuchungen hat sich gezeigt, dass einige Probleme auch struktureller Natur sind und nicht allein von den Kommunen gelöst werden können. Dieser Bericht[1] gibt die wichtigsten der Ergebnisse wieder.

6.2 Die rechtlichen und technischen Voraussetzungen zu Beginn des Projektes

Das Melderechtsrahmengesetz (MRRG) regelt in Deutschland die Aufgaben und Befugnisse der Meldebehörden. Sie haben in ihrem Zuständigkeitsbereich wohnhafte Personen, deren Adressdaten und noch diverse andere Daten zu registrieren. Das Melderechtsrahmengesetz bildet den Rahmen für die Meldegesetze der Länder, sie haben ihr Melderecht den Vorschriften dieses Gesetzes anzupassen.

Seit der Föderalismusreform ist das Melderecht Bundesangelegenheit. Die Meldegesetze der Länder bleiben nur noch solange in Kraft, bis das in Arbeit befindliche Bundesmeldegesetz in Kraft tritt. Dieses wird auch das Melderechtsrahmengesetz ablösen.[2]

Bestimmte Regelungen im Melderechtsrahmengesetz legen fest, dass die Rückmeldungen zwischen den Meldebehörden bei Umzügen ab 1. Januar 2007 nur noch elektronisch erfolgen dürfen. Bürger müssen sich somit nur noch bei der Zuzugsmeldebehörde anmelden. Die Abmeldung von der Wegzugsmeldebehörde durch den Bürger bei Umzügen innerhalb Deutschlands wurde abgeschafft. Auch Mecklenburg-Vorpommern war daher verpflichtet, sein Landesmeldegesetz[3] an diese Bedingungen anzupassen.

Mit den Vorschriften des Melderechtsrahmengesetzes wurde im Ergebnis eine verbindliche einheitliche Struktur festgelegt, auf der ein Austausch von Meldedaten zwischen den Meldebehörden bundesweit zu erfolgen hat. In Folge der Bestimmungen des Melderechtsrahmengesetzes wurden die Länder und Kommunen verpflichtet, bestimmte technische Voraussetzungen zu schaffen, die einen solchen Datenaustausch ermöglichen. Die Regelungen bedeuteten für alle Kommunen in Mecklenburg-Vorpommern zweierlei: Zum einen mussten alle Kommunen über ein Netz miteinander verbunden sein, das eine elektronische Datenübertragung ermöglicht, um die gesetzlich vorgeschriebenen Datenübermittlungen an andere Gemeinden vornehmen zu können. Zum anderen musste selbst die kleinste Gemeinde, die vielleicht bisher ihre Einwohnermeldedaten noch auf Karteikarten geführt hatte, diese Daten in elektronischer Form vorhalten.

Vieles von dem, was der Bundesgesetzgeber von den Ländern erwartete, war oft nicht oder nur sehr rudimentär vorhanden; so verhielt es sich auch in Mecklenburg-Vorpommern. Es gab zwar hier und da kleine kommunale Netze, die teilweise sogar mit der Kreisebene verbunden waren, aber es gab hier weder eine einheitliche Netztechnik, noch gab es auf kommunaler Ebene elektronische Übergabeknoten zu anderen Bundesländern. Die meisten Kommunen waren ohnehin nicht oder allenfalls „inhouse“ vernetzt. Ebenso unterschiedlich verhielt es sich mit der Software, mit der die Melderegister der Kommunen geführt wurden. Es gab kein einheitliches, von allen Kommunen genutztes Programm, auch waren bei den Programmen die eingesetzten Programmversionen oft nicht gleich und schließlich waren die meisten eingesetzten Programme zur Meldedatenverarbeitung nicht netzwerkfähig ausgelegt.

Das Land stand daher vor der Aufgabe, binnen eines Zeitraums von zwei Jahren[4] die genannten technischen Voraussetzungen zu schaffen, denn das Melderechtsrahmengesetz hatte eine Frist gesetzt, bis zu der ein funktionierendes System landesweit eingeführt sein musste. Fest stand dabei lediglich das Ergebnis; wie und in welcher Form das Ganze umgesetzt werden sollte, blieb den Ländern überlassen. So setzte denn neben einer gesetzgeberischen Debatte über das Landesmeldegesetz auch eine Diskussion über den Einsatz der Informations- und Kommunikationstechnik, Netztechnik und Netzstruktur und die damit verbundenen Kosten ein und alle Themen waren auch Datenschutzthemen und wurden daher vom Landesbeauftragten für den Datenschutz begleitet.

Tatsächlich, wenn auch gelegentlich mit heißer Nadel gestrickt, wurde es geschafft, alle Kommunen des Landes an das bundesweite Datenaustauschnetz der Meldebehörden anzuschließen, wobei im Groben das Land in Funktion des Innenministeriums mit Unterstützung der DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH (DVZ) den Ausbau des Landesdatennetzes (Corporate Network LAVINE), sprich der Datenübertragungswege und die Schaffung des für den sicheren Datenaustausch notwendigen zentralen Informationsregisters (ZIR) als landesseitigen Übergabeknoten, vorantrieb. Die Kommunen hingegen schufen die technischen Voraussetzungen dafür, dass ihre elektronischen Melderegister über das Netz die notwendigen Daten für den Datenaustausch mit anderen Meldebehörden zur Verfügung stellten.

Im Zuge der Umsetzung der Vorgaben des Melderechtsrahmengesetzes wurde in Mecklenburg-Vorpommern somit erstmalig eine einheitliche Datennetzstruktur geschaffen, die alle Kommunen und Kreise miteinander vernetzt. Um die Datenübertragung sicher zu gestalten, wurde nicht zuletzt auf Anraten des Landesbeauftragten für den Datenschutz an allen Endknoten des Netzes in den Gemeinden und Kreisen eine Kommunikationsbox (KOMM-Box) installiert, die eine OSCI-konforme verschlüsselte und signierte Übertragung der Daten sicherstellt.

Damit war nicht nur die erste bundesweit einheitliche Kommunikationsstruktur für die kommunale Ebene geschaffen, nein, auch im Land sind nun Land, Kreise und alle Kommunen miteinander vernetzt. Und das Datennetz ist so ausgelegt, dass es die Infrastruktur für einen Datenaustausch für andere Verfahren ermöglicht. Die mit dem Meldedatenaustauschverfahren verbundene Einführung einer E-Government-Anwendung im Bereich des Meldewesens ist daher nur der erste Schritt; zu erwarten ist, dass eine Vielzahl weiterer Verfahren sich dieser neu geschaffenen Infrastruktur bedienen wird.

Auch, wenn es dem Landesbeauftragten für den Datenschutz gelungen ist, sowohl im Gesetzgebungsverfahren wie auch bei der technischen Umsetzung Einfluss auf eine datenschutzrechtliche wie datenschutztechnische Ausgestaltung zu nehmen, so ist doch zu bedenken, dass mit einer derartig weiten Vernetzung natürlich auch die tatsächlichen und praktischen Datenschutzrisiken wachsen. Wichtig ist es daher sicherzustellen, dass alle am Netz partizipierenden Glieder gleichermaßen stark den Anforderungen des Datenschutzes und damit auch der Datensicherheit Rechnung tragen. Bevor also weitere Verfahren eingeführt werden, die das Landesnetz involvieren, lag es daher nahe, zunächst zu untersuchen, ob und in welchem Umfang auf der kommunalen Ebene den Regelungen der datenschutzrechtlichen Vorschriften Rechnung getragen wird. Dazu hat der Landesbeauftragte Anfang 2009 eine anhand von Anfangsbuchstaben ausgewählte Gruppe von Kommunen mit einer kleinen Umfrage gebeten, ihre Verfahrensverzeichnisse aus dem Meldebereich an ihn zu übersenden. Die Rückäußerungen der Kommunen ließen erahnen, dass der Datenschutz an vielen Stellen noch im Argen liegt.

Unter diesen Gesichtspunkten erschien es angeraten, in einer Stichprobe bei ausgewählten Kommunen eine genauere Untersuchung durchzuführen, wie die Regelungen des Datenschutzes in den Kommunen tatsächlich umgesetzt werden. Um zu erkennen, was und in welchem Umfang etwas für den Datenschutz getan wurde, mussten die Rahmenbedingungen aufgedeckt werden. Damit war vorprogrammiert, dass das Projekt sich auch mit den allgemeinen Bedingungen des Einsatzes personenbezogener elektronischer Datenverarbeitung auseinandersetzen musste.

6.3 Projektaufbau und Ablauf

Im ersten Schritt wurde allen Kommunen ein Fragebogen übersandt, mit dem neben einigen allgemeinen Angaben, z. B. über die Größe der Kommune, abgefragt wurde, ob ein behördlicher Beauftragter für Datenschutz ordentlich bestellt worden ist. Die generelle DV-Struktur der Kommunen wurde abgefragt, insbesondere, ob die elektronisch geführten Datenverarbeitungsverfahren selbst betrieben werden oder die Kommunen ihre Daten durch Dritte (z. B. Fremdfirmen) verarbeiten lassen oder ob Mischformen bestehen. In welchem Umfang welches der Modelle von den Kommunen favorisiert wird, war zum Zeitpunkt des Projektstarts nicht bekannt.[5] Ein Teil des Fragebogens beschäftigt sich speziell mit der Umsetzung des Datenschutzes im Meldewesen bei den Kommunen, hier insbesondere, inwieweit den bei Einführung des neuen Meldeverfahrens bekannt gegebenen Anforderungen des Datenschutzes tatsächlich Rechnung getragen wurde. Der Fragebogen, der auch in elektronischer Form zur Verfügung gestellt wurde[6] und im Anhang abgedruckt ist[7], wurde kurz gehalten, um die Belastungen der Kommunen angesichts der bevorstehenden Bundestagswahlen so gering wie möglich zu halten.[8]

Von wenigen Ausnahmen einmal abgesehen, haben alle Kommunen bei der Fragebogenaktion mitgemacht und die meisten auch in der zeitlichen Vorgabe vollumfängliche Angaben gemacht. Dieses Datenmaterial liefert an sich schon eine Fülle an Informationen über den allgemeinen Zustand des Datenschutzes in den Kommunen und gab weitere Ansatzpunkte für ein weiteres Vorgehen.[9] Einige Ergebnisse der Auswertung von Angaben aus den Fragebögen enthält das nächste Kapitel. Die Ergebnisse bedurften der Interpretation. In einem zweiten Schritt wurde dann eine Stichprobe von 20 Kommunen gezogen, die einer näheren Befragung vor Ort unterzogen wurden.

6.4 Statistische Auswertung[10] und wesentliche Ergebnisse der Fragebogenaktion

§ 20 Abs. 1 S. 1 DSG M-V (Behördlicher Datenschutzbeauftragter) verlangt: „Die Daten verarbeitende Stelle hat schriftlich einen behördlichen Datenschutzbeauftragten sowie einen Vertreter zu bestellen.“

In mittleren wie kleinen Kommunen unterblieben zu gleichen Teilen die Bestellungen von behördlichen Beauftragten für den Datenschutz.

Insgesamt waren in rund 20% die behördlichen Beauftragten für den Datenschutz nicht bestellt. Wie sich in der später vor Ort befragten Stichprobe herausstellte, war dies nicht eine Interimserscheinung, weil etwa ein(e) Beauftragte(r) ausgeschieden war, sondern in allen näher untersuchten Fällen war bisher trotz Geltung des Gesetzes seit 1992 noch nie eine(r) Beauftragte(r) für den Datenschutz bestellt worden. Wenn man zudem in der Vor-Ort-Stichprobe die Zahl derjenigen hochrechnet, die erst eigens aus Anlass des Rundschreibens bestellt wurden, so ist zu vermuten, dass sogar rund 30 % der behördlichen Beauftragten für den Datenschutz im Sommer 2009 nicht bestellt waren! Ist dieses Ergebnis schon ernüchternd, wird es dadurch noch einmal verschlechtert, dass wenigstens 15 % der mit der Aufgabe betrauten Personen nicht formell, wie das Gesetz es vorsieht, zur bzw. zum behördlichen Beauftragten für den Datenschutz offiziell ernannt worden waren, mit der Folge, dass dieser Gruppe die besonderen im Gesetz genannten Rechte bei ihrer Aufgabenwahrnehmung nicht zustanden.

Im Ergebnis waren zwischen 30 % und 40 % der behördlichen Beauftragten für den Datenschutz vor Start des Projektes nicht oder nicht dem Gesetz entsprechend bestellt!

§ 20 Abs.1 S. 3 DSG M-V (Behördlicher Datenschutzbeauftragter) lautet: „Bestellt werden darf nur, wer dadurch keinem Interessenkonflikt mit sonstigen dienstlichen Aufgaben ausgesetzt wird und ...“ In der Befragung genannt wurden u. a. die folgenden Tätigkeiten von behördlichen Datenschutzbeauftragten in der Verwaltung, die mit der Aufgabe im Interessenkonflikt stehen (können):

Abt.-Leiter Organisation und EDV
Arbeitsorganisation, Stellenplanung, EDV-Planung, eGov
Leiter Ordnungsamt
Kämmerer, Leiter Hauptamt
Hauptamt, Gewerbe + Liegenschaften
Leiter Meldebehörde
Leitende Verwaltungsbeamtin/Leitender Verwaltungsbeamter (LVB)
EDV-Administrator
AL, allg. OA
Hauptamtsleiter
Fachbereichsleiter Zentrale Dienste und Finanzmanagement
EDV-Verantwortlicher
Hauptamtsleiterin

Gerade auf kommunaler Ebene ist es natürlich schwer, geeignete Personen für diese Tätigkeit zu finden, die zum einen die vom Gesetz geforderte Sachkunde wie auch die notwendige Unabhängigkeit aufweisen. Hinzu kommt, dass neben Rechtskenntnissen auch ein ausgebildetes technisches Verständnis für die Aufgabe von Nöten ist. Angesichts der immer noch rasanten Entwicklung bei der IuK-Technologie eine nicht leichte Verantwortung. Der vom E-Government-Zweckverband eingeschlagene Weg, externen kommunalen Datenschutzsachverstand zur Verfügung zu stellen, ist eine Lösung und kann insbesondere bei der von den meisten Kommunen völlig außer Acht gelassenen Stellvertreterbestellung eine Hilfe sein.

Ergebnis: Ein nicht unbeträchtlicher Anteil der behördlichen Datenschutzbeauftragten war zugleich mit Verwaltungsaufgaben betraut, die eine unabhängige Kontrolle in Frage stellen.

Ganz überwiegend wird die personenbezogene elektronische Datenverarbeitung durch die Kommunen selbst durchgeführt, nur knapp 4 % der Kommunen haben ihre DV-Aufgaben komplett externen Dienstleistern übertragen. Rund 10 % der Kommunen haben beim Einsatz der eigenen Datenverarbeitungsanlagen dezentrale Organisationsstrukturen[11], der Rest hat die gesamte EDV-Betreuung oft in der Hand nur einer Person gebündelt. Eine geeignete Stellvertretung gibt es oft nicht. Nur wenige Kommunen haben Personal, das sich ausschließlich mit DV-Betreuungsaufgaben befassen kann. Fast alle Administrator(inn)en arbeiten am Limit und können sich um technische und damit auch datenschutztechnische Gestaltungsmöglichkeiten nicht kümmern.

Hinzu treten in vielen Fällen Dienstleistungsverträge mit externen DV-Dienstleistern, z. B. Wartungs- oder Notfallverträge, Netzadministration und andere Formen technischer Unterstützung. Die Leistungsfähigkeiten der Firmen werden oft falsch eingeschätzt oder verkannt. Häufig sind die erwarteten Leistungen nicht ausreichend vertraglich geregelt, die datenschutzrechtlichen Regelungen zur „Datenverarbeitung im Auftrag“ werden dabei oft nicht oder nicht ausreichend mit einbezogen.

Die qualitativen wie quantitativen Ressourcen zur EDV-Administration sind auf der kommunalen Ebene äußerst begrenzt, ihr Gewicht für ein kostengünstiges und reibungsloses Verwaltungshandeln wird oft unterschätzt. In Folge dessen leidet auch der Datenschutz.

In der Einführungsphase des eGovernment-Meldeverfahrens hatte sich das Innenministerium des Landes mit einem Rundschreiben an die Kreise und kreisfreien Städte gewandt und auf die notwendigen Datenschutz- und Sicherheitsvorkehrungen, die von den Gemeinden zu treffen sind, hingewiesen. Die Umfrage hat ergeben, dass immerhin knapp 20 % der Kommunen nicht bekannt war, dass und was das Innenministerium ihnen empfohlen hat. 50 % dieser Gruppe hat kein einziges Verfahrensverzeichnis erstellt.[12] Auch in anderem Zusammenhang wurde deutlich, dass nicht alle Informationen die zuständigen Empfänger erreichen. Die Verwaltungshierarchie bei der Informationsverteilung zu beachten, ist das eine, vernünftige Verteilerkreise, die eine unmittelbare Information derjenigen ermöglichen, die etwas umsetzen sollen, oft das Effektivere. Hier sollten Wege gesucht werden, beides zu verbinden.

Wichtige Informationen erreichen oft die richtigen Empfänger nicht. In Zeiten von E-Mailing ist es besonders einfach, vernünftige Verteilerkreise einzurichten, die eine unmittelbare Information derjenigen ermöglichen, die es angeht. Informationsempfang oder Weisungsumsetzung sollte in wichtigen Punkten ggf. durch Rückmeldeverfahren sichergestellt werden.

§ 18 DSG M-V (Verfahrensverzeichnis) lautet: „Die Daten verarbeitende Stelle ist verpflichtet, in einer Beschreibung für jedes von ihr eingesetzte Verfahren festzulegen ...(Anm. es folgen sieben Punkte, z. B. >Art der gespeicherten Daten< oder >Kreis der Betroffenen<).“

Die Kommunen wurden vom Innenministerium darüber unterrichtet, dass sie mit Einführung des neuen Meldeverfahrens auch entsprechende Verfahrensverzeichnisse zu erstellen hatten. Prozentual hatten

- 50 % aller Kommunen alle
- 23 % aller Kommunen teilweise Verzeichnisse und
- 27 % aller Kommunen kein einziges

Verfahrensverzeichnis erstellt.[13]

Nur 50 % der Kommunen hatten die gesetzlich verlangten Verfahrensverzeichnisse erstellt.

§ 18 Abs.1 Nr. 7 DSG M-V verlangt die Erstellung „einer allgemeinen Beschreibung der technischen und organisatorischen Maßnahmen ...“. Mit einem Rundschreiben des Innenministeriums vom Oktober 2006 wurde daher den Kommunen eine Reihe von Maßnahmeempfehlungen zugeleitet.

Die gemeinsam vom Innenministerium M-V und des DVZ erarbeiteten Empfehlungen dienten dazu, die Einhaltung des Datenschutzes und der Datensicherheit zu gewährleisten. Diese Empfehlungen hatten
- 25 % vollständig,
- 50 % nur teilweise und
- 25 % überhaupt nicht

umgesetzt.

75 % aller Kommunen hatten nicht oder in nicht ausreichendem Maße gemäß der gesetzlichen Anforderungen eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen erstellt.

Die Umfrage erbrachte folgendes Ergebnis für die Umsetzung der Datenschutzempfehlungen in Abhängigkeit zur Größe der Kommune[14]:

In den gebildeten Größenklassen sehen die Ergebnisse wie folgt aus:

- große Kommunen (>20.000 Einw.) 100 %, eine Umsetzung erfolgte in allen Kommunen
- Kommunen mittlerer Größe (>10.000 bis 20.000 Einw.), 31 % Umsetzung in dieser Größenklasse
- kleine Kommunen (<10.000 Einw.), hier sind es 35 % dieser Größenklasse, erstaunlicherweise also ein höherer Anteil, als bei den Kommunen mittlerer Größe, auch wenn der Unterschied nur marginal ist

Eine höhere Anzahl an Beschäftigten absolut wie in Abhängigkeit zur Einwohnerzahl[15] ist ausschlaggebend für eine bessere Einhaltung der Datenschutzbestimmungen.

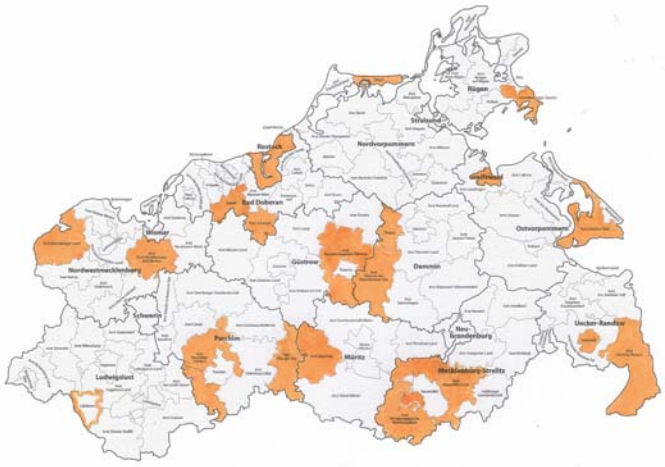
Die Umfrage lieferte auch Antworten zu der Frage, ob in den Kommunen, in denen ein behördlicher Datenschutzbeauftragter bestellt war, häufiger die Verfahrensbeschreibungen vollständig erstellt wurden, als in den Kommunen ohne eine(n) Beauftragte(n). Folgendes Bild ergibt sich: Während in der Gesamtheit wenigstens 20 % der Kommunen keinen behördlichen Beauftragten bestellt hatten, lag der Anteil der Nicht-Bestellung in der Gruppe der Kommunen, die alle Verfahrensbeschreibungen erstellt hatten, deutlich niedriger, nämlich bei einem Anteil von unter 10 %. Die Wahrscheinlichkeit dafür, dass den Anforderungen des Datenschutzes vollständig Rechnung getragen wird, liegt bei einer Bestellung einer/es behördlichen Datenschutzbeauftragten doppelt so hoch, wie wenn keine(r) bestellt wurde. Auch dieses Ergebnis verdeutlicht noch einmal das, was viele schon vorher geahnt haben:

Eine formelle Bestellung einer/es behördlichen Datenschutzbeauftragten erhöht die Wahrscheinlichkeit deutlich, dass den Datenschutzanforderungen in der jeweiligen öffentlichen Stelle in vollem Umfang Rechnung getragen wird.

6.5 Vor-Ort-Besuche

Um zu erkennen, was für den Datenschutz getan wurde bzw. warum nur wenig oder gar nichts für den Datenschutz getan wurde, mussten die Rahmenbedingungen aufgedeckt werden. Damit war vorprogrammiert, dass das Projekt sich nicht nur auf die Untersuchung des neuen Meldeverfahrens konzentrieren konnte, sondern sich auch mit den allgemeinen Bedingungen des Datenschutzes beim Einsatz personenbezogener elektronischer Datenverarbeitung auseinandersetzen musste.

Nach Zusammenstellung der Angaben aus den Fragebögen in einer Tabelle und Auswertung und Zuordnung der Antworten zu Größenklassen wurde daraus die Stichprobe der Kommunen gezogen, die einer näheren Untersuchung unterzogen werden sollten. Dazu wurden die Kommunen in drei Größenklassen eingeteilt[16], es wurden Städte und Landgemeinden entsprechend ihrer Verteilung auf die Gesamteinwohnerzahl berücksichtigt, es wurde bei vergleichbaren Gemeinden auf verschiedene Kreiszugehörigkeit geachtet und es wurden bei der Auswahl noch andere Kriterien, wie die Bestellung bzw. Nichtbestellung von behördlichen Datenschutzbeauftragten oder Datenverarbeitung in eigener Regie oder durch Externe berücksichtigt. 20 Kommunen wurden ausgewählt. Dabei entstand ein wahres Patchwork an Kommunen, die zu besuchen waren.



Nun galt es, die nach den vorgestellten Prinzipien ausgewählten Kommunen aufzusuchen[17] und in Gesprächen unter anderem herauszufinden, wie die Arbeitsbedingungen sind, wie die Einstellung zum Datenschutz ist, wie die behördlichen DSB vor Ort wirken und wie die Einführung des neuen Meldeverfahrens erfahren wurde. Einen breiten Raum sollten dabei aber auch die Feststellungen einnehmen, in welchem Umfang die gesetzlich vorgeschriebenen Maßnahmen, wie die Erstellung eines Verfahrensverzeichnisses, wie die Umsetzung technischer, organisatorischer und personeller Maßnahmen und die Beteiligung der behördlichen Datenschutzbeauftragten tatsächlich erfolgt waren. Zur Vorbereitung der Vor-Ort-Informationsgespräche wurde ein Gesprächsleitfaden[18] entwickelt.

„Durch die Bank weg“[19] waren vor allem das technische Personal in den Kommunen, aber auch die in den Meldeämtern Beschäftigten Datenschutzgedanken sehr aufgeschlossen. Überall bestand in den Gesprächen Aufmerksamkeit gegenüber Datenschutzfragen, und es war uneingeschränkt die Bereitschaft festzustellen, Datenschutzempfehlungen nachzukommen.

Anders gelegentlich das Leitungspersonal, das in einigen Fällen sehr reserviert auftrat. Das hatte in diesen Fällen aber auch seinen guten Grund, war es doch in der Regel ein schlechtes Gewissen verbunden mit dem Versuch, die bekannten Datenschutzmängel zu verstecken.

Die Datenschutzmängel waren oft bekannt, wurden aber als weniger dringlich eingestuft. Schlechter Datenschutz war sehr oft auch ein Leitungsproblem. Eine effektive Kontrolle durch den Landesbeauftragten für den Datenschutz kann hier Abhilfe schaffen.

6.6 Auswertung und Bewertung der vor Ort geführten Gespräche

Im Folgenden wird eine Auswahl der in den Gesprächen festgestellten Ergebnisse zusammenfassend dargestellt. Soweit die Antworten eine Quantifizierung zulassen, wird dies in Prozentsätzen wiedergegeben. Vorweggenommen sei: Es gab unter den besuchten Kommunen keine in allen Belangen „Guten“, noch konnten „tief schwarze Schafe“ festgestellt werden. Es gab überall Licht und Schatten. Vielmehr sind viele im Aufbruch zu einem besseren Datenschutz.

6.6.1 Die kommunalen behördlichen Datenschutzbeauftragten

Frage: Ist ein behördlicher Datenschutzbeauftragter bestellt? Gründe für eine Nichtbestellung?

Die Stichprobe wurde so gewählt, dass gerade ein größerer Teil von Kommunen ohne ordentlich bestellten behördlichen Datenschutzbeauftragten (DSB) ausgewählt wurde. Das Interesse bestand darin herauszufinden, warum eine Bestellung bisher unterblieben war[20]. Argumente für die Nichtbesetzung waren (nachfolgende Nennung in der Reihe der Häufigkeit):

- bisher habe keiner danach gefragt,
- man habe innerhalb der Gemeinde keine geeignete Person gefunden,
- es habe intern die Bereitschaft gefehlt, zusätzliche Aufgaben zu übernehmen,
- der Preis für Externe sei zu hoch,
- politische Gremien (z. B. der Gemeindeausschuss) hätten eine externe Bestellung abgelehnt,
- wegen ständig sich ändernder politischer Rahmenbedingungen wolle man keine langfristige Bindung eingehen.

Die meisten Argumente sind mehr oder weniger fadenscheinig, ein echtes Bemühen, diese Position zu besetzen, war bis dahin in keinem der Fälle zu erkennen. Fast alle aufgesuchten Kommunen gelobten, bis Ende des Jahres 2009 eine Bestellung vorzunehmen.

Ein echtes Bemühen, die Position der bzw. des behördlichen Datenschutzbeauftragten zu besetzen, war in keinem der festgestellten Fälle zu erkennen. Der Landesbeauftragte für den Datenschutz wird darauf drängen, dass bei allen Kommunen diese Bestellung umgehend nachgeholt wird.

Frage: Gibt es einen Grund, warum gerade Sie als behördliche/r Datenschutzbeauftragte/r für die Aufgabe bestimmt wurden?

Bis auf einen Fall verfügten alle behördlichen Datenschutzbeauftragten (DSB) über ein Stück IT-Sachverstand. Nicht allen bestellten behördlichen DSB war ihre gesetzliche Aufgabe hinlänglich bekannt. Alle hatten aber eine gewisse Vorstellung über IT-Sicherheitsfragen. Etwa die Hälfte der bestellten behördlichen DSB hatten gute bis sehr gute Kenntnisse über ihre Aufgaben, diese hatten sie in der Regel auf Schulungen in Mecklenburg-Vorpommern erworben.

Die Fähigkeiten der behördlichen DSB müssen ausgebildet werden. Checklisten, die von den behördlichen DSB abgearbeitet werden können, eine intensivere persönliche Betreuung, feste Ansprechpartner, die Ausbildung von regionalen Netzwerken und ein abgestuftes Schulungsangebot[21] (Basis, Aufbau, speziell auf Fragen der kommunalen Ebene ausgerichtet) können neben anderen Maßnahmen die Lage verbessern.

Die Fähigkeiten der behördlichen Datenschutzbeauftragten müssen mit speziellen, auf die kommunale Ebene ausgerichteten Maßnahmen entwickelt und verbessert werden.

Frage: Gab es eine Vorbereitung auf die Tätigkeit der/s behördlichen Datenschutzbeauftragten? Wenn ja, welche?

Ein Großteil der behördlichen DSB hatte irgendwann einmal Schulungen besucht, einige lagen schon Jahre zurück.

Interesse und Bereitwilligkeit zur Teilnahme an Schulungen ist eigentlich bei allen behördlichen DSB gegeben. Viele versinken im Alltagsgeschäft anderer Aufgaben, sie bräuchten den gezielten Anstoß. Elementar dabei ist aber auch, dass die Aufgabe des behördlichen DSB von der Leitungsebene/Hausspitze als wichtige Aufgabe mitgetragen, gefordert, finanziert und „belohnt“ wird. Da irgendwie „alles immer läuft“ und in vielen Kommunen scheinbar bisher keine gravierenden Schutzprobleme aufgetreten sind, wird die Notwendigkeit der kontrollierenden Funktion des behördlichen DSB oft unterschätzt.

Frage: Was wurde seit der Bestellung an Aufbau für die Tätigkeit als behördlicher Datenschutzbeauftragte/r getan?

Eine durchgängige Erkenntnis, dass man sich auch auf dem Gebiet des Datenschutzes regelmäßig fortbilden muss, um auf Augenhöhe mit der technischen Entwicklung zu bleiben, fehlt in den meisten Fällen. Die behördlichen DSB bemühen sich, Informationen für ihre Aufgabe auch über das Internet zu finden.[22] Der Landesbeauftragte für den Datenschutz sollte sich noch mehr gegenüber den behördlichen DSB als Info-Börse und Servicecenter ausweisen. Wichtig ist es dazu, einen konkreten Ansprechpartner zu haben, den man am besten schon einmal, z. B. auf einer Schulung, persönlich kennengelernt hat.

Frage: Gibt es ein festes Zeitkontingent für die Aufgabe als behördliche/r Datenschutzbeauftragte/r?

Nur die wenigsten haben ein konkretes Zeitbudget innerhalb der Woche oder eines Monats für die Aufgabenwahrnehmung des behördlichen DSB zur Verfügung. Die, die nicht für diese Aufgabe freigestellt sind, versinken oft im Alltagsgeschäft und finden daher keine oder kaum Zeit für den Datenschutz. Dies bildet sich auch bei den nachfolgenden Punkten ab, denn in der Regel hat es in einem bestimmten zurückliegenden Zeitraum keine Schulungen oder Ansprachen der Mitarbeiter in Datenschutzfragen gegeben. Die meisten behördlichen DSB agieren nur reaktiv auf an sie gerichtete Fragen.

Frage: Verständnis der Aufgabe als behördliche/r Datenschutzbeauftragte/r?

Die Aufgabe des behördlichen DSB wird überwiegend auf die eigene Verwaltung bezogen gesehen. Eine formale Beteiligung bei Änderungen in der IT der Kommune ist in den meisten Fällen nicht organisiert.[23] Informationen über Datenschutz für die Bürger in der jeweiligen Kommune, etwa auf der eigenen Homepage oder eine Unterrichtung/Beteiligung bei Beschwerde in Datenschutzangelegenheiten, sind nicht im Blickfeld. Bürgereingaben in Datenschutzfragen sind auf kommunaler Ebene scheinbar eher selten und landen nicht auf dem Tisch der/s behördlichen DSB zur Kenntnisnahme.

Die Regelung des § 20 Abs. 3 DSG M-V umfasst auch die Unterrichtung der behördlichen Datenschutzbeauftragten über Datenschutzbeschwerden und gibt ihnen das Recht, darauf hinzuwirken, dass die Bürger über den Datenschutz in der Kommune öffentlich unterrichtet werden.

Frage: Sind Ihnen DSB anderer Gemeinden persönlich bekannt?

Ein Informationsaustausch unter den behördlichen DSB findet eher zufällig und nur in wenigen Fällen in geringem Umfang und nicht regelmäßig statt. Eine strukturelle Einrichtung von Treffen oder Workshops z. B. auf Kreis- oder Landesebene ist nicht organisiert. Ein E-Mail-Verzeichnis von allen behördlichen Datenschutzbeauftragten ist nicht bekannt.

Die Kommunikation unter den behördlichen DSB sollte verbessert werden. Hierzu sind strukturelle Hilfestellungen erforderlich. Eine gemeinsame Kommunikationsebene organisiert sich zurzeit nicht selbst. Häufig bestand Interesse an einem Meinungsaustausch auf Kreisebene.

Die Kommunikation unter den behördlichen DSB sollte verbessert werden.

Frage: Gibt es ein festes Fortbildungskonzept für die Beschäftigten im Datenschutz oder geben Sie an die Mitarbeiter/innen in Abständen Informationen zum Datenschutz?

Gemäß § 20 Abs. 3 Nr. 2 DSG M-V gehört es zu den Aufgaben der behördlichen Datenschutzbeauftragten, „insbesondere die bei der Verarbeitung personenbezogener Daten tätigen Personen ... mit den Bestimmungen des“ ... Datenschutzes „vertraut zu machen.“

Ein festes Fortbildungskonzept oder regelmäßige Fortbildungen im Datenschutz gab es in keiner Kommune. Etwa 50 % aller Befragten geben keine eigenen Informationen zu Themen des Datenschutzes heraus. 30 % der Befragten geben nur gelegentlich und auf Anfrage Informationen an die Beschäftigten ihrer Kommune weiter. Etwa 20 % der Befragten haben eine aktive Unterrichtungspraxis in Datenschutzfragen entwickelt.

Aktuelle Themen und Entwicklungen könnten per Newsletter an die behördlichen Datenschutzbeauftragten herangetragen werden. Dadurch würden sie als Multiplikatoren in den Stand gesetzt, eine aktivere Rolle zu spielen.

6.6.2 Die Verpflichtung der Beschäftigten auf das Datengeheimnis

Frage: Wurden die Beschäftigten schriftlich auf das Datengeheimnis verpflichtet?

Beschäftigte, die personenbezogene Daten verarbeiten, sind gem. § 6 DSG M-V auf das Datengeheimnis zu verpflichten. Das Ergebnis war:

- in 97 % der Fälle wurden die Beschäftigten auf das allgemeine Amtsgeheimnis verpflichtet
- in 55 % der Fälle wurden die Beschäftigten schriftlich auf das Datengeheimnis verpflichtet
- nur in 5 % der besuchten Kommunen wurden die Beschäftigten der Meldestellen auf das Meldegeheimnis verpflichtet[24]

Mit den jeweils einschlägigen gesetzlichen Geheimhaltungsbestimmungen sollte man sich bei Aufnahme der Tätigkeit vertraut machen, ein Verstoß ist meistens strafbewährt.

6.6.3 Vorbereitung/Unterstützung für die Kommunen bei der Umsetzung des Landesmeldegesetzes

Im September 2004 wurde der Landesbeauftragte für den Datenschutz darüber unterrichtet, dass in einem Modellprojekt E-Government, das in der Region Westmecklenburg durchgeführt werden sollte, die Möglichkeiten zur Umsetzung der Vorgaben aus dem Melderechtsrahmengesetz im kommunalen Bereich getestet werden sollten. Im Juni 2006 verabschiedete der Landtag das Landesmeldegesetz mit seinen endgültigen Formulierungen, auch der technischen Rahmenbedingungen, bis Ende des Jahres musste die Umstellung auf das bundesweit einheitliche neue Meldeverfahren in den Kommunen abgeschlossen sein.

Die Änderung und Anpassung der technischen Bedingungen an ein neues DV-Verfahren wie auch die Ausbildung und Einarbeitung in die tatsächlichen wie auch die rechtlichen Veränderungen benötigen je nach Ausgangslage immer einen gewissen Vorlauf. Nur wenn hier rechtzeitig die nötigen Hilfestellungen gegeben werden, bleibt auch Zeit, sich um Fragen des Datenschutzes zu kümmern. Es lag daher auf der Hand zu untersuchen, wie dieser Prozess von den Kommunen wahrgenommen wurde.

Frage: Wann, wie und durch wen haben Sie zum ersten Mal erfahren, dass die Kommune ihr Meldeverfahren umstellen muss?

Der ganz überwiegende Teil der Befragten fühlte sich rechtzeitig informiert, für große Teile hat es wesentliche Informationen auf Anwendertreffen ihres Softwareherstellers, also von Privaten gegeben. Es gab aber auch Kritik wie diese: „Unterrichtung erfolgte im Sommer 2006 durch das IM, dann folgte lange Zeit nichts bis zur zentralen Veranstaltung am 13.12.2006. Am 13.12.2006 (!!!) und am 01.01.2007 war der Einführungszeitpunkt!“ Andere berichteten hingegen, es habe an anderer Stelle auch schon frühere Einführungen gegeben, so scheinbar bereits 2005 vom Städte- und Gemeindetag eine Schulung der Sachbearbeiter/innen und der behördlichen DSB in Schwerin. Hierzu wurde jedoch von mehreren Teilnehmer/innen kritisch berichtet: „Wir haben nichts verstanden, Fachbegriffe flogen uns nur so um die Ohren, irgendwas wird in den Raum geworfen, z. B. Testa, aber was ist TESTA?“ Auch Teilnehmer/innen an der Veranstaltung im Herbst 2006 in Rostock äußerten Kritik an der Großveranstaltung: "Bei den Vorträgen haben IM und DVZ fachliche und technische Kenntnisse vorausgesetzt, über die wir gar nicht verfüg(t)en. Wir haben dagesessen, uns das angehört und gestaunt."

Die Einstellung der Referate auf den Empfängerhorizont der kommunalen Sachbearbeiter und Administratoren bei den Einführungsveranstaltungen wird scheinbar vermisst. Eine etwas langfristigere Vorbereitungsphase und die Einbeziehung medialen Know-hows könnten von Vorteil sein. Nicht jeder Verwaltungsbeamte ist didaktisch geschult oder in der Lage, komplexe Materie in verdaubaren Häppchen zu servieren. Auch wenn die Schnittstelle Anwender, Systemadministration und Datenschutz gegeben ist und alle voneinander wissen müssen, wird von den Zuhörern offensichtlich in Frage gestellt, ob dies nur in einer einzigen gemeinsamen Veranstaltung geschehen soll.

Das Mittel zentraler Großveranstaltungen als Themenmix für Sachbearbeiter, Systemadministratoren und behördliche Datenschutzbeauftragte mag als Auftaktveranstaltung noch geeignet sein, es bleiben aber dabei viele Fragen liegen. Sie sollten daher durch dezentrale Einführungsveranstaltungen ergänzt werden, z. B. auf Kreisebene mit Schulungen vorher ausgebildeter Multiplikatoren und Ansprechpartner, die weiter zur Verfügung stehen.

Frage: Hatten Sie den Eindruck, Ihnen stand für die Umstellung genügend Zeit zur Verfügung (incl. Einarbeitung der Kräfte)?

- 55 % der Befragten meinten, es hätte ausreichend Zeit zur Verfügung gestanden. Zitat: „Wir sind Praktiker, wir legen los.“
- 10 % antworteten mit einem „Ja, aber“, wie z. B.: „Ja, nur Datenschutz kam zu spät.“ oder „Ja, es lief schließlich, es gab aber keine Einweisung, Information und Zusammenarbeit waren schlecht, Vorbereitung zu inkonkret, kurz vor Einführung plötzlich Probeläufe mit Listen von Daten, die noch zu bereinigen waren, es wurde knapp.“
- 25 % der Befragten hielten die zur Verfügung stehende Zeit nicht für ausreichend für eine geordnete Einführung.
- 10 % konnten sich nicht festlegen.

Einem Drittel der Kommunen stand keine ausreichende Zeit für eine geordnete Einführung zur Verfügung. Darunter leidet dann auch der Datenschutz.

Frage: Gab es im Vorfeld der Einführung eine Beteiligung ...
- der Kommune?
- der/s behördlichen DSB?

Wurden Sie oder die Kommune z. B. gefragt, ob Sie bei der Entwicklung miteinbezogen werden möchten?

Bis auf ganz wenige Ausnahmen (z. B. Modellregion) gab es im Vorfeld überwiegend keine Beteiligung der Kommunen noch eine Beteiligung der behördlichen DSB.

Frage: Wenn „Ja“: Welche Möglichkeiten hatten Sie, auf die Entwicklung einzuwirken oder mitzubestimmen? Wenn „Nein“: Hätten Sie sich überhaupt daran beteiligen wollen?

- Immerhin bei 40 % der Befragten bestand Interesse, sich an der Entwicklung eines solchen Systems im Vorfeld zu beteiligen. Antworten waren z. B.: „Ja, z.B. wie kommen wir ran ans TESTA-Netz/Bandbreite/über KOMM-Box ans KBA? So hieß es `überfallartig´, wir müssen bereitstellen.“ Oder: „Ja, nehmen jetzt an Gewerbe-Online teil.“ Auch die folgende Kritik gibt diesen Eindruck wieder: "Hatten den Eindruck, es wurde nichts an tatsächlichen Verhältnissen erprobt. Ordnungsgemäße Erstanwender-Tests gab es nicht.“
- Weitere 10% wären bereit, an Teil-Aspekten mitzuwirken.
- 15 % verneinten ihre Bereitschaft allerdings zum Beispiel mit dem Hinweis, man sei zu klein oder die Leistungsfähigkeit sei nicht gegeben.
- Die übrigen 35 % der Befragten hatten keine Meinung.

Das Aktenstudium legt den Eindruck nahe, dass, als man in die Testregion ging, die Rahmenbedingungen und die technischen Konfigurationen weitestgehend abgeschlossen waren. Es hat daher den Anschein, dass die relativ hohe Bereitschaft der Kommunen, an einer solchen Entwicklung mitzuwirken, nicht genutzt wurde. Eine solche Beteiligung der Anwender bei der technischen wie bei der Entwicklung des Datenschutzes könnte entscheidende Vorteile mit sich bringen und die Praxistauglichkeit erheblich verbessern. Ein für die Beteiligung offenes Entwicklungsforum z. B. für den Datenschutz könnte das nötige Feedback erzeugen.

Die Bereitschaft von ca. 50% der Kommunen, an der Entwicklung eines solchen Verfahrens mitzuwirken, sollte auch für die Entwicklung des Datenschutzes genutzt werden.

6.6.3.1 Vorbereitung/Unterstützung für die Kommunen bei der technischen Umsetzung

Frage: Welche technischen Hilfestellungen gab es bei der Einführung des neuen Online-Meldeverfahrens?

Auch die technische Unterstützung bei der Einführung des neuen Verfahrens scheint nicht für alle Kommunen gleichermaßen reibungslos verlaufen zu sein. Viele erklärten, sie seien vom Softwarehaus und vom DVZ unterstützt worden. Das verdeutlichen Antworten wie diese: „Fragebogen des DVZ zu den Systemkomponenten erhalten, DVZ-Mitarbeiter kam vorbei, Probleme wurden zusammen gelöst, teilweise sogar Hilfe vom Softwarehersteller (HSH).“ Andere haben sich darauf verlassen, was die externen Systembetreuer und das DVZ untereinander abgestimmt haben.

In einem Fall stellte man fest, als das DVZ die KOMM-Box anschließen wollte, dass die für LAVINE erforderliche Leitung fehlte und daher rasch noch eine Leitung verlegt werden musste, was auch nicht für eine geordnete Vorbereitung spricht. Aber es gab auch eine größere Anzahl von Kommunen, die mit der Unterstützung nicht zufrieden waren, was die folgenden Zitate belegen: „Keine Unterstützung, kalt erwischt, KOMM-Box wurde einfach eingebaut." Oder: „Nein, keine ausreichende Unterstützung, Hauruckverfahren, die Vorstellung der gesamten Konstruktion fehlte mir." Oder: „Nein, Unterstützung war nicht ausreichend, hätten uns Infos gewünscht, was kommt genau? Plötzlich stand die Hardware da." Oder: „Völlig unzureichend, das DVZ hat nur gefragt, wo die Box hin soll, eine Empfangsbestätigung wurde unterschrieben und dann waren die weg." Oder: „Hätten Informationen benötigt, um den Prozess in der Anfangsphase zu verstehen."

Mag sein, dass der eine oder andere Befragte übertreibt, ein wahrer Kern ist in der Regel immer an den Aussagen. Wenn man also den Äußerungen der Befragten folgt, müssen auch die technischen Unterstützungsleistungen bei der Einführung vergleichbarer Systeme deutlich verbessert werden. Niemand kann die richtigen Datenschutzmaßnahmen ergreifen, wenn er nicht weiß, was tatsächlich passiert. Ohne konkrete Kenntnis der Risiken und ohne ausreichende Information, Unterrichtung und Schulung können von den Verantwortlichen vor Ort auch nicht die adäquaten Datenschutzmaßnahmen ergriffen werden. Lediglich eine Kommune konnte berichten, dass ein Austausch auf Kreisebene und mit Nachbargemeinden stattgefunden habe. Es sollte versucht werden, viel mehr sich selbst organisierende Informationsbeziehungen und -strukturen zu entwickeln und zu verfestigen, Schneeball-systeme einzusetzen und direkte Information durch gezielte Verteilerkreise zu gewährleisten.

Die technischen Unterstützungsleistungen bei der Einführung vergleichbarer Systeme müssen deutlich verbessert werden. Nur wer informiert ist, kann die richtigen Datenschutzmaß-nahmen ergreifen.

Frage: Hielten Sie die technischen Unterstützungsleistungen für ausreichend?

- Nur 20 % der Befragten waren damit zufrieden, wie die technische Einführung vonstatten gegangen war.
- 35 % waren vollständig unzufrieden.
- Der Rest konnte sich keine eigene Meinung bilden, zum Teil, weil Fremdfirmen diese Aufgabe für sie erledigt hatten.

Ein Drittel der Kommunen hielt die technischen Unterstützungsleistungen bei der Einführung für nicht ausreichend.

Frage: Hat es zur Einführung des neuen Meldeverfahrens Schulungen gegeben, wenn ja, auf Kreisebene oder im Austausch mit Nachbargemeinden?

So etwas hat es wohl nicht gegeben, es wurde zur jetzigen Situation geantwortet. Ob und in welchem Umfang es Kommunikation, Erfahrungsaustausch mit den Nachbargemeinden oder auf Ebene des Kreises gibt, dies scheint von Fall zu Fall völlig unterschiedlich ausgeprägt zu sein.

Natürlich sind immer persönliche Beziehungen wie auch die politischen Verhältnisse ausschlaggebend dafür, ob sich eine solche Kultur herausbilden kann oder nicht. Angesichts der Haushaltslage der Länder und Gemeinden muss man darauf bedacht sein, Synergieeffekte zu erzeugen und einen effektiven Informationsaustausch zu gewährleisten. Letzterer ist gerade angesichts der entwickelten modernen Kommunikationsmöglichkeiten leichter als je zuvor.

Frage: Haben Sie den Eindruck, die gesamte Betreuung des Systems macht jetzt mehr Arbeit als vorher?

- 45 % der Befragten sehen keinen zusätzlichen Arbeitsaufwand oder fanden, dass dieser gleich geblieben sei.
- 30 % der Befragten sehen einen deutlich höheren Betreuungsaufwand für das neue Einwohnermeldesystem, Argumente sind z. B.: „Ist wesentlich komplexer geworden, die Pflege der Programme und Hardware macht mehr Arbeit. Unterstützung gibt es dabei nicht.“ Oder: „Das gesamte System muss ständig lauffähig gehalten werden, und im Gegensatz zum neuen Verfahren lief unser altes Melderegisterverfahren stabil.“
- 25 % hatten keine Einschätzung.

6.6.3.2 Vorbereitung / Unterstützung für die Kommunen bei der rechtlichen Umsetzung

Die nachfolgenden Fragen beschäftigen sich mit der Vorbereitung auf die Rechtsänderungen. Da es mit der Novellierung des LMG M-V auch einige datenschutzrechtliche Veränderungen gegeben hatte, führt eine dem neuen Recht nicht angepasste Sachbearbeitung zwangsläufig oft auch zu Datenschutzverstößen. Es lag daher auf der Hand zu untersuchen, wie die Vorbereitungen hierauf waren.

Frage: Welche rechtlichen Hilfestellungen gab es bei der Einführung des in vielen Teilen überarbeiteten Melderechts und wie sieht es heute aus?

Zusammengefasst lässt sich feststellen, dass ein großer Teil der Befragten durch die private Firma, die für viele Kommunen die Software für das Melderegister zur Verfügung stellt, über die Rechtsänderungen unterrichtet und teilweise sogar geschult wurde.

Aktuell sieht die Unterstützung in melderechtlichen Fragen wie folgt aus:

- Ein Anteil von etwa 50 % wird über die Kreise mit guten bis sehr guten Informationen versorgt.
- Bei etwa 25 % der Kommunen scheint der Austausch noch zufriedenstellend.
- Bei 25 % der Kommunen hingegen gibt es keine oder nur geringe Unterstützung in Fragen des Melderechts.

Ein Teil der Kreise führt regelmäßig Schulungsveranstaltungen oder Workshops für die sachbearbeitende Ebene durch, hier werden Fragen aus der Praxis zusammengetragen, vom Kreis vorbereitet und dann gemeinsam erörtert. In einem der Kreise wurde erst vor kurzem dieser Service eingestellt, weil einige sachbearbeitende Beschäftigte wegen starker Arbeitsbelastungen nicht mehr an dieser Veranstaltung teilnehmen konnten.

Es stimmt bedenklich, wenn einer privaten Firma ohne Auftrag und Kontrolle wesentliche Teile der Fortbildung der sachbearbeitenden Ebene im Recht überlassen wird. Ebenso bedenklich ist es, wenn Sachbearbeiterinnen/Sachbearbeiter wegen hoher Belastung ihre Teilnahme an Schulungen absagen. Die Teilnahme an Schulungen und Workshops, die nun wirklich nicht häufig veranstaltet werden, sollte für die Beschäftigten verpflichtend sein. Da die auf Kreisebene zusammengetragenen, in den Workshops behandelten Problemlagen sicherlich auch in den anderen Kreisen von Bedeutung sind, empfiehlt es sich, eine Informationsbörse auf Landesebene zu organisieren. Nur so kann eine einheitliche Rechtsanwendung auch in datenschutzrechtlichen Fragen sichergestellt werden. Auch sollte geschaut werden, wie in den Kreisen, die eine solche Fortbildungsmöglichkeit derzeit nicht anbieten, eine Unterstützung angeboten werden kann. Verfassungsrechtliche Begriffe wie "Rechtmäßigkeit der Verwaltung" können gerade im Bereich der Eingriffsverwaltung nicht allein durch pragmatisches Verwaltungshandeln ersetzt werden. Auch die Hilfeleistungen bei der Behandlung von rechtlichen Problemfällen sollten strukturierter erfolgen. Es erscheint fraglich, ob es sinnvoll ist, rechtlichen Sachverstand zu einem besonderen Rechtsgebiet, wie z.B. dem Einwohnermeldewesen, in allen Kreisen in gleicher Weise vorzuhalten, oder ob nicht hier auch innerhalb der Kreise eine gewisse Spezialisierung verbunden mit einer Verteilung der Aufgaben effektiver wäre. Im Moment erscheint es so, als würden sehr viele der Problemfälle früher oder später auf der ministeriellen Ebene landen.

Frage: Haben Sie auch die Gesetzesbegründungen erhalten?

In seltenen Fällen ist die Gesetzesbegründung scheinbar vorhanden. Ein nicht unerheblicher Teil weiß nicht, wo sie zu finden ist (LARIS):

55 % kannten die Gesetzesbegründung nicht,
40 % konnten mit der Frage nichts anfangen,
5 % kannten die Gesetzesbegründung.

Ein größerer Teil hält praxisorientierte Auslegungshilfen für wünschenswert:

- 50 % erachten dies als wünschenswert,
- 25 % halten das Vorhandene für ausreichend; diese haben z. B. einen Kommentar zum Melderecht bzw. bekommen Unterstützungsleistungen aus dem Kreis,
- 25 % sind unentschlossen.

6.6.4 Fragen zum Datenschutz in der Einführungsphase

Frage: Sie mussten sich natürlich bei der Einführung des neuen Online-Meldeverfahrens auch um die Datenschutz Belange kümmern. Aber wie ist Ihre Einstellung dazu?

Die Befragten sahen durchaus, dass es ihre Daten waren, die das ZIR und die Vermittlungsstelle verarbeiten, und waren daher bereit, einen einheitlichen und lückenlosen Datenschutz zu entwickeln. Dies ist aber nicht gelungen. Es setzte massive Kritik ein: Die meisten Kommunen fühlen sich überfordert. Sie sagen, das neue Verfahren sei ihnen aufgedrängt worden. Sie haben zwar ein Interesse daran, dass es funktioniert, sie fühlen sich aber nicht mitgenommen und betrachten es daher auch nicht als ihr „eigenes Kind“.

Die nachfolgenden Zitate geben eindrucksvoll wieder, wie die System-Einführungsphase von einer ganzen Reihe von Kommunen empfunden wurde: „Die Einführung kam überfallartig. Es hat eine zentrale Veranstaltung gegeben, auf der eine Vertreterin des IM erklärte, es sei Datenverarbeitung nach § 4 DSG M-V (Auftragsdatenverarbeitung). Da bin ich aus allen Wolken gefallen." „ Es wäre alles einfacher gewesen, wenn wir gewusst hätten, wie es laufen soll. Es fehlte z. B. an klaren Richtlinien der Landesverwaltung, die Verantwortlichkeiten waren nicht klar. So wollte das DVZ zunächst direkt auf die Server der Gemeinde zugreifen." „Wer ist denn wirklich für was verantwortlich?" „Da wird uns eine Blackbox hingestellt, hinzu kommt der peinliche Datenklau des DVZ, die Daten aus dem Meldewesen wurden uns heruntergezogen, angeblich zu Testzwecken. Test mit Echtdaten?!" „Die zentrale Frage ist doch, wie man die Karten legt, die E-Government-Truppe diskutiert, wir brauchen Lösungen." „Wir kennen dieses System nicht und fühlen uns überfordert, wir sollen uns um die elektronische Übermittlung kümmern, dass können wir gar nicht, wir sollen die verschiedenen Verfahren freigeben, das System lief aber schon, bevor wir es freigegeben haben! Wir haben uns gefragt, welche Konsequenzen es gehabt hätte, wenn wir es nicht freigegeben hätten." „Wir sind überfallen worden, das DVZ sagte, wir kommen mal mit einem HSH-Vertreter und ziehen Ihnen mal ein paar Daten ab."

Die in den Zitaten zum Ausdruck kommende Stimmung macht deutlich, dass hier etwas schief gelaufen ist. Und die mit der CD-ROM in letzter Minute versandten umfänglichen Datenschutzanweisungen mögen ein Übriges getan haben. Bei den meisten Kommunen, die eigentlich alle gewillt sind, etwas für den Datenschutz zu tun, kippte die Stimmung in die Richtung: "Wir machen jetzt gar nichts mehr, nur noch auf unmittelbare Anweisung." Eine aufbauende Vorbereitung mit visualisierendem Material, Begrifflichkeiten, die erklärt werden und der Möglichkeit, sich jederzeit mit Fragen zu den Materialien und zum Datenschutz an jemanden wenden zu können, wäre die notwendige Voraussetzung, damit ein Systemverständnis entsteht, auf dessen Basis dann auch jede Kommune für sich die bei ihr notwendigen Datenschutzmaßnahmen ergreifen kann.

Es wird überwiegend erkannt, dass ein nur zentral entwickelter Datenschutz sein Ziel nicht erreichen kann. Es besteht aber weiterhin große Unsicherheit, wer für was verantwortlich ist und wie ein effektiver Datenschutz umgesetzt werden kann.

Frage: Wer hat Ihnen tatsächlich die größte Unterstützung bei den mit der Umstellung anstehenden Datenschutzfragen gewährt?

- Unterstützung durch das IM,
- Unterstützung durch das DVZ,
- Unterstützung durch den LfDI,
- Unterstützung durch Meldesoftwarefirma.

Die meisten Gemeinden fühlten sich bei den Fragestellungen wenig bis gar nicht unterstützt; bei der Verfahrenseinführung hätte, wenn, dann wohl die Meldesoftwarefirma die meiste Unterstützung gewährt. Dieses Ergebnis kann die anderen Beteiligten wenig zufriedenstellen.

Frage: Hat sich die Datenqualität durch die Einführung des neuen Meldeverfahrens im Register verbessert? Fand zum Beispiel eine technische Bereinigung der Datensätze statt?

- 35 % bejahen die Frage, mehrere meinten, dies geschehe jährlich, jedoch nur in geringem Umfang, die letzte große Bereinigung habe es bei Einführung der Steuer-ID gegeben.
- 45 % sind überwiegend unentschieden.
- 20 % verneinen die Frage.

Frage: Wurden alte Datensätze vermehrt abgeklärt oder gelöscht?

Die ganz überwiegende Meinung ist, dass dies nicht im Zusammenhang mit der Einführung des neuen Meldeverfahrens geschehen sei.

Frage: Tragen Sie datenschutzrechtliche Verantwortung für:

a) für den Datenschutz in LAVINE?
   - 40 % antworteten mit „Nein.
   - 50 % waren unentschieden.
   - 10 % positiv einschränkend: „Ja, insoweit, als dass ich keine schlechten Daten in das Netz stellen darf und LAVINE technisch nicht gefährden darf.“

b) für den Datenschutz im ZIR?
   - 90 % mit „Nein“ oder unentschlossen

c) für den Datenschutz in der KOMM-Box?
   - 55 % haben keine Einschätzung, dabei ist in einem Fall nicht einmal die Existenz der KOMM-Box bekannt.
   - 35 % antworten mit „Nein“. Beispiel dafür: „Nein, wir haben zwar dafür bezahlt, ist aber nicht unser Eigentum. Wir würden uns mehr Kenntnisse über die KOMM-Box wünschen, denn alles läuft darüber, auch die neuen Ausweise.“
   - 10 % sehen eine Verantwortung, aber mit Einschränkungen.

Das Ergebnis lässt sich nicht besser zusammenfassen, als es die folgende Antwort einer Kommune wiedergibt: „Wir vertrauen auf das DVZ, was bleibt uns auch anderes.“ Die Antworten spiegeln die tatsächlichen Verhältnisse wider. Eine Verantwortung für den Datenschutz wird in diesen Bereichen ganz überwiegend abgelehnt oder nicht erkannt.[26]

Bei der rechtlichen Regelung technischer Sachverhalte müssen klare Verantwortungsbereiche definiert werden.[27]

6.6.5 Melderechtlicher Teil

Bei den Besuchen wurde auch eine ganze Reihe von Fragen zur Umsetzung datenschutzrechtlicher Regelungen im Meldeverfahren gestellt. Da nicht alle unmittelbar im Zusammenhang mit E-Government-Verfahren stehen, wird auf eine Darstellung in diesem Bericht verzichtet. Die Fragen gliederten sich dabei in einen Teil,

- der die Führung der Register betraf, wie Protokollierungspflichten und Löschfristen, automatisierte Zugriffe anderer Stellen einer Gemeinde auf das gemeindliche elektronische Melderegister oder zur Behandlung der Meldescheine, und es gab Fragen zur
- Gewährleistung der melderechtlich ausgeprägten Bürgerrechte, wie Umgang mit dem Widerspruchsrecht, Handhabung der Auskunftssperre oder der öffentlichen Bekanntmachungen wie auch die Handhabung der Unterrichtung der Betroffenen bei erweiterter Melderegisterauskunft (§ 34 Abs. 2 S. 3 LMG M-V).

6.6.6 Erfüllung der technischen Anforderungen nach Datenschutzrecht

Frage: Wurde zur Einführung des neuen Meldeverfahrens eine Freigabe nach § 19 Abs.1 DSG M-V durchgeführt und welche Gegenstände betraf die Freigabe?

a) die Hardware,
b) die Software einschließlich der Betriebssysteme,
c) die Datenbestände,
d) das aufbau- und ablauforganisatorische Regelwerk wie Zuständigkeitsregelungen und Dienstanweisungen, Benutzerhandbücher u. a.

Die Vorstellung, was eine Freigabe ist, warum eine Freigabe und wie diese zu erfolgen hat, ist in ganz weiten Teilen der kommunalen Verwaltung nicht vorhanden. Hinzu kommt, dass häufig die Erstellung eines Verfahrensverzeichnisses mit der Freigabe gleichgesetzt wurde. Dies dachte auch eine Reihe der behördlichen Datenschutzbeauftragten.[28]

- 50 % der Kommunen wissen nicht, ob es eine Freigabe gegeben hat, oder verneinen diese Frage.
- 30 % gaben an, eine Freigabe des Registerverfahrens gemacht zu haben. Dabei wurde allerdings oft die Erstellung des Verfahrensverzeichnisses als Freigabe gewertet.
- 10 % hatten etwas freigegeben, wussten aber nicht, welches Verfahren.
- 10 % hatten eine bedingte Freigabe vorgenommen. Eine Antwort hierzu lautete: Bedingte Freigabe, Sicherheitskonzept fehle, Kommune habe den Softwarehersteller um Zertifikat gebeten, von dort komme aber nichts.

Wenn ein Freigabeverfahren in einer Kommune durchgeführt wurde, dann ist dies offensichtlich nur durch die Aufforderung des Innenministeriums erfolgt[29], denn, obwohl andere Verfahren eingesetzt wurden, hat es zu keinem anderen als dem Meldeverfahren in den befragten Kommunen überhaupt eine Freigabe gegeben.

Die Einleitung einer Freigabe scheitert häufig schon daran, dass niemand in der kommunalen Verwaltung eine Verantwortung für die Erarbeitung und Vorlage einer solchen Freigabe sieht. Angesichts der Tatsache, dass die meisten behördlichen Datenschutzbeauftragten ihre Verfahren überhaupt nicht näher kennen, ist das Ergebnis mit 50 % Freigabe eher formaler, denn inhaltlicher Art. Lediglich die 10 %, die eine bedingte Freigabe machten, hatten sich definitiv Gedanken gemacht.

Freigabeverfahren sind in weiten Teilen der kommunalen Verwaltung ein Fremdwort. Wenigstens 50 % der Kommunen haben bisher weder im Meldebereich noch in anderen Bereichen kommunaler Datenverarbeitung ein Freigabeverfahren durchgeführt.

Frage: Welche technisch-organisatorischen Maßnahmen haben Sie im Rahmen eines Sicherheitskonzeptes getroffen?

Den Kommunen war eine CD-ROM übersandt worden, die eine Ausarbeitung für eine Vielzahl von IT-Sicherheitsstandards enthielt, die bei Einführung des neuen Meldeverfahrens umgesetzt werden sollten. Basis der Ausarbeitung war das IT-Grundschutzhandbuch des BSI. Aus diesem Konvolut von möglichen Maßnahmen wurde für die im Zuge des Projektes durchgeführten vor-Ort-Besuche eine Liste von essentiellen Fragen generiert, die beim allgemeinen Einsatz von IT strukturell beachtet und berücksichtigt werden müssen. Dabei beschränken sich die Überlegungen auf das Wesentliche. Damit sollte kein tiefgreifender, aber ein grundsätzlicher Eindruck gewonnen werden, ob und wie in den Kommunen über diese Themen gedacht wurde und was davon bereits verwirklicht worden war. Das Ergebnis dieses Teils der Untersuchungen findet sich in der nachfolgenden Tabelle.

IT-SICHERHEIT	
Aufgabe	**Zusammenfassung der Ergebnisse**
B 1.0 Management	
- Sicherheitsleitlinie	Nur bei zwei Großstädten feststellbar (entspricht 10 %), bei einer davon in Arbeit. Bei mittleren und kleinen Kommunen besteht keine Absicht, eine Sicherheitsleitlinie zu erstellen.
- Sicherheitsbeauftragter	In 20 % der Fälle bestellt.
- Sicherheitskonzept	Knapp die Hälfte der Kommunen hat sich in irgendeiner Weise schon dem Thema gewidmet. 5 % der Kommunen hat bereits ein Sicherheitskonzept. 10 % der Kommunen verfügen über einen Entwurf, bei 20 % der Kommunen ist ein Sicherheitskonzept in Arbeit, i.d.R. als Rahmenkonzept.[30]
- Regelungen für Sicherheitsvorfälle	In 25 % der Kommunen bestehen für Teilbereiche Regelungen. Ihre Güte wurde nicht geprüft, nach den Aussagen in den Gesprächen können diese oft nur rudimentär sein.

IT-SICHERHEIT	
Aufgabe	**Zusammenfassung der Ergebnisse**
B1.1 Organisation	
- IT-Regelungen (Dienstanweisung, Dienstvereinbarung o. ä.)	50 % der Kommunen haben IT-Regelungen per Dienstanweisung in Kraft gesetzt. Themen, Inhalte, Breite und Tiefe dieser Regelungen waren nicht Gegenstand der Befragung. Die Gespräche machten aber deutlich, dass häufig über Regelungen z. B. in Dienstbesprechungen geredet wurde. Dies wurde oft als ausreichend und verbindlich genug empfunden. Protokolle über diese Dienstbesprechungen gab es aber in der Regel nicht. Nur in seltenen Fällen bestand überhaupt eine Vorstellung darüber, was geregelt werden könnte/sollte.
- Zutrittsregelungen	In 60 % der Kommunen gibt es in gewissem Umfang Zutrittsregelungen. Diese sind aber ganz überwiegend nicht dokumentiert. Oft kommen differenzierte Schlüsselsysteme zum Einsatz, die die Zutrittsmöglichkeiten steuern.
- Vertretungsregelungen	In 90 % der Fälle gibt es Vertretungsregelungen, die überwiegend auch schriftlich festgehalten sind. Die Regelungen sind aber oft nicht durchstrukturiert und betreffen nur Teilbereiche, in der Regel für besonders wichtig erachtete Funktionen.
- Zugriffsrechte	In 80% der Fälle vergeben, wobei oft nicht schriftlich festgehalten, auch über die Tiefe der Zugriffsregelungen kann nichts gesagt werden. Der Eindruck war, dass häufig nur ein Passwortschutz eingerichtet war.
- Schlüsselverwaltung	Es gibt in 90% der Fälle eine differenzierte Schlüsselvergabe, die Ausgabe der Schlüssel wird i.d.R. zentral dokumentiert und per Unterschrift quittiert.
- Entsorgung (Datenträger, Hardware, Schlüsselmaterial ...)	In 60% der Fälle wird die Entsorgung von elektronischen Datenträgern und Papier durch zertifizierte Fremdfirmen erledigt. In weiteren 30% wird die Entsorgung durch mechanische Zerstörung bzw. durch eigene Schredder vorgenommen. In 10% der Fälle gab es keine oder unklare Antworten. Ganz überwiegend entstand der Eindruck, dass ausreichende Vorkehrungen getroffen waren.
B1.12 Archivierung	
- Datensicherungskonzept	Ein schriftlich festgelegtes Konzept gab es nur in den seltensten Fällen. Tägliche Versionssicherungen oder Vollsicherungen wurden ganz überwiegend getätigt.
- Rücksicherung getestet	In ca. 20-30 % der Fälle wurde eine komplette Daten- und Systemherstellung schon einmal getestet. In 60% und mehr waren es Echtfälle, die eine Datenwiederherstellung in bestimmten Bereichen erforderlich gemacht hatten. Viele wollten ihre laufenden Systeme nicht durch Tests in Gefahr bringen, zusätzliche separate Rechnerleistung war für solche Tests nicht vorhanden.
- Aufbewahrung der Datenträger	Die Aufbewahrungsorte waren nicht immer sicher bzw. vom Serverraum getrennt. Etwa 40% der Befragten hinterlegten die Sicherungskopien in Bankschließfächern.
B1.13 Sensibilisierung	
- Schulungen Mitarbeiter	Eigene Schulungen der Beschäftigten fanden so gut wie nie statt. Es fehlt an Kapazitäten und gelegentlich auch an Ideen. Die sachbearbeitende Ebene nimmt gelegentlich an sog. Anwendertreffen teil.
- Schulungen Administratoren	Gerade im technischen Bereich fehlt oft jegliche Fortbildung. In der Regel gibt es eine Firmenschulung vor dem ersten Einsatz neuer Software. Systematische firmenunabhängige Schulungen würden wahrgenommen, wenn die Teilnahmegebühren nicht so hoch wären und man wüsste, dass die angebotene Schulung für die Praxis tatsächlich etwas bringen würde.

IT-SICHERHEIT	
Aufgabe	**Zusammenfassung der Ergebnisse**
B1.6 Virenschutz	
- Virenschutzkonzept	Konzepte oder schriftliche Niederlegungen gibt es in den seltensten Fällen. Aber wohl in fast allen Fällen kommen die üblichen Abwehrsysteme zum Einsatz. Gerade dieser Bereich ist oft Fremdfirmen übertragen. Kenntnisse darüber, ob das, was diese Firmen machen oder im Einsatz haben, einen ausreichenden Schutz bietet, liegen nicht vor ("Blindes Vertrauen").
- Aktualisierungsintervalle	Die Angaben legen eine übliche Praxis nahe.
- regelmäßige Virenchecks	Etwa 1/3 der Befragten verfügte zu dieser Frage über keinerlei konkrete Kenntnisse (siehe wie vor bei Virenschutzkonzepte).
- Virenchecks bei externen Datenträgern (USB-Stick, CD/DVD ...)	In 20% der Fälle findet keine Prüfung statt. Oft ist der Einsatz dieser Medien nicht zugelassen. Nur in den wenigsten dieser Fälle ist der Einsatz auch technisch ausgeschlossen. In 25 % der Fälle scheint die technische Prüfung ausreichend sicher.
B1.9 SW-/HW-Management	
- Nutzungsverbot nicht freigegebener/privater HW/SW	Nutzungsverbote gibt es in 50 % der Fälle, davon in 10 % durch technische Vorkehrungen und in 40 % durch Dienstanweisung untersagt (DA oft mdl.). In den übrigen Fällen unklar oder nicht geregelt.
- Freigabe für jedes Verfahren	Siehe Ausführungen unter diesem Gliederungspunkt oberhalb der Tabelle.
- alle Netzzugänge dokumentiert	In ca. 50 % der Fälle vorhanden, in weiteren 20 % der Fälle veraltet, in 30 % der Fälle nicht vorhanden
- Verhinderung ungesicherter Netzzugänge (s. a. B4.01 und B5.3)	In 15 % der Fälle akzeptable Lösungen, in allen anderen Fällen unklar, oft bisher noch keine Gedanken gemacht.
B2.2 Verkabelung/ Schutzschränke	
- Verkabelung dokumentiert	In 60 % der Fälle aktualisiert vorhanden, in 15 % der Fälle veraltet. In vielen Fällen sind auch die Steckdosen der Rechneranschlüsse nummeriert und dokumentiert. In 25 % der Fälle ist nicht bekannt, ob es so etwas gibt, und wenn ja, wer diesen Plan hat. Antworten wie „Den Stromlaufplan hat der Hausmeister.“ lassen eher auf 230V-Kabel schließen.
- Kabel gekennzeichnet	In 80 % der Fälle ordnungsgemäß.
- Verteiler im Serverraum oder verschlossen in Schutzschränken	Serverraum oder Schutzschränke sind in allen Fällen wohl ausreichend gesichert.
B2.3 Büroraum	
- Zutrittsregelungen	Oft nicht erlassen, in der Regel nicht dokumentiert.
- Schlüsselverwaltung	Schlüsselverwaltung ganz überwiegend ausreichend, siehe auch oben unter B 1.1 dieser Tabelle. Die Schlüsselausgabe wird in der Regel quittiert.
- abgeschlossene Fenster und Türen	Rund 50 % der Kommunen haben besonders gesicherte Türen und Fenster. Einbrüche oder Einbruchsversuche hatte es auch bei den ungesicherten noch nicht gegeben.

IT-SICHERHEIT	
Aufgabe	**Zusammenfassung der Ergebnisse**
B2.4 Serverraum	
- Zutrittsregelungen und -kontrolle	In 80 % der befragten Kommunen gibt es schriftliche und/oder tatsächliche Vorkehrungen, die sicherstellen, dass nur ein befugter Zutritt erfolgen soll. In den anderen 20% der Fälle gab es keine oder nur unzureichende Sicherheitsvorkehrungen.
- Schlüsselverwaltung	Durchgängig restriktive Vergabe der Schlüssel.
- abgeschlossene Fenster und Türen	Die Serverräume befanden sich in der Regel im Gebäudeinneren oder in Teilen, die insbesondere vor Zugang von außerhalb des Gebäudes besonders geschützt waren.
B3.101 Server	
- spezielle Regelungen für Server (Planung, Installation und Konfiguration, Rechtevergabe ...)	In 30 % der Fälle gab es solche, in welchem Umfang und zu welchen Inhalten wurde nicht näher untersucht.
- hinterlegte Admin.-Passwörter	In 30 % der Fälle nicht geschehen, wie aktuell diese waren, wurde nicht immer deutlich.
- regelmäßige Sicherheitsupdates /-patches eingespielt	100 % positive Antworten, bei Firmenbetreuung geht man davon aus (s. o. „Blindes Vertrauen“).
- Notfallrichtlinie/ Notfallboot-medium	15-20 % mit positiver Antwort, in vielen Fällen Hoffnung auf die unterstützende externe Firma (wie überhaupt kaum vertragliche Regelungen zum Leistungsspektrum vorhanden sind).
- Protokollierung und Auswertung (z. B. syslog bei UNIX)	Hierzu sind überwiegend keine Kenntnisse vorhanden. Wenn bekannt, wurden diese oft auch regelmäßig ausgewertet.
B3.201 Client	
- Passwortschutz / Passwortricht-linien	Passwortschutz in 85 % der Kommunen eingesetzt, in den übrigen Fällen oft unklar. In 40 % der Fälle gibt es auch eine schriftliche Richtlinie zum Passworteinsatz.
- unerlaubte/ungesicherte Netzzugänge ausgeschlossen	In 60 % der Fälle unklar. In 10% der Fälle wird ein unerlaubter Zugang nicht ausgeschlossen.
- Systemkonfiguration dokumentiert/kontrolliert	Systemkonfiguration dokumentiert: 65 % ja, 15 % nein, 20 % unklar, Systemkonfigurationskontrollen wurden in 30% der Fälle durchgeführt, in 20 % nicht und in 50 % ist dies unklar.
- regelmäßige Sicherheitsupdates /-patche eingespielt	50 % ja, 25 % erwarten dies von ihrem sie unterstützenden Dienstleister (s.o.) und bei 25 % ist es unklar oder wurde mit „nein“ beantwortet.
- Nutzung transportabler Datenträger (USB-Stick, CD/DVD...) reglementiert, ggf. ausgeschlossen	65 % haben die Nutzung portabler Speichermedien verboten, oft per Dienstanweisung; oder aber die Nutzung war technisch ausgeschlossen. In 20 % der Fälle war die Nutzung nicht reglementiert, in 15 % der Fälle war nichts bekannt. (ähnliches Ergebnis wie bei privater Hard- und Softwarenut-zung)
- lokale Datenspeicherung	In 75 % der Fälle ist eine zentrale Speicherung vorgesehen, in einigen Fällen ist aber daneben noch eine lokale Speicherung möglich. In 25 % der Fälle findet nur eine lokale Datenspeicherung statt.

IT-SICHERHEIT	
Aufgabe	**Zusammenfassung der Ergebnisse**
B3.301 Sicherheitsgateway	
- eigene Firewall (neben KOMM-Box und DVZ-Firewall)	95 % verfügen über eine eigene Firewall, in 5% der Fälle ist es nicht bekannt.
- wer administriert (Aktualisierungen, Filterregeln ...)	In 70 % der Fälle ein externer Dienstleister, in 20% der Fälle die/der Administrator/in der Kommune und in 10% der Fälle ist es nicht bekannt.
- Protokollauswertung	In 45 % der Fälle wird eine Protokollauswertung vorgenommen, 15 % davon entfallen auf externe Dienstleister, 30 % haben keine (Protokollierung?) oder Protokollauswertung, in 25 % der Fälle ist dies nicht bekannt.
Extrapunkt KOMM-Box	
- Funktionsweise der KOMM-Box bekannt	Bekannt 20 %, teilweise 10 %, nicht bekannt 35 %, keine klare Antwort bei 35 % (letztere wohl eher nicht).
- Zugriff auf KOMM-Box (IRIS) via https auf Port 8443 schon genutzt/getestet	Ca. 50 % nicht genutzt oder getestet, 45 % nicht bekannt, 5 % „ja“.
- Umgang mit Zertifikaten und Schlüsseln für OSCI-Transport	Obwohl alle den Schlüssel gerade in diesem Jahr erneuern mussten, antworteten 50 % es sei ihnen nichts bekannt. Erst auf Nachfrage keimte die Erinnerung auf.
B4.01 Heterogene Netze	
- aktuelle Netzdokumentation	Bei 15 % liegt eine Netzdokumentation vor, bei 20 % explizit nicht, alle übrigen hatten keine Kenntnis.
- Zugang zu externen Netzen (Kreisnetz, Landesnetz, Internet ...)	45 % konnten die Frage nicht einordnen. 55 % antworteten mit „Ja“.
- Kopplung internes/externes Netz (siehe auch B3.301)	90 % mussten bei der Frage passen.
B5.3 Internet/E-Mail-Nutzung	
- Internet/E-Mail zugelassen, wenn ja, über welche Provider	Alle Kommunen und der überwiegende Teil der Beschäftigten haben Zugang zum Internet und können E-Mail nutzen. 25 % der Befragten gaben an, dass die Nutzung per Dienstanweisung geregelt sei. In 15 % der Fälle war die private Nutzung explizit ausgeschlossen, in 50 % der Fälle zugelassen. 5 % antworteten zu allen Fragen mit Nichtwissen.
- Anschluss von Meldeamtsrechnern an das Internet	95 % der Rechner in den Einwohnermeldeämtern hatten auch Internetzugang.
- Sicherheitsvorgaben	In ca. 50 % der Kommunen gab es keine (klaren) Vorgaben.
- Dienstvereinbarung	In 10 % der Fälle gab es eine Dienstvereinbarung, in 20 % der Fälle gab es explizit keine Dienstvereinbarung, in den übrigen Fällen war nichts bekannt.

Wie bereits eingangs gesagt, gab es unter den besuchten Kommunen keine „völlig schwarzen Schafe“, ganz wenige hatten sehr viel umgesetzt, die meisten von vielem etwas, dabei aber oft zufällig und nicht klar strukturiert. Nur in den Kommunen, in denen ein Sicherheitsbeauftragter bestellt war, wurden die Fragen systematischer angegangen.

Die IT-Sicherheitskonzepte weisen in weiten Teilen der kommunalen Verwaltung noch große Lücken auf. Neben zentraler Hilfe und Unterstützung, die es ermöglicht, die Fragen systematisch anzugehen, ist vor allem ein klar formulierter Auftrag durch die Leitungsebene erforderlich.

Frage: Wurde in Ihrer Gemeinde/Stadt bereits einmal eine Vorabkontrolle nach § 19 Abs. 2 DSG-MV (i. V. m. § 20 Abs. 3 S. 5 Nr. 5) durchgeführt?

In keiner der besuchten Kommunen hat es eine Vorabkontrolle gegeben, weder bei Einführung des elektronischen Melderegisters noch bei Einführung des neuen Meldeverfahrens. Da ein Teil der befragten Kommunen bisher keinen behördlichen DSB bestellt hatte, konnte insoweit auch keine Vorabkontrolle stattfinden. In weiten Teilen der Kommunen war das Instrument der Vorabkontrolle nicht oder nur unzulänglich bekannt. Die übrigen Kommunen berichteten, dass nicht genügend Zeit zur Verfügung gestanden hätte, um vor der Einführung des neuen Verfahrens eine Vorabkontrolle durchzuführen.

In weiten Teilen der Kommunen war den behördlichen Datenschutzbeauftragten das Instrument der Vorabkontrolle nicht oder nur unzulänglich bekannt.

Frage: Wurde ein Verfahrensverzeichnis nach § 18 DSG-MV erstellt und genügt es den folgenden[31] Anforderungen?

Einige Kommunen hatten zusammen mit dem Fragebogen Verfahrensverzeichnisse zum Meldeverfahren übersandt. Ganz überwiegend lagen keine weiteren Verfahrensverzeichnisse vor, übrigens oft auch nicht zu anderen in den Kommunen eingesetzten Verfahren.

Die Ergebnisse im Einzelnen: 75 % der befragten Kommunen verfügen über ein allgemeines, vom Anbieter der Software zum elektronischen Melderegister erstelltes Verfahrensverzeichnis. In fast allen Fällen fehlten aber die Angaben zur datenverarbeitenden Stelle, sodass nicht der Eindruck gewonnen werden konnte, dass man sich überhaupt mit dem Dokument auseinandergesetzt hatte. Lediglich in zwei Fällen (entspricht etwa 10 % der Gesamtmenge) hatten die Kommunen das von der Softwarefirma produzierte Standard-Verfahrensverzeichnis um ihre Angaben ergänzt. In einem Fall davon hatte man sich sogar die Mühe gemacht, ein eigenes Verfahrensverzeichnis zu erstellen. Begründung: „Dafür können wir geradestehen, und das, was darin steht, verstehen wir.“ In den wenigsten Fällen war das Verzeichnis dem behördlichen DSB zugeleitet worden. Die Notwendigkeit oder Sinnhaftigkeit der Verfahrensverzeichnisse erschloss sich den meisten Gesprächsteilnehmern nicht.

Auch wenn die Prozentzahl vielleicht nicht 1:1 auf die gesamten Mengen der Kommunen hochgerechnet werden kann, so bleibt doch die Zahl der vor Ort tatsächlich festgestellten Verfahrensverzeichnisse weit hinter der von diesen Kommunen in der Fragebogenaktion gemachten Angaben zurück. Eine inhaltliche Beschäftigung mit dem von einer Fremdfirma erzeugten Verfahrensverzeichnis hat nur in den allerwenigsten Fällen stattgefunden.

Ein besseres Ergebnis für den Datenschutz kann nur dann erzielt werden, wenn zum einen den Kommunen die Sinnhaltigkeit und Notwendigkeit derartiger Regelungen vermittelt werden kann, und wenn zum anderen die behördlichen DSB eine ordnungsgemäße Behandlung auch einfordern, indem sie die Übersendung und die Prüfung der Verfahrensverzeichnisse vor Inbetriebnahme der Systeme verlangen.

Auch, wenn man die rechtlichen Rahmenbedingungen ändern und zulassen würde, dass Teile der Verfahrensverzeichnisse zentral erstellt werden dürfen, verblieb es bei der Notwendigkeit, das jeweilige Verfahren an die örtlichen Gegebenheiten anzupassen und dies auch zu dokumentieren. Die nach § 18 Abs. 1 Nr. 7 vorgesehene „allgemeine Beschreibung der technischen und organisatorischen Maßnahmen“ muss bei der datenverarbeitenden Stelle verbleiben.

Nur etwa 10 % der Kommunen haben ordnungsgemäße Verfahrensverzeichnisse. Eine Änderung der gesetzlichen Regelungen könnte eine teilweise zentrale Erstellung erlauben. In jedem Fall muss jede Kommune für sich eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen vornehmen.

6.6.7 Online-Auskunft

Die Online-Auskunft wurde einer gesonderten Untersuchung unterzogen. Um den Rahmen dieses Berichtes nicht zu sprengen, sollen hier nur die wesentlichen Ergebnisse kurz dargestellt werden.

6.6.7.1 Vorbereitung / Unterstützung für die Kommunen bei der rechtlichen Umsetzung

Die Erhebung bei den besuchten Kommunen, die einen repräsentativen Durchschnitt darstellt, hat ergeben, dass (um Ausreißer bereits bereinigt) bei den Melderegisterauskünften pro Kommune durchschnittlich

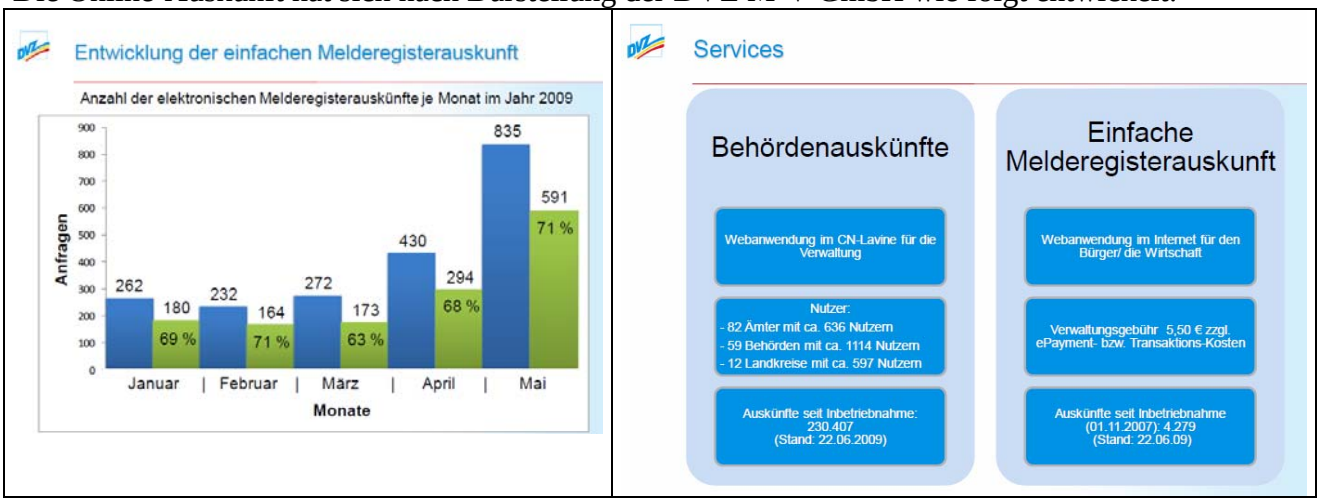
- 450 schriftliche und
- 330 telefonische

Anfragen pro Monat bearbeitet werden. Das entspricht pro Kommune einem Anteil von

- 15 schriftlich und
- 11 telefonisch

erteilten Melderegisterauskünften pro Tag.

Die Online-Auskunft hat sich nach Darstellung der DVZ M-V GmbH wie folgt entwickelt:



Schon das Stabdiagramm verdeutlicht, in welch geringem Umfang die elektronische Melderegisterauskunft genutzt wird. Dabei ist dieser Weg seit 2007 eröffnet. Noch klarer wird dies, wenn man die in dem daneben stehenden Schaubild angegebenen Zahlen auf den angegebenen Zeitraum umrechnet. Da telefonische Auskünfte i. d. R. öffentlichen, vornehmlich polizeilichen Stellen erteilt werden, entfallen die schriftlichen Anfragen ganz überwiegend auf private Anfragen. 4.279 online erteilte einfache Melderegisterauskünfte in rund 20 Monaten ergeben auf die Anzahl der Kommunen im Land verteilt durchschnittlich zwei Online-Auskünfte pro Monat. Im Gegensatz dazu werden durchschnittlich rund 450 schriftliche Melderegisterauskünfte pro Monat und Kommune erledigt, der überwiegende Teil davon sind einfache Melderegisterauskünfte.

Nicht öffentliche Stellen und Bürger nutzen in nur sehr geringem Umfang die Möglichkeiten der Online-Auskunft. Selbst sog. Power-User wie der Versandhandel oder Inkassobüros nutzen weiterhin die konventionelle Melderegisterauskunft.

Es besteht durchaus - auch aus Sicht des Datenschutzes - ein Interesse, möglichst viele Anfragen über das Online-Auskunftsverfahren abzuarbeiten. Nicht nur, dass die personellen Ressourcen der Meldeämter geschont würden, und nicht nur, dass eine elektronische Infrastruktur genutzt würde, die ohnehin vorgehalten wird und daher für die öffentliche Hand ohne Mehrkosten genutzt werden könnte, nein, auch der elektronische Weg ist der sicherere. Es ist garantiert, dass tatsächlich die Daten nur in dem Umfang übermittelt werden, wie dies gesetzlich zulässig ist, und es gibt parallel dazu eine zielgenaue Protokollierung, die es ermöglichen würde, dem Bürger im Falle der Inanspruchnahme seines Auskunftsanspruches zu sagen, wer wann von wem welche Daten über ihn erhalten hat.

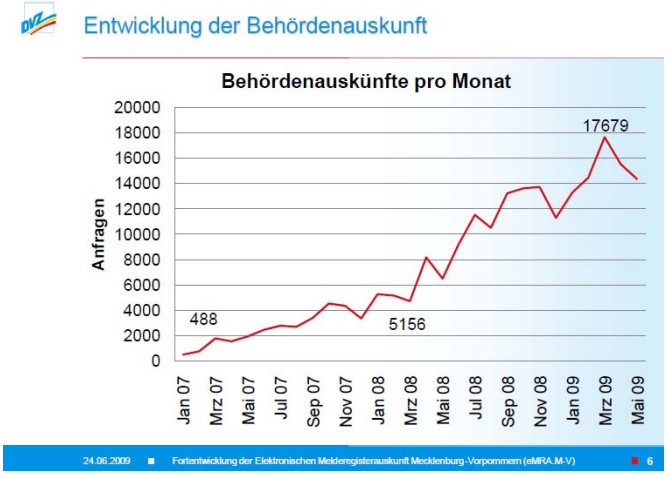
Aus Sicht des Datenschutzes besteht ein Interesse, möglichst viele Melderegisterauskünfte über das Online-Auskunftsverfahren abzuarbeiten.

Die Möglichkeit einer Online-Auskunft scheint noch nicht hinreichend bekannt.[32] Hinzu tritt, dass ca. 50 % der befragten Beschäftigten der Meldebehörden beklagten, sie seien nie ordentlich unterrichtet worden, wie die Online-Auskunft für den Bürger tatsächlich funktioniere, und könnten daher auch keine Hilfestellungen geben. Und weiter: Eine hohe Ausfallquote entstehe bei der Online-Auskunft dadurch, dass das System eine ganz bestimmte Schreibweise verlange (z. B. nicht Bergen, sondern Bergen auf Rügen) und keine technischen Hilfestellungen zur Fehlerkorrektur gebe. Es wurde gemutmaßt, dass auch bei Fehlanfragen, also Anfragen, in denen keine Auskunft erteilt werde, Kosten anfallen würden und deshalb von Anfragestellern lieber die konventionelle Auskunft genutzt werde. Der Bürger müsse auch in den Fällen bei der Online-Auskunft eine Gebühr entrichten, in denen er keine Auskunft bekomme, etwa weil eine Auskunftssperre eingetragen sei. Auch die Gebührenstaffelung scheint ein Grund dafür zu sein, dass der Weg der Online-Auskunft, der ja eigentlich eine Arbeitserleichterung für beide Seiten sein soll, nur sehr selten beschritten werde. Der Gebührenabstand zwischen Online- und Schrift-Auskunft sei zu gering[33].

Bei den vor-Ort-Gesprächen wurde speziell das Auskunftsverhalten der Polizei noch einmal thematisiert. Die Polizeidienststellen machen demnach am häufigsten von der telefonischen Melderegisterauskunft Gebrauch. Zur Erlangung einer Auskunft wird von den Polizeidienststellen ein Passwort genannt.[34] Sehr häufig wurde bemängelt, dass es sich hierbei um ein äußerst anfälliges und unsicheres Verfahren handele. Zum einen gebe es für das ganze Land Mecklenburg-Vorpommern ein einziges Passwort, das für einen oder mehrere Monate Gültigkeit habe, zum anderen sei auch die Unterrichtung der polizeilichen Dienststellen äußerst fragwürdig; so werde zum Teil dieses Passwort an die fraglichen Dienststellen ungeschützt über das Internet per Mail versandt. Mithin, auch diese Aspekte verdeutlichen, dass ein vitales Datenschutzinteresse darin besteht, dass die Online-Melderegisterauskunft auch von den Behörden möglichst intensiv genutzt wird.

6.6.7.2 Online-Auskunft an öffentliche Stellen

Es konnte nicht genau festgestellt werden, wie viele öffentliche Stellen zum Zeitpunkt der Durchführung des Projektes tatsächlich online die Behördenauskunft aus dem Melderegister nutzen konnten.[35] Es ist aber eindeutig, dass der Ausbau hier rasch voranschreitet, das macht auch die nachstehende Graphik deutlich.



Allerdings erscheint es bei der Behördenauskunft ein wenig transparentes Verfahren, wenn die Entscheidung und Verantwortung darüber, welche Daten aus dem zentralen Informationsregister ZIR tatsächlich zur Verfügung gestellt werden, den Administratoren in den einzelnen Dienststellen überlassen bleibt. Hier ist zu prüfen, ob nicht eine klare Struktur geschaffen werden muss, welchen Stellen im Einzelnen welche Daten zur Verfügung gestellt werden sollen.

Es sollte eine klare Regelung geben, welche Daten aus dem Melderegister von welchen Behörden abgerufen werden dürfen.

6.6.7.3 Zusammenfassung der Untersuchungen zur Melderegisterauskunft

Aus datenschutzrechtlicher Sicht ist die Online-Auskunft gegenüber der unmittelbaren Auskunft durch einzelne Meldebehörden sowohl für öffentliche wie für nicht-öffentliche Stellen und die Bürger zu favorisieren. Das Land hat die technischen Vorraussetzungen geschaffen, um alle Benutzergruppen auf dem elektronischen Weg mit den ihnen zustehenden Daten aus den Melderegistern zu versorgen. Selbst bei den meisten größeren Gemeinden findet sich auf deren Internetseiten kein Hinweis auf die Möglichkeit der Online-Auskunft.[36] Gegenüber den nicht-öffentlichen Stellen und den Bürgern bedarf es daher weiterer Anstrengungen, damit dieser Weg im größeren Ausmaß als bisher genutzt wird. Neben technischer Verbesserungen wie zum Beispiel Hilfestellungen bei der Schreibweise (Fehlerkorrektur) und einer besseren Öffentlichkeitsarbeit könnte insbesondere durch einen deutlichen Gebührenabstand zwischen der Auskunft durch die Meldebehörde und der Online-Auskunft eine bessere Nutzungsauslastung erreicht werden, damit insbesondere die kommerziellen „Poweruser“ das Instrument der Online-Auskunft vermehrt nutzen. Durch geeignete Maßnahmen sollten darüber hinaus auch die noch nicht angeschlossenen Behörden dazu angehalten werden, die Online-Auskunft einzurichten und tatsächlich zu nutzen. Das unsichere Passwort-Verfahren sollte überprüft werden.

Nicht nur das Online-Wetter in Mecklenburg-Vorpommern, auch die Online-Melderegisterauskunft sollte im Internet einfach zu finden sein. Die Internetseiten der Gemeinden sollten einen gezielten Link auf das Dienstleistungsportal des Landes enthalten.[37]

6.6.7.4 Nachbetrachtungen

Das Projekt gewährt Eindrücke über den Zustand des Datenschutzes auf der kommunalen Ebene in einem Umfang, der über das eigentliche Thema hinaus weist.

Viele Kommunen sind durch die Einführung des vernetzten Meldeverfahrens erstmals mit Formen komplexer moderner E-Government-Strukturen mit zentraler und dezentraler Datenverarbeitung in Berührung gekommen. Es gibt zwar immer noch die Einstellung, „das alles brauche man eigentlich nicht“, „das alte Verfahren sei völlig ausreichend gewesen“, „die Kosten für das Verfahren stünden in keinem Verhältnis zu den Verbesserungen“, aber viele Kommunen erkennen auch die Vorteile, die Ausbaumöglichkeiten, wie auch eine neu geschaffene DV-Infrastruktur, mit der man die eigenen kommunalen Aufgaben besser und effektiver erledigen kann. Kommunen mit dieser Einstellung erkennen, dass hier noch ein großes Potential schlummert und dass man erst ganz am Anfang von der Entwicklung effektiver Formen von elektronischer Verwaltung steht.

Eine solch aufgeklärte Einstellung steht dann oft auch zusammen mit der Erkenntnis, dass die bisherigen Datenschutzmaßnahmen für solch komplexe Systeme nicht ausreichend sind. Man trifft daher auf große Bereitschaft, den Datenschutz und insbesondere die Datensicherheit zu erhöhen. Allerdings fehlt oft das technische und vor allem strukturelle Wissen dafür, was zu tun ist, um einen auf die eingesetzten Systeme angepassten wie angemessenen Schutz zu erreichen. Oft wurden intensive punktuelle Maßnahmen ergriffen, die weitgehend ins Leere laufen, wenn man nicht an anderer Stelle ebenfalls die Schutzmaßnahmen erhöht. In der Not verlässt man sich oft auch auf externen Rat oder Hilfe. Dabei wird von der Verwaltungsseite häufig nicht überblickt, was diese externen Kräfte tatsächlich leisten und ob das, was sie tun, tatsächlich und in dem Umfang notwendig ist oder ob vorgeschlagene Maßnahmen ausreichend sind wie auch, ob es Alternativen gibt.[38] Hinzu tritt: Einmal gemachte negative Erfahrungen bei der Umstellung von Systemen führen häufig dazu, dass man lieber an einem veralteten System weiter „herumdoktert“, anstatt einen Schnitt zu machen und einen völlig neuen Weg einzuschlagen.

Externe Dienstleister, die für kommunale Stellen Datenverarbeitung oder DV-Support zur Verfügung stellen, sollten vorher einer unabhängigen Leistungskontrolle unterzogen werden. Dabei ist auch deren Datenschutzkompetenz mit einzubeziehen.

Verbreitet trifft man auch auf das Problem, dass den Kommunen die Hände gebunden sind, weil sie durch lange vertragliche Bindungen ihre Bewegungsfreiheit verloren haben. Erst langsam, z. T. zu spät, setzt sich in einigen Kommunen die Erkenntnis durch, dass man angesichts der schnell prosperierenden technischen Entwicklung keine Verträge mit einer Laufzeit von mehr als zwei Jahren abschließen sollte. Ergebnis langer Vertragslaufzeiten ist häufig, dass man bei technisch veralteten Verfahren gekoppelt mit einem veralteten Datenschutzstandard, der sich technisch nicht anpassen lässt, stehen bleibt.

Moderner Datenschutz lässt sich oft nicht bei veralteter Technik gewährleisten. Ob Einkauf von Software, Update-Optionen, Datenschutz- oder DV-Dienstleistung jeglicher Art - es sollten, wenn möglich, keine Verträge mit einer Laufzeit von mehr als zwei Jahren geschlossen werden. Eine einseitige Verlängerungsoption der öffentlichen Stelle stellt in der Regel eine ausreichende Garantie dar.

In vielen Gemeinden sind Verwaltungsbeamtinnen oder Verwaltungsbeamte mit der Aufgabe der Administration betraut; die meisten sind dafür nicht ausgebildet, und es fehlt häufig auch an Geld und ausreichender Zeit für Schulungen. Eine fachlich ausreichende Vertretung ist in der Regel nicht vorhanden. Viele Gemeinden sind daher jetzt schon am Limit ihrer Leistungsfähigkeit.

Die Leitungsebene verkennt oft, wie umfangreich und vielfältig die Anforderungen an die Administration eines sicheren IT-Netzwerkes geworden sind. Nur, wenn das hierfür eingesetzte Personal ausreichend ausgebildet ist und ihm ausreichend Zeit für konzeptionelle Arbeit zur Verfügung steht, gelingt es bei der Implementierung moderner E-Government-Strukturen, auch ein abgestimmtes Datenschutzmanagement als integralen Bestandteil zu etablieren.

Die Dokumentation des IT-Einsatzes weist in den meisten Kommunen große Lücken auf. Das unterstreichen auch die unter Gliederungspunkt 6.6 dargelegten Ergebnisse. Gerade im öffentlichen Dienst, wo in der Regel eine Stelle erst wieder neu besetzt werden kann, wenn sie frei wurde und damit keine Übergangs- und Einarbeitungszeit möglich ist, ist die Katastrophe vorprogrammiert, wenn keine ausreichende Systemdokumentation besteht.

Die festgestellten Mängel beim Vollzug der Datenschutzgesetze sind gravierend und bedürfen einer Reaktion. Die in weiten Teilen fehlende oder nicht ausreichende Dokumentation der IT-Systeme und der zugehörigen Datensicherheitsmaßnahmen stellt eine ernstzunehmende Gefahr für die Verfügbarkeit der Verfahren und für die Integrität des gesamten Netzes dar.

Nicht ordnungsgemäß laufende DV-Verfahren bergen die Gefahr eines Datenschutzverstoßes in sich. Ein großer Anteil der befragten Kommunen klagte in unterschiedlichen Ausprägungen und Fallgestaltungen über unzureichende Hilfe in Problemlagen. Gemeint sind sowohl landesweite Anwendungen als auch der Support bei kommunal gekaufter Software. Genannt wurden Service-Center, die nur per E-Mail-Anfrage erreichbar seien. Hier wurden lange Wartezeiten beklagt, auch wisse man oft nicht, wann eine Auskunft erfolge. Ebenfalls dazu zählen Call-Center mit langen, gebührenpflichtigen Warteschleifen oder Hilfezentren ohne konkrete Ansprechpartner. All diese Erscheinungsformen wurden als besonders abschreckende Leistungen empfunden. Der Zeitraum von einer Stunde, bis zu dem effektive Hilfe verfügbar ist, und eine möglichst persönliche Beziehung, bei der an Inhalte früherer Gespräche angeknüpft werden kann, wurden als Qualitätsmerkmale für Serviceleistungen genannt. Solche Leistungsmerkmale lassen sich sicherlich vertraglich vereinbaren, sie sind aber nicht umsonst zu haben. Leider besteht oft der Irrglaube, eine „lahmgelegte“ Verwaltung koste nichts. Kostengünstiger lassen sich solche Vereinbarungen mit Anbietern erreichen, wenn mehrere Kommunen an einem Strang ziehen.

Entsprechendes gilt für die Fernwartung. Auch hier sollten keine Verträge abgeschlossen werden, die nicht die Leistungen genau definieren und den dabei zu beachtenden Datenschutz regeln. Das wurde häufig vergessen.[39]

Hilfe, auch in Datenschutzfragen, sollte in angemessener zeitlicher Frist zur Verfügung stehen und vertraglich garantiert sein. Bei vertraglich vereinbarten IT-Leistungen Externer sind in der Regel die Bestimmungen für die Auftragsdatenverarbeitung unmittelbar oder entsprechend anzuwenden; eine Datenschutzklausel hat Bestandteil solcher Verträge zu sein.

Auch wäre es der Mühe wert festzustellen, wie hoch die Kosten der Kommunen insgesamt für die Vorhaltung der kommunalen DV im Allgemeinen und des Meldesystems im Besonderen sind. Die Dimensionen würden den Handlungsdruck erhöhen. Aber es scheint so, dass nicht einmal jede einzelne Kommune für sich diese Rechnung aufgemacht hat. Die immer leistungsfähigeren und komplexen Systeme verlangen immer mehr Know-how und Arbeitszeit vor Ort. Es ist zu befürchten, dass viele - insbesondere der kleinen und mittleren - Kommunen schon bald merken werden, dass sie an ihre finanziellen Leistungsgrenzen stoßen. Das parallele Vorhalten derselben Systeme an einer Vielzahl kommunaler Orte könnte zu einer Kostenexplosion führen, die den politischen Druck zum Zusammenschluss verschiedener Gemeinden erhöht. Man mag das gutheißen oder nicht, aber im Prinzip ist Technik nur dazu da, politische Entscheidungen zu unterstützen, aber nicht, politische Vorgaben zu machen.

Insofern muss dringend an Möglichkeiten gearbeitet werden, die für die Kommunen noch bezahlbar sind und die es den Kommunen ermöglichen, wieder freier zu agieren. Zu hoffen ist, dass die geschilderte Entwicklung vom E-Government-Zweckverband aufgegriffen wird und an Lösungen gearbeitet wird, die den Interessen der Kommunen entsprechen.

Es sollte versucht werden, viel mehr sich selbst organisierende Informationsbeziehungen und -strukturen zu entwickeln und zu verfestigen, zur Informationsverteilung Schneeballsysteme einzusetzen und direkte Information durch gezielte Verteilerkreise zu gewährleisten.

Es ist festzustellen, dass an vielen Orten verteilt bereits gute Ideen auch für die Gestaltung des Datenschutzes umgesetzt wurden. Notwendig wäre, eine Kommunikationsstruktur unter den Kommunen zu entwickeln, die einen Erfahrungsaustausch ermöglicht. Der Austausch über eine „Beste Datenschutzpraxis“ sollte durch Anreize und Belohnungen gefördert werden.

Auch die Informationspolitik zwischen Innenministerium, Kreisen und Kommunen verdient noch, dass ein Blick auf sie geworfen wird. Betrachtet man die vielen verschiedenen Interessen, Ebenen und ihre Beteiligten, die vielfältigen technischen und rechtlichen Ausgestaltungsmöglichkeiten, die Kosten und den politischen Beratungsbedarf, ist die Einführung des neuen Meldeverfahrens ein großes Werk, das unter enormem Zeitdruck fertig gestellt werden musste. Ohne Masterplan besteht die Gefahr, dass das eine oder andere schnell aus dem Blickfeld gerät. Die Einlassungen der Kommunen haben gezeigt, dass sie gern frühzeitig unterrichtet werden wollen und gern in dem laufenden Prozess ihren Erfahrungshorizont einbringen möchten. Sie würden es bevorzugen, auf dem Laufenden gehalten zu werden, auch wenn die Lösungen noch nicht fertig sind.

Natürlich ist die Gesetzgebung keine kommunale Angelegenheit. Wenn sie auf dieser Ebene umgesetzt werden soll, müssen die Betroffenen frühzeitig einbezogen werden. Auch auf kommunaler Ebene braucht man ausreichenden zeitlichen Vorlauf für die Anpassung der eigenen Systeme. Nur so können die anfallenden Kosten im Rahmen gehalten und ein vernünftiger Datenschutz entwickelt werden. Aber um aus Fehlern zu lernen, würde es sich vielleicht auch lohnen, nachträglich noch einmal das Gesetzgebungsverfahren des Bundes zu betrachten und dabei nachzuvollziehen, welche Rolle das Land gespielt hat und ob wirklich erkannt wurde, was diese Regelungen für Mecklenburg-Vorpommern bedeuteten.

Eine möglichst frühzeitige Einbeziehung der Kommunen in die grundlegenden Änderungen eines ihrer IT-Verfahren kann die Gewähr dafür bieten, dass bereits bei Einführung eines neuen Verfahrens der Datenschutz mitentwickelt worden ist.

6.7 Endnoten

[1] Aufgabe des Projektes war es, den Landesbeauftragten für den Datenschutz über die Ergebnisse des Untersuchungsgegenstandes möglichst umfassend und lückenlos zu unterrichten. Den Befragten und Gesprächsteilnehmern wurde im Interesse einer möglichst offenen und wahrheitsgetreuen Darstellung des Sachverhalts jeweils zugesichert, dass die Informationen im Falle einer Veröffentlichung anonymisiert und nicht zum Gegenstand datenschutzrechtlicher Beanstandungen gemacht würden. Diesen Anforderungen wird mit der für die Veröffentlichung vorgesehenen Vorlage dieses Berichtes Rechnung getragen werden.

[2] Die gesetzliche Frist zur technischen Umsetzung der neuen Regelungen im MRRG war noch nicht einmal verstrichen, da entbrannte bereits eine vom damaligen Innenminister Schäuble eröffnete Debatte über die Einführung eines zentralen Bundesmelderegisters. Vorläufiges Ergebnis war der Referentenentwurf eines Gesetzes zur Fortentwicklung des Meldewesens vom 25. April 2008 (dort die §§ 39 ff. BMeldG-E). Diese gegenüber einer verteilten Datenverarbeitung datenschutzfeindliche Variante wurde u. a. von den Datenschutzbeauftragten des Bundes und der Länder entschieden zurückgewiesen und ist wohl mit Wechsel des Ministers an die Spitze des Finanzministeriums vorerst vom Tisch.

[3] Die Änderung melderechtlicher Vorschriften des Landes beinhalteten im Wesentlichen Folgendes: Mit dem Gesetzentwurf der Landesregierung zum LMG M-V sollten vor allem zwingende bundesrechtliche Vorgaben des Melderechtsrahmengesetzes, das in den vorgehenden Jahren mehrfach geändert worden war, umgesetzt werden. Zu diesen Änderungen zählten u. a. die Abschaffung der Abmeldepflicht sowie der Mitwirkungspflicht des Vermieters bei der An- und Abmeldung eines Mieters. Die Abschaffung der Abmeldepflicht soll durch eine effektivere Rückmeldung zwischen den beteiligten Meldebehörden auf der Grundlage elektronischer Datenübertragung kompensiert werden. Hier liegt einer der wesentlichen Punkte, der mit gravierenden technischen Änderungen verbunden ist. Des Weiteren werden in dem Gesetzentwurf in Anpassung an das Melderechtsrahmengesetz zahlreiche Bestimmungen, u. a. das Selbstauskunftsrecht eines Einwohners, die Ausnahmen von der Meldepflicht sowie die besondere Meldepflicht in Beherbergungsstätten, Krankenhäusern, Heimen und ähnlichen Einrichtungen, neu gefasst. Der Gesetzentwurf macht aber auch von den bundesrechtlich eröffneten Regelungsspielräumen des Melderechtsrahmengesetzes Gebrauch. So wird den Meldebehörden beispielsweise ermöglicht, eine Anmeldung mittels eines sog. vorausgefüllten Meldescheins zuzulassen. Die Meldebehörde des Zuzugsortes kann in diesem Falle bestimmte Meldedaten eines Einwohners bei der Meldebehörde des Wegzugsortes elektronisch abrufen und ihm in seiner Anwesenheit oder elektronisch zur Kenntnis geben. Dadurch soll der Aufwand des Einwohners und der beteiligten Meldebehörden bei einer Anmeldung reduziert werden sowie der Grad der Richtigkeit der Melderegister erhöht werden. Die Möglichkeit der Anmeldung durch vorausgefüllten Meldeschein soll damit wohl auch bei einem länderübergreifenden Umzug eröffnet werden.

[4] Das ist angesichts der Fülle der Aufgaben für ein Flächenland ohne homogene DV-Struktur ein kurzer Zeitraum.

[5] Es hat sich gezeigt, dass der ganz überwiegende Teil der Befragten ihre kommunale Datenverarbeitung in eigener Regie betreibt. Allerdings wurde dabei oft in unterschiedlichem Umfang externe Hilfe bei der Systembetreuung in Anspruch genommen.

[6] Siehe unter: http://www.datenschutz.mvnet.de/dschutz/informat/everwaltung/fragebogen-elektronische-verwaltung.rtf

[7] Anhang 1

[8] Da jeweils mehrere Alternativen im Fragebogen enthalten sind, aber nur eine für eine Kommune einschlägig sein konnte, reduziert sich der Fragebogen im Grunde genommen auf eine bis anderthalb Seiten.

[9] Allerdings, nicht alle schriftlich gemachten Angaben der Kommunen konnten vor Ort auch immer in der Form tatsächlich bestätigt werden. So wurde z. B. die auf dem Fragebogen angegebene Bestellung einer/s Beauftragten den Datenschutz erst später rasch nachgeholt oder aber Datumsangaben wiesen aus, dass die Verzeichnisse erst nach Eingang des Fragenkatalogs erstellt wurden. Es ist daher davon auszugehen, dass die Ergebnisse aus der Fragebogenaktion zum Stichtag in Teilen tatsächlich noch schlechter ausgefallen wären. Trotzdem waren die Fragebogen eine gute Grundlage, um eine nach statistischen Methoden entwickelte Auswahl der Kommunen für die Besuche auszuwählen. Im Ergebnis hat die Fragebogenaktion dazu beigetragen, dass einige Gemeinden diese Aktion zum Anlass genommen haben, ihr Haus „auf Vordermann zu bringen“. So haben selbst Gemeinden, die korrekter Weise wahrheitsgemäß angegeben hatten, keine Verfahrensverzeichnisse erstellt zu haben, diese noch nachgeliefert.

[10] Es haben nicht alle Kommunen innerhalb der festgesetzten Fristen geantwortet. Am 14.08.2009 hatten 12 Kommunen noch überhaupt nicht reagiert, andere aus unterschiedlichen Gründen um Fristverlängerung gebeten. Einige Kommunen hatten auch Ende November 2009 noch nicht geantwortet. Die nachträglich eingehenden Angaben wurden zwar nachgetragen, um aber eine Verfälschung der Ergebnisse zu vermeiden, werden nur die Antworten, die innerhalb der Frist abgegeben wurden, als Grundlage für die statistische Auswertung verwendet.

[11] Hier sind die jeweiligen Sachbearbeiter(innen) zugleich die Administrator(inn)en ihrer eigenen Verfahren, was ebenfalls nicht ganz unproblematisch ist.

[12] Die fehlende Information ist gleichwohl keine Entschuldigung für fehlende Verfahrensverzeichnisse, schließlich handelt es sich um eine gesetzliche Pflicht.

[13] Wie sich bei besuchten Kommunen herausstellte, hatten viele noch nicht einmal für das bereits vorher bestehende elektronische Verfahren zur Führung des Melderegisters eine Verfahrensbeschreibung erstellt.

[14] Betrachtet wurden dabei die Kommunen, die nach ihren Angaben alle mit einem Aufforderungsschreiben des Innenministeriums verlangten Verfahrensverzeichnisse erstellt hatten.

[15] Pro 1000 Einwohner haben die
- großen Kommunen durchschnittlich 13 (12,9) Beschäftigte, die
- mittleren Kommunen durchschnittlich rund 5 (4,8) Beschäftigte und die
- kleinen Kommunen durchschnittlich rund 4 (3,7) Beschäftigte.

[16] Die Anzahl der Kommunen im Land beläuft sich auf die Zahl von knapp 120. Diese wurden für die Untersuchung in drei Größenklassen eingeteilt:
- über 20.000 Einwohner (große Kommunen),
- mehr als 10.000 bis 20.000 Einwohner (mittlere Kommunen) und
- 10.000 und weniger Einwohner (kleine Kommunen).

Von der Gesamtzahl der Kommunen gehören gerundet
- 10% der Klasse der großen Kommunen an,
- 35% der Klasse der mittlere Kommunen an und
- 55% der Klasse der kleineren Kommunen an.

Dementsprechend wurden 2 große, 7 mittlere und 11 kleine Kommunen für Besuche ausgewählt.

[17] Im Folgenden wurden dann Besuchstermine für die Informationsgespräche gemacht. Die jeweiligen Kommunen und soweit vorhanden auch die bzw. der behördliche Datenschutzbeauftragte wurden angeschrieben. An den Gesprächen nahmen in der Regel eine Person der Leitungsebene, eine sachbearbeitende Person aus der Meldestelle, ein(e) Systemverantwortliche(r) und soweit vorhanden die/der behördliche Beauftragte für den Datenschutz teil.

[18] Siehe Anhang 2

[19] Eine treffende Redewendung in der Finanzkrise.

[20] Vorauszuschicken ist, dass in allen Fällen der Nichtbestellung es auch vorher in diesen Gemeinden keinen Beauftragten für den Datenschutz gegeben hat. Es handelte sich also nicht um eine lediglich vorübergehende Nichtbesetzung.

[21] Überwiegend besteht die Tendenz, an ein- bis zweitägigen Schulungen im eigenen Land teilzunehmen.

[22] Etwa 35% der Befragten haben sich in irgendeiner Weise auf den Internetseiten des LfDI M-V informiert.

[23] § 20 Abs. 3 Nr. 1 DSG M-V zählt zu den Aufgaben der behördlichen Datenschutzbeauftragten insbesondere, „auf die Einhaltung bei der Einführung von Datenverarbeitungsmaßnahmen hinzuwirken“, aber auch jede Änderung muss „eingeführt“ werden.

[24] In der überwiegenden Anzahl der Dienststellen war nicht bekannt, dass ein Meldegeheimnis überhaupt existiert.

[25] Bei der erwähnten „zentralen Veranstaltung“ am 13. Dezember 2006 handelte es sich um einen vom Landesdatenschutzbeauftragten organisierten und gemeinsam mit der DVZ M-V GmbH und dem Innenministerium M-V durchgeführten Workshop, zu dem Vertreter aller Meldebehörden des Landes eingeladen waren. Angesichts der bis dahin unzureichenden Informationen sollten in diesem Workshop wenigstens Grundkenntnisse zu datenschutzrechtlichen und -technischen Aspekten des neuen Verfahrens vermittelt werden.

[26] Selbst, welche Funktion die KOMM-Box hat, ist weitestgehend unbekannt. Die befragten Kommunen sahen auch keinerlei oder nur in sehr geringem Umfang technische Verantwortung für die KOMM-Box, was die folgenden Äußerungen wiedergeben: „Wir schauen, ob die Lampen leuchten.“

[27] Diesen definierten Bereichen folgt die datenschutzrechtliche Verantwortung.

[28] Das macht etwa auch die folgende Antwort deutlich: “Freigabe, ja, aber keine förmliche Freigabe.“

[29] Einige Kommunen gaben an, sie seien vom Innenministerium dazu angehalten worden und hätten deshalb eine Freigabe dorthin übersandt. Soweit dort eingereicht, gab es scheinbar keine Kontrolle, meinten die Befragten, jedenfalls habe es keine Rückmeldung gegeben. „Wir hatten uns Hinweise und Anregungen erhofft.“

[30] Einmal auf der Basis des IT-Grundschutz-Handbuches, einmal auf der Basis einer Ausarbeitung vom Zweckverband eGovernment und eine Kommune hat einen externen Dienstleister mit der Erstellung beauftragt.

[31] Hier sollten die vom Gesetz bezeichneten Punkte genauer untersucht werden, wie die Bezeichnung des Verfahrens und der verarbeitenden Stelle, der Zweck und die Rechtsgrundlage der Verarbeitung usw. Wegen der Ergebnisse wurde dieser Gedanke nicht weiter verfolgt.

[32] Formularmäßig könnte bei jeder schriftlich erteilten Melderegisterauskunft auf die Möglichkeit einer Online-Auskunft hingewiesen werden.

[33] Die Abrechnung der DVZ M-V GmbH über einzelne Online-Auskünfte wurde von den Kommunen als zu intransparent empfunden. Trotz der von der DVZ M-V GmbH ausgewiesenen Steigerungsrate kommen scheinbar bei den Kommunen im Schnitt wohl nur marginale Beträge an. Es wurde darüber hinaus in Frage gestellt, ob der mit der Auszahlung der Beträge verbundene Verwaltungsaufwand (Einrichtung einer Haushaltsstelle etc.) ein solches Verteilsystem rechtfertige. Auch wurde von einigen bemängelt, dass bei eingehenden Zahlungen der Zahlungsgrund nicht klar erkennbar sei.

[34] Die genauen Regelungen dieses Verfahrens standen bei der Durchführung des Projekts nicht zur Verfügung, es wird aber davon ausgegangen, dass dieses Verfahren in einem Erlass geregelt ist.

[35] Nach Angabe der DVZ M-V GmbH (Stand 20.04.2009) wurden für die Behördenauskunft folgende Online-Zugänge eingerichtet:
- Ämter: 81 Ämter mit ca. 636 Nutzern
- Behörden: 57 Behörden mit 1.114 Nutzern
- Landkreise: 12 Landkreise mit 571 Nutzern

[36] Auf dem Dienstleistungsportal des Landes findet man die Online-Auskunft nur unter „Einfache Melderegisterauskunft“

[37] Beispielhaft vgl. http://www.wismar.de/index.phtml?mNavID=1800.1&sNavID=1800.121 oder http://www.glinde.de/index.php?id=43#c1698

[38] Einige Kommunen haben derweil schon schlechte Erfahrungen sammeln müssen, weil sie darauf vertrauten, dass die Externen das Richtige und Notwendige in ausreichendem Maße tun würden. Teure Rettungsmaßnahmen waren die Folge.

[39] Viele Anregungen enthält der Download des Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern, vgl. hier z. B. http://www.datenschutz.mvnet.de/dschutz/musterve/mv_dviau.html

6.8 Fragebogen

Projekt „Elektronische Verwaltung und Datenschutz“
des Landesbeauftragten für Datenschutz und Informationsfreiheit
Mecklenburg-Vorpommern

1. Allgemeine Angaben

1.1 Name der Gemeinde, Anschrift (kreisfreie Stadt, amtsfreie Gemeinde, Amt)

(Name)……

1.2 Größe der Gemeinde

(ungefähre Zahl der Einwohner) ……

1.3 Bürgermeister/Oberbürgermeister, Name und Erreichbarkeit

(Titel/Name)……

(Anschrift)……

(Mail oder Telefon)……

1.4 Wie viele Beschäftigte sind ungefähr in der Gemeindeverwaltung tätig?

(Anzahl der Beschäftigten in etwa)……

1.5 Ist ein behördlicher Datenschutzbeauftragter gem. § 20 DSG M-V bestellt?

☐ Ja
☐ Nein

Wenn ja, bitte noch folgende Angaben machen:
Name und Erreichbarkeit des behördlichen Beauftragten für den Datenschutz

(Name)……

(Anschrift)……

(Mail und Telefon)……

– Förmliche Bestellung mit Urkunde?

☐ Ja, Datum der Bestellung .....
☐ Nein

– Gibt es eine feste zeitliche Freistellung für diese Aufgabe?

☐ Ja, Anzahl der Stunden pro Woche .....
☐ Nein

Werden noch andere Verwaltungsaufgaben von der/von dem behördlichen Beauftragten wahrgenommen oder nimmt sie/er ihre/seine Aufgaben ausschließlich wahr?

☐ Ja, auch andere Verwaltungsaufgaben, und zwar: .....
☐ Nein, ausschließlich in Vollzeit/Teilzeit (bitte das nicht Zutreffende streichen)

2. Zu den Datenverarbeitungsverfahren der Kommunen

2.1 Werden die DV-Verfahren der Kommunen

☐ vollständig selbst geführt bei
- ○ zentraler Verantwortlichkeit (Name der/des Systemverantwortlichen)……
- ○ dezentraler Verantwortlichkeit
- ○ Zahl der Administratoren/innen (Zahl) .....
- ○ ungefähre Zahl der in der/den DV-Abteilung/en Beschäftigten (Zahl)

☐ ausschließlich durch externe Datenverarbeiter
- ○ ein externer Dienstleister führt alle Verfahren der Kommune durch
- ○ mehrere externe Dienstleister

○ Ist bekannt, ob der/die DV-Dienstleister einen betrieblichen Datenschutzbeauftragten bestellt hat/haben?

◊ Ja, hat/haben bestellt

◊ Nein, ist nicht bekannt

□ teilweise durch externe Datenverarbeitungsfirmen ausgeführt?

- Hier zu den extern vergebenen Verfahren

Welche Verfahren wurden an externe DV-Dienstleister vergeben?

○.....

○.....

○.....

○ (ggf. weitere am Ende des Fragebogens auf der letzten Seite aufführen)

○ Ist bekannt, ob der/die DV-Dienstleister einen betrieblichen Datenschutzbeauftragten bestellt hat/haben?

◊ Ja, hat/haben bestellt

◊ Nein, ist nicht bekannt

- Hier zu den von der Kommune selbst betriebenen Verfahren

Die Verfahren werden geführt:

○ zentrale Verantwortlichkeit (Name des/der Systemverantwortlichen).....

○ dezentrale Verantwortlichkeit

○ Zahl der Administratoren/innen (Zahl) .....

○ ungefähre Zahl der in der/den DV-Abteilung/en Beschäftigten (Zahl) .....

2.2 Fragen zum Betrieb der DV-Verfahren „Meldewesen“

□ Das DV-Verfahren zum Meldewesen wird von einem externen Dienstleister betrieben?[1]

○ privaten Dienstleister

○ öffentlichen Dienstleister

□ Das DV-Verfahren wird von der Kommune selbst betrieben?

- Wie ist der Name des Verfahrens, mit dem die Meldedatenverarbeitung betrieben wird?

○ MESO

○ anderes Verfahren (Name) .....

- Wurde ein Verfahrensverzeichnis (gem. § 18 DSG-MV) erstellt für

▪ Melderegisterauskünfte an Behörden, sonstige öffentliche Stellen

▪ an öffentlich-rechtliche Religionsgemeinschaften

○ Ja[2]

○ Nein

▪ die einfache Melderegisterauskunft

○ Ja[2]

○ Nein

[1] Falls vorhanden, fügen Sie bitte die vertragliche Regelung mit dem externen Dienstleister bei.

[2] Wenn Sie mit „Ja“ geantwortet haben, fügen Sie bitte jeweils eine Kopie/ elektronische Kopie des Verfahrensverzeichnisses bei.

- die Anbindung der Meldebehörden an das Zentrale Informationsregister (ZIR) des Landes (über Corporate Network LAVINE)
  - ○ Ja[2]
  - ○Nein

- Wurden die Maßnahmeempfehlungen, die gemeinsam vom Innenministerium M-V und von der DVZ M-V GmbH erarbeitet wurden, umgesetzt (siehe CD-ROM vom Oktober 2006)?
  - ○ Ja
  - ○ Nein
  - ○ teilweise
  - ○ nicht bekannt

- Betreibt Ihre Kommune eine eigene Internetseite?
  - ○ Ja unter www.....
  - ○ Nein

  Wenn Sie eine eigene Internetseite betreiben, befinden sich darauf irgendwelche Ausführungen oder Hinweise zum Meldeverfahren/-wesen?
  - ○ Ja
  - ○ Nein

Bemerkungen zu den Antworten:
.....
.....
.....
.....
.....
.....

Hinweis: Bitte kreuzen Sie die zutreffenden Kästchen an und senden Sie den ausgefüllten Fragebogen in der im Anschreiben benannten Frist (20. Juli 2009) an den

Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern
E-Mail: datenschutz@mvnet.de
Fax: 03 85 / 5 94 94-58
Postanschrift: Johannes-Stelling-Str. 21, 19053 Schwerin

[2] Wenn Sie mit „Ja“ geantwortet haben, fügen Sie bitte jeweils eine Kopie/ elektronische Kopie des Verfahrensverzeichnisses bei.

Name Gemeinde (Datum):	
Teilnehmer:	
Fragenkatalog der Informationsgespräche vor Ort	
A)	**Allgemeiner Teil**
1.	**Behördlicher DSB**
1.1	Ist ein behördlicher DSB bestellt (§ 20 DSG M-V)?
1.2	Förmliche Bestellung (Datum/Urkunde)?
1.3	Gibt es einen Grund, warum gerade Sie für die Aufgabe bestimmt wurden?
1.4	Gab es eine Vorbereitung auf die Tätigkeit? Wenn Ja welche?
1.5	Was wurde seit der Bestellung an Aufbau für die Tätigkeit getan?
1.6	Zeitkontingente? Andere Tätigkeiten in der Verwaltung?
1.7	Als DSB durchgeführte Tätigkeiten in diesem Jahr:
1.8	Bisherige Teilnahme an Schulungen? Schulungsmöglichkeiten bekannt?
1.9	Verständnis der Aufgabe Wo sehen Sie den Schwerpunkt Ihrer Aufgaben? (Gegenüber der Verwaltung, den Bürgern o. a.? Kennen Sie DSB anderer Gemeinden persönlich?)
1.10	Hatten Sie bereits Bürgeranfragen? Womit beschäftigte sich die letzte (wann)?
1.11	Kennen Sie das Internet-Angebot des LfDI M-V? Wie finden Sie es?
2.	**Schulung der Beschäftigten im Datenschutzrecht**
2.1	Wie viele Beschäftigte?
2.2	Wie viele davon verarbeiten personenbezogene Daten?
2.3	Geben Sie in Abständen Informationen zum Datenschutz an die Mitarbeiter?
2.4	Gibt es ein festes Fortbildungskonzept für die Beschäftigten im Datenschutz?
2.5	Was wurde in den letzten 2 Jahren mit den Beschäftigten erreicht?

2.6	Wurden die Beschäftigten schriftlich verpflichtet auf a) das Datengeheimnis, b) das Meldegeheimnis, c) das allgemeine Amtsgeheimnis oder d) gar nicht?
3.	**Allgemeine Eindrücke / Bewertung**
3.1	Haben Sie ganz allgemein den Eindruck, das neue Verfahren erleichtert die Melderegisterführung?
3.2	Haben Sie den Eindruck, die Melderegisterauskunft unter den Gemeinden des Landes wird dadurch erleichtert?
3.3	Haben Sie den Eindruck, das neue Verfahren erleichtert den Meldedatenaustausch mit anderen Behörden des Landes?
3.4	Haben Sie den Eindruck, der Datenaustausch mit den Kommunen anderer Länder wird dadurch verbessert?
3.5	Welche besonders positiven Punkte sehen Sie seit der Einführung des Verfahrens?
3.6	Welche negativen Punkte sehen Sie?
4.	**Fragen zu den Angaben im Hauptfragebogen**
4.1	Wie fanden Sie Aufbau und Inhalt der mitgelieferten CD-ROM zur Verfahrenseinführung?
5.	**Konventionelle Auskunft**
5.1	Ist Ihnen bekannt, in welchem Umfang tatsächlich die elektronische Melderegisterauskunft genutzt wird?
5.2	Ist Ihnen bekannt, in welchem Umfang die telefonische bzw. die schriftliche Melderegisterauskunft genutzt wird?
5.3	Gibt es eine Entlastung seit Einführung des ZIR?
5.4	Gibt es Kenntnis (Untersuchungen) darüber, ob insbesondere die Nachfragen der sogenannten „Power-User“ nachgelassen haben?
5.5	Welchen Eindruck haben Sie von der Qualität der elektronischen Melderegisterauskunft? (Hat sich jemand schon bei Ihnen beschwert?)
5.6	Die Einführung eines solchen Systems bedeutet ja zunächst in der Umstellungsphase mehr Arbeit. a) Wurden Sie dabei unterstützt? b) Wurde für die Umstellung Mehrarbeit angeordnet oder wurde das Personal der Meldebehörde vorübergehend verstärkt? c) Konnte die Mehrarbeit durch Effektivitätsgewinne später ausgeglichen werden? d) Konnte Personal nach der Einführungsphase wieder abgezogen werden?

6.	**Fragen zum Datenschutz bei der Einführung**
6.1	Sie mussten sich natürlich bei der Einführung des neuen Online-Meldeverfahrens auch um die Datenschutzbelange kümmern. Aber wie ist Ihre Einstellung dazu: Muss sich in einem solchen Fall in erster Linie a) die Gemeinde selbst um den Datenschutz kümmern oder b) wäre es Aufgabe derer gewesen, die das System in Gemeinden abverlangten oder c) wäre es Aufgabe des LfDI?
6.2	Wer hat Ihnen tatsächlich die größte Unterstützung bei den mit der Umstellung anstehenden Datenschutzfragen gewährt? a) Unterstützung durch das IM b) Unterstützung durch das DVZ c) Unterstützung durch den LfDI d) Unterstützung durch Meldesoftware-Firma
6.3	Haben Sie das Gefühl, dass der Datenschutz durch die Umstellung der Melderegister der Gemeinden von der Qualität her verbessert wurde? Fand zum Beispiel eine Bereinigung der Datensätze statt? Wurden alte Datensätze vermehrt abgeklärt oder gelöscht?
6.4	Tragen Sie datenschutzrechtliche Verantwortung für: a) LAVINE b) den Datenschutz im ZIR c) den Datenschutz in der KOMM-Box
6.5	Abgrenzung der Einwohnermeldestellen zur Pass-Stelle?
B)	**Tatsächliche Umsetzung des neuen Landesmeldegesetzes**
7.	**Vorbereitung / Unterstützung bei der Umsetzung des Landesmeldegesetzes**
7.1	Etwa wann und wie haben Sie zum ersten Mal erfahren, dass die Kommunen ihre Meldeverfahren umstellen müssen?
7.2	Wann und durch wen wurden Sie über die Neuerungen unterrichtet?
7.3	Hatten Sie den Eindruck, Ihnen stand für die Umstellung genügend Zeit zur Verfügung (incl. Einarbeitung der Kräfte)?
7.4	Hatten Sie damals den Eindruck, dieser Schritt der Vernetzung mit anderen Kommunen und dem Land war längst überfällig?

7.5	Gab es im Vorfeld der Einführung eine Beteiligung a) der Kommune? b) der/s behördlichen DSB? Wurden Sie oder die Kommune z.B. gefragt / bei der Entwicklung miteinbezogen? Wenn „Ja“: Welche Möglichkeiten hatten Sie, auf die Entwicklung einzuwirken oder mitzubestimmen? Auf welchem Wege? Wenn „Nein“: Hätten Sie sich überhaupt daran beteiligen wollen? Hatten Sie den Eindruck, alle Entscheidungen wurden in der mit Modell-Region geprägt?	
7.4	Welche rechtlichen Hilfestellungen gab es bei der Einführung des in vielen Teilen überarbeiteten Melderechts? Haben Sie auch die Gesetzesbegründungen erhalten? Halten Sie diese für ausreichend oder sind zusätzliche Auslegungshilfen erforderlich? An wen wenden Sie sich in rechtlichen Zweifelsfällen?	
7.5	Welche technischen Hilfestellungen gab es bei der Einführung des neuen Online-Meldeverfahrens?	
7.6	Hielten Sie diese Unterstützungsleistungen für ausreichend?	
7.7	Ist die Kommunikation über Probleme bei der Einführung über a) die Kreisebene oder b) direkt mit dem IM oder c) nur mit dem DVZ oder d) andere gelaufen?	
7.8	Was macht die DVZ M-V GmbH derzeit für die Gemeinde und welche Einflussmöglichkeiten haben Sie dabei?	
7.9	Hat es zur Einführung des neuen Meldeverfahrens Schulungen gegeben; wenn ja, auf Kreisebene oder im Austausch mit Nachbargemeinden?	
7.10	Haben Sie den Eindruck, die gesamte Betreuung des Systems macht jetzt mehr Arbeit als vorher? oder Hat es nur während der Einführungsphase mehr Belastung gegeben?	
8.	**Melderechtlicher Teil**	
8.1	Gibt es Alltagsprobleme bei der Verarbeitung der Meldedaten, die immer wieder auftreten?	
8.2	Ausführung der Protokollierungspflichten im gemeindlichen **E**inwohner**M**elde**R**egister? (Wo und wie lange aufbewahrt? Wer löscht?)	

8.3	Gibt es einen automatisierten Zugriff anderer Stellen Ihrer Gemeinde auf das gemeindliche EMR? Wenn ja: Gibt es Regelungen zur Einrichtung autom. Verfahren innerhalb einer Gemeinde / eines Amtes (Zulassungsverfahren gem. § 31 Abs. 8 LMG)	
8.4	Behandlung der Daten bei Wegzug/Tod? (Ggf. Sicherung durch t.-org. Maßnahmen?)	
8.5	Können Sie feststellen, ob die laufende Aktualisierung der Daten im ZIR (§ 3 Abs. 1 S. 3 LMG) tatsächlich stattgefunden hat?	
8.6	Meldescheine: a) Aufbewahrung der Meldescheine b) Art der Vernichtung c) Löschfrist	
8.7	Kann man sich bei Ihrer Gemeinde bereits elektronisch anmelden?	
8.8	Wurden der Vermittlungsstelle im Wege der Auftragsdatenverarbeitung (§ 3a Abs. 4 LMG MV i. V. m. § 4 DSG M-V) weitere Aufgaben übertragen?	
9.	**Bürgerrechtlicher Teil**	
	Fragen zur Einhaltung der Rechte der Betroffenen	
9.1	Welche Widerspruchsrechte kennen Sie? a) Adressverlage b) Parteien c) Jubilare d) automatisierte Registerauskunft e) Kirchen	
9.2	Wie werden diese Rechte bei einer elektronischen Anmeldung gewährleistet?	
9.3	Handhabung der Auskunftssperre	
9.4	Handhabung der öffentlichen Bekanntmachungen	
9.5	Handhabung der Unterrichtung der Betroffenen bei erweiterter Melderegisterauskunft (§ 34 Abs. 2 S. 3 LMG)	
10.	**Erfüllung der insbesondere technischen Anforderungen nach Datenschutzrecht**	
10.1	**Freigabe** nach § 19 Abs.1 DSG M-V; Gegenstände der Freigabe: - die Hardware - die Software einschließlich der Betriebssysteme - die Datenbestände - das aufbau- und ablauforganisatorische Regelwerk wie Zuständigkeitsregelungen und Dienstanweisungen, Benutzerhandbücher u. a.	
10.2	**Sicherheitskonzept** (vgl. Extra-Bogen)	

10.3	**Vorabkontrolle** nach § 19 Abs. 2 DSG M-V, (i. V. m. § 20 Abs. 3 S. 5 Nr. 5) Vor dem beabsichtigten Einsatz eines Verfahrens und nach vorläufigem Abschluss aller von der datenverarbeitenden Stelle zu treffenden Vorkehrungen hat die/der behördliche Datenschutzbeauftragte gemäß § 19 Abs. 2 i. V. m. § 20 Abs. 3 Satz 5 Nr. 5 DSG M-V eine Kontrolle durchzuführen, ob die rechtlichen Voraussetzungen für die Datenverarbeitung vorliegen und ausreichende technische und organisatorische Maßnahmen vorgesehen sind. Eine Vorabkontrolle hat zu erfolgen bei: ▪ den Verbund- und Abrufverfahren (§ 17 Abs. 1 DSG M-V) und ▪ den Verfahren, bei denen die in § 7 Abs. 2 DSG M-V aufgeführten sensiblen Daten automatisiert verarbeitet werden? Das Ergebnis der Vorabkontrolle ist zu dokumentieren. Dabei sind folgende Punkte schriftlich festzuhalten: ▪ Gegenstand der Prüfung ▪ Risikoabwägung ▪ Zweifelsfälle und (soweit möglich) Lösungsvorschläge ▪ Gründe für den Vorschlag von Alternativen ▪ Ergebnis der Vorabkontrolle. Die schriftlichen Aufzeichnungen sind dem Behördenleiter bzw. dem Verfahrensverantwortlichen zuzuleiten. Das Ergebnis der Vorabkontrolle wird zum Sicherheitskonzept genommen.	
10.4	**Verfahrensverzeichnis** nach § 18 DSG M-V Wurde es erstellt und genügt es den folgenden Anforderungen an ▪ die Bezeichnung des Verfahrens und der verarbeitenden Stelle, ▪ den Zweck und die Rechtsgrundlage der Verarbeitung, ▪ die Art der gespeicherten Daten, ▪ den Kreis der Betroffenen, ▪ den Kreis der Empfänger, denen die Daten mitgeteilt werden, ▪ den geplanten Datenübermittlungen in Drittländer, ▪ die allgemeine Beschreibung der technischen und organisatorischen Maßnahmen nach den §§ 21, 22 DSG M-V? Wurde eine Beschreibung für jedes von der jeweiligen Meldebehörde eingesetzte Verfahren dem behördlichen Datenschutzbeauftragten zur Führung des Verzeichnisses übermittelt?	
10.5	**LAVINE**	
10.5.1	Wie ist die Rechtsstellung der Gemeinde gegenüber LAVINE?	
10.5.2	Wie sind die tatsächlichen technischen Einflussmöglichkeiten auf LAVINE?	
10.5.3	Fühlen Sie sich in irgendeiner Form technisch verantwortlich für LAVINE?	
10.5.4	Fühlen Sie sich in irgendeiner Form verantwortlich für die Meldedaten in LAVINE?	

10.6	**KOMM-Box-Anschluss**	
10.6.1	Welche Funktion hat die KOMM-Box?	
10.6.2	Welche technischen Aufgaben hat Ihre Behörde gegenüber der KOMM-Box wahrzunehmen?	
10.6.3	Wie ist die Schlüsselverwaltung? (Zertifikat und Laufzeit)	
10.6.4	Wurde die KOMM-Box schon einmal aktualisiert oder administriert?	
10.6.5	Hat es in der vergangenen Zeit Probleme mit dem Einsatz der KOMM-Box gegeben?	
10.6.6	Welche Tätigkeiten haben Sie in der letzten Zeit gegenüber der KOMM-Box vorgenommen?	
10.6.7	Fühlen Sie sich in irgendeiner Form technisch verantwortlich für die KOMM-Box?	
10.6.8	Wo endet Ihre Verantwortung für die Verarbeitung der Meldedaten?	
10**.7**	Meldeverfahren **MESO** (HSH) **oder anderes**? a) Vertragliche Bindung? b) Fernwartung? c) Hat es schon einen Notfall mit dem Meldeverfahren gegeben, den Sie nicht selbst und ohne fremde Hilfe lösen konnten?	
10.8	**Fazit:** In wieweit ist Ihre Kommune nach Ihrer Einschätzung in der Lage, die hohen technischen Sicherheitsanforderungen umzusetzen?	

7. Anlagen

Anlage 1 Öffentlicher Bereich

Anlage 1.1 Berliner Erklärung: Herausforderungen für den Datenschutz zu Beginn des 21. Jahrhunderts

Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3. und 4. April 2008 in Berlin

Regelungen insbesondere zum großen Lauschangriff, zur Telekommunikationsüberwachung, zur Rasterfahndung, zur Online-Durchsuchung, zur automatischen Auswertung von Kfz-Kennzeichen und zur Vorratsspeicherung von Telekommunikationsdaten haben die verfassungsrechtlich zwingende Balance zwischen Sicherheitsbefugnissen der staatlichen Behörden und persönlicher Freiheit der Bürgerinnen und Bürger missachtet. Das Bundesverfassungsgericht hat mit einer Reihe von grundlegenden Entscheidungen diese Balance wieder hergestellt und damit auch den Forderungen der Datenschutzbeauftragten des Bundes und der Länder größtenteils Rechnung getragen.

Die Herausforderungen für den Datenschutz gehen aber weit über die genannten Bereiche hinaus. Datenverarbeitungssysteme dringen immer stärker in alle Lebensbereiche ein und beeinflussen den Alltag. Das Internet ist zum Massenmedium geworden. Vielfältig sind dabei die Möglichkeiten, das persönliche Verhalten zu registrieren und zu bewerten. Der nächste Quantensprung der Informationstechnik steht unmittelbar bevor: Die Verknüpfung von Informationstechnik mit Körperfunktionen, insbesondere bei der automatisierten Messung medizinischer Parameter und bei der Kompensation organischer Beeinträchtigungen. Die Miniaturisierung von IT-Systemen geht so weit, dass demnächst einzelne Komponenten nicht mehr mit bloßem Auge wahrgenommen werden können (Nanotechnologie).

Das Handeln staatlicher und nicht-öffentlicher Stellen ist verstärkt darauf gerichtet, viele Daten ohne klare Zweckbestimmung zu sammeln, um sie anschließend vielfältig auszuwerten, beispielsweise um versteckte Risiken aufzudecken oder um persönliches Verhalten unbemerkt zu beeinflussen. Geht es der Wirtschaft etwa darum, durch Scoringverfahren die Kundinnen und Kunden vorab einzuschätzen, gewinnt die immer exzessivere Registrierung und automatisierte Beobachtung für staatliche Stellen an Bedeutung. In beiden Bereichen wird ganz normales Verhalten registriert, unabhängig von konkreten Gefahren oder Verdachtsmomenten. Auch diejenigen, die sich nichts haben zu schulden kommen lassen, werden einem verstärkten Kontroll- und Anpassungsdruck ausgesetzt, der Einschüchterungseffekte zur Folge haben wird.

Der Schutz der Grundrechte, nicht zuletzt des Datenschutzes, dient in einer demokratischen Gesellschaft auch dem Gemeinwohl und ist zunächst Aufgabe jeglicher Staatsgewalt. Darüber hinaus ist er eine gesamtgesellschaftliche Aufgabe. Schließlich ist jede Bürgerin und jeder Bürger auch zur Eigenverantwortung aufgerufen. Hilfen zum informationellen Selbstschutz müssen zur Verfügung gestellt werden, die es den Betroffenen ermöglichen, eine Erfassung ihres Verhaltens zu vermeiden und selbst darüber zu entscheiden, ob und wem gegenüber sie Daten offenbaren. Von zunehmender Bedeutung sind auch Projekte, die das Datenschutzbewusstsein fördern, um vor allem jüngere Menschen von einem fahrlässigen Umgang mit ihren persönlichen Daten abzuhalten.

Alle diese Maßnahmen tragen zur Entwicklung einer neuen Datenschutzkultur bei. Voraussetzung dafür ist auch, dass nicht länger versucht wird, die verfassungsrechtlichen Grenzen und Spielräume auszureizen. Stattdessen muss dem Gebot der Datenvermeidung und -sparsamkeit Rechnung getragen werden.

Anlage 1.2 Mehr Augenmaß bei der Novellierung des BKA-Gesetzes

Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3. und 4. April 2008 in Berlin

Der vom Bundesministerium des Innern erarbeitete Referentenentwurf eines Gesetzes zur Abwehr des internationalen Terrorismus durch das Bundeskriminalamt hat zum Ziel, das Bundeskriminalamt mit umfassenden polizeilichen Befugnissen zur Verhütung von terroristischen Straftaten und zur Abwehr von Gefahren für die öffentliche Sicherheit in diesem Zusammenhang auszustatten. Insbesondere sind Befugnisse zur Durchsuchung, Rasterfahndung, Wohnraumüberwachung und Telekommunikationsüberwachung vorgesehen. Außerdem will das Bundesinnenministerium eine Befugnis zum heimlichen Zugriff auf informationstechnische Systeme („Online-Durchsuchung“) in das BKA-Gesetz aufnehmen.

Die Datenschutzbeauftragten des Bundes und der Länder sprechen sich dagegen aus, dass dem Bundeskriminalamt nach dem Gesetzentwurf mehr Befugnisse eingeräumt werden sollen, als einzelnen Landespolizeien zur Erfüllung ihrer eigenen Gefahrenabwehraufgaben zustehen. Sie halten es daher für geboten, im weiteren Gesetzgebungsverfahren die Befugnisse des BKA auf die zur Aufgabenerfüllung zwingend notwendigen Kompetenzen zu beschränken.

Die bisherige informationelle Gewaltenteilung zwischen den Polizeien der Länder und dem BKA diente auch dem Datenschutz. Die Konferenz fordert deshalb eine klare, d. h. hinreichend trennscharfe Abgrenzung der spezifischen Befugnisse des Bundeskriminalamts einerseits zu denen der Landespolizeien und Verfassungsschutzbehörden andererseits.

Dem Referentenentwurf zufolge soll die Aufgabenwahrnehmung durch das Bundeskriminalamt die Zuständigkeit der Landespolizeibehörden auf dem Gebiet der Gefahrenabwehr unberührt lassen. Dies führt zu erheblichen datenschutzrechtlichen Problemen, da nach geltendem Recht auch die Länder bei Abwehr einer durch den internationalen Terrorismus begründeten Gefahr parallele Abwehrmaßnahmen ergreifen können. Angesichts der Weite der für das Bundeskriminalamt vorgesehenen und den

Landespolizeibehörden bereits eingeräumten Datenerhebungs- und Datenverarbeitungsbefugnisse steht zu befürchten, dass es zu sich überlappenden und in der Summe schwerwiegenderen Eingriffen in das informationelle Selbstbestimmungsrecht Betroffener durch das Bundeskriminalamt und die Landespolizeibehörden kommen wird.

Ebenso stellt sich die grundsätzliche Frage der Abgrenzung von Polizei und Verfassungsschutz. In den vergangenen Jahren sind die Polizeigesetze des Bundes und der Länder zunehmend mit Befugnissen zur verdeckten Datenerhebung (z. B. heimliche Video- und Sprachaufzeichnungen, präventive Telekommunikationsüberwachung) ausgestattet worden. Zudem wurden die Eingriffsbefugnisse immer weiter ins Vorfeld von Straftaten und Gefahren erstreckt. Damit überschneiden sich die polizeilichen Ermittlungsbefugnisse zunehmend mit denen des Verfassungsschutzes.

Das Bundesverfassungsgericht hat in seinem Urteil zur „Online-Durchsuchung“ vom 27.02.2008 den Gesetzgeber erneut verpflichtet, den unantastbaren Kernbereich privater Lebensgestaltung zu gewährleisten. Diese Vorgabe des Gerichts gilt nicht nur für eine etwaige gesetzliche Regelung zur „Online-Durchsuchung“, sondern für alle Eingriffsmaßnahmen. Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber deshalb auf, im Rahmen der Novellierung des BKA-Gesetzes den Schutz des Kernbereichs privater Lebensgestaltung für alle Eingriffsmaßnahmen zu regeln.

Anlage 1.3 Unzureichender Datenschutz beim deutsch-amerikanischen Abkommen über die Zusammenarbeit der Sicherheitsbehörden

Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3. und 4. April 2008 in Berlin

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder beobachtet mit Sorge, dass die Datenschutzrechte der Bürgerinnen und Bürger im Rahmen der internationalen Zusammenarbeit der Sicherheitsbehörden immer häufiger auf der Strecke bleiben. Aktuelles Beispiel ist das am 11.03.2008 paraphierte deutsch-amerikanische Regierungsabkommen über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität. Die Konferenz fordert Bundestag und Bundesrat auf, dem Abkommen solange nicht zuzustimmen, bis ein angemessener Datenschutz gewährleistet ist.

Mit dem Abkommen wurde ein gegenseitiger Online-Zugriff auf Fundstellendatensätze von daktyloskopischen Daten und DNA-Profilen im hit/no-hit-Verfahren nach dem Muster des Prümer Vertrages vereinbart. Zudem wurden dessen Regelungen über den Austausch personenbezogener Daten zur Verhinderung terroristischer Straftaten weitgehend übernommen. Eine Übertragung des als Bedingung für diese umfangreichen Zugriffs- und Übermittlungsbefugnisse im Prümer Vertrag geschaffenen Datenschutzregimes erfolgte jedoch nicht.

Die Voraussetzungen, unter denen ein Datenaustausch erlaubt ist, sind nicht klar definiert. Der Datenaustausch soll allgemein zur Bekämpfung von Terrorismus und schwerer Kriminalität möglich sein. Welche Straftaten darunter konkret zu verstehen sind, wird nicht definiert. Es erfolgt hier lediglich der Verweis auf das jeweilige nationale Recht. Damit trifft nach dem Abkommen die USA einseitig eine Entscheidung über die Relevanz der abgerufenen Daten.

Bevor in so großem Umfang zusätzliche Datenübermittlungen erlaubt werden, muss zunächst geklärt werden, warum die bisherigen Datenübermittlungsbefugnisse für die internationale Polizeizusammenarbeit mit den USA nicht ausreichen.

Für die weitere Verarbeitung aus Deutschland stammender Daten in den USA bestehen für die Betroffenen praktisch keine Datenschutzrechte. Das Abkommen selbst räumt den Betroffenen keine eigenen Rechte ein, sondern verweist auch hierzu auf die Voraussetzungen im Recht der jeweiligen Vertragspartei. In den USA werden aber Datenschutzrechte, wie sie in der Europäischen Union allen Menschen zustehen, ausschließlich Bürgerinnen und Bürgern der Vereinigten Staaten von Amerika und dort wohnenden Ausländerinnen und Ausländern gewährt.

Anderen Personen stehen Rechtsansprüche auf Auskunft über die Verarbeitung der eigenen Daten, Löschung unzulässig erhobener oder nicht mehr erforderlicher Daten oder Berichtigung unrichtiger Daten nicht zu. Außerdem besteht in den USA keine unabhängige Datenschutzkontrolle. Vor diesem Hintergrund sind die im Abkommen enthaltenen weiten Öffnungsklauseln für die weitere Verwendung der ausgetauschten Daten sowie der Verzicht auf Höchstspeicherfristen aus datenschutzrechtlicher Sicht nicht akzeptabel.

Anlage 1.4 Datenschutzförderndes Identitätsmanagement statt Personenkennzeichen

Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3. und 4. April 2008 in Berlin

Elektronische Identitäten sind der Schlüssel zur Teilnahme an der digitalen Welt. Die Möglichkeiten der pseudonymen Nutzung, die Gewährleistung von Datensparsamkeit und -sicherheit und der Schutz vor Identitätsdiebstahl und Profilbildung sind wichtige Grundpfeiler moderner Informations- und Kommunikationstechnologien. Darauf hat die Bundesregierung zu Recht anlässlich des Zweiten Nationalen IT-Gipfels im Dezember 2007 (Hannoversche Erklärung) hingewiesen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass der gesetzliche Rahmen für die anonyme oder pseudonyme Nutzung elektronischer Verfahren bereits seit langem vorhanden ist. Beispielsweise hat jeder Diensteanbieter die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist (§ 13 Abs. 6 Telemediengesetz).

Bisher werden jedoch anonyme oder pseudonyme Nutzungsmöglichkeiten nur sehr selten angeboten. Vielmehr speichern Wirtschaft und Verwaltung immer mehr digitale Daten mit direktem Personenbezug. Erschlossen werden diese Datenbestände in der Regel über einheitliche Identifizierungsnummern. Mit der lebenslang geltenden, bundeseinheitlichen Steuer-Identifikationsnummer (Steuer-ID) oder der mit der Planung der Gesundheitskarte zusammenhängenden, ebenfalls lebenslang geltenden Krankenversichertennummer werden derzeit solche Merkmale eingeführt. Auch mit der flächendeckenden Einführung des ePersonalausweises wird jeder Bürgerin und jedem Bürger eine elektronische Identität zugewiesen, mit der sie bzw. er sich künftig auch gegenüber eGovernment-Portalen der Verwaltung oder eCommerce-Angebo-ten der Wirtschaft identifizieren soll.

Einheitliche Personenkennzeichen bergen erhebliche Risiken für das Recht auf informationelle Selbstbestimmung. So könnte sich aus der Steuer-ID ein Personenkennzeichen entwickeln, über das alle möglichen Datenbestände personenbezogen verknüpft und umfassende Persönlichkeitsprofile erstellt werden. Angesichts der stetig verbesserten technischen Möglichkeiten, zunächst verteilt gespeicherte Daten anwendungsübergreifend zu verknüpfen, wachsen entsprechende Begehrlichkeiten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die effektive Nutzung von Informationstechnik und hohe Datenschutzstandards keinen Widerspruch bilden. Ein datenschutzförderndes Identitätsmanagement kann den Einzelnen vor unangemessener Überwachung und Verknüpfung seiner Daten schützen und zugleich eine moderne und effektive Datenverarbeitung ermöglichen. Entsprechende EU-Projekte wie PRIME (Privacy and Identity Management for Europe) und FIDIS (Future of Identity in the Information Society) werden im Rahmen des 6. Europäischen Forschungsprogramms „Technologien für die Informationsgesellschaft2 gefördert.

Identitätsmanagement sollte auf der anonymen oder pseudonymen Nutzung von elektronischen Verfahren und der dezentralen Haltung von Identifikationsdaten unter möglichst weitgehender Kontrolle der betroffenen Bürgerinnen und Bürger basieren. Datenschutzfördernde Identitätsmanagementsysteme schließen Verknüpfungen nicht aus, wenn die Nutzenden es wünschen oder wenn dies gesetzlich vorgesehen ist. Sie verhindern jedoch, dass unkontrolliert der Bezug zwischen einer elektronischen Identität und einer Person hergestellt werden kann. Unter bestimmten, klar definierten Bedingungen kann mit Hilfe von Identitätsmanagementsystemen sichergestellt werden, dass ein Pseudonym bei Bedarf bezogen auf einen bestimmten Zweck (z.B. Besteuerung) einer Person zugeordnet werden kann.

Identitätsmanagementsysteme werden nur dann die Akzeptanz der Nutzerinnen und Nutzer finden, wenn sie einfach bedienbar sind, ihre Funktionsweise für alle Beteiligten transparent ist, möglichst alle Komponenten standardisiert sind und die Technik von unabhängigen Dritten jederzeit vollständig nachprüfbar ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung daher auf, den Absichtserklärungen des IT-Gipfels Taten folgen zu lassen und den Einsatz datenschutzfördernder Identitätsmanagementsysteme voranzutreiben. Sowohl die öffentliche Verwaltung als auch die Wirtschaft sollte die Einführung solcher datenschutzfördernder Systeme unterstützen.

Anlage 1.5 Vorgaben des Bundesverfassungsgerichts bei der Online-Durchsuchung beachten

Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3. und 4. April 2008 in Berlin

1. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass das Bundesverfassungsgericht die Regelung zur Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalen für nichtig erklärt hat. Hervorzuheben ist die Feststellung des Gerichts, dass das allgemeine Persönlichkeitsrecht auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme umfasst. 25 Jahre nach dem Volkszählungsurteil hat das Bundesverfassungsgericht damit den Datenschutz verfassungsrechtlich weiter gestärkt und ihn an die Herausforderungen des elektronischen Zeitalters angepasst.

2. Ein solches Grundrecht nimmt auch den Staat in die Verantwortung, sich aktiv für die Vertraulichkeit und Integrität informationstechnischer Systeme einzusetzen. Das Bundesverfassungsgericht verpflichtet den Staat, im Zeitalter der elektronischen Kommunikation Vertraulichkeit zu gewährleisten. Nunmehr ist der Gesetzgeber gehalten, diesen Auftrag konsequent umzusetzen. Dazu müssen die Regelungen, welche die Bürgerinnen und Bürger vor einer "elektronischen Ausforschung" schützen sollen, gemäß den Vorgaben des Gerichts insbesondere im Hinblick auf technische Entwicklungen verbessert werden. Hiermit würde auch ein wesentlicher Beitrag geleistet, Vertrauen in die Sicherheit von E-Government- und E-Commerce-Verfahren herzustellen.

3. Die Konferenz unterstützt die Aussagen des Gerichts zum technischen Selbstschutz der Betroffenen. Ihre Möglichkeiten, sich gegen einen unzulässigen Datenzugriff zu schützen, etwa durch den Einsatz von Verschlüsselungsprogrammen, dürfen nicht unterlaufen oder eingeschränkt werden.

4. Die Konferenz begrüßt außerdem, dass das Bundesverfassungsgericht das neue Datenschutzgrundrecht mit besonders hohen verfassungsrechtlichen Hürden vor staatlichen Eingriffen schützt. Sie fordert die Gesetzgeber in Bund und Ländern auf, diese Eingriffsvoraussetzungen zu respektieren. Die Konferenz spricht sich in diesem Zusammenhang gegen Online-Durchsuchungen durch die Nachrichtendienste aus.

5. Das Bundesverfassungsgericht hat den Gesetzgeber erneut verpflichtet, den unantastbaren Kernbereich privater Lebensgestaltung auch bei Eingriffen in informationstechnische Systeme zu gewährleisten. Unvermeidbar erhobene kernbereichsrelevante Inhalte sind unverzüglich zu löschen. Eine Weitergabe oder Verwertung dieser Inhalte ist auszuschließen.

6. Auch wenn Online-Durchsuchungen innerhalb der durch das Bundesverfassungsgericht festgelegten Grenzen verfassungsgemäß sind, fordert die Konferenz die Gesetzgeber auf, die Erforderlichkeit von Online-Durchsuchungsbefugnissen kritisch zu hinterfragen. Sie müssen sich die Frage stellen, ob sie den Sicherheitsbehörden entsprechende Möglichkeiten an die Hand geben wollen. Die Konferenz bezweifelt, dass dieser weiteren Einbuße an Freiheit ein adäquater Gewinn an Sicherheit gegenüber steht.

7. Sollten gleichwohl Online-Durchsuchungen gesetzlich zugelassen werden, sind nicht nur die vom Bundesverfassungsgericht aufgestellten verfassungsrechtlichen Hürden zu beachten. Die Konferenz hält für diesen Fall zusätzliche gesetzliche Regelungen für erforderlich. Zu ihnen gehören vor allem folgende Punkte:

8. Soweit mit der Vorbereitung und Durchführung von Online-Durchsuchungen der Schutzbereich von Art. 13 GG (Unverletzlichkeit der Wohnung) betroffen ist, bedarf es dafür jedenfalls einer besonderen Rechtsgrundlage.

9. Der vom Bundesverfassungsgericht geforderte Richtervorbehalt ist bei Online-Durchsuchungen mindestens so auszugestalten wie bei der akustischen Wohnraumüberwachung. Ergänzend zu einer richterlichen Vorabkontrolle ist eine begleitende Kontrolle durch eine unabhängige Einrichtung vorzuschreiben.

10. Gesetzliche Regelungen, welche Online-Durchsuchungen zulassen, sollten befristet werden und eine wissenschaftliche Evaluation der dabei gewonnenen Erkenntnisse und Erfahrungen anordnen.

11. Informationstechnische Systeme, die von zeugnisverweigerungsberechtigten Berufsgruppen genutzt werden, sind von heimlichen Online-Durchsuchungen auszunehmen.

12. Für die Durchführung von "Quellen-Telekommunikationsüberwachungen", die mit der Infiltration von IT-Systemen einhergehen, sind die gleichen Schutzvorkehrungen zu treffen wie für die Online-Durchsuchung selbst.

13. Schließlich sind die Gesetzgeber in Bund und Ländern aufgrund der Ausstrahlungswirkung der Entscheidung des Bundesverfassungsgerichts gehalten, die sicherheitsbehördlichen Eingriffsbefugnisse in Bezug auf informationstechnische Systeme, z.B. bei der Überwachung der Telekommunikation im Internet sowie der Beschlagnahme und Durchsuchung von Speichermedien, grundrechtskonform einzuschränken.

Anlage 1.6 Keine Daten der Sicherheitsbehörden an Arbeitgeber zur Überprüfung von Arbeitnehmerinnen und Arbeitnehmern

Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3. und 4. April 2008 in Berlin

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Übermittlung polizeilicher und nachrichtendienstlicher Erkenntnisse an Arbeitgeber zur Überprüfung von Bewerberinnen und Bewerbern, Beschäftigten und Fremdpersonal (z. B. Reinigungskräfte) außerhalb gesetzlicher Grundlagen. In zunehmendem Maß bitten Arbeitgeber die Betroffenen, in eine Anfrage des Arbeitgebers bei der Polizei oder dem Verfassungsschutz zu etwaigen dort vorliegenden Erkenntnissen zu ihrer Person einzuwilligen. In anderen Fällen sollen die Betroffenen eine solche Auskunft („fremdbestimmte Selbstauskunft“) selbst einholen und ihrem Arbeitgeber vorlegen. Eine solche „Einwilligung des Betroffenen“ ist regelmäßig keine wirksame Einwilligung. Die Betroffenen sehen sich oftmals dem faktischen Druck des Wohlverhaltens zum Zwecke des Erhalts und der Sicherung des Arbeitsplatzes ausgesetzt.

Die gesetzliche Grundentscheidung, in einem "Führungszeugnis" dem Arbeitgeber nur ganz bestimmte justizielle Informationen zu einer Person verfügbar zu machen, wird dadurch unterlaufen. Es stellt einen Dammbruch dar, wenn jeder Arbeitgeber durch weitere Informationen direkt oder indirekt an dem Wissen der Sicherheitsbehörden und Nachrichtendienste teilhaben kann. Die Übermittlung dieser Informationen an Arbeitgeber kann auch den vom Bundesarbeitsgericht zum "Fragerecht des Arbeitgebers" getroffenen Wertentscheidungen widersprechen. Danach darf der Arbeitgeber die Arbeitnehmerinnen und Arbeitnehmer bei der Einstellung nach Vorstrafen und laufenden Ermittlungsverfahren fragen, wenn und soweit die Art des zu besetzenden Arbeitsplatzes dies erfordert.

Polizei und Nachrichtendienste speichern - neben den in ein „Führungszeugnis“ aufzunehmenden Daten - auch personenbezogene Daten, die in das Bundeszentralregister gar nicht erst eingetragen werden oder Arbeitgebern in einem „Führungszeugnis“ nicht übermittelt werden dürfen. Es stellt eine grundsätzlich unzulässige Durchbrechung des Zweckbindungsgrundsatzes dar, wenn ein Arbeitgeber diese Daten - über den Umweg über die Polizei oder einen Nachrichtendienst - für Zwecke der Personalverwaltung erhält. Dabei ist besonders zu beachten, dass polizeiliche oder nachrichtendienstliche Daten nicht zwingend gesicherte Erkenntnisse sein müssen, sondern oftmals lediglich Verdachtsmomente sind. Die Folgen von Missdeutungen liegen auf der Hand.

Anlage 1.7 Medienkompetenz und Datenschutzbewusstsein in der jungen „online-Generation“

Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3. und 4. April 2008 in Berlin

1. Die Nutzung moderner Informationssysteme ist auch mit Risiken verbunden. Diese begründen ein besonderes Schutzbedürfnis der Bürgerinnen und Bürger. Dieses verlangt aber nicht nur rechtliche Vorkehrungen und Sicherungen, sondern auch Aufklärung und Information darüber, mit welchen Risiken die Nutzung dieser Informationssysteme verbunden sind. Dies gilt vor allem für die junge „online-Generation“, die in der Altersgruppe der 14- bis 19-Jährigen zu 96 % regelmäßig das Internet nutzt und zwar im Durchschnitt länger als zweieinhalb Stunden täglich.

2. Die Datenschutzbeauftragten des Bundes und der Länder sehen es daher als wichtige Aufgabe an, Kinder und Jugendliche für einen sorgsamen und verantwortungsbewussten Umgang mit den eigenen Daten und den Daten anderer zu sensibilisieren. Diese Aufgabe obliegt gesellschaftlichen Einrichtungen ebenso wie staatlichen Organen.

   Die Erfahrungen, die anlässlich des 2. Europäischen Datenschutztages am 28. Januar 2008 gemacht wurden, stützen dies. Zu dem Motto „Datenschutz macht Schule“ wurde von den Datenschutzbeauftragten des Bundes und der Länder eine Vielzahl von Veranstaltungen und Schulbesuchen organisiert. Eltern, Lehrkräfte, Schülerinnen und Schüler, aber auch Studierende hatten dabei die Möglichkeit, sich z. B. bei Podiumsdiskussionen, Rollenspielen und Workshops über datenschutzrelevante Fragen bei der Nutzung moderner Medien zu informieren. Die dabei gewonnenen Erfahrungen lassen nicht nur einen enormen Informationsbedarf, sondern auch ein großes Informationsinteresse erkennen, und zwar bei allen Beteiligten, bei den Jugendlichen ebenso wie bei ihren Eltern und den Lehrkräften.

   Bei den Informationsangeboten, die derzeit den Schulen angeboten werden, um die Medienkompetenz junger Menschen zu verbessern, spielt das Thema „Datenschutz“ aber nur eine untergeordnete Rolle. Es beschränkt sich überwiegend auf Fragen der Datensicherheit und wird zudem häufig von Fragen des Jugendmedienschutzes und des Verbraucherschutzes überlagert.

3. Die Datenschutzbeauftragten des Bundes und der Länder halten es daher für notwendig, dass die für die schulische Bildung zuständigen Ministerinnen und Minister der Landesregierungen bei der Förderung der Medienkompetenz von Kindern und Jugendlichen - schon im Grundschulalter - deren Datenschutzbewusstsein stärken. Der Datenschutz muss bei den Angeboten und Projekten zur Förderung der Medienkompetenz eine größere Rolle spielen. Die bisherigen Ansätze reichen bei weitem nicht aus. Gerade bei jungen Menschen muss das Bewusstsein über den Datenschutz als Bürgerrecht und Bestandteil unserer demokratischen Ordnung stärker gefördert werden.

Anlage 1.8 Keine Vorratsspeicherung von Flugpassagierdaten

Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3. und 4. April 2008 in Berlin

Die EU-Kommission hat den Entwurf eines Rahmenbeschlusses des Rates zur Speicherung von Flugpassagierdaten und zu deren Weitergabe an Drittstaaten vorgelegt. Künftig sollen die Fluggesellschaften bei Flügen aus der EU und in die EU zu jedem Fluggast insgesamt 19 Datenelemente, bei unbegleiteten Minderjährigen sechs weitere Datenelemente, an eine von dem jeweiligen Mitgliedstaat bestimmte „Zentralstelle“ übermitteln. Die Daten sollen bei den Zentralstellen anlass- und verdachtsunabhängig insgesamt 13 Jahre lang personenbezogen gespeichert werden und zur Durchführung von Risikoanalysen dienen. Unter im Einzelnen noch unklaren Voraussetzungen sollen die Daten an Strafverfolgungsbehörden von Nicht-EU-Staaten (z. B. die USA), übermittelt werden dürfen. Neben Grunddaten zur Person, über Reiseverlauf, Buchungs- oder Zahlungsmodalitäten und Sitzplatzinformationen sollen auch andere persönliche Angaben gespeichert werden. Unklar ist, welche Daten unter "allgemeine Hinweise" gespeichert werden dürfen. Denkbar wäre, dass beispielsweise besondere Essenswünsche erfasst werden.

Mit der beabsichtigten Vorratsspeicherung und der Datenübermittlung wird die EU es auswärtigen Staaten ermöglichen, Bewegungsbilder auch von EU-Bürgerinnen und -Bürgern zu erstellen. In Zukunft besteht die Gefahr, dass Menschen Angst haben werden, durch ihre Reisegewohnheiten aufzufallen.

Die in dem Rahmenbeschluss vorgesehene Vorratsdatenspeicherung von Daten sämtlicher Fluggäste, die EU-Grenzen überschreiten, verstößt nicht nur gegen Art. 8 der Europäischen Menschenrechtskonvention und die Europaratskonvention 108, sondern ist auch mit dem im Grundgesetz verankerten Recht auf informationelle Selbstbestimmung nicht vereinbar. Grundrechtseingriffe "ins Blaue hinein", also Maßnahmen ohne Nähe zu einer abzuwehrenden Gefahr sind unzulässig.

Der Vorschlag für den Rahmenbeschluss erfolgte, ohne den Nutzen der erst jüngst in nationales Recht umgesetzten Richtlinie 2004/82/EG [1], die bereits alle Beförderungsunternehmen verpflichtet, die Daten von Reisenden an die Grenzkontrollbehörden zu übermitteln, auszuwerten. Hinzu kommt, dass der Vorschlag kaum datenschutzrechtliche Sicherungen enthält. Er bezieht sich nur auf eine bisher nicht bestehende und im Entwurf mit Mängeln behaftete EU-Datenschutzregelung. Diese Mängel wirken sich dadurch besonders schwerwiegend aus, dass in den Drittstaaten ein angemessenes Datenschutzniveau nicht immer gewährleistet ist und eine Änderung dieser Situation auch in Zukunft nicht zu erwarten ist.

Die EU-Kommission hat nicht dargelegt, dass vergleichbare Maßnahmen in den USA, in Kanada oder in Großbritannien einen realen, ernst zu nehmenden Beitrag zur Erhöhung der Sicherheit geleistet hätten. Sie hat die kritischen Stellungnahmen der nationalen und des Europäischen Datenschutzbeauftragten sowie der Art. 29-Datenschutzgruppe nicht berücksichtigt.

Die Konferenz fordert die Bundesregierung auf, den Entwurf abzulehnen. Sie teilt die vom Bundesrat geäußerten Bedenken an der verfassungsrechtlichen Zulässigkeit der Speicherung der Passagierdaten.

[1] *RL 2004/82 EG v. 29.4.2004 Amtsbl. L 261 (2004) S. 24 ff., Richtlinie über die Verpflichtung von Beförderungsunternehmen, Angaben über die Beförderten zu übermitteln*

Anlage 1.9 Entschlossenes Handeln ist das Gebot der Stunde

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. September 2008

Nie haben sich in der jüngeren Geschichte die Skandale um den Missbrauch privater Daten in der Wirtschaft so gehäuft wie heute und damit deutlich gemacht, dass nicht nur im Verhältnis Bürger-Staat das Grundrecht auf informationelle Selbstbestimmung bedroht ist. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat wiederholt - zuletzt in ihrer Berliner Erklärung vom 4. April dieses Jahres - auf diese Gefahren hingewiesen, die von massenhaften Datensammlungen privater Unternehmen und ihrer unkontrollierten Nutzung ausgehen. Sie hat auch deshalb den Gesetzgeber zu einer grundlegenden Modernisierung und Verbesserung des Datenschutzrechts aufgefordert und eine neue Datenschutzkultur angemahnt.

Dass jetzt endlich im politischen und gesellschaftlichen Raum die Problematik erkannt und diskutiert wird, ist zu begrüßen. Dabei kann und darf es aber nicht bleiben, nur entschlossenes Handeln kann die Bürgerinnen und Bürger vor weiterem Missbrauch ihrer persönlichen Daten schützen und das verlorene Vertrauen wiederherstellen.

Das vom Grundgesetz garantierte Recht eines Jeden, selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu entscheiden, muss endlich die ihm gebührende Beachtung finden Die Weitergabe von persönlichen Angaben zu Werbezwecken darf nur mit ausdrücklicher Einwilligung der Betroffenen zulässig sein. Daten sind mit einem Vermerk über ihre Quelle zu kennzeichnen. Der Abschluss von Verträgen darf nicht von der Einwilligung in die Datenübermittlung zu Werbezwecken abhängig gemacht werden. Verstöße gegen den Datenschutz dürfen nicht ohne Konsequenzen bleiben, sondern müssen strikt geahndet werden. Deshalb müssen die bestehenden Lücken in den Bußgeld- und Strafbestimmungen geschlossen und der Bußgeld- und Strafrahmen für Datenschutzverstöße deutlich erhöht werden. Diese Sofortmaßnahmen, die bereits Gegenstand des Spitzentreffens im Bundesministerium des Innern am 4. September 2008 waren, können vom Deutschen Bundestag noch in den bereits vorliegenden Gesetzentwurf zur Änderung des Bundesdaten-schutzgesetzes aufgenommen werden.

Gesetzgeberische Maßnahmen allein helfen aber nicht weiter, wenn ihre Einhaltung nicht ausreichend kontrolliert und Verstöße nicht sanktioniert werden können. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deswegen, die Datenschutzaufsichtsbehörden endlich organisatorisch, personell und finanziell in die Lage zu versetzen, ihren Beratungs- und Kontrollaufgaben flächendeckend, unabhängig und wirkungsvoll nachkommen zu können, und entsprechend der EU-Datenschutzrichtlinie mit wirksamen Einwirkungsbefugnissen auszustatten, die sie bisher nicht haben. Außerdem müssen Konzepte zur grundlegenden Modernisierung des Datenschutzes entwickelt und umgesetzt werden. Wichtige Themen sollten dabei noch in dieser Legislaturperiode angegangen werden:

- Verbesserung der Protokollierung des Datenzugriffs in automatisierten Verfahren

- Stärkung der datenschutzrechtlichen Auskunftsrechte

- Pflicht zur Information der betroffenen Personen und der Aufsichtsbehörden bei Datenpannen und missbräuchlicher Datennutzung

- Gewinnabschöpfung aus unbefugtem Datenhandel

- Einführung eines gesetzlich geregelten Datenschutzaudits, mit dem unabhängig und qualifiziert die Datenschutzkonformität von Verfahren und Produkten bestätigt wird

- Stärkung der betrieblichen Datenschutzbeauftragten als Organ der Selbstkontrolle

- Spezialisierung der Strafverfolgungsbehörden

- Anerkennung von Datenschutzbestimmungen als verbraucherschützende Normen

Nur wenn jetzt den Ankündigungen Taten folgen und entschlossen gehandelt wird, können die Bürgerinnen und Bürger künftig vor Datenmissbrauch und Verletzung ihres Grundrechts auf informationelle Selbstbestimmung besser als in der Vergangenheit geschützt werden.

Anlage 1.10 Mehr Transparenz durch Informationspflichten bei Datenschutzpannen

Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn

In den letzten Monaten hat eine Reihe von gravierenden Datenschutzverstößen die Aufmerksamkeit der Öffentlichkeit und der Medien gefunden. In vielen dieser Fälle lag der Verlust oder Missbrauch personenbezogener Daten längere Zeit zurück und war der verantwortlichen Stelle bekannt, ohne dass die Betroffenen oder die zuständige Datenschutzaufsichtsbehörde hierüber informiert worden wären. Dadurch wurde ihnen die Möglichkeit genommen, Sicherheitsmaßnahmen zu ergreifen und mögliche Schäden zu begrenzen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt deswegen die Forderung, alle verantwortlichen Stellen - grundsätzlich auch alle öffentlichen Stellen - gesetzlich zu verpflichten, bei Verlust, Diebstahl oder Missbrauch personenbezogener Daten unverzüglich die hiervon betroffenen Bürgerinnen und Bürger und die zuständigen Aufsichts- oder Kontrollbehörden sowie gegebenenfalls auch die Öffentlichkeit zu unterrichten. Dies entspricht ihrer datenschutzrechtlichen Verantwortung und ermöglicht es den Betroffenen, negative Konsequenzen solcher Datenschutzpannen abzuwenden oder einzugrenzen. Hinter diesem Interesse hat der Wunsch der entsprechenden Stellen zurückzustehen, solche Vorkommnisse geheim zu halten, um keinen Imageschaden oder keine wirtschaftlichen Nachteile zu erleiden.

Etliche Staaten haben bereits entsprechende Regelungen. Eine solche Informationspflicht würde die Transparenz erhöhen und das Vertrauen der Betroffenen in eine korrekte Datenverarbeitung stärken. Darüber hinaus würde sie einen wichtigen Anstoß geben, mehr für Datenschutz und Datensicherheit zu tun.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deswegen, entsprechende umfassende Informationspflichten für Unternehmen und öffentliche Stellen im Bundesdatenschutzgesetz und den Landesdatenschutzgesetzen zu schaffen. Die übrigen aus Anlass der Datenschutzskandale in einer Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 16.09.2008 erläuterten Forderungen zur Novellierung des Bundesdatenschutzgesetzes werden bekräftigt.

Anlage 1.11 Angemessener Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in der EU dringend erforderlich

Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn

Auf europäischer Ebene ist eine Vielzahl von Vorhaben beschlossen bzw. initiiert worden, die in ihrer Gesamtheit zu erheblichen Eingriffen in die Persönlichkeitsrechte führt:

- Die Telekommunikationsunternehmen in den Mitgliedstaaten der EU sind verpflichtet, die bei der Nutzung öffentlich zugänglicher Telekommunikationsdienste anfallenden Verkehrsdaten über das Kommunikationsverhalten der Einzelnen für die Sicherheitsbehörden ohne konkreten Anlass auf Vorrat zu speichern.

- Die Pässe der Bürgerinnen und Bürger der EU-Mitgliedstaaten werden mit biometrischen Merkmalen ausgestattet.

- Fluggastdaten (PNR) werden in die USA übermittelt, um sie den dortigen Behörden zur Verfügung zu stellen. Die Nutzung von Fluggastdaten zu Strafverfolgungszwecken wird auch in der Europäischen Union vorbereitet.

- Der Vertrag von Prüm, der in den Rechtsrahmen der Union überführt wird, ermöglicht den Polizei- und Strafverfolgungsbehörden der Mitgliedstaaten einen gegenseitigen Zugriff auf Fingerabdruck-, DNA- und Kfz-Daten.

- Es soll ein Europäisches Strafregisterinformationssystem geschaffen werden, mit dem Informationen über strafrechtliche Verurteilungen zwischen den Mitgliedstaaten ausgetauscht werden können.

- Das Schengener Informationssystem wird weiter ausgebaut, u. a. durch die Speicherung von biometrischen Merkmalen. Zudem wird der Kreis der Nutzer erweitert um das Europäische Polizeiamt EUROPOL und die Einheit für justizielle Zusammenarbeit in der EU (EUROJUST).

- Ein Europäisches Visa-Informationssystem (VIS) wird eingeführt, um den Austausch von Visa-Daten zwischen den Mitgliedstaaten zu erleichtern. Auch für EUROPOL, die Sicherheitsbehörden und die Nachrichtendienste soll dieser Datenbestand zugänglich sein.

- Das europäische Verfahren EURODAC, in dem die Fingerabdrücke von Asylbewerberinnen und Asylbewerbern gespeichert sind, soll auch von der Polizei und den Strafverfolgungsbehörden genutzt werden können.

- Der Aufgabenbereich von EUROPOL soll über die Bekämpfung der Organisierten Kriminalität hinaus auch auf andere Formen der schweren Kriminalität erweitert werden. Außerdem soll EUROPOL erstmals die Befugnis erhalten, Daten auch von privaten Stellen entgegenzunehmen und Zugriff auf alle polizeilich relevanten Datenbanken in der EU bekommen.

- Der Informationsaustausch zwischen den Strafverfolgungsbehörden der EU wird entsprechend dem Rahmenbeschluss des Rates vom 18. Dezember 2006 („Schwedische Initiative“) ausgebaut. Danach soll der Austausch verfügbarer Daten innerhalb der EU zu den gleichen Bedingungen erfolgen wie nach nationalem Recht.

Neben diesen Vorhaben gibt es zudem Abkommen auf bilateraler Ebene zwischen EU-Mitgliedstaaten und Drittstaaten, wie z. B. das Abkommen der Bundesrepublik Deutschland mit den Vereinigten Staaten für einen erweiterten Informationsaustausch zwischen den Sicherheitsbehörden.

Der Aufbau zentraler Datenbestände und der Ausbau der grenzüberschreitenden Datenübermittlung greifen erheblich in das Grundrecht auf informationelle Selbstbestimmung ein und führen dadurch zu Gefahren für jede Einzelne und jeden Einzelnen. Diese werden noch gesteigert durch die angestrebte Verknüpfbarkeit der bestehenden und geplanten Datenbanken.

Umso wichtiger ist deshalb ein hoher und gleichwertiger Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Europa. Dies wurde von den Datenschutzbeauftragten auf nationaler und europäischer Ebene mehrfach angemahnt. Der hierzu im Oktober 2005 vorgelegte Rahmenbeschluss-Vorschlag genügt diesen Anforderungen nicht (siehe dazu die Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006 „Mehr Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen“). Zur Wahrung des erforderlichen Gleichgewichts zwischen Freiheit und Sicherheit sollten die Parlamente und Regierungen ihre Einflussmöglichkeiten bei europäischen Vorhaben stärker nutzen und dabei auch datenschutzrechtliche Aspekte einbringen. Wie notwendig ein angemessener Datenschutz ist, hat sich beim Verfahren der Aufnahme Verdächtiger in die sogenannte EU-Terrorliste gezeigt, das durch den Europäischen Gerichtshof für rechtswidrig erklärt wurde.

Die Datenschutzbeauftragten fordern deshalb:

- Bei jeder neuen Initiative ist das Verhältnismäßigkeitsprinzip zu wahren und deren Auswirkung auf das bestehende System von Eingriffsmaßnahmen zu berücksichtigen.

- Im Hinblick auf den Kumulationseffekt sind die verschiedenen europäischen Initiativen zudem grundrechtskonform aufeinander abzustimmen. Redundanzen und Überschneidungen müssen verhindert werden.

- Ein Rechtsakt muss unverzüglich beschlossen werden, der über den Rahmenbeschluss-Vorschlag hinaus einen hohen und gleichwertigen Datenschutzstandard bei der Verarbeitung personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit verbindlich vorschreibt. Die gesamte nationale und grenzüberschreitende Informationsverarbeitung in diesem Bereich muss davon erfasst sein, um ein einheitliches Datenschutzniveau in den EU-Mitgliedstaaten zu gewährleisten.

- Ein unabhängiges, beratendes Datenschutzgremium sowie eine unabhängige und umfassende datenschutzrechtliche Kontrolle müssen für die polizeiliche und justizielle Zusammenarbeit eingerichtet bzw. gewährleistet werden.

Anlage 1.12 Besserer Datenschutz bei der Umsetzung der "Schwedischen Initiative" zur Vereinfachung des polizeilichen Datenaustausches zwischen den EU-Mitgliedstaaten

Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn

Der Rahmenbeschluss des Rates zur Vereinfachung des Informationsaustausches zwischen den Strafverfolgungsbehörden der EU-Mitgliedstaaten (sog. „Schwedische Initiative“) vom 18.12.2006 verpflichtet diese, an die grenzüberschreitende Übermittlung personenbezogener Daten innerhalb der EU keine höheren Anforderungen zu stellen, als auf nationaler Ebene für den Datenaustausch zwischen Polizei- und Strafverfolgungsbehörden gelten. Seine Umsetzung wird zu einem deutlichen Anstieg und zur Beschleunigung des Informationsaustausches und damit zu einer weiteren Intensivierung der polizeilichen und justiziellen Zusammenarbeit in Strafsachen auf EU-Ebene führen. Das erstrebte Ziel, nämlich die Schaffung eines Raumes der Freiheit, der Sicherheit und des Rechts setzt aber auch voraus, dass in den Mitgliedstaaten ein möglichst gleichwertiger Datenschutz auf hohem Niveau besteht. Dies ist bislang nicht erfüllt. Es besteht nach wie vor der aus datenschutzrechtlicher Sicht unhaltbare Zustand, dass die auf EU-Ebene ausgetauschten polizeilichen Informationen in den jeweiligen EU-Mitgliedstaaten unterschiedlichen Datenschutzregelungen hinsichtlich ihrer Verwendung unterworfen sind. Zudem gelten keine einheitlichen Rechte auf Auskunft, Berichtigung und Löschung der Datenverarbeitung für die Betroffenen in den Empfängerstaaten.

Vor diesem Hintergrund fordern die Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber auf, den bei der innerstaatlichen Umsetzung der „Schwedischen Initiative“ verbleibenden Spielraum zu nutzen und die Befugnisse zum Informationsaustausch mit den Strafverfolgungsbehörden der EU-Mitgliedstaaten für die nationalen Polizei- und Strafverfolgungsbehörden normenklar und unter Beachtung des Grundsatzes der Verhältnismäßigkeit gesetzlich zu regeln. Dazu zählen insbesondere:

- Ausschluss der gesonderten Erhebung der angefragten Daten durch die Strafverfolgungsbehörden allein um diese zu übermitteln,

- eindeutige inhaltliche Anforderungen, die an ein Ersuchen um Datenübermittlung zu stellen sind, um Überschussinformationen zu vermeiden,

- Regelung enger Voraussetzungen für sog. Spontanübermittlungen, um für den Empfänger nutzlose und damit nicht erforderliche Übermittlungen auszuschließen,

- Nutzung des Spielraums bei der Ausgestaltung der Verweigerungsgründe, um unverhältnismäßige Datenübermittlungen zu verhindern,

- normenklare Abgrenzung der Befugnis zur Übermittlung von Daten zu präventiven Zwecken gegenüber der justiziellen Rechtshilfe,

- vollständige Umsetzung der Datenschutzbestimmungen in Art. 8 des Rahmenbeschlusses und begrenzende Regelungen zur Weiterübermittlung an Drittstaaten,

- normenklare Bestimmung, welche Behörden als zuständige Strafverfolgungsbehörden im Sinne des Rahmenbeschlusses gelten und welche Informationen nur durch Ergreifen von Zwangsmaßnahmen im Sinne des Rahmenbeschlusses verfügbar sind,

- normenklare Bestimmung, welche Informationen nicht vom Rahmenbeschluss erfasst werden, weil sie für die Strafverfolgungsbehörden nur durch das Ergreifen von Zwangsmaßnahmen verfügbar sind.

Anlage 1.13 Datenschutzgerechter Zugang zu Geoinformationen

Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn

Die Einführung einer einheitlichen Geodateninfrastruktur und die Veröffentlichung der staatlichen Daten eröffnen ein großes Potential an volkswirtschaftlichem Nutzen und ist geeignet, vielen E-Government- und E-Commerce-Anwendungen die erforderliche Infrastruktur zur Verfügung zu stellen. Als einen ersten Schritt regelt das europäische Recht mit der sogenannten INSPIRE-Richtlinie, die bis Mai 2009 in nationales Recht umgesetzt werden muss, die Bereitstellung von amtlichen Geodaten nach einheitlichen Standards für europaweite behördliche, kommerzielle und private Nutzungen.

Durch diese neue Infrastruktur werden georeferenzierbare Angaben auf Grund der Erschließungsmöglichkeit über Wohnanschriften oder Eigentümer- bzw. Standortdaten als personenbezogene Daten zur Verfügung gestellt. Diesem Umstand müssen die gesetzlichen Regelungen gerecht werden und angemessene Datenschutzregelungen enthalten.

Bei der Bereitstellung amtlicher Geodaten ist sowohl nach der europäischen Richtlinie als auch nach deutschem Verfassungsrecht der Schutz personenbezogener Daten angemessen zu gewährleisten. Der Entwurf der Bundesregierung zur Umsetzung dieser Richtlinie in einem Geodatenzugangsgesetz (BT-Drs. 16/10530) sieht eine entsprechende Anwendung der Schutzvorschriften des Umweltinformationsgesetzes vor. Im Gegensatz zum einzelfallbezogenen Zugang nach den Umweltinformationsgesetzen birgt der im Entwurf eines Geodatenzugangsgesetzes vorgesehene massenhafte Abruf solcher Daten aber ein höheres datenschutzrechtliches Gefährdungspotenzial. Der Verweis auf das Umweltinformationsgesetz ist nach Ansicht der Konferenzen der Datenschutz- und der Informationsfreiheitsbeauftragten des Bundes und der Länder deshalb nicht interessengerecht. Ein Geodatenzugangsgesetz muss einen differenzierenden Ausgleich zwischen Informations- und Schutzinteressen für die spezielle Problematik der Geobasis- und der Geofachdaten vornehmen. Es ist insbesondere zu berücksichtigen, dass nach der INSPIRE-Richtlinie die Zugangsmöglichkeit eingeschränkt werden soll, wenn der Zugang nachteilige Auswirkungen auf die Vertraulichkeit personenbezogener Daten haben kann.

Anlage 1.14 Weiterhin verfassungsrechtliche Zweifel am ELENA-Verfahren

Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn

Die Bundesregierung hat am 25.06.2008 den Gesetzentwurf über das Verfahren des elektronischen Entgeltnachweises (ELENA-Verfahrensgesetz) beschlossen (BT-Drs. 16/10492). Danach haben Beschäftigte die monatliche Übermittlung ihrer Einkommensdaten an die Zentrale Speicherstelle zu dulden, obwohl zurzeit nicht verlässlich abgeschätzt werden kann, in welchem Umfang die Speicherung der Daten tatsächlich erforderlich ist. Ein großer Anteil der Betroffenen wird die dem Anwendungsbereich des ELENA-Verfahrens unterfallenden Sozialleistungen niemals oder erst zu einem erheblich späteren Zeitpunkt geltend machen. Es steht somit bereits jetzt zu vermuten, dass eine große Zahl der übermittelten Daten von der Zentralen Speicherstelle wieder zu löschen sein wird, ohne jemals für irgendein Verfahren genutzt worden zu sein.

Die Datenschutzbeauftragten des Bundes und der Länder haben deshalb wiederholt verfassungsrechtliche Bedenken unter dem Gesichtspunkt der Verhältnismäßigkeit und speziell der Erforderlichkeit geltend gemacht und eine substantiierte Begründung gefordert. Diese ist nicht erfolgt. Bisher bestehen lediglich höchst vage Erwartungen auf langfristige Effizienzsteigerungen insbesondere der Arbeitsverwaltung. Angesichts dieser Unklarheiten verbleiben erhebliche Zweifel an der Verfassungsmäßigkeit des Gesetzes. Hinzu kommt, dass derartige umfangreiche Datensammlungen Begehrlichkeiten wecken, die Daten für andere Zwecke zu verwenden.

Für den Fall, dass diese verfassungsrechtlichen Bedenken ausgeräumt werden können, sind unter dem Gesichtspunkt des technisch-organisatorischen Datenschutzes noch folgende Verbesserungen durch den Gesetz- bzw. Verordnungsgeber erforderlich:

Es muss sichergestellt werden (z. B. durch die Einrichtung eines Verwaltungsausschusses der Zentralen Speicherstelle), dass unter Mitwirkung von Datenschutzbeauftragten gemeinsame Grundsätze zur Wahrung des Datenschutzes und der technischen Sicherheit berücksichtigt werden.

Für die Zentrale Speicherstelle muss ein Datenschutzbeauftragter eingesetzt werden, der dazu verpflichtet ist, regelmäßig an den Verwaltungsausschuss zu berichten.

Schlüssel zur Ver- und Entschlüsselung der bei der Zentralen Speicherstelle gespeicherten Daten dürfen nicht in der Verfügungsgewalt der Zentralen Speicherstelle liegen. Die Ver- und Entschlüsselungskomponente muss von einer unabhängigen Treuhänderstelle verantwortet werden.

Mittelfristig ist ein Verfahren anzustreben, das die technische Verfügungsmöglichkeit über die individuellen Daten den Betroffenen überträgt.

Das im Rahmen der ELENA-Modellvorhaben erarbeitete differenzierte Löschungskonzept muss weiterentwickelt und umgesetzt werden.

Für abrufende Stellen sind starke Authentisierungsverfahren vorzuschreiben, die dem Stand der Technik entsprechen und den Forderungen der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Oktober 2006 zur sachgemäßen Nutzung von Authentisierungs- und Signaturverfahren genügen.

Für die technischen Komponenten muss eine Zertifizierung durch eine unabhängige Prüfung vorgeschrieben werden.

Anlage 1.15 Abfrage von Telekommunikationsverkehrsdaten einschränken: Gesetzgeber und Praxis müssen aus wissenschaftlichen Erkenntnissen Konsequenzen ziehen

Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn

Das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg hat im Auftrag des Bundesministeriums der Justiz die Nutzung von Telekommunikationsverkehrsdaten für Zwecke der Strafverfolgung (§§ 100g, 100h StPO alte Fassung) evaluiert. Die Studie geht zu Recht davon aus, dass Verkehrsdaten ein hohes Überwachungspotential in sich tragen und besser als andere Daten dazu geeignet sind, soziale Netzwerke nachzuweisen, Beziehungen zu identifizieren und Informationen über Individuen zu generieren. Der Studie zufolge ist die Zahl der Verkehrsdatenabfragen erheblich und kontinuierlich von 10.200 (2002) auf 40.000 Abfragen (2005) angestiegen. Zudem erfasst die Maßnahme regelmäßig auch eine Vielzahl unbescholtener Bürgerinnen und Bürger.

Das Bundesministerium der Justiz hat die Studie erst im Februar dieses Jahres und somit nach der Neuregelung der Telekommunikationsüberwachung und Einführung der Vorratsdatenspeicherung veröffentlicht. Das Gutachten liefert Erkenntnisse, deren Berücksichtigung im Gesetz vom 21. Dezember 2007 erforderlich gewesen wäre. Die Datenschutzbeauftragten des Bundes und der Länder sehen sich durch die Studie in ihrer schon früher geäußerten Kritik (vgl. ihre Entschließung vom 8./9. März 2007) bestätigt. Sie fordern den Gesetzgeber auf, die gesetzliche Regelung unter folgenden Aspekten nun zügig nachzubessern:

Die Straftatenschwelle für Verkehrsdatenabfragen sollte insbesondere im Hinblick auf die inzwischen eingeführte Vorratsdatenspeicherung auf schwere Straftaten angehoben werden. Ein bedeutsamer Anteil der überprüften Verfahren war allenfalls der mittleren Kriminalität zuzuordnen.

Die gesetzliche Höchstdauer der Maßnahme sollte von drei auf zwei Monate reduziert werden. Das Gutachten hat gezeigt, dass die praktischen Bedürfnisse, wie sie sich in den Aktendaten und Befragungsergebnissen äußern, dadurch vollständig abgedeckt würden.

Für die Verkehrsdatenabfrage sollten (nach dem Vorbild der Regelungen für die akustische Wohnraumüberwachung) qualifizierte Begründungspflichten in der StPO vorgesehen werden. Dabei sollten auch die Rechtsfolgen für erhebliche Verstöße gegen die Begründungsanforderungen gesetzlich geregelt werden (z. B. Beweisverwertungsverbote). Wesentliche Kritikpunkte der Studie waren insbesondere die lediglich formelhafte Wiedergabe des Gesetzestextes sowie die häufig wörtliche Übernahme der staatsanwaltschaftlichen Anträge in den Begründungen.

Zur Vermeidung von Rechtsunsicherheit und zur Stärkung des Richtervorbehalts sollte in den Fällen staatsanwaltschaftlicher Eilanordnung die Verwertbarkeit der erlangten Daten davon abhängig gemacht werden, dass ein Gericht rückwirkend die formelle und materielle Rechtmäßigkeit der Maßnahme feststellt. Dem Gutachten zufolge besteht insbesondere bei den Telekommunikationsunternehmen Unsicherheit, inwieweit sie zur Herausgabe der Verkehrsdaten verpflichtet sind, wenn eine staatsanwaltschaftliche Eilanordnung nicht innerhalb der gesetzlichen Frist richterlich bestätigt wird.

Der tatsächliche Nutzen der Vorratsdatenspeicherung für die Strafverfolgung und damit die Erforderlichkeit der Maßnahme müssen in Frage gestellt werden. Bereits bei der früheren Höchstspeicherdauer von 3 Monaten waren nach der Studie 98 % der Abfragen erfolgreich.

Auch in der praktischen Anwendung der Regelungen zur Verkehrsdatenabfrage hat die Studie Defizite deutlich gemacht. Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher auch an die Strafverfolgungsbehörden und Gerichte, aus dem Gutachten Konsequenzen zu ziehen. Besonderes Augenmerk ist vor allem auf die Prüfung der Angemessenheit der Maßnahme zu richten. Dies muss auch in substantiierten Begründungen zum Ausdruck kommen. Die gesetzlich festgeschriebenen, dem Grundrechtsschutz dienenden Benachrichtigungs-, Löschungs- und Dokumentationspflichten müssen - trotz hoher Belastungen in der Praxis - unbedingt eingehalten werden. Der Richtervorbehalt muss seine grundrechtssichernde Funktion effizient erfüllen können. Die Justizverwaltungen sind in der Verantwortung, hierfür ausreichende personelle Ressourcen zur Verfügung zu stellen.

Eine Fortführung der wissenschaftlichen Evaluation der Verkehrsdatenabfrage ist - unter den neuen rechtlichen Rahmenbedingungen und aufgrund der Weiterentwicklung der Technik - unerlässlich. Insbesondere sollten dabei Notwendigkeit und Nutzen der Verkehrsdatenabfrage - auch im Vergleich zu anderen möglichen Maßnahmen - mit Blick auf den Verhältnismäßigkeitsgrundsatz auf den Prüfstand gestellt werden.

Anlage 1.16 Adress- und Datenhandel nur mit Einwilligung der Betroffenen

Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn

Der auf dem „Datenschutzgipfel“ im September 2008 gefundene Konsens, den Adress- und Datenhandel zukünftig nur auf der Grundlage einer Einwilligung zuzulassen, ist in Politik und Gesellschaft auf breite Zustimmung gestoßen. Nur eine solche Lösung respektiert das informationelle Selbstbestimmungsrecht und damit die Wahlfreiheit der Verbraucherinnen und Verbraucher. Wer davon jetzt abrücken will, verkennt die auf Grund der jüngsten Datenskandale ans Licht gekommenen Missstände, deren Ursache nicht nur in der kriminellen Energie Einzelner zu suchen ist. Um die Daten der Betroffenen tatsächlich wirksam schützen zu können, muss die Wahlmöglichkeit der Menschen von Maßnahmen flankiert werden, die die Herkunft der Daten jederzeit nachvollziehbar machten.

Die von der Werbewirtschaft gegen die Einwilligungslösung ins Feld geführten Argumente sind nicht überzeugend. Die behaupteten negativen Folgen für den Wirtschaftsstandort sind nicht zu belegen. Unabhängig davon gilt: Es gibt keine schutzwürdigen Interessen für die Beibehaltung von Geschäftsmodellen, die darauf beruhen, hinter dem Rücken und ohne Information der Betroffenen mit deren Daten Handel zu treiben.

Die Einführung des Einwilligungsprinzips würde im Gegenteil zielgenaueres und wirksameres Direktmarketing erlauben. Die Bundesregierung sollte sich deshalb nicht von ihrer Absicht abbringen lassen, die beim „Datenschutzgipfel“ gegebenen Zusagen zur schnellen Verbesserung des Datenschutzes einzulösen. Sie würde es sonst versäumen, die notwendigen Lehren aus den jüngsten Skandalen zu ziehen. Der Referentenentwurf des Bundesinnenministeriums zur Änderung des Bundesdatenschutzgesetzes im Bereich des Adress- und Datenhandels (Stand: 22.10.2008) zieht mit der Einwilligungslösung - bei aller Verbesserungswürdigkeit im Detail - die einzig richtige und notwendige Konsequenz aus den zahlreichen Datenskandalen und darf nicht verwässert werden.

Anlage 1.17 Steuerungsprogramme der gesetzlichen Krankenkassen datenschutzkonform gestalten

Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn

Mit der Gesundheitsreform soll über die Einführung von Wettbewerbsmechanismen die Qualität und Effizienz der gesetzlichen Krankenkassen verbessert werden. Die Kassen sind daher bemüht und auch vom Gesetzgeber gehalten, Versicherten ein Versorgungsmanagement anzubieten. Von zentraler Bedeutung sind dabei Patientenschulungsmaßnahmen und strukturierte Behandlungsprogramme für chronisch kranke Versicherte, die jedoch lediglich Angebotscharakter haben dürfen. Ihre Teilnahme soll nach dem Willen des Gesetzgebers freiwillig sein und eine eingehende Unterrichtung voraussetzen. Diese Vorgaben werden von einzelnen Krankenkassen nicht beachtet, wenn sie versuchen, die Versicherten in ihrem Gesundheitsverhalten zu steuern und sie in bestimmte Maßnahmen und Programme zu drängen.
Um Teilnehmerinnen und Teilnehmer zu gewinnen und um Maßnahmen durchzuführen, bedienen sich die Kassen vielfach privater Dienstleister und offenbaren diesen teils höchst sensible Gesundheitsdaten ihrer Versicherten. Dies ist datenschutzrechtlich nach dem Sozialgesetzbuch unzulässig, wenn die Übermittlung ohne Kenntnis und vorherige Einwilligung der jeweiligen Versicherten erfolgt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält die Einhaltung insbesondere der folgenden Eckpunkte bei gesundheitlichen Steuerungsprogrammen der Krankenkassen für unerlässlich:

- Die Krankenkassen dürfen Versichertendaten nur dann zur Auswahl von Personen für besondere Gesundheitsmaßnahmen verwenden, wenn dies gesetzlich ausdrücklich vorgesehen ist. Es muss sich um valide und erforderliche Daten handeln. Mit der Auswahl darf kein privater Dienstleister beauftragt werden.

- Die erstmalige Kontaktaufnahme mit potenziell für eine Gesundheitsmaßnahme in Betracht kommenden Versicherten muss durch die Krankenkasse selbst erfolgen, auch wenn ein privater Dienstleister mit der späteren Durchführung der Gesundheitsmaßnahme beauftragt worden ist.

- Die Versicherten sind vor Übermittlung ihrer Daten umfassend zu informieren. Die Information muss auch den Umstand umfassen, dass ein privates Unternehmen mit der Durchführung betraut werden soll. Soweit die Versicherten ausdrücklich in die Teilnahme eingewilligt haben, dürfen die für die Durchführung der Maßnahme erforderlichen Daten an den Dienstleister übermittelt werden.

- Wenn Versicherte - zu welchem Zeitpunkt auch immer - eindeutig zum Ausdruck bringen, nicht an einer Maßnahme teilnehmen zu wollen oder nicht an weitergehenden Informationen, einer konkreten Anwerbung oder einer fortgesetzten Betreuung interessiert zu sein, ist dies zu respektieren. Weitere Maßnahmen (auch telefonische Überredungsversuche) sind zu unterlassen.

Anlage 1.18 Elektronische Steuererklärung sicher und datenschutzgerecht gestalten

Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn

Mit dem Steuerbürokratieabbaugesetz (BR-Drs. 547/08) sollen u. a. verfahrenstechnische Regelungen für die elektronische Übermittlung von Steuererklärungen durch Steuerpflichtige festgelegt werden. Zu diesem Zweck soll § 150 Abgabenordnung (AO) durch Abs. 7 Satz 1 dahingehend ergänzt werden, dass bei Einführung einer Verpflichtung zur elektronischen Abgabe die übermittelten Steuerdaten mit einer qualifizierten Signatur nach dem Signaturgesetz zu versehen sind.

Die Konferenz sieht es kritisch, dass § 150 Abs. 7 Satz 2 Nr. 6 und 7 AO auch vorsieht, zur Erleichterung und Vereinfachung des automatisierten Besteuerungsverfahrens anstelle der qualifizierten elektronischen Signatur ein sogenanntes anderes sicheres Verfahren im Benehmen mit dem Bundesinnenministerium zuzulassen oder sogar auf beide Verfahren vollständig zu verzichten. In der Gesetzesbegründung wird darauf verwiesen, dass neben der qualifizierten elektronischen Signatur künftig auch eine Übermittlung der Daten unter Nutzung der Möglichkeiten des neuen elektronischen Personalausweises möglich sein soll.
Bereits in ihrer Entschließung zur sachgemäßen Nutzung von Authentisierungs- und Signaturverfahren vom 11. Oktober 2006 hat die Konferenz gefordert, Nutzenden die Möglichkeit zu eröffnen, die elektronische Kommunikation mit der Verwaltung durch eine qualifizierte elektronische Signatur abzusichern. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt daher die vorgesehene Regelung in der AO zur Nutzung der qualifizierten elektronischen Signatur, da dieses Verfahren geeignet ist, die Authentizität und Integrität eines elektronisch übermittelten Dokuments sicherzustellen, und somit die handschriftliche Unterschrift ersetzen kann.

Die Datenschutzbeauftragten des Bundes und der Länder erklären hierzu:

1) Das Verfahren der qualifizierten elektronischen Signatur nach dem Signaturgesetz ist im Hinblick auf die Authentizität und Integrität elektronisch übermittelter Dokumente derzeit alternativlos.

2) Für die Bewertung anderer Verfahren sollte unmittelbar auf die Fachkenntnis unabhängiger Gutachter abgestellt werden. Als Gutachter für die Beurteilung der technischen Sicherheit kämen etwa die Bundesnetzagentur oder das BSI in Frage.

3) Steuerpflichtige müssen auch im elektronischen Besteuerungsverfahren die Möglichkeit haben, die elektronische Kommunikation mit der Finanzverwaltung durch das hierfür geeignete Verfahren der qualifizierten elektronischen Signatur abzusichern.

Anlage 1.19 Gegen Blankettbefugnisse für die Software-Industrie

Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn

Gegenwärtig wird auf europäischer Ebene über Änderungen der Richtlinie zum Datenschutz in der elektronischen Kommunikation (2002/58/EG) beraten. Dabei geht es auch um die Frage, ob in Zukunft einzelfallunabhängig Verkehrsdaten zur Gewährleistung der Netz- und Informationssicherheit, also etwa zur Verfolgung von Hackerangriffen, verarbeitet werden dürfen.

Bereits auf der Grundlage der geltenden Richtlinie erlaubt § 100 Telekommunikationsgesetz den Telekommunikationsdiensteanbietern eine zielgerichtete, einzelfallbezogene Datenverarbeitung zur Fehlerbeseitigung und Missbrauchsbekämpfung. Diese Regelung hat sich in der Praxis bewährt. Es ist daher nicht erforderlich, zur Gewährleistung der Netz- und Informationssicherheit einzelfallunabhängig personenbezogene Verkehrsdaten zu speichern. Die Anbieter von Telekommunikationsdiensten sind aufgefordert, ihre Systeme so sicher zu gestalten, dass Angriffe von vornherein erfolglos bleiben.

Obwohl die Europäische Kommission eine Änderung der bisherigen Rechtslage nicht für erforderlich hält, schlagen mehrere Mitgliedstaaten bei den gegenwärtigen Beratungen im Rat vor, entsprechend den Vorstellungen der Software-Industrie (Business Software Alliance) eine generelle Ermächtigung in die Richtlinie aufzunehmen, wonach „jede natürliche oder juristische Person mit einem berechtigten Interesse“ berechtigt sein soll, Verkehrsdaten zu verarbeiten, um „technische Maßnahmen zur Gewährleistung der Sicherheit eines öffentlichen Telekommunikationsdienstes, eines öffentlichen oder privaten Telekommunikationsnetzes, eines Dienstes der Informationsgesellschaft oder von Endgeräten zu deren Nutzung“ zu ergreifen. Damit wäre nicht nur der jeweilige Diensteanbieter, der Maßnahmen zum Schutz des eigenen Angebots treffen will, zur einzelfallunabhängigen Speicherung von Verkehrsdaten berechtigt, sondern praktisch jeder mit einem wirtschaftlichen Verarbeitungsinteresse, insbesondere auch die Hersteller von Sicherheitssoftware.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt eine solche zeitlich unbegrenzte und inhaltlich unbestimmte Blankett-Ermächtigung als inakzeptabel ab. Der Hinweis auf die „Informationssicherheit“ rechtfertigt es nicht, dass Verkehrsdaten nahezu uferlos auch von Dritten verarbeitet werden. Die Bundesregierung wird aufgefordert, einer derartigen Aufweichung des Telekommunikationsgeheimnisses im Rat ihre Zustimmung zu verweigern.

Anlage 1.20 Auskunftsanspruch der Steuerpflichtigen im Besteuerungsverfahren gewährleisten!

Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26. und 27. März 2009 in Berlin

Das Bundesministerium der Finanzen (BMF) hat mit einer einfachen Verwaltungsanweisung den Auskunftsanspruch der Bürgerinnen und Bürger im Besteuerungsverfahren weitgehend eingeschränkt. Es macht die Auskunftserteilung von einem „berechtigten Interesse“ abhängig, was zu einer Einschränkung des Auskunftsrechts führt.

Die Vorgehensweise des BMF steht im krassen Widerspruch zum Beschluss des Bundesverfassungsgerichts vom 10. März 2008 (1 BvR 2388/03). Danach sind auch von der Finanzverwaltung die Grundrechte auf informationelle Selbstbestimmung und auf effektiven Rechtsschutz zu gewährleisten. Der in § 19 Bundesdatenschutzgesetz (BDSG) verankerte umfassende Auskunftsanspruch findet auch im Besteuerungsverfahren unmittelbare Anwendung.

Es ist inakzeptabel, dass verfassungsrechtlich garantierte Auskunftsrechte der Steuerpflichtigen ausgehebelt werden. Auch die Finanzverwaltung ist an Recht und Gesetz gebunden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass das BMF die Verwaltungsanweisung vom 17. Dezember 2008 unverzüglich aufhebt. Die Finanzbehörden des Bundes und der Länder sind zu verpflichten, entsprechend der Rechtslage den Auskunftsanspruch zu erfüllen. Die Datenschutzbeauftragten des Bundes und der Länder appellieren zudem an den Bundesgesetzgeber, den Auskunftsanspruch der Steuerpflichtigen durch eine eindeutige Regelung in der Abgabenordnung klarzustellen, die dem § 19 BDSG entspricht.

Anlage 1.21 Eckpunkte für ein Gesetz zum Beschäftigtendatenschutz

Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26. und 27. März 2009 in Berlin

Datenskandale der letzten Zeit haben deutlich gemacht, dass bei der Verarbeitung von Beschäftigtendaten weder Transparenz noch Rechtssicherheit besteht. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, nach jahrelanger Untätigkeit jetzt unverzüglich einen entsprechenden Gesetzentwurf vorzulegen.

Ziel des neuen Beschäftigtendatenschutzgesetzes muss sein, Rechtssicherheit herzustellen, Regelungslücken zu schließen und bereits vorhandene Regelungsaspekte sowie Vorgaben der Rechtsprechung in einem Spezialgesetz zusammenzufassen. Die Konferenz der Datenschutzbeauftragten hält deshalb vor allem folgende Eckpunkte für unverzichtbar:

Die Regelungen des Beschäftigtendatenschutzgesetzes müssen sowohl für die Beschäftigten der Privatwirtschaft als auch für die Beschäftigten im öffentlichen Dienst gelten.

Es muss klar geregelt werden, welche Daten Unternehmen und öffentliche Stellen im Rahmen des Einstellungsverfahrens und im weiteren Verlauf des Arbeitslebens über ihre Beschäftigten erheben dürfen, wie sie damit verfahren müssen und wozu sie die Daten nutzen dürfen. Es bedarf besonderer Festlegungen im Hinblick auf Gesundheitsdaten (u. a. zur Frage der Zulässigkeit von Drogen-Screening, psychologischen Testverfahren, ärztlichen Untersuchungen etc.).

Einen umfassenden anlass- und verdachtslosen Datenabgleich darf es nicht geben. Der Zugriff von Kontrollinstanzen wie z. B. der Innenrevision auf erhobene Personaldaten bedarf enger gesetzlicher Vorgaben.

Moderne Informations- und Kommunikationstechnologien dürfen nicht zu lückenlosen Verhaltens- und Leistungskontrollen eingesetzt werden. Da die Nutzung von Telefon, Internet und E-Mail-Diensten nicht mehr aus dem Arbeitsleben wegzudenken ist, sind auch die Voraussetzungen für eine beschäftigtenbezogene Auswertung dieser Kommunikationsmittel eindeutig und restriktiv festzulegen. Dabei ist auch zu regeln, welcher Personenkreis solche Auswertungen durchführen darf und ab welchem Verfahrensstand ggf. Dritte (z. B. Mitarbeitervertretungen oder Datenschutzbeauftragte) hinzugezogen werden müssen. Auswertungen von Datenbeständen der Zugangs- und Personalinformationssysteme sind strikt zu begrenzen.

Der Einsatz von Überwachungssystemen, wie z. B. Videokameras und Ortungssystemen, ist auf das unbedingt notwendige Maß zu beschränken und unter Wahrung der Beteiligungsrechte der Mitarbeitervertretungen zulässig. Die Verwendung biometrischer Verfahren bedarf besonders enger Vorgaben.

Es bedarf der Festlegung der Rechte der Beschäftigten, z. B. im Hinblick auf Auskunfts-, Einsichts-, Widerrufs-, Berichtigungs-, Löschungs- und Schadensersatzansprüche.

Der Schutz von Persönlichkeitsrechten der in Deutschland tätigen Beschäftigten weltweit agierender Unternehmen oder Konzerne ist sicherzustellen.

Eine effektive Kontrolle durch die zuständigen Datenschutzbehörden muss gewährleistet werden. Die betrieblichen und behördlichen Datenschutzbeauftragten sind bei allen personaldatenschutzrechtlich relevanten Verfahren und Entscheidungen frühzeitig einzubinden und umfassend zu beteiligen. Ihre Rechte und Befugnisse gegenüber den Mitarbeitervertretungen sind gesetzlich festzulegen.

Verstöße gegen die Bestimmungen des Beschäftigtendatenschutzgesetzes müssen ein gesetzliches Verwertungsverbot der dadurch gewonnenen Daten nach sich ziehen. Zur Abschreckung bedarf es wirksamer Sanktionen.

Anlage 1.22 Defizite beim Datenschutz jetzt beseitigen!

Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26. und 27. März 2009 in Berlin

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Gesetzgeber in Deutschland auf, endlich die nötigen Konsequenzen aus den nicht mehr abreißenden Datenskandalen zu ziehen. Dazu sind mindestens folgende Schritte geboten:

Der Deutsche Bundestag wird aufgefordert, noch in dieser Legislaturperiode die von der Bundesregierung vorgelegten Gesetzentwürfe für erste notwendige Korrekturen des Bundesdatenschutzgesetzes im Bereich der Auskunfteien und des Adresshandels zu verabschieden. Ansonsten verlieren die Bürgerinnen und Bürger das Vertrauen in die Zusagen der Bundesregierung nach den Skandalen des Jahres 2008. Insbesondere mit Adressen darf nur noch mit ausdrücklicher Einwilligung der Betroffenen Handel getrieben werden. Der Entwurf für ein Datenschutzauditgesetz muss gründlich überarbeitet werden, damit dieser notwendige Schritt hin zu einem modernen Datenschutzrecht von der Praxis auch umgesetzt werden kann.

Mit Beginn der nächsten Legislaturperiode muss endlich eine grundlegende Modernisierung des Datenschutzrechts in Angriff genommen werden, die bereits zu lange aufgeschoben wurde. Nur so kann das Datenschutzrecht den Herausforderungen der Informationsgesellschaft zu Beginn des 21. Jahrhunderts gerecht werden.

Der Einsatz datenschutzfreundlicher Technik muss vorangetrieben und rechtlich verpflichtend vorgeschrieben werden. Darin liegt auch eine Chance für den Wirtschaftsstandort Deutschland in Zeiten der Krise.

Anlage 1.23 Die polizeiliche Datenverarbeitung in INPOL hat keine Rechtsgrundlage

Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26. und 27. März 2009 in Berlin

Die Speicherung von Daten im polizeilichen Informationssystem INPOL durch die Polizeien des Bundes und der Länder ist nur dann rechtmäßig, wenn eine Rechtsverordnung gemäß § 7 Abs. 6 Bundeskriminalamtsgesetz das Nähere über die Art der Daten bestimmt, die in dieser Datei gespeichert werden dürfen. Eine solche Rechtsverordnung existiert nicht. Mit Urteil vom 16. Dezember 2008 (Az. 11 LC 229/08) hat das Niedersächsische Oberverwaltungsgericht dies in Bezug auf die Verbunddatei „Gewalttäter Sport“ bekräftigt. Das Urteil ist nicht nur für die Rechtmäßigkeit der Hooligan-Datei bedeutsam, sondern hat Auswirkung auf alle im Rahmen von INPOL geführten Verbunddateien.

Mit der Entscheidung des Gerichts wird die Auffassung der Datenschutzbeauftragten des Bundes und der Länder bestätigt. Die vom Bundesministerium des Innern bisher vertretene Auffassung, wonach die Rechtsverordnung keine Zulässigkeitsvoraussetzung für die Datenverarbeitung in den Verbunddateien sei, wird durch die einschlägigen Regelungen nicht gestützt.

Ohne eine derartige Rechtsverordnung ist die Gesamtheit der in Verbunddateien stattfindenden polizeilichen Datenverarbeitungen rechtswidrig. Die Datenschutzbeauftragten von Bund und Länder fordern das Bundesministerium des Innern und die Landesregierungen auf, unverzüglich daraus Konsequenzen zu ziehen und die polizeiliche Datenverarbeitung auf den Prüfstand zu stellen.

Anlage 1.24 Datenschutz beim vorgesehenen Bürgerportal unzureichend

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. April 2009

Der Gesetzentwurf zur Regelung von Bürgerportalen (BR-Drs. 174/09) soll rechtliche Rahmenbedingungen für eine sichere und vertrauenswürdige elektronische Kommunikation zwischen Bürgerinnen und Bürgern und der Wirtschaft und Verwaltung im Internet schaffen. Private Anbieter sollen die Portale betreiben, über die der sichere E-Mail-Verkehr De-Mail, eine sichere Dokumentenablage De-Safe und ein Identitätsbescheinigungsdienst abgewickelt werden sollen. Eine solche Infrastruktur stellt hohe Anforderungen an die IT-Sicherheit und den Datenschutz.

Der Gesetzentwurf wird diesen Anforderungen noch nicht gerecht und ist zumindest in folgenden Punkten zu korrigieren:

- Der Entwurf sieht vor, dass nur akkreditierte Anbieter Portale betreiben dürfen. Voraussetzung für die Akkreditierung darf nicht allein der Nachweis der technischen und administrativen Sicherheit, sondern muss auch die tatsächliche Einhaltung datenschutzrechtlicher Standards sein. Die dabei zu erfüllenden Mindestanforderungen müssen verbindlich im Gesetz vorgegeben werden. Portalbetreiber sollten zudem erst dann die Akkreditierung erhalten, wenn die Umsetzung dieser Anforderungen durch unabhängige Prüfstellen bescheinigt wurde.

- Die Sicherung der Vertraulichkeit, Integrität und Authentizität von Nachrichteninhalten soll lediglich durch eine Verschlüsselung auf dem Transport zwischen den Dienstanbietern und durch die Sicherung des Zugangs zu den Bürgerportalen erfolgen. Es muss jedoch sichergestellt werden, dass Nachrichten auch bei den Portalbetreibern nicht durch Dritte gelesen oder verändert werden können. Deshalb muss die Kommunikation standardmäßig durch eine Ende-zu-Ende-Verschlüsselung zwischen Absendenden und Empfangenden nach dem Stand der Technik gesichert und nicht nur als Option angeboten werden.

- Das Bürgerportal soll gerade zwischen Bürgerinnnen und Bürgern und Verwaltung eine rechtlich gesicherte Kommunikation ermöglichen. Insbesondere sind über das Bürgerportal förmliche Zustellungen mit den entsprechenden Rechtsfolgen beabsichtigt. Dies darf nur auf Basis einer sicheren Anmeldung erfolgen. Die nach der Gesetzesbegründung ebenfalls mögliche unsichere Anmeldung mit Passwort wird abgelehnt.

- Der Nachweis der Absenderin oder des Absenders soll lediglich durch Anmeldung am Bürgerportal erfolgen. Das ermöglicht Angriffe durch Schadsoftware auf dem Rechner der Nutzenden. So könnten Zugangsdaten beschafft und widerrechtlich dazu verwendet werden, De-Mails zu versenden, empfangene De-Mails zu unterdrücken, zu verzögern und zu verändern oder unberechtigt auf Daten im De-Safe zuzugreifen. Deshalb sind zusätzliche Sicherungsmaßnahmen vorzusehen.

- Die Möglichkeit, eine pseudonyme Bürgerportaladresse zu nutzen, muss - entgegen der Stellungnahme des Bundesrates vom 03.04.2009 - erhalten bleiben. Denn die pseudonyme Nutzung ermöglicht gerade einen sinnvollen Kompromiss zwischen hinreichender Identifizierbarkeit im Rechtsverkehr und Datenschutz für die Nutzerinnen und Nutzer.

- Die Nutzerinnen und Nutzer müssen bei der Eröffnung des Bürgerportalkontos auf mögliche Rechtsfolgen - etwa zur verbindlichen Kommunikation mit staatlichen Stellen - hingewiesen werden. Die Aufklärungs- und Informationspflichten müssen im Gesetzestext klarer als bislang geschehen gefasst werden. Gleiches gilt für die Feststellung von Identitätsdaten und der Aufdeckung von Pseudonymen.

- Eine Benachteiligung von Bürgerinnen und Bürgern, die über kein Bürgerportalkonto verfügen, muss ausgeschlossen werden. Auch dürfen Bürgerportale nicht dazu führen, dass staatliche Stellen dazu übergehen, bei jeder Inanspruchnahme einer E-Government-Anwendung eine persönliche Identifizierung zu verlangen, selbst wenn dies für die konkrete Dienstleistung nicht erforderlich ist.

- Der Entwurf sieht vor, dass grundsätzliche Fragen der technischen Ausgestaltung der Bürgerportale und der darüber angebotenen Dienste in einer Rechtsverordnung geregelt werden sollen. Dies widerspricht der Rahmenkonzeption des Art. 80 GG und dient auch sonst nicht der Normenklarheit des Gesetzes. Zumindest die grundsätzlichen technisch-organisatorischen Anforderungen an die Eröffnung des Kontos, den Postfach- und Versanddienst, den Speicherplatz, den Identitätsbescheinigungsdienst und das Akkreditierungsverfahren sollten in das Gesetz selbst aufgenommen werden.

- Der Entwurf des Bürgerportalgesetzes sieht jetzt auch vor, dass nicht nur die Datenerhebung, sondern auch die Verarbeitung und Nutzung der erhobenen Daten durch den akkreditierten Dienstanbieter an eine enge Zweckbestimmung gebunden ist. Allerdings ist der pauschale Verweis auf die Regelungen des Bundesdatenschutzgesetzes, des Telemediengesetzes und des Telekommunikationsgesetzes in diesem Zusammenhang zu weitgehend, da so für die Diensteanbieter die Möglichkeit eröffnet wird, die personenbezogenen Daten für Werbung oder Marktforschungszwecke zu nutzen. Die Bürgerinnen und Bürger müssen jedoch sicher sein können, dass ihre Daten ausschließlich zur Teilnahme am Bürgerportal genutzt werden.

Anlage 1.25 Kein Ausverkauf von europäischen Finanzdaten an die USA!

Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. Oktober 2009 in Berlin

Für Zwecke der Terrorismusbekämpfung verhandeln die USA gegenwärtig mit der Europäischen Union über den Zugriff auf Daten über Finanztransaktionen, die auf SWIFT-Servern in Europa gespeichert werden, selbst wenn sie keinerlei Bezug zu den Vereinigten Staaten aufweisen. Besonders kritisch sieht es die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass US-Behörden Zugriffsmöglichkeiten auf Transaktionsdaten anstreben, auch wenn gegen die Betroffenen kein hinreichend konkreter Verdacht besteht, dass sie an Terroraktivitäten oder an deren Unterstützung mitwirken oder beteiligt waren. Ein derartiges Abkommen würde US-Behörden Befugnisse einräumen, die in Deutschland den Sicherheitsbehörden von Verfassungs wegen verwehrt sind.

Ein derartiger weit reichender Eingriff in das Recht auf informationelle Selbstbestimmung weit im Vorfeld des strafrechtlichen Anfangsverdachtes wäre datenschutzrechtlich nicht zu rechtfertigen. Dies wäre auch im Hinblick auf den Vertrauensschutz europäischer Wirtschaftsunternehmen höchst fragwürdig. Der Datentransfer wäre auch deshalb bedenklich, weil die datenschutzrechtlichen Garantien in den USA deutlich hinter den entsprechenden Anforderungen in der Europäischen Union zurückbleiben. Insbesondere besteht dort keine unabhängige Datenschutzkontrolle; Personen ohne ständigen Wohnsitz in den USA haben kein Recht auf gerichtliche Überprüfung der Verwendung ihrer Daten durch US-Behörden.

Im Übrigen bestehen bereits an der Notwendigkeit eines so weit reichenden Zugriffs ausländischer Behörden auf in Europa gespeicherte Daten erhebliche Zweifel. So können Strafverfolgungsbehörden im Rahmen der Rechtshilfe schon heute einzelfallbezogen personenbezogene Daten zur Aufklärung von Terrorismusverdachtsfällen übermitteln.

Schließlich ist zu befürchten, dass eine derartige Regelung über den Zugriff auf SWIFT-Daten Präzedenzwirkung entfalten würde. Zum einen könnten die Vereinigten Staaten mit derselben Begründung Zugriff auf andere in Europa gespeicherte sensible Datenbestände verlangen, etwa die Vorratsdaten der Telekommunikation. Zum anderen wäre es schwer nachvollziehbar, warum die Europäische Union den USA einen so weitgehenden Zugriff auf in Europa gespeicherte Daten einräumt, entsprechende Forderungen anderer Drittstaaten aber zurückweisen sollte.

Die Konferenz erwartet von der Bundesregierung, dass sie die besonders sensiblen Bankdaten der Bürgerinnen und Bürger wirksam schützt und einem Abkommen nicht zustimmt, das eine Datenübermittlung weit unterhalb der Schwelle des strafrechtlichen Anfangsverdachts erlaubt und keine angemessenen datenschutzrechtlichen Standards festlegt.

Anlage 1.26 "Reality-TV" - keine Mitwirkung staatlicher Stellen bei der Bloßstellung von Menschen

Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. Oktober 2009 in Berlin

„Reality-TV“-Produktionen über behördliche Einsätze haben in den letzten Jahren erheblich zugenommen. Justiz-, Polizei- und Sozialbehörden scheinen mittlerweile wichtige „Lieferanten“ für solche Fernsehsendungen zu sein, die einzelne Bürgerinnen und Bürger bloßstellen und dadurch erheblich in ihre Rechte eingreifen. Das Fernsehpublikum ist dabei, wenn etwa eine Gerichtsvollzieherin versucht, einen Haftbefehl gegen einen Schuldner zu vollziehen - wobei auch schon einmal eine Wohnung zwangsgeöffnet wird - oder wenn die Polizei Verdächtige überprüft oder bei Verkehrsdelikten zur Rede stellt. Es kann vom heimischen Fernsehsessel aus bequem mitverfolgen, ob Betroffene glaubwürdig Einsicht zeigen, unbelehrbar bleibt oder gar ausfällig werden. Aufgrund des Erfolgs derartiger „Unterhaltungssendungen“ ist abzusehen, dass die Intensität und die Eingriffstiefe der gezeigten staatlichen Maßnahmen zukünftig immer weiter zunehmen werden.

Presse- und Öffentlichkeitsarbeit sind zwar grundsätzlich notwendig, um die behördliche Aufgabenerfüllung darzustellen und den Informationsanspruch der Öffentlichkeit zu erfüllen. Dabei muss aber das Persönlichkeitsrecht der Betroffenen gewahrt werden, gerade wenn Unterhaltung und Befriedigung von Sensationslust im Vordergrund stehen.

Wird das Fernsehen durch zielgerichtete behördliche Unterstützung in die Lage versetzt, personenbezogene Filmaufnahmen anzufertigen, ist dies rechtlich als Datenübermittlung an private Dritte zu werten. Für einen solchen massiven Eingriff in das Datenschutzgrundrecht der Betroffenen gibt es keine Rechtsgrundlage. Der Staat, der die Betroffenen zur Duldung bestimmter Eingriffsmaßnahmen zwingen kann, ist grundsätzlich nicht befugt, Dritten die Teilnahme daran zu ermöglichen. Auch das Vorliegen einer wirksamen vorherigen Einwilligung der Betroffenen wird regelmäßig zweifelhaft sein. Für eine solche Einwilligung ist es insbesondere notwendig, die betroffene Person rechtzeitig über Umfang, Dauer und Verwendungszwecke der Aufnahmen aufzuklären und auf die Freiwilligkeit seiner Einwilligung hinzuweisen. Angesichts der Überraschungssituation sowie der mit dem staatlichen Eingriff nicht selten verbundenen Einschüchterung ist hier eine besonders sorgfältige Prüfung geboten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb alle Behörden auf, grundsätzlich von der Mitwirkung an solchen „Reality“-Reportagen Abstand zu nehmen.

Anlage 1.27 Staatsvertrag zum IT-Planungsrat - Datenschutz darf nicht auf der Strecke bleiben

Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. Oktober 2009 in Berlin

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die informationstechnische Kooperation von Bundes- und Landesbehörden zunehmend die Verarbeitung von personenbezogenen Daten betrifft, die durch technische und organisatorische Maßnahmen vor Missbrauch zu schützen sind, etwa durch wirksame Verschlüsselungsverfahren.

Das Bundesverfassungsgericht hat die besondere Bedeutung der informationellen Selbstbestimmung und der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme für den Schutz des Persönlichkeitsrechts hervorgehoben. Der in einem Staatsvertrag vorgesehene IT-Planungsrat muss diesen Vorgaben bei der Festlegung verbindlicher Interoperabilitäts- und IT-Sicherheitsstandards für die Datenverarbeitung Rechnung tragen. Für Entscheidungen in grundrechtssensiblen Fragestellungen muss auch der IT-Planungsrat die Zuständigkeit der Parlamente in Bund und Ländern berücksichtigen.

Die im Staatsvertrag vorgesehene vorrangige Verwendung bestehender Marktstandards darf nicht dazu führen, dass Verfahren ohne angemessenen Datenschutz beschlossen werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, dass der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit an den Sitzungen des IT-Planungsrats teilnehmen soll. Sie hält es für geboten, auch die Landesdatenschutzbeauftragten einzubeziehen.

Anlage 1.28 Krankenhausinformationssysteme datenschutzgerecht gestalten!

Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. Oktober 2009 in Berlin

Krankenhausinformationssysteme sind heute zu unverzichtbaren Hilfsmitteln ärztlicher Behandlung in Krankenhäusern geworden. Ein Abruf der darin elektronisch gespeicherten Patientendaten ist jederzeit, ortsungebunden und sekundenschnell möglich und bietet damit die Grundlage für effiziente Behandlungsentscheidungen. Diesen Vorteilen stehen allerdings erhebliche Datenschutzrisiken gegenüber. Die Möglichkeiten für Klinikpersonal, Behandlungsdaten von Bekannten, Kolleginnen und Kollegen oder Prominenten einzusehen und privat zu nutzen, sind groß. Prüfungen der Datenschutzaufsichtsbehörden und bekannt gewordene Missbrauchsfälle belegen dies.

Das Datenschutzrecht und die ärztliche Schweigepflicht gebieten, dass ein Zugriff auf die Daten von Kranken grundsätzlich nur denjenigen Krankenhausbeschäftigten möglich sein darf, die diese Kranken behandeln oder die Behandlung verwaltungsmäßig abwickeln.

Die Konferenz der Datenschutzbeauftragten fordert daher die datenschutzkonforme Gestaltung der internen Abläufe und der Erteilung von Zugriffsrechten in der Informationstechnik von Krankenhäusern.

Darüber hinaus fordert die Konferenz, dass Patienten nachvollziehen können, wer auf ihre Daten tatsächlich zugegriffen hat. Das ist Teil des Menschenrechts auf Achtung des Privatlebens nach Art. 8 der Europäischen Menschenrechtskonvention, wie der Europäische Gerichtshof für Menschenrechte klargestellt hat. Durch Protokollierung ist zu gewährleisten, dass eine nachträgliche Überprüfung der Zugriffe auf ihre Zulässigkeit möglich ist. Die Systeme müssen behandlungs- und patientenbezogen den technischen Zugriff gemäß den rechtlichen Befugnissen ermöglichen.

Die Krankenhäuser sind in der Pflicht, datenschutzgerechte Systeme einzusetzen. Die Software-Hersteller sind gehalten, entsprechende Systeme anzubieten.

Anlage 1.29 Datenschutzdefizite in Europa auch nach Stockholmer Programm

Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. Oktober 2009 in Berlin

Die Europäische Union will im Stockholmer Programm ihre politischen Zielvorgaben zur Entwicklung eines Raums der Freiheit, der Sicherheit und des Rechts für die kommenden fünf Jahre festschreiben. Dazu hat die Kommission der Europäischen Gemeinschaften einen Entwurf vorgelegt.

Zwar erwähnt der Kommissionsentwurf die Wahrung der persönlichen Freiheitsrechte und des Schutzes der Privatsphäre als Prioritäten der Innen- und Sicherheitspolitik in einem „Europa der Bürger“. Schritte wie der geplante Beitritt der Europäischen Union zur Europäischen Menschenrechtskonvention, Aufklärungs- und Informationskampagnen zum Datenschutz und die Förderung und ggf. Zertifizierung von datenschutzfreundlichen Technologien weisen auch in diese Richtung.

Allerdings bleiben die konkreten Überlegungen für einen verbesserten Datenschutz deutlich hinter den Zielsetzungen für eine verbesserte Sicherheitsarchitektur zurück. Hierzu enthält der Kommissionsentwurf einen umfangreichen Katalog von zum Teil äußerst eingriffsintensiven Maßnahmen, wie z. B. ein elektronisches Registrier- sowie Vorabgenehmigungssystem für Ein- und Ausreisen in oder aus der EU oder den Aufbau eines europäischen Strafregister-informationssystems. Die ebenfalls angestrebte einheitliche Plattform der Informationsverarbeitung mit beinahe beliebigen Datenverarbeitungsmöglichkeiten gefährdet ohne angemessene Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit die Bürgerrechte.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder bedarf es weiterer Schritte, um in Europa ein ausgewogenes Verhältnis von Sicherheit und Freiheit zu erreichen. Hierzu zählen insbesondere:

- Die Weiterentwicklung des Rahmenbeschlusses 2008/977/JI zu einem harmonisierten und auch für die innerstaatliche Datenverarbeitung verbindlichen Datenschutzrecht, das im Bereich der polizeilichen und justiziellen Zusammenarbeit ein hohes Datenschutzniveau gewährleistet.

- Abschluss von Übereinkommen mit Drittstaaten nur unter der Voraussetzung, dass die zwingenden Datenschutzgrundsätze dort beachtet werden.

- Ein unabhängiges datenschutzrechtliches Beratungs- und Kontrollorgan für alle Bereiche der polizeilichen und justiziellen Zusammenarbeit der EU-Mitgliedstaaten.

- Die Evaluation der vielen auf EU-Ebene beschlossenen sicherheitspolitischen Vorhaben im Hinblick auf ihre Effektivität, den Umfang der mit ihnen verbundenen Grundrechtseingriffe sowie mögliche Überschneidungen der Maßnahmen untereinander, bevor weitere Rechtsakte verabschiedet werden.

- Die Verbesserung von Transparenz und demokratischer Kontrolle bei der Rechtsetzung im Bereich der polizeilichen und justiziellen Zusammenarbeit auf europäischer Ebene, ungeachtet der Annahme des Vertrages von Lissabon.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, sich für diese Forderungen - auch unter Berücksichtigung der Kritik des Bundesrates etwa zu der Schaffung von Exekutivbefugnissen für EUROPOL und EUROJUST - im weiteren Verfahren einzusetzen.

Anlage 1.30 Aktueller Handlungsbedarf beim Datenschutz - Förderung der Datenschutzkultur

Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. Oktober 2009 in Berlin

Zunehmende Überwachung und die ausufernde Verknüpfung von Daten in Staat und Wirtschaft gefährden unser aller Persönlichkeitsrecht. Zusätzliche Herausforderungen ergeben sich aus der technologischen Entwicklung und der Sorglosigkeit der Bürgerinnen und Bürger.

Das aus den 70er Jahren des vorigen Jahrhunderts stammende Datenschutzrecht stellt längst keinen wirksamen Schutz mehr dar. Dies gilt ungeachtet der punktuellen Anpassungen, die das Bundesdatenschutzgesetz seither erfahren hat.

Zu Beginn der neuen Legislaturperiode des Deutschen Bundestags fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Generalrevision des Datenschutzrechts, einschließlich der jüngsten Novellierung zum Adresshandel.

Die Konferenz hält es insbesondere für erforderlich:

- das Datenschutzrecht an die Herausforderungen neuer Technologien anzupassen und dabei z. B. die Rechte der Betroffenen bei der Nutzung des Internets, insbesondere auf Löschung ihrer Daten, zu verbessern;

- die Integrität und Vertraulichkeit informationstechnischer Systeme zu gewährleisten;

- ein Beschäftigtendatenschutzgesetz zu erlassen und dabei vor allem die Überwachung am Arbeitsplatz effektiv zu begrenzen;

- die Vorratsdatenspeicherung und Online-Durchsuchung zurückzunehmen;

- die übrigen in den letzten Jahren verschärften Einschränkungen der Grundrechte durch Sicherheitsgesetze des Bundes und der Länder kritisch zu überprüfen;

- auf europäischer und internationaler Ebene auf hohe datenschutzrechtliche Grundstandards hinzuwirken und z. B. den verdachtslosen Zugriff auf Fluggast- und Bankdaten zurückzuweisen;

- im Fall der Einführung der elektronischen Gesundheitskarte die Betroffenenrechte umfassend zu realisieren;

- die Videoüberwachung in Staat und Gesellschaft einzuschränken;

- den Schutz der Meldedaten zu verbessern;

- ein praktikables Datenschutzaudit zu schaffen;

- die Datenschutzaufsichtsbehörden so auszugestalten, dass sie ihre Kontroll- und Beratungsaufgaben unabhängig und effektiv wahrnehmen können.

Datenschutz kann jedoch nicht nur verordnet, er muss auch gelebt werden. Dies setzt eine Datenschutzkultur in Staat, Wirtschaft und Gesellschaft voraus, die gepflegt und weiterentwickelt werden muss.

Die Konferenz spricht sich deshalb dafür aus, den Datenschutz auch als Bildungsaufgabe zu verstehen. Sie fordert Staat, Wirtschaft und Gesellschaft auf, ihre entsprechenden Bildungsanstrengungen zu verstärken. Ziel muss es sein, die Fähigkeit und Bereitschaft der Bürgerinnen und Bürger, insbesondere von Kindern und Jugendlichen, zu fördern, verantwortungsvoll mit ihren eigenen Daten und respektvoll mit den Daten anderer Menschen umzugehen.

Anlage 2 Nichtöffentlicher Bereich

Anlage 2.1 Keine fortlaufenden Bonitätsauskünfte an den Versandhandel

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 17./18. April 2008 in Wiesbaden

Auskunfteien dürfen Bonitätsauskünfte gemäß § 29 Absatz 2 Nr. 1a BDSG grundsätzlich nur erteilen, wenn der Dritte, dem die Daten übermittelt werden sollen, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat. Besteht zwischen diesem Dritten (also dem anfragenden Unternehmen) und dem Betroffenen ein Dauerschuldverhältnis, aufgrund dessen das anfragende Unternehmen während der gesamten Dauer des Bestehens ein finanzielles Ausfallrisiko trägt (z.B. Ratenzahlungskredit, Girokonto, Energielieferungs-, Telekommunikationsvertrag), so dürfen Bonitätsauskünfte nicht nur zu dem Zeitpunkt erteilt werden, zu dem der Betroffene ein solches Vertragsverhältnis beantragt hat, sondern während der gesamten Laufzeit des Vertragsverhältnisses und bis zur Erfüllung sämtlicher Pflichten des Betroffenen.

Ein Versandhandelsgeschäft stellt als solches kein Dauerschuldverhältnis dar. Die aufgrund der bisherigen Erfahrungen mit den Kunden möglicherweise bestehende Wahrscheinlichkeit und darauf gegründete Erwartung, dass der Kunde nach der ersten Bestellung wiederholt bestellen wird, und die zur Erleichterung der Bestellvorgänge möglicherweise erfolgte Einrichtung eines „Kundenkontos“ rechtfertigten es nicht, ein Versandhandelsgeschäft mit einem Dauerschuldverhältnis gleichzusetzen. Ein berechtigtes Interesse seitens des Versandhandels gem. § 29 BDSG ist demnach nur gegeben, wenn aufgrund eines konkreten Bestellvorgangs ein finanzielles Ausfallrisiko vorliegt.

Nach Vertragsschluss sind Bonitätsauskünfte an Versandhändler dann nicht zu beanstanden, wenn ein Ratenzahlungskredit vereinbart wurde oder noch ein offener Saldo besteht. In allen anderen Fällen ist das Rechtsgeschäft nach Abwicklung des einzelnen Kaufgeschäftes für den Versandhandel abgeschlossen, ein berechtigtes Interesse an Bonitätsauskünften ist dann nicht mehr zu belegen. Damit sind Nachmeldungen oder sonstige Beauskunftungen in dieser Konstellation rechtlich unzulässig.

Hinweis:
Die Vertreter des Versandhandels und der Auskunfteien haben sich bereit erklärt, ihre Verfahren entsprechend den vorgenannten gesetzlichen Anforderungen bis spätestens Ende September 2008 umzustellen.

Anlage 2.2 Datenschutzkonforme Gestaltung sozialer Netzwerke

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 17./18. April 2008 in Wiesbaden

Der datenschutzgerechten Gestaltung sozialer Netzwerke im Internet kommt eine zentrale Bedeutung zu. Die Aufsichtsbehörden rufen in diesem Zusammenhang in Erinnerung, dass Anbieter in Deutschland zur Einhaltung des Regulierungsrahmens zum Datenschutz verpflichtet sind.

Insbesondere sind folgende rechtliche Rahmenbedingungen einzuhalten:

Anbieter sozialer Netzwerke müssen ihre Nutzer umfassend gemäß den gesetzlichen Vorschriften über die Verarbeitung ihrer personenbezogenen Daten und ihre Wahl- und Gestaltungsmöglichkeiten unterrichten. Das betrifft auch Risiken für die Privatsphäre, die mit der Veröffentlichung von Daten in Nutzerprofilen verbunden sind. Darüber hinaus haben die Anbieter ihre Nutzer aufzuklären, wie diese mit personenbezogenen Daten Dritter zu verfahren haben.

Die Aufsichtsbehörden weisen darauf hin, dass nach den Bestimmungen des Telemediengesetzes (TMG) eine Verwendung von personenbezogenen Nutzungsdaten für Werbezwecke nur zulässig ist, soweit die Betroffenen wirksam darin eingewilligt haben. Bei Werbemaßnahmen aufgrund von Profildaten müssen die Betroffenen nach den Bestimmungen des Bundesdatenschutzgesetzes (BDSG) mindestens eine Widerspruchsmöglichkeit haben. Die Aufsichtsbehörden empfehlen, dass die Anbieter die Nutzer selbst darüber entscheiden lassen, ob – und wenn ja, welche – Profil- oder Nutzungsdaten zur zielgerichteten Werbung durch den Anbieter genutzt werden.

Die Aufsichtsbehörden erinnern weiterhin daran, dass eine Speicherung von personenbezogenen Nutzungsdaten über das Ende der Verbindung hinaus ohne Einwilligung der Nutzer nur gestattet ist, soweit die Daten zu Abrechnungszwecken gegenüber dem Nutzer erforderlich sind.

Für eine vorauseilende Speicherung von Daten über die Nutzung sozialer Netzwerke (wie auch anderer Internet-Dienste) für eventuelle zukünftige Strafverfolgung besteht keine Rechtsgrundlage. Sie wird insbesondere auch nicht durch die Regelungen zur Vorratsdatenspeicherung vorgeschrieben.

Schließlich weisen die Aufsichtsbehörden darauf hin, dass das TMG die Anbieter dazu verpflichtet, das Handeln in sozialen Netzwerken anonym oder unter Pseudonym zu ermöglichen. Dies gilt unabhängig von der Frage, ob ein Nutzer sich gegenüber dem Anbieter des sozialen Netzwerks mit seinen Echtdaten identifizieren muss.

Die Anbieter sind verpflichtet, die erforderlichen technisch-organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit zu treffen. Sie müssen insbesondere einen systematischen oder massenhaften Export oder Download von Profildaten aus dem sozialen Netzwerk verhindern.

Bei der datenschutzfreundlichen Gestaltung von sozialen Netzwerken kommt den Standardeinstellungen - z. B. für die Verfügbarkeit von Profildaten für Dritte - eine zentrale Bedeutung zu. Die Aufsichtsbehörden fordern die Anbieter sozialer Netzwerke auf, datenschutzfreundliche Standardeinstellungen für ihre Dienste zu wählen, durch die die Privatsphäre der Nutzer möglichst umfassend geschützt wird. Diese Standardeinstellungen müssen besonders restriktiv gefasst werden, wenn sich das Portal an Kinder richtet. Der Zugriff durch Suchmaschinen darf jedenfalls nur vorgesehen werden, soweit der Nutzer ausdrücklich eingewilligt hat.

Der Nutzer muss die Möglichkeit erhalten, sein Profil auf einfache Weise selbst zu löschen. Schließlich sollten die Anbieter sozialer Netzwerkdienste die Einführung von Verfallsdaten oder zumindest automatische Sperrungen erwägen, die von den Nutzern selbst festgelegt werden können.

Anlage 2.3 Internet-Portale zur Bewertung von Einzelpersonen

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 17./18. April 2008 in Wiesbaden

Die Datenschutzaufsichtsbehörden weisen darauf hin, dass es sich bei Beurteilungen und Bewertungen von Lehrerinnen und Lehrern sowie von vergleichbaren Einzelpersonen in Internet-Portalen vielfach um sensible Informationen und subjektive Werturteile über Betroffene handelt, die in das Portal eingestellt werden, ohne dass die Urheber erkennbar sind und die jederzeit von jedermann abgerufen werden können.

Anbieter entsprechender Portale haben die Vorschriften des Bundesdatenschutzgesetzes über die geschäftsmäßige Verarbeitung personenbezogener Daten einzuhalten.

Bei der danach gesetzlich vorgeschriebenen Abwägung ist den schutzwürdigen Interessen der bewerteten Personen Rechnung zu tragen. Das Recht auf freie Meinungsäußerung rechtfertigt es nicht, das Recht der Bewerteten auf informationelle Selbstbestimmung generell als nachrangig einzustufen.

Anlage 2.4 Novellierung des Bundesdatenschutzgesetzes in den Bereichen Adressenhandel, Werbung und Datenschutzaudit

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 13./14. November 2008 in Wiesbaden

Der Düsseldorfer Kreis begrüßt, dass die Bundesregierung durch eine Novellierung des Bundesdatenschutzgesetzes aus den jüngst bekannt gewordenen Datenschutzverstößen im Bereich der Privatwirtschaft Konsequenzen ziehen möchte. Die uneingeschränkte Streichung des Listenprivilegs und die Pflicht zur Einholung einer Einwilligung des Betroffenen bei der Übermittlung an Dritte oder bei der Nutzung für Werbezwecke für Dritte sind erforderlich, um das informationelle Selbstbestimmungsrecht der Bürgerinnen und Bürger zu stärken. Hiervon wird künftig auch die Wirtschaft profitieren. Die geplanten Änderungen ermöglichen es, Werbung zielgerichteter und ohne Streuverluste vorzunehmen und unerwünschte Belästigungen zu vermeiden, sodass das Verbrauchervertrauen in die Datenverarbeitung der Wirtschaft gestärkt wird. Die vorgesehenen Regelungen zur Klarstellung, wann eine wirksame Einwilligung in die Werbenutzung vorliegt, und dass diese nicht mit wichtigen vertraglichen Gegenleistungen gekoppelt werden darf, verbessern die Transparenz und die Freiwilligkeit für den Betroffenen.

Darüber hinaus hat die beim Datenschutzgipfel am 4. September 2008 eingesetzte Länderarbeitsgruppe weitere Vorschläge zur Verbesserung des Bundesdatenschutzgesetzes unterbreitet, die jedoch bisher nicht berücksichtigt wurden.

Die derzeit geplanten Vorschriften genügen nicht, um künftig im Bereich der privaten Wirtschaft ein ausreichendes Datenschutzniveau zu verwirklichen. Hierzu bedarf es zum einen einer angemessenen Ausstattung der Datenschutzaufsichtsbehörden. Es bedarf zum anderen gemäß den europarechtlichen Vorgaben wirksamer Einwirkungsbefugnisse. Hierzu gehört neben adäquaten Kontroll- und Sanktionsmitteln die Möglichkeit, bei schwerwiegenden Datenschutzverstößen die Erhebung und Verwendung personenbezogener Daten zu untersagen. Auch die Stellung der betrieblichen Datenschutzbeauftragten sollte gestärkt werden.

Die bisherigen Vorschläge des Bundesministeriums des Innern zur Einführung eines Datenschutzaudits sind nicht geeignet, den Datenschutz in der Wirtschaft zu verbessern.

Anlage 2.5 Datenschutzrechtliche Bewertung von digitalen Straßenansichten insbesondere im Internet

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 13./14. November 2008 in Wiesbaden

Bei digital erfassten Fotos von Gebäude- und Grundstücksansichten, die über Geokoordinaten eindeutig lokalisiert und damit einer Gebäudeadresse und dem Gebäudeeigentümer sowie den Bewohnern zugeordnet werden können, handelt es sich in der Regel um personenbezogene Daten, deren Erhebung und Verarbeitung nach dem Bundesdatenschutzgesetz zu beurteilen sind. Die Erhebung, Speicherung und Bereitstellung zum Abruf ist nur zulässig, wenn nicht schutzwürdige Interessen der Betroffenen überwiegen. Bei der Beurteilung schutzwürdiger Interessen ist von Bedeutung, für welche Zwecke die Bilddaten verwendet werden können und an wen diese übermittelt bzw. wie diese veröffentlicht werden. Die obersten Aufsichtsbehörden sind sich einig, dass die Veröffentlichung von georeferenziert und systematisch bereitgestellten Bilddaten unzulässig ist, wenn hierauf Gesichter, Kraftfahrzeugkennzeichen oder Hausnummern erkennbar sind. Den betroffenen Bewohnern und Grundstückeigentümern ist zudem die Möglichkeit einzuräumen, der Veröffentlichung der sie betreffenden Bilder zu widersprechen und dadurch die Bereitstellung der Klarbilder zu unterbinden. Keine schutzwürdigen Interessen bestehen, wenn die Darstellung der Gebäude und Grundstücke so verschleiert bzw. abstrakt erfolgt, dass keine individuellen Eigenschaften mehr erkennbar sind. Um die Möglichkeit zum Widerspruch schon vor der Erhebung zu eröffnen, sollte die geplante Datenerhebung mit einem Hinweis auf die Widerspruchsmöglichkeit rechtzeitig vorher bekannt gegeben werden. Die Widerspruchsmöglichkeit muss selbstverständlich auch noch nach der Veröffentlichung bestehen.

Anlage 2.6 Telemarketing bei NGOs

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 23./24. April 2009 in Schwerin

Auch die sogenannten NGOs (non governmental organization), also nichtstaatliche Organisationen, die gemeinnützig oder auch als Interessenverbände tätig sind, haben in den letzten Jahren zunehmend damit begonnen, Telefonmarketing zu betreiben. Beworben werden insbesondere Personen, die schon einmal für die jeweilige NGO gespendet haben. Wenn der Spender seine Telefonnummer in den früheren Kontakten nicht angegeben hat, wird dieses Datum mit Hilfe des Telefonbuches oder einer Telefon-CD ermittelt.

Die Aufsichtsbehörden erklären, dass auch NGOs ohne Einwilligung der Betroffenen nicht zu telefonischer Werbung berechtigt sind. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu diesem Zweck ist ohne Einwilligung rechtswidrig.

Anlage 2.7 Datenschutzrechtliche Aspekte des Mitarbeiter-Screenings in international tätigen Unternehmen

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 23./24. April 2009 in Schwerin

Viele Unternehmen sind dazu übergegangen, ihre Mitarbeiter gegenüber Listen abzugleichen, die terrorverdächtige Personen und Organisationen enthalten. Insbesondere Unternehmen, die internationalen Konzernen angehören, werden von ihren teilweise in Drittländern ansässigen Muttergesellschaften hierzu aufgefordert. Letztere stellen auch darüber hinausgehende Listen z.B. mit gesuchten Personen zur Verfügung, die aufgrund nationaler Vorschriften in den Drittländern einzusetzen sind.

Nach § 4 Abs. 1 BDSG sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Zwar kann § 28 Abs. 1 BDSG eine Rechtsgrundlage im Sinne des BDSG sein, diese Vorschrift kann jedoch für ein Screening nicht herangezogen werden. Der Abgleich mit den Listen dient nicht dem Vertragsverhältnis. Eine Abwägung der Unternehmens- und Betroffeneninteressen führt zu überwiegenden schutzwürdigen Interessen der Betroffenen. Dies gilt insbesondere vor dem Hintergrund, dass die Rechtsstaatlichkeit des Zustandekommens der Listen nachvollziehbar und gesichert sein muss sowie Rechtsschutzmöglichkeiten bestehen müssen. Angesichts der fehlenden Freiwilligkeit einer solchen Erklärung im Arbeitsverhältnis kann auch das Vorliegen einer Einwilligung eine konkrete Rechtsgrundlage nicht ersetzen.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich stellen daher fest, dass im Geltungsbereich des Bundesdatenschutzgesetzes lediglich solche Listen verwendet werden dürfen, für die eine spezielle Rechtsgrundlage im Sinne des § 4 Abs. 1 BDSG vorliegt.

In diesem Zusammenhang weisen die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich auch auf die Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006 in Magdeburg hin.

Anlage 2.8 Unzulässige Übermittlungen von Passagierdaten an britische Behörden verhindern!

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 13. Juli 2009

Der Düsseldorfer Kreis stellt fest, dass die Übermittlung von Passagierdaten (Ausweis- und Reservierungsdaten) durch Fluggesellschaften in Deutschland an die britischen Zoll- und Sicherheitsbehörden für innereuropäische Flüge unzulässig ist. Die Bundesregierung wird gebeten, entsprechenden Forderungen der britischen Behörden entgegenzutreten.

Großbritannien verlangt im Rahmen des sog. eBorders-Projekts die Erhebung und Übermittlung von Ausweisdaten der Reisenden für innereuropäische Flüge von und nach Großbritannien und die Übermittlung von Daten aus den Reservierungsdatenbanken der Fluggesellschaften. Die britischen Behörden berufen sich bei ihrer Forderung auf die britische Gesetzgebung für Grenzkontrollen. Diese durch das eBorders-Projekt konkretisierte Gesetzgebung berührt einerseits den freien Reiseverkehr in der Europäischen Union. Andererseits bezieht sie sich auf Sachverhalte, die nicht alleine in der Regelungskompetenz des britischen Gesetzgebers liegen, weil sie Datenerhebungen in anderen Mitgliedstaaten der Europäischen Union vorschreibt und Übermittlungen aus Datenbanken verlangt, die sich in anderen Mitgliedstaaten befinden.

Die Übermittlung von Reservierungsdaten der Passagiere an britische Grenzkontrollbehörden, die sich in Datenbanken der verantwortlichen Fluggesellschaften in Deutschland befinden, ist nach deutschem Recht nicht erlaubt. Insbesondere enthält das Bundesdatenschutzgesetz (BDSG) keine Rechtsgrundlage, auf die die Fluggesellschaften die geforderte Übermittlung stützen könnten.

Bereits bei entsprechenden Forderungen der USA, Kanadas und Australiens bestand in Europa Konsens, dass die Übermittlung nicht zur Erfüllung der Flugreiseverträge erfolgt (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG) und wegen der Zwangslage nicht auf eine Einwilligung (§ 4a BDSG) der Reisenden gestützt werden kann. Sie dient auch nicht den berechtigten Interessen der Fluggesellschaften, die selbst den Forderungen der britischen Behörden entgegentreten, weil sie sich als Reiseunternehmen und nicht als Gehilfen der Grenzkontrollbehörden verstehen. Außerdem besteht ein überwiegendes Interesse der Flugreisenden daran, dass eine Übermittlung ihrer Daten unterbleibt, solange die Vereinbarkeit der britischen Forderung mit vorrangigem europäischen Recht nicht geklärt ist (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG). Schließlich kann eine solche verdachts- oder gefahrunabhängige Übermittlung der Daten aller Reisenden für Sicherheitszwecke nicht auf § 28 Abs. 3 Satz 1 Nr. 2 BDSG gestützt werden, da diese Vorschrift das Vorliegen einer konkreten Gefahr oder Straftat voraussetzt.

Die Übermittlung der Reservierungsdaten ist außerdem verfassungsrechtlich bedenklich und auch fraglich im Hinblick auf die Vereinbarkeit mit der Europäischen Menschenrechtskonvention.

Was die Erhebung von Ausweisdaten anbelangt, gehen die britischen Behörden über die Europäische Richtlinie 2004/82/EG über die Verpflichtung von Beförderungsunternehmen, Angaben über beförderte Personen zu übermitteln, insoweit hinaus, als Daten auch für innereuropäische Flüge erhoben werden sollen. Die Europäische Kommission prüft zurzeit, ob diese einseitige Regelung eine Verletzung der Richtlinie 2004/82/EG darstellt.
Jedenfalls dürfte eine solche Maßnahme im Hinblick auf die Freizügigkeit in der Europäischen Union kontraproduktiv sein. Der Düsseldorfer Kreis erwartet, dass die Erhebung und Übermittlung von Pass- und Ausweisdaten für innereuropäische Flüge bis zu einer Bewertung durch die Europäische Kommission unterbleiben.

Anlage 2.9 Bonitätsauskünfte über Mietinteressenten nur eingeschränkt zulässig

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 22. Oktober 2009

Häufig holen Vermieter Informationen bei Auskunfteien über die Bonität von Mietinteressenten ein, bevor sie Wohnraum vermieten. Hierfür gelten folgende Anforderungen:

1. Vermieter dürfen erst dann eine Auskunft zu einem Mietinteressenten einholen, wenn der Abschluss des Mietvertrags mit diesem Bewerber nur noch vom positiven Ergebnis einer Bonitätsprüfung abhängt.

2. Es dürfen nur folgende Datenkategorien nach Darlegung eines konkreten berechtigten Interesses an Vermieter übermittelt werden, sofern diese Daten zulässigerweise an die Auskunftei übermittelt bzw. von dieser erhoben wurden:

   - Informationen aus öffentlichen Schuldner- und Insolvenzverzeichnissen;

   - sonstige Daten über negatives Zahlungsverhalten, bei denen
     - die dem jeweiligen Eintrag zugrunde liegende Forderung noch offen ist oder - sofern sie sich zwischenzeitlich erledigt hat - die Erledigung nicht länger als ein Jahr zurückliegt und
     - eine Bagatellgrenze von insgesamt 1.500 € überschritten wird.

3. Die Übermittlung von Scorewerten an Vermieter ist unzulässig, sofern darin andere als die unter Nummer 2. erwähnten Daten verwendet werden.

4. Vermieter dürfen weitergehende als die unter 2. genannten Daten grundsätzlich auch nicht im Wege einer Einwilligung oder einer Selbstauskunft des Mietinteressenten von einer Auskunftei erheben.

Hintergrund:

Nach § 29 Absatz 2 Nr. 1a Bundesdatenschutzgesetz ist die Erteilung von Bonitätsauskünften nur zulässig, wenn der Vermieter ein berechtigtes Interesse hieran hat und wenn kein Grund zu der Annahme besteht, dass der betroffene Mietinteressent ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

Da Vermieter mit dem Abschluss eines Mietvertrages das Risiko eingehen, dass ein Mieter aufgrund von Zahlungsunfähigkeit oder -unwilligkeit den Mietzins oder Nebenkosten nicht begleicht, erkennen die Aufsichtsbehörden an, dass Vermieter aufgrund dieses finanziellen Ausfallrisikos grundsätzlich ein berechtigtes Interesse an einer Bonitätsauskunft über einen Mietinteressenten haben.

Bei der erforderlichen Abwägung sind allerdings auch die schutzwürdigen Belange der Mietinteressenten im Hinblick auf die Bedeutung der Wohnung für die Lebensgestaltung zu berücksichtigen. Ferner ist zu beachten, dass Mietkautionen in Höhe von bis zu drei Monatsmieten, das Vermieterpfandrecht und die bei nachträglicher Zahlungsunfähigkeit vielfach in die Zahlungspflicht eintretenden Sozialbehörden das finanzielle Risiko der Vermieter teilweise reduzieren.

Schließlich ist zu berücksichtigen, dass Auskunfteien an Vermieter nur Bonitätsdaten übermitteln dürfen, die eindeutig Rückschlüsse auf Mietausfallrisiken zulassen. Da das Zahlungsverhalten je nach Vertragsverhältnis unterschiedlich sein kann und teilweise auch ist, lassen zu spät oder nicht gezahlte Kleinbeträge etwa aus Handyverträgen und Internetgeschäften nicht unbedingt einen spezifischen Rückschluss auf die Zahlungsmoral bei Mietverträgen zu.

Aufgrund dieser Erwägungen haben die Aufsichtsbehörden nach Gesprächen mit den Auskunfteien und der Wohnungswirtschaft bereits im Jahr 2004 festgestellt, dass Auskunfteien keine uneingeschränkten Bonitätsauskünfte über Mietinteressenten erteilen dürfen. Vorzuziehen - so der damalige Beschluss - seien branchenspezifische Auskunftssysteme, die auf gesicherte Daten zu negativem Zahlungsverhalten aus öffentlichen Schuldnerverzeichnissen und dem Mietbereich beschränkt sind.

Die eingangs dargelegten Anforderungen berücksichtigen wesentliche Kritikpunkte der Wohnungswirtschaft und der Auskunfteien. So enthält der nunmehr definierte Katalog weder eine Beschränkung auf Daten aus dem Mietbereich noch eine Beschränkung auf titulierte Negativmerkmale. Eine derartige Beschränkung hatten mehrere Aufsichtsbehörden bislang auf Grundlage des Beschlusses aus dem Jahr 2004 gefordert und gegenüber sogenannten Mieterwarndateien auch durchgesetzt.

Selbstverständlich dürfen nur Daten, die zulässigerweise bei der Auskunftei eingemeldet wurden, von dieser an Vermieter übermittelt werden. Das heißt, die allgemeinen Einmeldevoraussetzungen, die der Gesetzgeber im neuen § 28a BDSG präzisiert hat und die bereits bisher von den Aufsichtsbehörden gefordert wurden, müssen eingehalten werden.

Die Bagatellgrenze von 1500 € errechnet sich aus drei Monatsmieten der durchschnittlichen Kaltmiete. Nach der jüngsten Einkommens- und Verbrauchsstichprobe des Statistischen Bundesamtes beträgt sie monatlich 515 €.

Auch wenn die Speicher- bzw. Überprüfungsfrist der Auskunfteien bei Forderungen, die nach der Einmeldung beglichen wurden, drei Jahre beträgt (§ 35 Abs. 2 Nr. 4, 2. Halbsatz BDSG neu), ist ein berechtigtes Interesse von Vermietern an der Kenntnis solcher Daten nur für ein Jahr anzuerkennen. Daher ist auch nur innerhalb dieses Zeitraums eine Übermittlung an Vermieter zulässig. Ansonsten wäre dem Schuldner die Eingehung eines Mietverhältnisses unvertretbar erschwert.

Die Unzulässigkeit der Übermittlung von Scorewerten an Vermieter ergibt sich daraus, dass abgesehen von der allgemeinen Problematik der Scoreberechnung im Mietbereich die besondere Problematik besteht, dass die spezifischen Einschränkungen unterlaufen würden, wenn eine Scoreberechnung mit Daten erfolgte, die über den unter Nummer 2. genannten Katalog hinausgehen.

Die Einforderung von unbegrenzten Selbstauskünften oder Einwilligungen zur Einholung weit gefasster Auskünfte vom Mietinteressenten würde eine Umgehung der sich aus der Abwägung nach § 29 BDSG ergebenden gesetzlichen Begrenzungen darstellen, was demzufolge nicht zulässig ist.

Die bisherige Praxis der Auskunfteien entsprach den hier gestellten Anforderungen nicht bzw. nicht in ausreichendem Maße. Obwohl den Auskunfteien ausdrücklich die Möglichkeit eingeräumt wurde, ggf. alternative Lösungen zu den im Beschluss genannten Anforderungen zu entwickeln, die auf das jeweilige Geschäftsmodell der Auskunfteien und deren speziellen Datenbestand zugeschnitten sind, haben die Auskunfteien diese Möglichkeit bislang nicht genutzt.

Die Aufsichtsbehörden haben in Gesprächen mit den Auskunfteien angekündigt, dass sie bei datenschutzwidrigen Übermittlungen ggf. aufsichtsrechtliche Maßnahmen ergreifen werden.

Anlage 2.10 Gesetzesänderung bei der Datenverwendung für Werbezwecke

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 26./27. November 2009 in Stralsund

Vom 1. September 2009 an gelten nach § 28 Abs. 3 BDSG neue Datenschutzregelungen bei der Datenverwendung für Werbezwecke. Diese Regelungen gelten spätestens ab dem 31. August 2012, jedoch sofort für Daten, die nach dem 1. September 2009 erhoben oder von einer Stelle erstmalig gespeichert werden.

Die Datenschutzaufsichtsbehörden weisen darauf hin, dass für Daten, deren erstmalige Speicherung nicht eindeutig erkennbar ist, die neuen Regelungen angewendet werden. Sie weisen weiterhin darauf hin, dass eine Übermittlung für Werbezwecke nur zulässig ist, wenn Herkunft der Daten und Empfänger gespeichert werden und eine Gruppenauswahl nach einem Merkmal erfolgt (Listenübermittlung). Bei der Werbemaßnahme muss die erstmalig erhebende Stelle den Adressaten mitgeteilt werden. Die bisher weit verbreitete Praxis der Übermittlung von nach mehr als einem Merkmal selektierten Adressen ist unzulässig, wenn keine Einwilligung vorliegt.

Anlage 2.11 Keine Internetveröffentlichung sportgerichtlicher Entscheidungen

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 26./27. November 2009 in Stralsund

Entgegen der Auffassung des OLG Karlsruhe in seinem Urteil vom 30. Januar 2009 gehen die zuständigen Aufsichtsbehörden in Anwendung des BDSG davon aus, dass die uneingeschränkt zugängliche Veröffentlichung von sportgerichtlichen Entscheidungen im Internet unzulässig ist. Entsprechendes gilt auch für die Veröffentlichung von personenbezogenen Sperrlisten.

Eine Veröffentlichung in geschlossenen Benutzergruppen ist zulässig, wenn gewährleistet ist, dass in den Vereinen nur zuständige Personen zugreifen können. Soweit der Personenbezug nicht erforderlich ist, sind sportgerichtliche Entscheidungen zu anonymisieren.

Bei der mit der Veröffentlichung im Internet verbundenen Datenübermittlung an Dritte wird der Eingriff in das informationelle Selbstbestimmungsrecht der Betroffen meist deswegen als besonders gravierend empfunden, weil hierdurch nicht nur ein weltweiter Zugriff auf die Daten, sondern darüber hinaus vor allem eine elektronische Recherchierbarkeit ermöglicht wird, welche auch zur Erstellung eines Persönlichkeitsprofil genutzt werden kann.

Der beabsichtigten „Prangerwirkung“ mit Abschreckungsfunktion könnte bereits dadurch Genüge getan werden, dass entsprechende Ahndungen organisations-/verbandsintern in zugriffsgeschützten Internetforen „für die, die es angeht“ publiziert würden. Die intendierte Information der Öffentlichkeit über das Vorgehen gegen Rechtsverstöße könnte ohne Personenbezug im Rahmen einer Ahndungsstatistik erfolgen.

Anlage 2.12 Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 26./27. November 2009 in Stralsund

Viele Web-Seitenbetreiber analysieren zu Zwecken der Werbung und Marktforschung oder bedarfsgerechten Gestaltung ihres Angebotes das Surf-Verhalten der Nutzerinnen und Nutzer. Zur Erstellung derartiger Nutzungsprofile verwenden sie vielfach Software bzw. Dienste, die von Dritten kostenlos oder gegen Entgelt angeboten werden.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen darauf hin, dass bei Erstellung von Nutzungsprofilen durch Web-Seitenbetreiber die Bestimmungen des Telemediengesetzes (TMG) zu beachten sind. Demnach dürfen Nutzungsprofile nur bei Verwendung von Pseudonymen erstellt werden. Die IP-Adresse ist kein Pseudonym im Sinne des Telemediengesetzes.

Im Einzelnen sind folgende Vorgaben aus dem TMG zu beachten:

- Den Betroffenen ist eine Möglichkeit zum Widerspruch gegen die Erstellung von Nutzungsprofilen einzuräumen. Derartige Widersprüche sind wirksam umzusetzen.

- Die pseudonymisierten Nutzungsdaten dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden. Sie müssen gelöscht werden, wenn ihre Speicherung für die Erstellung der Nutzungsanalyse nicht mehr erforderlich ist oder der Nutzer dies verlangt.

- Auf die Erstellung von pseudonymen Nutzungsprofilen und die Möglichkeit zum Widerspruch müssen die Anbieter in deutlicher Form im Rahmen der Datenschutzerklärung auf ihrer Internetseite hinweisen.

- Personenbezogene Daten eines Nutzers dürfen ohne Einwilligung nur erhoben und verwendet werden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Jede darüber hinausgehende Nutzung bedarf der Einwilligung der Betroffenen.

- Die Analyse des Nutzungsverhaltens unter Verwendung vollständiger IPAdressen (einschließlich einer Geolokalisierung) ist aufgrund der Personenbeziehbarkeit dieser Daten daher nur mit bewusster, eindeutiger Einwilligung zulässig. Liegt eine solche Einwilligung nicht vor, ist die IP-Adresse vor jeglicher Auswertung so zu kürzen, dass eine Personenbeziehbarkeit ausgeschlossen ist.

Werden pseudonyme Nutzungsprofile durch einen Auftragnehmer erstellt, sind darüber hinaus die Vorgaben des Bundesdatenschutzgesetzes zur Auftragsdatenverarbeitung durch die Anbieter einzuhalten.

Anlage 3 Organigramm

Der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern

Landesbeauftragter für Informationsfreiheit
Aufsichtsbehörde gemäß § 38 BDSG

Stand: 01.07.2009

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

Enrico Wilcke
5 94 94-55

- 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

Stellvertreter des LfD

Gabriel Schulz
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

Jana Behnke
5 94 94-33

- 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 4 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, Telefon, IP-Telefonie 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 MV
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 (Auslegungsfragen, Novellierungsbedarf)
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
1.2.5 Arbeitsgemeinschaft christlicher Kirchen
1.3 Medien in den Ländern
1.3.0 Allgemeines
1.3.1 Verfassungsbeschwerden/Gerichtsentscheidungen/Aufsätze
1.3.2 Rundfunk/Fernsehen
1.3.3 Telekommunikation
1.3.4 Presse
1.3.5 E-Mail/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
3.0.6 Normen/Standards/Grundsätze
3.0.7 Post / Telekommunikation / Internet / VoIP
3.0.8 Einzelprobleme/Beratungsersuchen
3.0.9 Eingaben
3.1 Datenschutz beim Einsatz von ADV
3.1.0 Allgemeines
3.1.1 Hardware
3.1.2 Anwendungsunabhängige Software
3.1.3 Anwendersoftware
3.1.4 Datenfernverarbeitung
3.1.5 Datenerfassung
3.1.6 Ordnungsgemäße Anwendung von Hard- und Software
3.1.7 Datenhandhabung
3.1.8 Einzelprobleme/Beratungsersuchen
3.2 Datenschutz beim Einsatz von konventioneller Technik
3.2.0 Allgemeines
3.2.1 Vernichtung/Entsorgung von Datenträgern
3.2.2 Schutz von Gesprächen vertraulichen Inhalts
3.2.3 Datensicherung bei Führung von Akten
3.2.4 Datensicherung beim Transport von Akten
3.2.7 Datenhandhabung
3.2.8 Einzelprobleme/Beratungsersuchen
3.3 Datenschutz und Organisation
3.3.0 Allgemeines
3.3.1 Interne Kontrolle
3.3.2 Dienstanweisungen
3.3.3 Sicherheits- und IT-Konzepte
3.3.4 IT-Schulung
3.3.5 Regelungen zu PKI-Strukturen
3.3.6 Risikobetrachtungen
3.3.7 IT-Management
3.3.8 Einzelprobleme/Beratungsersuchen

3.4 Baulicher Datenschutz
3.4.0 Allgemeines
3.4.1 Bautechnische Sicherheit
3.4.2 Verkabelung
3.4.8 Einzelprobleme/Beratungsersuchen
3.5 Technisch-organisatorische Maßnahmen
3.5.0 Allgemeines
3.5.1 Zugangskontrolle
3.5.2 Datenträgerkontrolle
3.5.3 Transportkontrolle
3.5.4 Eingabekontrolle
3.5.5 Speicher-/Benutzerkontrolle
3.5.6 Zugriffskontrolle
3.5.7 Übermittlungskontrolle
3.5.8 Organisationskontrolle
3.5.9 Auftragskontrolle
3.6 Kontroll- und Informationsbesuche
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 MV
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
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 Arbeitnehmerdatenschutz
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 Telekommunikation, 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 Telekommunikation und Telefonanbieter
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
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 Auftragsdatenverarbeitung
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
5.3.1 Tätigkeitsberichte
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 BVerwG, 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
5.7.0 Hinweise/Orientierungshilfen
5.8 Einzelprobleme
5.8.0 Allgemeines
5.8.1 Sachgebiete
6 Projektbereich
6.1 Projekt Grunddatenerfassung
6.1.1 Projekt Grunddatenerfassung
6.2 Projekt E-Governmentfähigkeit der Kommunen
6.2.1 Projekt E-Governmentfähigkeit der Kommunen
6.3 ID-Management in sozialen Netzen
6.3.0 ID-Management in sozialen Netzen

8 Abkürzungsverzeichnis

ADAC	Allgemeiner Deutscher Automobilclub e. V.
ADV	automatisierte Datenverarbeitung
AGnES	Arzt-entlastende, Gemeinde-nahe, E-Health-gestützte, Systemische Intervention
AKLS	automatisiertes Kfz-Kennzeichen-Lesesystem
AK Technik	Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Ständigen Konferenz der Datenschutzbeauftragten des Bundes und der Länder
ALB	automatisiertes Liegenschaftsbuch
ALG	Arbeitslosengeld
AO	Abgabenordnung
ARGE	Arbeitsgemeinschaft
AZVO	Arbeitszeitverordnung
BAO KAVALA	Besondere Aufbauorganisation der Polizeidirektion Rostock
BDSG	Bundesdatenschutzgesetz
BeamtStG	Beamtenstatusgesetz
BEM	Betriebliches Eingliederungsmanagement
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BKA	Bundeskriminalamt
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten
BlnDSG	Berliner Datenschutzgesetz
BMeldG-E	Gesetz zur Fortentwicklung des Meldewesens
BMF	Bundesministerium der Finanzen
BMFSFJ	Bundesministerium für Familie, Senioren, Frauen und Jugend
BMI	Bundesministerium des Innern
BMWi	Bundesministerium für Wirtschaft und Technologie
BRNG	Beamtenrechtsneuordnungsgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BStatG	Bundesstatistikgesetz
BT	Bundestag
BUGA	Bundesgartenschau
BVerfG	Bundesverfassungsgericht
BZRG	Bundeszentralregistergesetz
CN-LAVINE	Corporate Network der Landesverwaltung
DDV	Deutscher Direkt-Marketing-Verband
DEKRA	Deutscher Kraftfahrzeug-Überwachungs-Verein
DNA	Desoxyribonukleinsäure – Träger der Erbinformationen
DRG	Diagnosis Related Groups
DSB	Datenschutzbeauftragter
DSG M-V	Landesdatenschutzgesetz
DVZ M-V GmbH	Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH

EDV	elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
EG-DLRG	EG-Dienstleistungsrichtlinie
EGMR	Europäischer Gerichtshof für Menschenrechte
EGVP	elektronischer Geschäftsverteilungsplan
eID	elektronischer Identitätsnachweis
ELENA	elektronischer Einkommensnachweis
EnWG	Energiewirtschaftsgesetz
EPOS	Elektronisches Personal-, Organisations- und Stellenmanagementsystem
ERFA-Kreis	Erfahrungsaustauschkreis
EU	Europäische Union
EURODAC	Europäische Datenbank zur Speicherung von Fingerabdrücken (engl. European Dactyloscopy)
EUROJUST	Europäische Einheit für justizielle Zusammenarbeit
EUROPOL	Europäisches Polizeiamt
EuroPriSe	European Privacy Seal
EZB	Europäische Zentralbank
FDP	Freie Demokratische Partei
FIDIS	Future of Identity in the Information Society
GDD	Gesellschaft für Datenschutz und Datensicherung e. V.
GewO	Gewerbeordnung
GEZ	Gebühreneinzugszentrale
GG	Grundgesetz
GGO	gemeinsame Geschäftsordnung
GPS	Global Positioning System
GrdstVG	Grundstücksverkehrsgesetz
HandwO	Handwerksordnung
HKB	Haus der Kultur und Bildung
HmbDSG	Hamburger Datenschutzgesetz
HTTP	Hypertext Transport Protocol
ICM	Institut für Community Medicine
ID	Identifikationsnummer
IFG M-V	Informationsfreiheitsgesetz Mecklenburg-Vorpommern
IHK	Industrie- und Handelskammer
IM M-V	Innenministerium Mecklenburg-Vorpommern
ISDN	Integrated Services Digital Network
IT-NetzG	Gesetz über die Verbindung der informationstechnischen Netze des Bundes und der Länder
INPOL	polizeiliches Informationssystem
INSPIRE	Infrastructure for Spatial Information in Europe – EU-Richtlinie zur Schaffung einer Geodateninfrastruktur
IP	Internet Protocol
IPSEC	Internet Protocol Security
IRI	Institut für Rechtsinformatik
ISO	International Organization for Standardization
ITIL	IT Infrastructure Library

ITSG	Informationstechnische Servicestelle der gesetzlichen Krankenversicherung
IWG	Informationsweiterverwendungsgesetz
JGG	Jugendgerichtsgesetz
KAN	Kriminalaktennachweis
KAG M-V	Kommunalabgabengesetz Mecklenburg-Vorpommern
KBA	Kraftfahrtbundesamt
Kfz	Kraftfahrzeug
KiföGÄndG	Kindertagesförderungsgesetz
KIS	Krankenhausinformationssystem
Koop A ADV	Kooperationsausschuss von Bund und Ländern für automatisierte Datenverarbeitung
KUG	Kunsturhebergesetz
KV M-V	Kommunalverfassung des Landes Mecklenburg-Vorpommern
KWG M-V	Kommunalwahlgesetz Mecklenburg-Vorpommern
LaGuS	Landesamt für Gesundheit und Soziales
LArchivG M-V	Landesarchivgesetz Mecklenburg-Vorpommern
LARIS	Landesrechts-Informationssystem
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	Ministerium für Landwirtschaft, Umwelt und Verbraucherschutz
LMG M-V	Landesmeldegesetz Mecklenburg-Vorpommern
LRKG M-V	Landesreisekostengesetz des Landes Mecklenburg-Vorpommern
LT-Drs.	Landtags-Drucksache
LWaG	Landeswassergesetz
MDK	Medizinischer Dienst der Krankenversicherung
MfS	Ministerium für Staatssicherheit
MRRG	Melderechtsrahmengesetz
MVDS	multifunktionaler Verdienstdatensatz
NDR	Norddeutscher Rundfunk
NGO	nichtstaatliche Organisationen (engl. non governmental organization)
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (engl.: Organization for Economic Co-operation and Development)
ÖGDG	Gesetz über den Öffentlichen Gesundheitsdienst
OLG	Oberlandesgericht
OSCI	Online Services Computer Interface
OWiG	Gesetz über Ordnungswidrigkeiten
PACE	Password Authenticated Connection Establishment
PassDEÜV	Passdatenerfassungs- und Übermittlungsverordnung
PD	Polizeidirektion
PDF	Portable Document Format - plattformunabhängiges Dateiformat für Dokumente
PIN	Persönliche Identifikationsnummer
PKI	Public-Key-Infrastruktur
PNR	Fluggastdaten (engl. Passenger Name Record)

PRIME	Privacy and Identity Management for Europe
RFID	Radio Frequency Identification
SAP	Systemanalyse und Programmentwicklung
SchfHwG	Schornsteinfeger-Handwerksgesetz
SCHUFA	SCHUFA Holding AG
SchulG M-V	Schulgesetz Mecklenburg-Vorpommern
SCCP	Skinny Client Control Protocol
SGB I	Sozialgesetzbuch Erstes Buch
SGB II	Sozialgesetzbuch Zweites Buch
SGB VII	Sozialgesetzbuch Siebtes Buch
SGB VIII	Sozialgesetzbuch Achtes Buch
SGB IX	Sozialgesetzbuch Neuntes 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
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StVO	Straßenverkehrsordnung
StVollzG	Strafvollzugsgesetz
SÜG M-V	Sicherheitsüberprüfungsgesetz Mecklenburg-Vorpommern
SWIFT	Society for Worldwide Interbank Financial Telekommunications
TAN	Transaktionsnummer
TESTA	Transeuropäische Telematikdienste zwischen Verwaltungen (engl.: Trans-European Services for Telematics between Administrations)
TFG	Transfusionsgesetz
TKG	Telekommunikationsgesetz
TLS	Transport Layer Security
TMG	Telemediengesetz
TMS	Travel Management System
UIG	Umweltinformationsgesetz
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
USA	Vereinigte Staaten von Amerika (engl. United States of America)
USB	Universal Serial Bus - serielles Bussystem zur Verbindung eines Computers mit externen Geräten
USV	unterbrechungsfreie Stromversorgung
Verf M-V	Verfassung des Landes Mecklenburg-Vorpommern
VermGeoG M-V	Vermessungs- und Geoinformationsgesetz Mecklenburg-Vorpommern
VermKatG M-V	Gesetz über die Landesvermessung und das Liegenschaftskataster des Landes Mecklenburg-Vorpommern
VGH	Verfassungsgerichtshof
VIS	Visa-Informationssystem
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network
VKS	Verkehrskontrollsystem

VwGO	Verwaltungsgerichtsordnung
VwVfG M-V	Verwaltungsverfahrensgesetz Mecklenburg-Vorpommern
WLAN	Wireless Local Area Network - drahtloses lokales Netzwerk
ZensAG	Zensusausführungsgesetz
ZensG	Gesetz über den registergestützten Zensus
ZIR	Zentrales Informationsregister
ZKA	Zentraler Kreditausschuss
ZSS	Zentrale Speicherstelle

9 Stichwortverzeichnis

10 Publikationen

Beim Landesbeauftragten für den Datenschutz sind derzeit folgende Publikationen kostenlos erhältlich:

Broschüren (A4)

8. Tätigkeitsbericht (DSG M-V), 3. Tätigkeitsbericht (BDSG) und 1. Tätigkeitsbericht (IFG M-V) für den Zeitraum 2006/2007

2. Tätigkeitsbericht (IFG M-V) für den Zeitraum 2008/2009 (inkl. Bericht zur Evaluierung des IFG M-V)

9. Tätigkeitsbericht (DSG M-V), 4. Tätigkeitsbericht (BDSG) für den Zeitraum 2008/2009

Faltblätter (A5)

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

Broschüren (A5)

Datenschutzgerechtes eGovernment (Empfehlungen, datenschutzfreundliche Lösungen für die Verwaltung)

Vom Bürgerbüro zum Internet (Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung)

Die Virtuelle Poststelle im datenschutzgerechten Einsatz

Datenschutz bei Dokumentenmanagementsystemen (Orientierungshilfe)

Privatsphäre – Gefangen im Netz der Koordinaten (Tagungsband: Datenschutz-Fachtagung 2009)

Ein modernes Datenschutzrecht für das 21. Jahrhundert (Konferenz der DSB des Bundes und der Länder; 2010)

Ihr Recht auf Information (Das Informationsfreiheitsgesetz Mecklenburg-Vorpommern)

DATENSCHUTZ: GANZ EINFACH (Pin- und Passwort-Merkkarte im Scheckkarten-Format)

Muster/Formulare (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/zum behördlichen Datenschutzbeauftragten

Verfahrensbeschreibung nach § 18 DSG M-V und Hinweise zur Führung der Verfahrensbeschreibung

Widerspruch gegen die Weitergabe meiner Daten gemäß §§ 32, 34 a, 35 Meldegesetz für das Land Mecklenburg-Vorpommern

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 des Anschlusses 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 kryptographischer Verfahren
Datenschutz bei technikunterstützten Verfahren der Personal- und Haushaltsbewirtschaftung
Common Criteria Protection Profile - Software zur Verarbeitung von personenbezogenen Bilddaten
Datenschutzgerechter Einsatz von RFID
Datenschutz und Datensicherheit in Projekten: Projekt- und Produktivbetrieb
Protokollierung
Biometrische Authentisierung - Möglichkeiten und Grenzen

Weitere Informationen im Internet:

(u. a. auch die Beiträge von den jährlichen Datenschutz-Fachtagungen ab 2005)

www.datenschutz-mv.de
www.informationsfreiheit-mv.de
www.bfdi.bund.de
www.datenschutz.de (Virtuelles Datenschutzbüro)