

UNTERRICHTUNG

durch den Landesbeauftragten für Datenschutz und Informationsfreiheit

**Zehnter Tätigkeitsbericht gemäß § 33 Abs. 1 Landesdatenschutzgesetz
Mecklenburg-Vorpommern (DSG M-V)**

Fünfter Tätigkeitsbericht gemäß § 38 Abs. 1 Bundesdatenschutzgesetz (BDSG)

**Dritter Tätigkeitsbericht nach dem Informationsfreiheitsgesetz
Mecklenburg-Vorpommern (IFG M-V)**

Berichtszeitraum: 1. Januar 2010 bis 31. Dezember 2011

Vorwort

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern hat dem Landtag und der Landesregierung für jeweils zwei Kalenderjahre einen Bericht über seine Tätigkeit vorzulegen.

Der Zehnte Tätigkeitsbericht gemäß § 33 Abs. 1 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V), der Fünfte Tätigkeitsbericht gemäß § 38 Abs. 1 Bundesdatenschutzgesetz (BDSG) sowie der Dritte Tätigkeitsbericht nach dem Informationsfreiheitsgesetz Mecklenburg-Vorpommern (IFG M-V) umfassen den Zeitraum vom 1. Januar 2010 bis zum 31. Dezember 2011. Dabei sind die Beiträge nach dem DSG M-V und nach dem BDSG nicht separat aufgeführt, weil es schon seit einiger Zeit bei etlichen Sachverhalten fachliche Überschneidungen gibt, sodass die Themen im Zusammenhang betrachtet werden.

Die hier dargestellten Vorgänge sollen 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.

Reinhard Dankert

Landesbeauftragter für Datenschutz
und Informationsfreiheit Mecklenburg-Vorpommern

Inhaltsverzeichnis		Seite
0.	Einleitung	7
1.	Empfehlungen	9
1.1	Zusammenfassung aller Empfehlungen	9
1.2	Umsetzung der Empfehlungen des 9. Tätigkeitsberichtes	11
2.	Tätigkeitsschwerpunkte	15
2.1	Datenschutz ist Bildungsaufgabe	15
2.2	Soziale Netze	17
2.2.1	Facebook & Co.	17
2.2.2	Darf die Polizei soziale Netzwerke nutzen?	20
2.2.3	Fachtagung 2011: Privatsphäre - die nächste Generation	21
2.2.4	Projekt „Netzwerkstar“ - Computerspiel für Kinder	22
3.	Entwicklung des Datenschutzrechts	23
3.1	Europarecht	23
3.1.1	Neuer europäischer Rechtsrahmen	25
3.1.2	Artikel-29-Gruppe - Datenschutzkoordinierung in Europa	26
3.2	Bundesrecht	27
3.2.1	Beschäftigtendatenschutz	27
3.2.2	BDSG Novelle - Neue Regelungen zu Auskunfteien und zum Scoring	28
3.2.3	Novellierung des Internetrechts erforderlich	29
3.2.4	Änderung des Bundesverfassungsschutzgesetzes	31
3.2.5	Elektronischer Entgeltnachweis ELENA	32
3.2.6	De-Mail: Vorsicht bei sensiblen Daten!	34
3.2.7	IT-Planungsrat	37
3.2.8	Stiftung Datenschutz	38
3.3	Neue Entwicklungen im Landesrecht	39
3.3.1	Landesdatenschutzgesetz	39
3.3.2	Sicherheits- und Ordnungsgesetz	42
3.3.3	Landeskrankenhausgesetz	43
3.3.4	Klinisches Krebsregistergesetz	44
4.	Technik und Organisation	46
4.1	Neue Technologien	46
4.1.1	Datenschutzgerechtes Cloud-Computing - geht das?	46
4.1.2	IPv6 - neue Adressen für das Internet	48
4.1.3	Smart Meter - Energieverbrauchsmessung der Zukunft	50
4.1.4	Smartphone & Tablet PC im professionellen Einsatz	52
4.1.5	Sicheres Löschen von Daten	55
4.1.6	Biometrische Authentisierung mit Augenmaß	56

Inhaltsverzeichnis		Seite
4.2	Internet und E-Mail	58
4.2.1	Google Street View/Microsoft Streetside	58
4.2.2	Google Analytics - Wo warst Du surfen?	60
4.2.3	Das Internet vergisst nicht	61
4.2.4	Kontrolle des E-Mail-Verkehrs durch eine Gemeindevertretung	62
4.2.5	Umgang mit E-Mails am Arbeitsplatz	64
4.2.6	Fragwürdige Sicherheit mit SSL-Verschlüsselung	65
4.3	IT-Verfahren der Landesverwaltung	68
4.3.1	IP-Telefonie - Organisation verbesserungswürdig	68
4.3.2	Elektronisches Dokumentenmanagement in der Landesverwaltung (DOMEA®)	69
4.3.3	EPOS - Personaldatenverarbeitung in der Landesverwaltung	70
4.3.4	Anlasslose Kontrolle der Arbeitszeit durch Vorgesetzte	72
4.3.5	Das Elektronische Gerichts- und Verwaltungspostfach EGVP	73
4.3.6	IT-Management für die Landesverwaltung	74
4.3.7	Einsicht in die Protokolldaten bei Internetverkehr	75
4.3.8	Flüssiger Verkehr dank Bluetooth-Sensoren	76
4.4	Service Internet	78
4.4.1	Gewerbedienst online	78
4.4.2	Beschäftigtendaten im Internet	79
4.4.3	Wohngeldantrag online	80
4.4.4	Geburtsurkunden aus dem Rechner	81
4.5	Technologischer Datenschutz in der Medizin	83
4.5.1	Telemedizin	83
4.5.2	Anforderungen an Krankenhausinformationssysteme	85
4.5.3	KV SafeNet - eine Kommunikationslösung für Ärzte	86
4.6	Videoüberwachung	87
4.6.1	Polizeiliche Videoüberwachung in der Rostocker Innenstadt	87
4.6.2	„Spicken“ und „Schummeln“ verboten	87
4.6.3	Videoüberwachung in der Psychiatrie	88
4.6.4	Videoüberwachung in Unternehmen	89
4.6.5	„Nachbarschaftliche“ Videoüberwachung	90
4.6.6	Webcams	91
4.6.7	Mitarbeiterüberwachung	92
4.6.8	Videoüberwachung in Einkaufszentren	92
5.	Datenschutz in verschiedenen Rechtsgebieten	93
5.1	Rechtswesen	93
5.1.1	Handyortung und mehr	93
5.1.2	Überwachungskonzept für besonders rückfallgefährdete Sexual- und Gewaltstraftäter	94

Inhaltsverzeichnis	Seite	
5.2	Polizei/Ordnungsbehörden	95
5.2.1	Ahndung bei unerlaubten Datenabfragen	95
5.2.2	Zweifelsfälle bei der DNA-Analyse	96
5.2.3	Polizei: Uni soll Studenten erziehen	97
5.2.4	Übermittlung zusätzlicher Daten beim Lichtbildabgleich	98
5.2.5	Gemeinsame Telekommunikationsüberwachung der norddeutschen Bundesländer	99
5.3	Wer wird künftig sicherheitsüberprüft?	100
5.4	Einwohnerwesen/Kommunales	101
5.4.1	Visa-Warndatei und Änderung des Aufenthaltsgesetzes	101
5.4.2	Bioenergieverbund - Voraussetzungen für freiwillige Datenerhebungen	101
5.4.3	Personenbezogene Daten in einem Planfeststellungsbeschluss?	102
5.4.4	MfS-Überprüfung von Gemeindevertretern und kommunalen Wahlbeamten	104
5.4.5	Löschen von Informationen im Google-Cache	105
5.4.6	Melddaten an die Polizei	106
5.4.7	Der neue Personalausweis	107
5.4.8	Kopieren von Personalausweisen nur ausnahmsweise	109
5.4.9	Kreismusikschule: Dissonanzen bei der IT-Sicherheit	110
5.5	Zensus 2011	110
5.5.1	Anfragen und Petitionen	110
5.5.2	Prüfung von Erhebungsstellen	112
5.6	Finanzwesen	113
5.6.1	Steuer-ID	113
5.6.2	Gemeinsame Steuerdatenverarbeitung der norddeutschen Bundesländer	114
5.6.3	Elektronische Kommunikation mit der Finanzverwaltung	115
5.6.4	Ablösung der Lohnsteuerkarte	116
5.7	Medien und Telekommunikation	118
5.7.1	Vorratsdatenspeicherung	118
5.7.2	Recht am eigenen Bild	119
5.7.3	15. Rundfunkänderungsstaatsvertrag	120
5.8	Soziales	121
5.8.1	Kinder- und Jugendhilfe	121
5.8.2	Zuständigkeit für Hartz IV neu geregelt	123
5.8.3	Betriebliches Eingliederungsmanagement oder Fahrtauglichkeitsprüfung?	123
5.8.4	Akte auf dem Postweg verschwunden	125
5.9	Gesundheitswesen	126
5.9.1	Umgang mit Patientendaten	126
5.9.2	Zentrales Klinisches Krebsregister	129
5.10	Verarbeitung von Personalaktendaten	130
5.11	Verarbeitung von Schülerdaten	134
5.12	Datenschutz im Verein	135
5.12.1	„Schwarzes Brett“ als Pranger	135
5.12.2	Gruppenversicherungsverträge	136

Inhaltsverzeichnis		Seite
6.	Arbeitskreis „Technische und organisatorische Datenschutzfragen“	138
6.1	Turnusmäßige Sitzungen	138
6.2	Workshops des AK Technik	139
6.3	Gemeinsame Weiterbildung	140
6.4	Technology Subgroup - Zusammenarbeit auf europäischer Ebene	140
7.	Informationsfreiheitsgesetz Mecklenburg-Vorpommern (IFG M-V)	140
7.1	Novellierung des Informationsfreiheitsgesetzes Mecklenburg-Vorpommern	140
7.2	Fachtagung 2010: Informationsfreiheit - die nächste Generation	142
7.3	Open Data/Open Government	144
7.4	Verwaltungskosten für Auskünfte nach dem IFG M-V	146
7.5	Muss jede Information herausgegeben werden?	147
7.6	Immer Ärger mit den Kosten!	147
7.7	Auskunftsbegehren über Spenden an einen Sportverein	148
7.8	Einsicht in Zirkusunterlagen	149
8.	Organigramm	151
9.	Abkürzungsverzeichnis	152
10.	Stichwortverzeichnis	154
11.	Publikationen	162

0. Einleitung

Datenschutz und Informationsfreiheit haben im Berichtszeitraum 2010/2011 bei vielen Bürgerinnen und Bürgern an Bedeutung gewonnen. Dies spiegelt sich in allen Tätigkeitsbereichen meiner Behörde wider und wird auch durch die hier ausgewählten Sachverhalte deutlich. Als Landesbeauftragter für den Datenschutz mit der Zuständigkeit für Fragen des Datenschutzes im Verhältnis zwischen Bürgerinnen und Bürgern und öffentlicher Verwaltung, in meiner Funktion als Aufsichtsbehörde für den Datenschutz im Verhältnis zwischen Bürgerinnen und Bürgern und Unternehmen und auch in meiner Funktion als Landesbeauftragter für die Informationsfreiheit erreichen mich immer wieder sehr viele Anfragen zu allen Bereichen des täglichen Lebens, in denen das Grundrecht auf informationelle Selbstbestimmung bzw. das Recht auf Informationsfreiheit betroffen sein können.

Die im Berichtszeitraum verstärkte öffentliche Wahrnehmung des Datenschutzes und der Informationsfreiheit führte zu einem weiteren Anstieg von Anfragen und Petitionen der Bürgerinnen und Bürger. Auch wenden sich zunehmend öffentliche Stellen des Landes, Unternehmen, Verbände und Vereine an mich. Schwerpunkte dabei waren der Zensus 2011, die Videoüberwachung, gesundheitliche, soziale und personalrechtliche Sachverhalte, zahlreiche Themen rund um das Internet wie Google Street View, soziale Netze oder das neue Internetprotokoll IPv6 und nicht zuletzt technische Entwicklungen wie De-Mail, der neue Personalausweis oder Cloud-Computing. Vor allem die Informations- und Kommunikationstechnik entwickelt sich in außerordentlicher Geschwindigkeit. Die Nutzung von Internet, Mobiltelefonen, Navigationssystemen oder elektronischen Zahlungssystemen gehört inzwischen zum Alltag vieler Menschen. Insbesondere die junge Generation kann sich ein Leben ohne Smartphone und ohne ständige Erreichbarkeit in sozialen Netzen im Internet häufig nicht mehr vorstellen. Die moderne Technik birgt jedoch in zunehmendem Maße Gefahren für die Privatsphäre der Menschen. Für den Einzelnen wird es immer schwieriger, den Überblick über die eigenen Daten zu behalten. Entwickler und Betreiber von Informations- und Kommunikationstechnik sind mehr denn je gefordert, datenschutzfreundliche Produkte anzubieten.

Hier eröffnet sich ein neuer Tätigkeitsschwerpunkt für meine Behörde. Auch wenn Fragen der Öffentlichkeitsarbeit im Landesdatenschutzgesetz nur als sogenannte „Weitere Aufgaben und Befugnisse“ in § 33 Abs. 4 fast beiläufig erwähnt werden, erscheint mir die Vermittlung von Medienkompetenz und die Bildung in Sachen Datenschutz als zunehmend wichtige Aufgabe. In den kommenden Jahren wird die Prävention im Bereich des Datenschutzes weiterhin an Bedeutung gewinnen. Und auch der Wechsel des Amtsinhabers, der in diesen Berichtszeitraum fiel, ist immer eine gute Gelegenheit, um neue Schwerpunkte zu setzen oder die vom Amtsvorgänger schon anvisierte Richtung endgültig einzuschlagen.

An dieser Stelle möchte ich noch einmal die Gelegenheit nutzen, meinem Vorgänger im Amt, Karsten Neumann, herzlich zu danken. Er hat mir am 2. Dezember 2010 eine funktionsfähige Behörde mit motivierten und kompetenten Mitarbeiterinnen und Mitarbeitern übergeben. Und er hat den zuvor erwähnten Richtungswechsel bereits eingeleitet. Zahlreiche Beratungs- und Fortbildungsangebote der Behörde wurden unter seiner Federführung konzipiert.

Das betrifft nicht nur die inzwischen jährlich stattfindende Datenschutz-Fachtagung zu einem aktuellen Thema, die sich als ein breit akzeptiertes Informations- und Diskussionspodium für alle Interessierten aus den verschiedensten Bereichen etabliert hat. Es betrifft unter anderem auch die Zusammenarbeit mit den Universitäten und Hochschulen des Landes, die unter der Regie von Karsten Neumann erheblich intensiviert wurde.

Ein Beispiel für die erfolgreiche Zusammenarbeit mit den Universitäten und Hochschulen des Landes ist das Online-Spiel „Netzwerkstar“ (www.netzwerkstar.de), das meine Behörde gemeinsam mit Studenten der Hochschule Wismar im Rahmen des Projektes „Soziale Netzwerke im Internet“ entwickelt hat. Insbesondere Kinder und Jugendliche übersehen in der Regel noch nicht die Gefahren für die eigene Person und für Dritte, die sich speziell aus der Kommunikation über soziale Netze im Internet ergeben können. Dieses Spiel soll bereits Kinder im Alter von acht bis zwölf Jahren für den sorgsameren Umgang mit persönlichen Daten sensibilisieren und Hinweise zur datenschutzgerechten Anmeldung an soziale Netzwerke wie SchülerVZ oder Facebook geben. Es soll helfen, Risiken aufzuzeigen und persönliche Nachteile durch leichtfertigen Umgang mit persönlichen Daten zu vermeiden. Im Rahmen des Projektes wurde auch eine Online-Umfrage zur Nutzung sozialer Netzwerke im Internet bei Schülerinnen und Schülern im Alter von 8 bis 21 Jahren in Mecklenburg-Vorpommern durchgeführt. Sowohl die Ergebnisse der Umfrage als auch das Spiel stehen im Internet-Angebot unter www.datenschutz-mv.de zur Verfügung.

Aber auch der Gesetzgeber ist in der Pflicht, mit modernen Gesetzen auf die schnelle technische Entwicklung zu reagieren, um einen zeitgemäßen Rahmen für den vertrauenswürdigen und transparenten Umgang mit personenbezogenen Daten bereitzustellen.

In Mecklenburg-Vorpommern gibt es seit 1992 ein Landesdatenschutzgesetz (DSG M-V). Das Gesetz wurde im Laufe der Jahre einige Male novelliert, zuletzt im Mai 2011. Der Gesetzgeber reagierte damit nicht nur auf die zahlreichen Datenskandale in den zurückliegenden Jahren und auf die rasante technische Entwicklung, sondern auch auf die Anforderungen der Europäischen Kommission zur Unabhängigkeit der Datenschutzaufsicht. Nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ist vorgesehen, dass die entsprechenden Kontrollstellen (hier: der Landesbeauftragte für den Datenschutz) die ihnen zugewiesenen Aufgaben „in völliger Unabhängigkeit“ wahrzunehmen haben. Mit der Novellierung im Jahr 2011 wurde nicht nur die von der Kommission geforderte Unabhängigkeit realisiert, sondern das Landesdatenschutzgesetz wurde darüber hinaus auch im Hinblick auf einen effektiven Datenschutz an rechtliche und technische Entwicklungen angepasst. Mit der Definition des Gemeinsamen Verfahrens wurde insbesondere auf verschiedene Entwicklungen im Bereich des E-Government reagiert, bei denen viele Behörden zentrale Verfahrensbestandteile gemeinsam nutzen. Darüber hinaus enthält das Gesetz nun auch Bußgeldtatbestände bei Verstößen gegen Datenschutzvorschriften und die Obergrenze der Summen bei Schadensersatzansprüchen bei Verletzung der Rechte von Betroffenen wurde geändert. Zudem verlangt das Gesetz nun die Einrichtung eines Datenschutzbeirates als Beratungsgremium für den Landesbeauftragten für den Datenschutz.

Aber auch im Bereich der Informationsfreiheit gab es bemerkenswerte Entwicklungen. Ein Informationsfreiheitsgesetz (IFG M-V) gibt es in Mecklenburg-Vorpommern zwar schon seit 2006. Es galt zunächst jedoch befristet bis zum 30. Juni 2011. Im Mai 2011 wurde es novelliert und ist seit dem 11. Juli 2011 unbefristet in Kraft. Dabei wurden wichtige Erkenntnisse aus der Evaluation des Gesetzes im Jahr 2010 berücksichtigt (www.informationsfreiheit-mv.de). Positiv anzumerken ist, dass die Informationskostenverordnung (IFGKostVO M-V) überarbeitet worden ist und in diesem Zusammenhang auch einige Gebühren und Auslagen gesenkt worden sind.

1. Empfehlungen

1.1 Zusammenfassung aller Empfehlungen

Ich empfehle der Landesregierung, sich hinsichtlich der Umsetzung der Koalitionsziffer 390 bis 392 für ein breites Verständnis von Datenschutz als Bildungsherausforderung einzusetzen und hierzu interministeriell sowie in enger Kooperation mit dem Landesbeauftragten für Datenschutz und Informationsfreiheit vorzugehen (siehe Punkt 2.1).

Ich empfehle der Landesregierung, sich in Umsetzung der Ziffern 390 und 391 der Koalitionsvereinbarung gegenüber der Bundesregierung und dem Bundestag für eine unverzügliche Umsetzung der Richtlinie in nationales Recht einzusetzen (siehe Punkt 3.1).

Ich empfehle sowohl der Landesregierung als auch allen anderen öffentlichen Stellen unseres Bundeslandes, von der Einbindung von Social-Plugins und der Einrichtung von Fanseiten bis zur Klärung der offenen Fragen und bis zur datenschutzkonformen Ausgestaltung von sozialen Netzwerken abzusehen (siehe Punkt 2.2.1).

Ich empfehle der Landesregierung hinsichtlich des weiteren Abstimmungsverfahrens im Rat und im europäischen Parlament eine aktive, zwischen den Bundesländern koordinierte und kritische Begleitung des Prozesses zum neuen europäischen Rechtsrahmen für den Datenschutz. Dies insbesondere mit Blick auf die weitere Gewährleistung bisher in Deutschland gesicherter Datenschutzstandards, einen bisher vertretbaren Verwaltungsaufwand und einer bisher gesicherten (föderalen) Unabhängigkeit der Aufsichtsbehörden (siehe Punkt 3.1.1).

Ich empfehle der Landesregierung, den De-Mail-Dienst nur dann einzusetzen, wenn vorher geprüft wurde, ob ein ausreichendes Sicherheitsniveau erzielt werden kann. Insbesondere bei der Verarbeitung sensibler personenbezogener Daten sind zusätzlich Maßnahmen erforderlich, wie Ende-zu-Ende-Verschlüsselung und gegebenenfalls die qualifizierte elektronische Signatur (siehe Punkt 3.2.6).

Ich empfehle der Landesregierung, sich für die personelle und finanzielle Unabhängigkeit der geplanten Stiftung Datenschutz einzusetzen und darauf hinzuwirken (siehe Punkt 3.2.8).

Ich empfehle dem Landesgesetzgeber, bestehende Unklarheiten im jetzigen § 18 DSGVO M-V zu beseitigen und im dortigen § 42 eine Regelungsschwäche hinsichtlich der Zuständigkeit bei Ordnungswidrigkeiten nach dem SGB X bzw. nach dem TMG zu beseitigen (siehe Punkt 3.3.1).

Ich empfehle der Landesregierung, Cloud-Dienste allenfalls von solchen Cloud-Anbietern in Anspruch zu nehmen, die dem europäischen Datenschutzrecht unterliegen und die Vorgaben der Orientierungshilfe Cloud-Computing vollständig berücksichtigen. Die Landesregierung sollte zudem prüfen, ob der IT-Landesdienstleister DVZ M-V GmbH mit der Schaffung einer Cloud für die Landes- und Kommunalverwaltung beauftragt werden kann (siehe Punkt 4.1.1).

Ich empfehle der Landesregierung, die Erforderlichkeit des Einsatzes von Smartphones und Tablet PC eingehend zu prüfen und die damit einhergehenden Risiken detailliert zu bewerten. In keinem Fall sollten diese Geräte ohne geeignete Administrationsumgebungen eingesetzt werden, die einerseits eine klare Trennung zwischen dienstlicher und privater Nutzung ermöglichen und andererseits die Administrationsmöglichkeiten der Nutzer wirkungsvoll verhindern oder zumindest erheblich einschränken. Die Anbindung solcher Geräte an Cloud-Strukturen ist allenfalls unter den Bedingungen möglich, die ich in Punkt 4.1.1 beschrieben habe (siehe Punkt 4.1.4).

Ich empfehle der Landesregierung, die Hinweise der Broschüre bei der Planung und beim Einsatz biometrischer Verfahren zu berücksichtigen. Vor dem Einsatz biometrischer Verfahren zur Authentisierung und Identifizierung von Personen sollte allerdings sorgfältig geprüft werden, ob nicht Verfahren mit geringerer Eingriffstiefe den gleichen Zweck erfüllen (siehe Punkt 4.1.6).

Ich empfehle der Landesregierung, regelmäßig zu prüfen, ob alle Details von Verträgen, die mit IT-Dienstleistern ausgehandelt wurden, eingehalten werden. Ebenso sollte regelmäßig geprüft werden, ob die in Dienstvereinbarungen festgeschriebenen Rechte und Pflichten vollständig umgesetzt werden (siehe Punkt 4.3.1).

Ich empfehle der Landesregierung, das IT-Managementsystem auf die gesamte Landesverwaltung auszudehnen, um auf der Basis geordneter und transparenter Managementprozesse auch ein zuverlässiges und robustes Datenschutzmanagement realisieren zu können. Der Pilotbetrieb sollte schnellstmöglich in einen stabilen Produktivbetrieb überführt werden. Vorrangig sollten die wesentlichen Kernprozesse einer solchen Management-Lösung einheitlich für die gesamte Landesverwaltung realisiert werden (siehe Punkt 4.3.6).

Ich empfehle der Landesregierung, sich dafür einzusetzen, dass eine einheitliche Handhabung beim Aufbau und der Formulierung der Attribute für elektronische Personenstandsregister oder sogar für alle behördlichen Signaturen realisiert wird. Darüber hinaus sollte geprüft werden, wo in Anlehnung an die Definition der Elektronischen Form in § 126 a BGB eine einheitliche Festlegung aufzunehmen ist, dass und wie in dem zu signierenden Personenstands-Dokument der Name des Standesbeamten (und ggf. der Behörde) hinzugefügt wird (siehe Punkt 4.4.4).

Ich empfehle der Landesregierung, gegenüber den Behörden und öffentlichen Stellen im Land sowie der Landespolizei sicherzustellen, dass die automatisierte Datenübermittlung im Sinne des § 31 Abs. 10 LMG über das ZIR erfolgt, und gegebenenfalls die hierfür erforderlichen Schritte einzuleiten (siehe Punkt 5.4.6).

Ich empfehle der Landesregierung, sich dafür einzusetzen, dass Berechtigungszertifikate für die Nutzung des neuen Personalausweises für Anwendungen im öffentlichen Bereich und insbesondere bei den Kommunen vom Bundesverwaltungsamt kostenlos erteilt werden (siehe Punkt 5.4.7).

Ich empfehle der Landesregierung, sich dafür einzusetzen, dass für den praktischen Vollzug der Regelungen des 15. Rundfunkänderungsstaatsvertrages Konkretisierungen und Differenzierungen vorgenommen werden bzw. diese auf einer Ebene unterhalb des Staatsvertrages unter Berücksichtigung der genannten elementaren datenschutzrechtlichen Grundsätze geregelt werden. Auch im Hinblick auf die geplante Evaluierung des Modellwechsels empfehle ich der Landesregierung, darauf hinzuwirken, dass die vorgetragenen datenschutzrechtlichen Belange, insbesondere hinsichtlich der Erhebung und Verarbeitung personenbezogener Daten sowie der Einhaltung des Grundsatzes der Verhältnismäßigkeit, überprüft werden und ich hierbei mit einbezogen werde (siehe Punkt 5.7.3).

1.2 Umsetzung der Empfehlungen des Neunten Tätigkeitsberichtes

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt
1	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.	Der Bundesbeauftragte und die Landesbeauftragten für den Datenschutz werden jetzt angemessen in die Arbeit des IT-Planungsrates einbezogen (siehe Punkt 3.2.7).	2.1.3
2	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.	Die Landesregierung hat erklärt, meiner Empfehlung folgen zu wollen. Weitere Aktivitäten sind mir nicht bekannt.	2.1.4
3	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.	Das Innenministerium hat hierzu am 8. März 2010 die EG-Dienstleistungsrichtlinien-Verfahrensverordnung erlassen. Hierin sind (obwohl eingefordert) keine Regelungen zur qualifizierten elektronischen Signatur getroffen worden.	2.1.8
4	Ich empfehle der Landesregierung, §§ 34 Abs. 6 i. V. m. Abs. 5 SOG M-V in der Novellierung des Sicherheits- und Ordnungsgesetzes zu berücksichtigen.	Eine entsprechende Änderung ist in der Novellierung erfolgt.	2.2.2

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt
5	Ich empfehle der Landesregierung, darauf hinzuwirken, dass durch den zuständigen parlamentarischen Gesetzgeber eine normenklare und verhältnismäßige gesetzliche Grundlage zur Videoüberwachung im Straßenverkehr geschaffen wird.	Dieses ist nicht erfolgt. Nach wie vor, wird sich bei Videoüberwachungsmaßnahmen im Straßenverkehr auf die Regelungen des § 46 Abs. 1 OWiG in Verbindung mit § 100 h StPO bezogen. Eine Änderung dieser Vorgehensweise ist aufgrund einer im Nachgang ergangenen Entscheidung des Bundesverfassungsgerichts vom 12. August 2010 (2BVR 1447/10) nicht zu erwarten.	2.2.3
6	Ich empfehle der Landesregierung deshalb, darauf hinzuwirken, dass künftige Wahltermine so festgelegt und veröffentlicht werden, dass eine fristgerechte Bekanntmachung der Widerspruchsmöglichkeit durchgeführt werden kann.	Die Landesregierung erklärte, der Empfehlung Folge zu leisten, soweit dem nicht besondere Hinderungsgründe entgegenstehen.	2.4.4
7	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.	Die Landesregierung verweist an dieser Stelle auf eine Unterstützung der Kommunen durch den Zweckverband Elektronische Verwaltung M-V. Dieses reicht meines Erachtens nicht aus, zumal nicht alle Verwaltungen Mitglied in diesem Zweckverband sind.	2.4.8
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.	- siehe Umsetzungsstand zu Punkt 7 Zum Einsatz von Lesegeräten mit eigenem Tastaturfeld verweist die Landesregierung lediglich auf die Inhalte einer Informationsbroschüre, die jedem Antragsteller auszuhändigen ist.	2.4.9

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt
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.	Die Landesregierung hält die materiellen Vorschriften in der Grundbuchordnung für ausreichend und erachtet eine Prüfungskompetenz des Landesdatenschutzbeauftragten im Bereich der Rechtspflege bei Gerichten für nicht erforderlich. Der Empfehlung wurde nicht gefolgt.	2.4.10
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.	Da sich bei den in den Finanzämtern durchgeführten Geschäftsprüfungen zum Kontenabruf keine Beanstandungen ergeben haben und keine Anhaltspunkte dafür bestehen, dass von dem Instrument des Kontenabrufs nicht in ebenso umsichtiger wie rechtlich zulässiger Weise Gebrauch gemacht wird, wurde der Empfehlung nicht gefolgt.	2.7.3
11	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.	Die Landesregierung will weiterhin kein landeseigenes Audit-Verfahren, sondern auf die Bundesstiftung Datenschutz warten. Obwohl die Stiftung mittlerweile existiert, sind ihre finanzielle Ausstattung und ihr Aufgabenprofil immer noch unklar (siehe Punkt 3.2.8).	2.10.5
12	Ich empfehle der Landesregierung, vor dem Einsatz von EPOS in jeder Dienststelle das behörden-spezifische 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.	Die Landesregierung hat eine Prüfung der Datenbankverschlüsselung in Aussicht gestellt. Über etwaige Ergebnisse ist mir jedoch nichts bekannt. Im Übrigen wurden meine Empfehlungen umgesetzt.	2.11.6
13	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.	Die Voraussetzungen für den Einsatz der qualifizierten elektronischen Signatur sind gegeben. Diese Technik wird jedoch nach wie vor kaum eingesetzt und ihr Einsatz wird von der Landesregierung nicht gefördert.	2.14.3

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt
14	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.	Das Projekt befindet sich in der Pilotphase. Ein stabiler Produktivbetrieb findet noch nicht statt.	2.14.4
15	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.	Mir sind keine Aktivitäten der Landesregierung bekannt, anhand derer eine wesentliche Verbesserung auf diesem Gebiet festzustellen wäre.	2.14.5
16	Ich empfehle der Landesregierung, die öffentlichen Stellen des Landes für eine datenschutzgerechte Ausgestaltung der Webseitenprotokollierung mit entsprechender Anonymisierung zu sensibilisieren.	Die Landesregierung lässt bei ihren eigenen Webservern, die vom DVZ im Auftrag betrieben werden, die IP-Adressen datenschutzgerecht anonymisieren. Aktivitäten in anderen Bereichen sind nicht bekannt.	2.14.6
17	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.	2011 ist ein neues, verbessertes De-Mail-Gesetz verabschiedet worden (siehe Punkt 3.2.6). Einige datenschutzrechtliche Kritikpunkte sind geblieben.	2.14.7
18	Ich empfehle der Landesregierung, die Kernausagen der Orientierungshilfen des AK Technik in ihre entsprechenden Planungsgrundsätze, etwa das IT-Sicherheitsrahmen-Konzept der Landesverwaltung, zu übernehmen und somit verbindlich einzuführen.	Die Landesregierung lehnt die Empfehlung ab.	2.14.8
19	Ich empfehle der Landesregierung, die „Besonderen Beförderungsbedingungen“ um eine entsprechende Regelung zu ergänzen und dabei eine Lösungsfrist von einem Jahr vorzusehen.	Eine entsprechende Regelung wurde in den „Besonderen Beförderungsbedingungen“ gültig ab 1. Dezember 2010 mit einer Lösungsfrist von zwei Jahren aufgenommen. Die Regelungen wurden mit dem Landesdatenschutzbeauftragten abgestimmt. Das Landesamt für Straßenbau und Verkehr hat auf Grund des § 1 Abs. 1 der Verordnung über die Allgemeinen Beförderungsbedingungen (AllgBefBed) den Abweichungen von den AllgBefBed zugestimmt.	3.6

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt
20	Ich empfehle der Landesregierung sicherzustellen, dass von einer Sperrklärung nur unter den in § 99 VwGO aufgeführten strengen Voraussetzungen Gebrauch gemacht wird.	Die Landesregierung erklärte, dass sie sicherstellen wird, dass von einer Sperrklärung nur unter den in § 99 Abs. 1 Satz 2 VwGO aufgeführten strengen Voraussetzungen Gebrauch gemacht wird. Da zu Sperrklärungen im aktuellen Berichtszeitraum keine weiteren Petitionen eingereicht wurden, kann nicht eingeschätzt werden, ob dies tatsächlich der Fall ist.	2.
21	Ich empfehle der Landesregierung sicherzustellen, dass die Anwendbarkeit des IFG M-V für den Bereich der Finanzverwaltung gewährleistet ist.	Die Landesregierung erklärte in ihrer Stellungnahme zum 2. Tätigkeitsbericht, dass sie an ihrer Auffassung, Finanzbehörden (soweit sie in Steuer-sachverfahren tätig sind) vom Anwendungsbereich des IFG M-V auszunehmen, festhält. Es wurde indes aber auf eine diesbezüglich geplante Änderung des IFG M-V verzichtet.	3.
22	Ich empfehle der Landesregierung, die Informationskostenverordnung dahingehend zu ändern, dass die bisherigen Kostenpositionen bürgerfreundlicher gestaltet werden.	Das Innenministerium überarbeitet derzeit die Kostenverordnung. Dabei ist (anlehnend an die Kostenverordnung für das Bundes-IFG) vorgesehen, die Maximalgebühren erheblich zu reduzieren.	7.

2. Tätigkeitsschwerpunkte

2.1 Datenschutz ist Bildungsaufgabe

Bisherige Erfahrungen zeigen, dass Verstöße gegen das Recht auf informationelle Selbstbestimmung überwiegend auf schlichter Unkenntnis bzw. nicht zweckentsprechender Auslegung der einschlägigen Rechtsregelungen beruhen. Hinzu kommt mangelnde Kenntnis von Verbraucherrechten und von der Tragweite getroffener Entscheidungen mit Auswirkungen unter anderem auf den Datenschutz.

So wird im Beschluss der 82. Konferenz der Datenschutzbeauftragten von Bund und Ländern vom 21. September 2011 „Datenschutz als Bildungsaufgabe“ ausgeführt:

„Vielen sind die Grundlagen, Funktionsbedingungen und wirtschaftlichen Spielregeln des Internet nicht oder nur zum Teil bekannt. Die meisten Internetnutzerinnen und -nutzer haben außerdem den Überblick darüber verloren, wer wann und zu welchem Zweck welche Daten von ihnen speichert, sie mit anderen Datensätzen verknüpft und ggf. auch an Dritte weitergibt. Wer aber nicht weiß, was mit seinen Daten geschieht oder geschehen kann, kann auch das informationelle Selbstbestimmungsrecht nicht effektiv ausüben.“

Um dieser Entwicklung entgegenzuwirken, muss der Datenschutz auch als Bildungsaufgabe verstanden und praktiziert werden. Es genügt nicht, allein auf rechtliche Regelungen sowie auf datenschutzfreundliche technische Voreinstellungen und Anwendungen zu setzen. Die digitale Aufklärung ist unverzichtbar als Teil einer Datenschutzkultur des 21. Jahrhunderts. Sie beinhaltet zum einen die Vermittlung von Wissen und zum anderen die Entwicklung eines wachen, wertebezogenen Datenschutzbewusstseins.

So wie Bildung eine gesamtgesellschaftliche Aufgabe ist, so ist auch die Bildung im Hinblick auf die Datenschutzfragen unserer Zeit eine Aufgabe, die nicht nur dem Staat, sondern ebenso der Wirtschaft und der Zivilgesellschaft wie auch den Eltern im Verhältnis zu den Kindern obliegt ...

Digitale Aufklärung und Erziehung zum Datenschutz bestimmen letztlich auch über den Stellenwert, den Privatsphäre und Persönlichkeitsrecht und damit Menschenwürde und Demokratie künftig in der internetgeprägten Gesellschaft insgesamt haben werden.“

In Umsetzung dieses Beschlusses und der Koalitionsvereinbarung in den Ziffern 390 bis 392 wurde daher in Abstimmung mit zahlreichen Kooperationspartnern auch auf Landesregierungsebene ein umfangreiches und differenziertes Maßnahmenpaket entwickelt, das als Bildungsoffensive insbesondere auf die Zielgruppe der jungen Menschen in Mecklenburg-Vorpommern ausgerichtet ist.

Im Rahmen dieser Bildungsoffensive sollen insbesondere mit ausgewählten Schülern unterschiedlicher Jahrgangsstufen, mit Lehrern an allgemeinbildenden Schulen und mit Schulsozialarbeitern Schulungs- bzw. Fortbildungsprojekte durchgeführt werden, um diese dann in die Lage zu versetzen, als Multiplikatoren im Bereich Schule selbst Datenschutzbildungsmaßnahmen durchführen zu können. Des Weiteren sollen in Umsetzung der Ziffer 392 der Koalitionsvereinbarung die Lehrpläne der Bereiche Schule, Hochschule sowie Aus-, Fort- und Weiterbildung um das Thema „Datenschutz“ ergänzt werden, um auch auf curricularer Ebene der soeben skizzierten Bildungsaufgabe zu entsprechen.

In Ergänzung dieser Projekte und Maßnahmen werde ich auch weiterhin mit verstärkten Mitteln Schulungen und Informationsveranstaltungen für Schüler, Lehrer und Eltern an Schulen anbieten, um dem dortigen Bedarf noch besser zu entsprechen. Zudem werden Multiplikatoren mit jugendaffinen Tätigkeiten (Erzieher, Sozialarbeiter, soziale Fachkräfte etc.) in den entsprechenden Fort- und Weiterbildungseinrichtungen des Landes regelmäßig im Bereich Datenschutz geschult bzw. zu Lehrveranstaltungen eingeladen. Gleiches gilt für geplante vor-Ort-Workshops und -Seminare bei großen Trägern der Jugendhilfe oder in vergleichbaren Jugendeinrichtungen.

Bewährt haben sich in den vergangenen Jahren Schulungsangebote des Landesbeauftragten an den Hochschulen im Lande für Studenten einschlägiger Studiengänge. So wurden an der Universität Rostock und an der Hochschule Wismar in beiden Berichtsjahren mehrtägige Blockseminare für Studierende der Informatik durchgeführt, die auch künftig angeboten werden.

Auch am Kommunalen Studieninstitut wurden und werden auch künftig durch den Landesbeauftragten Schulungsmaßnahmen im technischen und rechtlichen Datenschutzbereich durchgeführt, die sich gezielt an Multiplikatoren in der öffentlichen Verwaltung richten.

Der große Zuspruch zu den in diesem Berichtszeitraum durchgeführten Datenschutz-Fachtagungen zu den Themen Informationsfreiheit und soziale Netze im Internet (jeweils rund 150 Teilnehmer) ermutigt zur Beibehaltung dieses wichtigen Informations- und Vernetzungsinstrumentes nicht nur für Multiplikatoren. Die auch künftig stattfindenden Fachtagungen werden sich thematisch auch weiterhin an aktuellen Fragestellungen des Datenschutzes bzw. der Informationsfreiheit orientieren.

Ich empfehle der Landesregierung, sich hinsichtlich der Umsetzung der Koalitionswertungen 390 bis 392 für ein breites Verständnis von Datenschutz als Bildungsherausforderung einzusetzen und hierzu interministeriell sowie in enger Kooperation mit dem Landesbeauftragten für Datenschutz und Informationsfreiheit vorzugehen.

2.2 Soziale Netze

2.2.1 Facebook & Co.

Soziale Netzwerke im Internet wie MeinVZ, StudiVZ, StayFriends oder Facebook haben sich binnen weniger Jahre in der Gesellschaft etabliert. Sie sind zu einem Massenmedium geworden, welches heute einen großen Teil der Bevölkerung anspricht und auch abbildet. Bei dem weltweit größten Online-Netzwerk Facebook sind in Deutschland laut einer aktuellen Studie mehr als 72,7 Prozent der deutschen Internet-Nutzer im Alter über 15 Jahren angemeldet. Genutzt werden soziale Netzwerke vor allem für die Kontaktpflege und den Austausch von Informationen zwischen Freunden und Bekannten. Jeder Nutzer legt ein sogenanntes Profil über sich selbst an, mit dem er zahlreiche persönliche Daten preisgibt. Das Angebot persönlicher Profile und die vermeintlich unkomplizierte Kommunikation über oftmals frei einsehbare Statusmeldungen verleiten viele Menschen zu einer bislang nicht gekannten Form der Selbstdarstellung. Vor allem unerfahrene Internetnutzer erliegen der Versuchung, sich und ihre Lebensumstände detailliert und offen im Netz zu präsentieren. Damit werden ihre Daten für Suchmaschinen und eine wachsende Zahl professioneller Datensammler verfügbar, welche daraus unbemerkt immer präzisere Persönlichkeits- und Beziehungsprofile erstellen können. Dass die bei Facebook eingestellten Daten in die USA übermittelt und dort gespeichert werden, wissen viele Nutzer jedoch nicht.

Soziale Netzwerke sind inzwischen auch für Unternehmen zu einem offenbar wichtigen Marketinginstrument geworden. Mit Hilfe sogenannter Fan-Pages werben Unternehmen für ihre Produkte oder unterbreiten Job-Angebote.

Durch das Einbinden von sogenannten Social-Plugins wie dem „Gefällt-mir“-Button in Fan-Pages aber auch in eigene Webseiten werden Nutzer ermuntert, das Webangebot oder einzelne Produkte zu bewerten oder anderen Facebook-Nutzern zu empfehlen. Facebook analysiert diese Bewertungen hauptsächlich mit Hilfe von Cookies, die auf dem Rechner des Nutzers abgelegt werden, und liefert den Webseitenbetreibern aussagekräftige Nutzungsstatistiken und Reichweitenanalysen. Vor allem aber ist Facebook aufgrund dieser Technik in der Lage, die Nutzer selbst zu analysieren, denn Facebook kann nachvollziehen, wer sich wie lange auf welcher Webseite aufgehalten hat. Durch die Auswertung des Nutzerverhaltens und die Zusammenführung dieser Daten mit den Daten, die die Nutzer selbst in ihrem persönlichen Profil hinterlegt haben, lassen sich sehr detaillierte individuelle Nutzungsprofile erstellen. Mit dem Verkauf dieser Profile an private Unternehmen ist sehr viel Geld zu verdienen, da sich diese Informationen für zielgruppenorientierte Werbung hervorragend eignen.

In zunehmendem Maße entdecken auch politische Parteien und öffentliche Stellen Facebook für ihre Zwecke. Politiker scheinen überzeugt davon zu sein, dass sie über Facebook Wählerschichten erreichen, zu denen sie bisher nur wenig Zugang hatten. Die Polizei unseres Landes bittet auf der eigenen Fan-Page beispielsweise um Mithilfe bei der Aufklärung von Straftaten oder bei der Suche nach Vermissten und veröffentlicht eigene Stellenausschreibungen.

Attraktiv für alle Facebook-Nutzer ist die Tatsache, dass die Dienste kostenlos angeboten werden. Dass das Angebot jedoch nicht kostenlos ist, durchschauen viele Nutzer nicht. Denn bezahlt wird mit der neuen Währung des Informationszeitalters - mit personenbezogenen Daten. Und jeder Nutzer überlässt Facebook zahlreiche personenbezogene Daten. Dazu gehören nicht nur die im Profil gespeicherten Daten wie Fotos, Videos, Kontakte und persönliche Meinungen, sondern auch alle Daten, die bei einem Besuch und bei einer Bewertung verschiedenster Web-Seiten anfallen.

Nur wenige Nutzer stellen sich die Frage, was mit diesen Daten wo passiert oder worin für Facebook eigentlich der Nutzen eines kostenlosen Netzwerkes besteht. Kaum jemand sieht neben den unbestrittenen Vorteilen von Facebook auch die Risiken der Nutzung, zum Beispiel im Hinblick auf die Privatsphäre, also das Recht auf informationelle Selbstbestimmung.

Diese und weitere Fragen beschäftigen die Datenschutzbeauftragten des Bundes und der Länder schon geraume Zeit. Auch haben immer wieder neue Funktionalitäten bei Facebook Anlass gegeben, die Datenverarbeitung bei Facebook unter datenschutzrechtlichen Gesichtspunkten genauer zu untersuchen. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat beispielsweise das Verfahren von Facebook zur biometrischen Gesichtserkennung untersucht und erhebliche Datenschutzverstöße festgestellt. Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) hat die oben beschriebene Reichweitenanalyse von Facebook datenschutzrechtlich bewertet. Die technische und rechtliche Untersuchung hat gezeigt, dass diese Analysen nach Einschätzung der Datenschutzbehörden gegen das Telemediengesetz (TMG) und das Bundesdatenschutzgesetz (BDSG) bzw. die jeweiligen Landesdatenschutzgesetze verstoßen.

Ich teile wie meine Kollegen von Bund und Ländern die Auffassung, dass diese Analysen mit deutschem Datenschutzrecht nicht vereinbar sind. Diese Datenverarbeitung ist aus mehreren Gründen unzulässig. Werden bei der Bereitstellung von Telemedien - und soziale Netze wie Facebook sind solche Dienste - personenbezogene Daten verarbeitet, ist eine datenschutzrechtlich wirksame Einwilligung des Nutzers erforderlich (§ 12 Abs. 1 TMG, § 4a BDSG). Entgegen der Darlegung von Facebook ist der Nutzer nicht in der Lage, bei der Registrierung und ersten Anmeldung an Facebook zu übersehen, in welcher ganz konkreten Weise seine Daten verarbeitet werden, sodass mit der Anmeldung gerade keine wirksame Einwilligung vorliegt. Erst recht unzulässig ist natürlich die Verarbeitung der Daten von Nutzern, die keine Facebook-Mitglieder sind.

Auch eine Bildung von Nutzungs-Profilen ist unzulässig. Zwar dürfen gemäß § 15 Abs. 3 TMG zum Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellt werden. Voraussetzung ist jedoch, dass der Nutzer dem nicht widerspricht. Auf dieses Widerspruchsrecht hat der Diensteanbieter den Nutzer hinzuweisen. Die Betreiber von deutschen Fan-Pages sind jedoch derzeit technisch gar nicht in der Lage, eine solche Widerspruchsmöglichkeit anzubieten. Ohne dass den Nutzern ein Wahlrecht zugestanden wird und ohne hinreichende Informationen werden mit Hilfe der oben genannten Cookies Profile gebildet. Dies betrifft sowohl Facebook-Mitglieder - unabhängig davon, ob sie gerade angemeldet sind oder nicht - als auch schlichte Nutzer, die keine Facebook-Mitglieder sind.

Schließlich ist in § 15 Abs. 3 Satz 3 TMG geregelt, dass die erstellten Nutzungsprofile nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden dürfen. Indem man die mit Hilfe der Cookies gebildeten, zunächst pseudonymen Nutzungsstatistiken mit den persönlichen Profilen der Nutzer zusammenführt und somit namentlich zuordnet, wäre auch dieser Tatbestand erfüllt. Einiges spricht dafür, dass Facebook eine solche Zusammenführung durchführt, eine eindeutige Klärung dieser Frage wird jedoch wohl erst im Zuge der derzeitigen Prüfung durch den Irischen Datenschutzbeauftragten erfolgen.

Auch wenn Facebook seinen Hauptsitz nicht in Deutschland hat, unterliegt Facebook hinsichtlich der Daten von Betroffenen in Deutschland gemäß § 1 Abs. 5 Satz 2 BDSG dem hiesigen Datenschutzrecht, soweit die Datenerhebungen durch Rückgriff auf Rechner von deutschen Nutzern realisiert werden, also die Erhebung und Verarbeitung von deutschen Nutzerdaten erfolgt.

Auch die Datenschutz-Aufsichtsbehörden für den nicht-öffentlichen Bereich („Düsseldorfer Kreis“) haben sich daher mit Datenschutzfragen bei Facebook befasst und mit ihrem Beschluss vom 8. Dezember 2011 (siehe http://www.datenschutz-mv.de/dschutz/ddk/ds_soz_netzw.html) auf die wesentlichen Eckpunkte des geltenden Rechts hingewiesen sowie die eigene Verantwortung der deutschen Webseitenbetreiber beim Einbinden von Social-Plugins oder beim Präsentieren von Fan-Pages verdeutlicht. Die 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte zuvor in ihrer EntschlieÙung vom 28./29. September 2011 (siehe http://www.datenschutz-mv.de/dschutz/beschlue/82_DSK/Nutzerdaten.pdf) bereits alle öffentlichen Stellen aufgefordert, von der Nutzung von Social-Plugins abzusehen, die den geltenden Standards nicht genügen.

Ende Dezember 2011 hat der Irische Datenschutzbeauftragte einen Auditbericht über seine Datenschutzprüfung von Facebook Ireland Ltd. vorgelegt. Facebook hatte bereits im August 2011 über seine sehr umstrittene Auffassung informiert, dass allein die irische Niederlassung als verantwortliche Stelle für die Verarbeitung der Daten Facebooks im Sinne des europäischen Datenschutzrechts anzusehen sei und deshalb allein der Irische Datenschutzbeauftragte für die Datenschutzkontrolle zuständig sei.

Auch der Irische Datenschutzbeauftragte stellte erhebliche Datenschutzmängel fest und bestätigte im Wesentlichen die Ergebnisse der technischen Analysen des ULD. Insbesondere kritisierte er die unzulänglichen Informationen und fehlenden Wahlmöglichkeiten der Nutzer und bestätigte Datensammlungen über Mitglieder und Nichtmitglieder von Facebook. Er räumte dem Unternehmen eine Frist von sechs Monaten ein, um die Datenschutzmängel zu beseitigen.

Ich empfehle sowohl der Landesregierung als auch allen anderen öffentlichen Stellen unseres Bundeslandes, von der Einbindung von Social-Plugins und der Einrichtung von Fanseiten bis zur Klärung der offenen Fragen und bis zur datenschutzkonformen Ausgestaltung von sozialen Netzwerken abzusehen.

2.2.2 Darf die Polizei soziale Netzwerke nutzen?

Soziale Netzwerke geben ihren Nutzern die verschiedensten Möglichkeiten zu kommunizieren bzw. miteinander in Kontakt zu treten. Mehr als je zuvor sind heute personenbezogene Daten im Internet auffindbar. Ebenso groß wie das Angebot an Kommunikation und personenbezogenen Daten im Netz ist auch die strafrechtliche Relevanz von Informationen und Aktivitäten aus den sozialen Netzwerken. Somit eröffnen sich für die Polizei zahlreiche Betätigungsfelder und Informationsquellen. Neben der taktischen Vorbereitung von Maßnahmen (Observation, Durchsuchung) mit Hilfe von Informationen aus sozialen Netzwerken, ergreift die Polizei auch Maßnahmen zur Vorbeugung von Straftaten, indem sie sich auf Facebook mit einer eigenen Facebook-Fanpage an Facebooknutzer wendet.

Auch in Mecklenburg-Vorpommern hat die Polizei seit September 2011 als Pilotprojekt eine eigene Seite bei Facebook geschaltet. Dort wendet sie sich mit Zeugenaufrufen, Vermisstenmeldungen, Hinweisen, Pressemitteilungen und Ausschreibungen an die Facebook-Gemeinschaft.

Die Schaltung dieser Fan-Seite wird von mir kritisch bewertet und auf der Grundlage der bisherigen Erkenntnisse abgelehnt. Da sämtliche Facebook-Daten auf Servern in den USA gespeichert werden, ist zu befürchten, dass anhand der Daten über die Nutzer der Polizeiseiten umfassende Nutzungsprofile erstellt werden und damit die Wahrung des Rechts auf informationelle Selbstbestimmung nicht gewährleistet wird.

Problematisch ist insbesondere, dass von Facebook Cookies gesetzt werden, die zwei Jahre lang gespeichert werden und Aufschluss darüber geben, auf welcher Seite sich ein Nutzer zu welchem Zeitpunkt und wie lange aufgehalten hat. Mit Hilfe dieser Cookies kann Facebook also die Nutzungsdaten einem individuellen Facebook-Nutzer namentlich zuordnen und so ein individuelles Nutzungsprofil anlegen. Damit verstößt Facebook gegen das in § 15 Abs. 3 Satz 3 Telemediengesetz (TMG) festgelegte Trennungsgebot, das regelt, dass Nutzungsprofile nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden dürfen.

Einen weiteren Verstoß gegen das Telemediengesetz sehe ich darin, dass für die Verarbeitung der personenbezogenen Daten der Fan-Seite keine Einwilligung der Nutzer gemäß § 4 Abs. 1 BDSG, § 12 Abs. 1 TMG vorliegt. Ein Hinweis auf die Nutzungsbedingungen von Facebook reicht nicht aus, zumal diese nicht ausreichend transparent und bestimmt sind. Ein Nutzer muss auf den ersten Blick klar und eindeutig erkennen können, welche personenbezogenen Daten von wem, wo, für welchen Zweck und wie lange gespeichert werden.

Ich vertrete die Auffassung, dass die Polizei als öffentliche Stelle aufgrund des Legalitätsprinzips besonders verpflichtet ist und eine Vorbildfunktion hat. So muss sie sicherstellen, dass personenbezogene Daten gesetzeskonform verarbeitet werden. Das betrifft selbstverständlich auch den Umgang mit personenbezogenen Daten bei allen Formen der Nutzung sozialer Netzwerke. Meinen Standpunkt habe ich in einem persönlichen Gespräch mit Vertretern des Innenministeriums und der Landespolizei Mecklenburg-Vorpommern im Dezember 2011 erörtert. Die Vertreter des Innenministeriums und des Landeskriminalamtes haben auf die aus polizeilicher Sicht bestehenden Vorteile der Fan-Seite hingewiesen und mitgeteilt, dass sie die Seite zumindest bis zur Innenministerkonferenz im Februar 2012, auf der dieses Thema ebenfalls diskutiert wird, weiter betreiben.

Da die Frage nach der Anwendbarkeit des deutschen Rechts bei Verstößen seitens Facebook bzw. der Verantwortlichkeit zu Fanpage-Betreibern bzw. Social-Plugins-Benutzern bisher noch nicht gerichtlich entschieden ist, möglicherweise aber in baldigen Rechtsverfahren in Irland bzw. Schleswig-Holstein geklärt wird, werde ich diese Verfahren im Interesse einer bundesweit einheitlichen Vorgehensweise abwarten und dann erneut mit dem Innenministerium in Kontakt treten.

2.2.3 Fachtagung 2011: Privatsphäre - die nächste Generation

Soziale Netzwerke im Internet wie Facebook, MySpace oder studiVZ werden immer beliebter. Nicht nur Kinder und Jugendliche, auch Erwachsene nutzen solche Netzwerke, um z. B. auf bequeme Art und Weise Verabredungen zu treffen, Kontakte zu pflegen, Fotos einzustellen oder Erlebnisberichte zu veröffentlichen. Soziale Netzwerke im Internet bergen aber auch ein großes Missbrauchspotenzial in sich: Informationen werden mitunter ohne Wissen der Betroffenen eingestellt, Daten werden rechtswidrig für Werbezwecke genutzt und so mancher Arbeitgeber versucht, etwas über den künftigen Mitarbeiter zu erfahren. Auf der Fachtagung 2011 zum Thema „Privatsphäre - die nächste Generation“ an der Hochschule Wismar diskutierten unter anderem Datenschützer, Pädagogen, Wissenschaftler und Politiker über mögliche Auswirkungen dieser sozialen Netze auf die Privatsphäre.

Dr. Christiane Rohleder, Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz, ging in ihrem Vortrag „Privatsphäre im Wandel - Einflussmöglichkeiten der Politik“ darauf ein, dass soziale Netzwerke im Internet unser Leben tiefgreifend verändern. Dieser Wandel bringt Herausforderungen für alle gesellschaftlichen Kräfte mit sich.

Christian Hawellek, Universität Hannover, Institut für Rechtsinformatik, befasste sich in seinem Vortrag „Soziale Netzwerke - Angriff auf die Privatsphäre“ mit folgenden Fragen: Ist Privatsphäre eine soziale Norm der Vergangenheit, wie Mark Zuckerberg es einmal ausdrückte? Entsprechen damit auch die datenschutzrechtlichen Rechtsnormen nicht mehr der sozialen Wirklichkeit des 21. Jahrhunderts? Oder sind sie gerade deswegen wichtiger denn je?

Michael Baumann, Universität Leipzig, Institut für Linguistik, stellte in seinem Vortrag „Bis nachher im VZ - Forschungsergebnisse des Medienkonvergenz Monitorings“ die Ergebnisse der Studie vor. Im öffentlichen Diskurs und in politischen Debatten sorgt das Phänomen soziale Online-Netzwerke derzeit für Diskussionsbedarf, insbesondere mit Blick auf den Jugendmedienschutz, die Förderung von Medienkompetenz und Datenschutzfragen.

Prof. Dr. Hannes Federrath, Universität Hamburg, Fachbereich Informatik, erläuterte in seinem Vortrag „Das Internet vergisst nicht“ an Fallbeispielen die grundsätzlichen Möglichkeiten und Grenzen eines technischen Schutzes personenbezogener Daten.

Diese und weitere Beiträge zur Fachtagung sind zu finden unter www.datenschutz-mv.de.

2.2.4 Projekt „Netzwerkstar“ - Computerspiel für Kinder

Im Rahmen des Projektes „Identitätsmanagement in sozialen Netzwerken im Internet“ entstand gemeinsam mit Frau Prof. Dr. Antje Düsterhöft von der Hochschule Wismar die Idee, ein (Online-)Lernspiel zu entwickeln, anhand dessen Kinder die Anmeldung und die Nutzung eines sozialen Netzwerkes im Internet durchspielen können. Mit Hilfe dieses Lernspiels sollen ihnen spielerisch die Vor- und Nachteile der Offenlegung bestimmter persönlicher Informationen vor Augen geführt und eine Sensibilisierung für Gefahren und Risiken erreicht werden. Im Verlaufe des Jahres 2011 wurde diese Idee zügig realisiert und das Lernspiel ist als erfolgreiches und kostenloses Bildungsangebot für Kinder (und auch für deren Eltern) im Internet verfügbar (www.netzwerkstar.de).

Das Spiel soll in geeigneter Weise auf einen Beitritt zu sozialen Netzwerken wie SchülerVZ oder Facebook vorbereiten. Zudem zeigt es Risiken auf und hilft, persönliche Nachteile durch leichtfertigen Umgang mit persönlichen Daten zu vermeiden. Zielgruppe sind Kinder von 8 bis 12 Jahren. In diesem Alter findet häufig der erste Kontakt mit sozialen Netzwerken im Internet statt. Das Spiel kann (und soll) aber auch Erwachsenen dazu dienen, sich in die Thematik einzuarbeiten.

Im Quiz-Stil werden zehn Fragen zum Thema „soziale Netzwerke im Internet“ gestellt. Zu jeder Frage stehen drei Antworten zur Auswahl; beim Markieren einer Antwort erscheint ein Hinweistext mit Tipps oder Denkanstößen. Übernommen wird die Antwort erst durch eine ausdrückliche Bestätigung. Nach jeweils drei Fragen besteht die Möglichkeit, die Spielfigur optisch zu verändern. Die verfügbaren Styling-Optionen hängen vom Spielverlauf ab. Am Ende des Spiels erscheint abhängig von der Punktezahl entweder eine Aufforderung zum erneuten Spieldurchlauf oder die Möglichkeit zum Ausdrucken der Spielfigur als Urkunde. Über den Knopf „Auswertung“ kann eine Beurteilung der Antworten eingesehen werden. In der Online-Version unter www.netzwerkstar.de besteht zusätzlich die Möglichkeit, die Spielfigur auch als Bild-Datei zu speichern. Diese kann beispielsweise als Profilbild (sog. „Avatar“) in einem sozialen Netzwerk verwendet werden.

Öffentlich vorgestellt wurde das Spiel auf der KinderUni der Hochschule Wismar, wo über 200 Kindern der Umgang mit sozialen Netzwerken im Internet erläutert wurde (www.kinderuni-wismar.de). Sowohl Kinder als auch Familien freuten sich über das Spiel, welches sie auf einem USB-Stick am Ende der Uni-Vorlesung mitnehmen konnten.

Auch auf der Datenschutz-Fachtagung 2011 zum Thema „Privatsphäre - die nächste Generation“ sorgte die Vorstellung des Spiels für reges Interesse beim zahlreich erschienenen Fachpublikum (www.datenschutz-mv.de).

Im Ergebnis ist festzustellen, dass dieses Projekt sehr erfolgreich war. Das Lernspiel fand sehr große Resonanz, sodass eine Nachfolgeversion - Netzwerkstar II (für die darauffolgende Altersgruppe) - geplant ist.

3. Entwicklung des Datenschutzrechts

Auf der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im März 2010 haben sich alle Konferenzmitglieder auf unverzichtbare Eckpfeiler eines Datenschutzrechtes geeinigt und diese veröffentlicht in einer Broschüre mit dem Titel „Ein modernes Datenschutzrecht für das 21. Jahrhundert“. Bewusst enthält diese Broschüre nur erweiterungsfähige und konkretisierbare Eckpunkte, die keinen Anspruch auf Vollständigkeit erheben, aber für die gegenwärtige und künftige Gestaltung datenschutzrechtlicher Regelungen eine relevante Orientierung geben können. Die im Folgenden kurz zusammengefassten Eckpfeiler dienen alle einem schlichten Grundrecht: Jeder Mensch soll selbst bestimmen können, wer was wann über ihn weiß (Recht auf informationelle Selbstbestimmung).

Zur Gewährleistung dieses Grundrechtes empfehlen die Datenschutzbeauftragten des Bundes und der Länder, sowohl im einschlägigen Bundesrecht als auch im Landesrecht verbindliche Mindeststandards festzulegen. Sie sollten allgemeine Vorgaben enthalten, die als Grundlage aller datenschutzrechtlichen Regelungen und Maßnahmen für öffentliche und nicht-öffentliche Stellen dienen. Neu eingeführt werden sollte zudem ein grundsätzliches Verbot der Profilbildung. Des Weiteren sollen technikneutrale Vorgaben definiert werden, die für konkrete Systeme und Anwendungsfelder durch Auslegung und Normierung konkretisiert werden können. Zudem sind die Betroffenenrechte zu stärken. Die Datenverarbeitung muss für Betroffene transparenter werden, dies gilt sowohl für Einwilligungsprozedere als auch für Auskunftsverfahren. Die Konferenz empfiehlt darüber hinaus die verstärkte Anwendung des Prinzips „Mehr Eigenkontrolle statt Zwang“ (etwa durch die Einführung freiwilliger Auditverfahren oder durch den Ausbau verbindlicher Datenschutzkonzepte), die Herstellung der Eignung des geltenden Rechts für das Internet und die Stärkung der Unabhängigkeit der Datenschutzaufsicht durch Gewährleistung der finanziellen, organisatorischen und rechtlichen Mittel.

Letztlich wird von der Konferenz auf die nur sehr eingeschränkte Eignung der jetzigen rechtlichen Regelungen hingewiesen, welche sich als starkes Hindernis für einen gelingenden Datenschutz behaupten. Das Datenschutzrecht ist durch wiederholte Änderungen und Ergänzungen selbst für Fachleute nur noch schwer verständlich und bedarf der dringenden Überarbeitung. Erforderlich sind etwa Änderungen in der Struktur und bei den Definitionen, die zusätzliche Spezialvorschriften entbehrlich machen würden.

Konkrete Ausführungen zu jedem der soeben skizzierten Eckpfeiler sind der genannten Broschüre zu entnehmen, die auf der Internetseite (www.datenschutz-mv.de) einzusehen ist.

3.1 Europarecht

Der Ministerrat und das Europäische Parlament verabschiedeten am 24. Oktober 1995 eine allgemeine Datenschutzrichtlinie (Richtlinie 95/46/EG), die bis Ende 1998 in das Recht der Mitgliedsstaaten umgesetzt werden musste. Dies ist inzwischen weitgehend geschehen. Zweck der Richtlinie ist es, nach Erwägungsgrund 10 ein möglichst hohes und gleichwertiges Datenschutzniveau für den Binnenmarkt herzustellen. Die Richtlinie ist mit dem am 23. Mai 2001 in Kraft getretenen „Gesetz zur Änderung des Bundesdatenschutzgesetzes (BDSG)“ aus dem Jahre 1990 zum „BDSG 2001“ entwickelt worden. Damit kam Deutschland der Verpflichtung zur Rechtsangleichung endgültig nach.

Mit der Richtlinie 97/66/EG vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation wurden die Grundsätze der Richtlinie 95/46/EG in spezielle Vorschriften für den Telekommunikationssektor umgesetzt. Schließlich wurde mit der Richtlinie 2002/58/EG eine zusätzliche Diversifizierung für den Schutz der Privatsphäre in der elektronischen Kommunikation vorgenommen (Datenschutzrichtlinie für elektronische Kommunikation). Ende 2009 hat das EU-Parlament dann eine Revision dieser Richtlinie beschlossen (sog. „E-Privacy-Richtlinie“), die in den Mitgliedsstaaten bis zum 25. Mai 2011 in dortiges Recht umzusetzen war. Deutschland kam dieser Verpflichtung bisher nicht nach.

Kernpunkte dieser Richtlinie sind (in verkürzter Form) das Verbot von Spam, der Schutz vor unerwünschten Cookies und die konkretisierte Informationspflicht bei Datenpannen.

So haben die Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste im Fall einer Verletzung des Schutzes personenbezogener Daten unverzüglich die zuständige nationale Behörde von der betreffenden Verletzung zu benachrichtigen - in besonderen Fällen sind auch die Betroffenen selbst unverzüglich zu unterrichten. Es ist nicht nachvollziehbar, wieso Deutschland der Umsetzungsverpflichtung bis heute nicht nachgekommen ist.

Ich empfehle der Landesregierung daher, sich in Umsetzung der Ziffern 390 und 391 der Koalitionsvereinbarung gegenüber der Bundesregierung und dem Bundestag für eine unverzügliche Umsetzung der Richtlinie in nationales Recht einzusetzen.

Für die Diskussion des europäischen (und damit auch des deutschen) Datenschutzes ist es jedoch immer wieder hilfreich, sich an die Wurzeln dieser internationalen Rechtsangleichung zu erinnern. Rechtsgrundlage für alle (auch späteren) europäischen Regelungen zum Datenschutz ist die generelle Notwendigkeit der Rechtsangleichung im Binnenmarkt (Art. 100 a EGV). Nach dem Subsidiaritätsprinzip (Art.3 lit. b Abs. 2 EGV) dürfen die EG-Organen dann tätig werden, wenn ein Ziel besser auf der Gemeinschaftsebene als auf derjenigen der einzelnen Mitgliedsstaaten erreicht werden kann.

Nicht zuletzt aus ökonomischer Sicht erfordern der (wettbewerbsorientierte) Warenverkehr oder die Anbahnung und Abwicklung von Dienstleistungen eine europäische Regelung für die Verarbeitung von personenbezogenen Daten, da die Übermittlung personenbezogener Daten wesentlicher Bestandteil des Geschäftsverkehrs ist. Datenschutz ist zugleich aber auch wesentlicher Bestandteil eines elementaren Menschenrechts. So hat der Europäische Gerichtshof das in Artikel 8 der Europäischen Menschenrechtskonvention (EMRK) verankerte Recht auf Achtung des Privatlebens in seiner Entscheidung vom 5. Oktober 1994 als „ein von der Gemeinschaftsordnung geschütztes Grundrecht“ bewertet und damit auch die hohe Bedeutung dieses Grundrechts auf Privatheit bzw. Datenschutz für die Gemeinschaftsordnung betont.

Offenbar nicht zuletzt aufgrund der wettbewerbsbedingten Harmonisierungsbedarfe des EU-Binnenmarktes plant die EU-Kommission nunmehr eine umfassende Novellierung des bisherigen Regelwerkes - als Verordnung in den Bereichen der Wirtschaft, des Privatlebens und im öffentlichen Sektor und als Richtlinie in den Bereichen Justiz und Polizei.

3.1.1 Neuer europäischer Rechtsrahmen

Die EU-Kommission plant eine neue EU-Datenschutzverordnung, die einen völlig neuen Rechtsrahmen für den EU-weiten Datenschutz festlegen wird.

Der bisherige bekannt gewordene Entwurf einer „Allgemeinen Datenschutzverordnung“ (die offizielle Veröffentlichung erfolgte nicht mehr rechtzeitig vor dem Redaktionsschluss dieses Berichtes) enthält wesentliche Änderungen gegenüber dem bisher geltenden Rechtsrahmen und entfaltet als Verordnung (im Unterschied zu einer Richtlinie) unmittelbar geltende Rechtswirkung in allen Mitgliedsstaaten. Gestützt auf Art. 16 Abs. 2 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV) wird mit der neuen Verordnung ein einheitliches Niveau des Datenschutzes in der EU angestrebt. Da es sich zum Zeitpunkt der Erstellung dieses Berichtes lediglich um einen inoffiziellen Entwurf handelt, möchte ich an dieser Stelle noch nicht auf einzelne (mögliche) Regelungen eingehen, sondern eine lediglich allgemeine Einschätzung vornehmen und diese mit einer Empfehlung an die Landesregierung verbinden.

Zu begrüßen sind die offenbar geplanten Konkretisierungen und Stärkungen der Einwilligungserfordernisse, die Klarstellungen zum anwendbaren Recht bei multinational operierenden Anbietern und Datenverarbeitern, die Technologieneutralität, die Einführung der „Rechte auf Vergessenwerden, des Ausradierens und der Datenportabilität, die Konkretisierung der Erfordernisse zur Unabhängigkeit der Aufsichtsbehörden und die Flexibilisierung sowie Stärkung der Sanktionsmaßnahmen bei etwaigen Verstößen“.

Sehr bedenklich sind hingegen die offenbar geplante Nichtanwendung der Verordnung auf die Bereiche Justiz und Polizei (hier sind jeweils eigene Richtlinien geplant), das sogenannte one-shop-Modell und die ebenfalls wohl beabsichtigte Regelung zu internen bzw. externen Datenschutzbeauftragten bei nicht-öffentlichen Stellen, die erst ab 250 Mitarbeiter zur Pflicht erhoben werden soll - damit bliebe die Verordnung deutlich unter dem geltenden deutschen Standard des Bundesdatenschutzgesetzes. Zudem bleibt nach dem bisherigen Entwurf unnötig vage, inwieweit die Mitgliedsstaaten eigene (ergänzende oder konkretisierende) Regelungen treffen können, um etwaige Lücken (z. B. beim Beschäftigtendatenschutz) oder eigene Rechtstraditionen (wie z. B. im deutschen Sozialrecht) schließen bzw. weiter pflegen zu können.

Nach alledem ist wahrscheinlich, dass die von der EU-Kommission als Wirkungsabsicht der Verordnung angekündigte Entbürokratisierung wohl hauptsächlich auf der Seite der Wirtschaft eintreten wird, während die Aufsichtsbehörden - jedenfalls bei Realisierung des one-shop-Modells - mit deutlich mehr an Bürokratie zu kämpfen haben werden. Nicht zuletzt würden viele Aufsichtsbehörden als jeweilige Anlauf- und Kommunikationsstellen für Petitionen von dann auch europaweiter Bedeutung enorme (auch finanzielle) Anstrengungen zur Herstellung bzw. Gewährleistung der personellen „EU-Fähigkeit“ unternehmen müssen.

Hinsichtlich des weiteren Abstimmungsverfahrens im Rat und im europäischen Parlament empfehle ich der Landesregierung eine aktive, zwischen den Ländern koordinierte und kritische Begleitung des Prozesses. Dies insbesondere mit Blick auf die weitere Gewährleistung bisher in Deutschland gesicherter Datenschutzstandards, einen bisher vertretbaren Verwaltungsaufwand und eine bisher bestehende (föderale) Unabhängigkeit der Aufsichtsbehörden.

3.1.2 Artikel-29-Gruppe - Datenschutzkoordinierung in Europa

Die Artikel-29-Datenschutzgruppe wurde im Rahmen der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr gegründet (siehe dort Artikel 29). Die Gruppe ist eine beratende und unabhängige Einrichtung.

Die Aufgaben der Datenschutzgruppe sind in Artikel 30 der Europäischen Datenschutzrichtlinie und Artikel 15 der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) festgelegt. Danach hat die Gruppe vornehmlich beratende Funktion. Sie kann aber auch in eigener Initiative Empfehlungen und Stellungnahmen zu allen Fragen abgeben, die den Schutz von Personen bei der Verarbeitung personenbezogener Daten in der Europäischen Gemeinschaft betreffen.

Seit ihrer Gründung hat sich die Gruppe zu verschiedenen datenschutzrechtlichen Themen geäußert, beispielsweise zur Videoüberwachung, zum E-Government, zur unerwünschten E-Mail-Werbung, zum Einsatz biometrischer Verfahren, zum Arbeitnehmerdatenschutz, zum Datentransfer in Drittländer außerhalb der EU und zum Datenschutz im Internet - so zuletzt insbesondere im Zusammenhang mit der Nutzung sozialer Netzwerke (z. B. Facebook etc.).

Die Beschlüsse der Gruppe sind zwar nicht bindend, entfalten jedoch nicht selten eine relevante faktische Bindungswirkung, da sich sowohl die Gerichte als auch nationale Gesetzgeber sowie Selbstregulierungsinitiativen in ihrer Praxis bisweilen an diesen orientieren. Leider gilt dies nicht immer. So äußerte 2005 die Gruppe Bedenken gegen die Rechtmäßigkeit der geplanten Richtlinie über die Vorratsdatenspeicherung. Ungeachtet dessen beschloss das EU-Parlament am 14. Dezember 2005 die umstrittene Richtlinie.

Die Artikel-29-Gruppe ist gegenüber den EU-Organen und -Einrichtungen unabhängig, sie hat per Geschäftsordnung und Rechtsgrundlage eine beratende Funktion. Sie trifft ihre Entscheidungen nach dem Mehrheitsprinzip.

Die Gruppe besteht aus je einem Vertreter der jeweiligen nationalen Datenschutzbehörden, dem Europäischen Datenschutzbeauftragten und einem nicht stimmberechtigten Vertreter der Europäischen Kommission. Sie trifft sich in der Regel fünf Mal pro Jahr zu zweitägigen Sitzungen an ihrem Amtssitz in Brüssel. Vertreter der Datenschutzbehörden der Bundesrepublik Deutschland ist der derzeitige Bundesbeauftragte für den Datenschutz Peter Schaar, der zeitweise auch der gewählte Vorsitzende der Gruppe war. Als Vertreter der Länder ist derzeit zudem der Landesbeauftragte für den Datenschutz des Landes Berlin ständiger Gast. Vorsitzender der Artikel-29-Gruppe ist derzeit (Stand 2011) Jacob Kohnstamm, Leiter der niederländischen Datenschutzbehörde. Die Amtszeit des Vorsitzenden und des Stellvertreters währt zwei Jahre. Eine einmalige Wiederwahl ist zulässig.

Die Datenschutzgruppe wird durch ein Sekretariat unterstützt, das bei der Generaldirektion Justiz der Europäischen Kommission in Brüssel angesiedelt ist. Das Sekretariat fungiert insbesondere als zentrale Koordinierungsstelle.

Zukünftig soll durch einen neuen europäischen Rechtsrahmen die Wirkung und der Status der Gruppe gestärkt werden. So ist unter anderem vorgesehen, die Gruppe strukturell zu stärken und sie als EU-weites Koordinationsgremium mit Einigungs-, Abstimmungs- und Empfehlungskompetenzen zu betrauen.

3.2 Bundesrecht

3.2.1 Beschäftigtendatenschutz

Während meines Vorsitzes im Düsseldorfer Kreis im Jahr 2009 (siehe Neunter Tätigkeitsbericht, Punkt 3.1) ist unter anderem beschlossen worden, eine Arbeitsgruppe Beschäftigtendatenschutz zu gründen und sie, soweit möglich, in enger Zusammenarbeit mit dem Arbeitskreis Personalwesen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder einzuberufen sowie inhaltlich zu gestalten. Bei der Herbsttagung des Düsseldorfer Kreises im November 2009 in Stralsund habe ich mich bereit erklärt, die erste Sitzung der Arbeitsgruppe mit dem Ziel zu leiten, sie danach mit dem Arbeitskreis Personalwesen zu verbinden.

Zu Beginn des Jahres 2010 zeichnete sich ab, dass die Bundesregierung einen Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes vorlegen wird. Vor diesem Hintergrund war es dringlich, möglichst rasch eine Sitzung der Arbeitsgruppe einzuberufen, um frühzeitig zu dem Entwurf Stellung zu nehmen.

Ich habe deshalb die Aufsichtsbehörden und die Datenschutzbeauftragten des Bundes und der Länder für den 6. Mai 2010 zur ersten Sitzung der AG Beschäftigtendatenschutz nach Berlin in die Dienststelle des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit eingeladen. Der Bundesbeauftragte hat mich bei der Organisation der Sitzung tatkräftig unterstützt. Im Mittelpunkt dieser Sitzung stand dann auch der Entwurf des Bundesministeriums des Innern für ein Beschäftigtendatenschutzgesetz.

Aber auch in der Folge haben sich die Aufsichtsbehörden und die Datenschutzbeauftragten in mehreren Sitzungen einer Unterarbeitsgruppe Beschäftigtendatenschutzgesetz mit den Regelungen in dem Entwurf befasst. Die 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat auf ihrer Sitzung am 16./17. März 2011 in Würzburg unter dem Titel „Beschäftigtendatenschutz stärken statt abbauen“ an den Bundestag appelliert, die notwendigen datenschutzrechtlichen Anforderungen durch die Gesetzgebung sicherzustellen (siehe z. B. unter <http://www.datenschutz-mv.de/dschutz/beschlue/entsch81.html#nr4>). Die in der Entschließung genannten Anforderungen haben an Aktualität nichts verloren, sie sind nach wie vor gültig. Das Gesetzgebungsverfahren scheint allerdings ins Stocken geraten zu sein, sodass nicht absehbar ist, ob und wann die gesetzlichen Regelungen in Kraft treten. Es ist auch zu befürchten, dass der Entwurf, statt ihn datenschutzrechtlich zu verbessern, möglicherweise weiter an datenschutzrechtlicher Qualität verliert.

3.2.2 BDSG Novelle - Neue Regelungen zu Auskunfteien und zum Scoring

Mit dem am 1. April 2010 in Kraft getretenen Gesetz zur Änderung des Bundesdatenschutzgesetzes (sogenannte „Novelle I“) hat der Gesetzgeber wesentliche Vorschriften zur Datenübermittlung an Auskunfteien und zu Scoring-Verfahren neu geregelt. Mangels einer speziellen gesetzlichen Regelung für die Datenübermittlung von Unternehmen an Auskunfteien musste bisher auf die allgemeinen Regelungen gemäß § 28 Abs. 1 Nr. 2 und § 28 Abs. 2 Nr. 2 BDSG zurückgegriffen werden (Abwägung zwischen den Interessen der Wirtschaft, insbesondere der Banken, an Bonitätsdaten über ihre Kunden einerseits und den schutzwürdigen Interessen der Kunden andererseits).

Angesichts der Vielzahl der Fallkonstellationen im Bereich der Datenübermittlungen an Auskunfteien in verschiedenen Wirtschaftsbereichen hatten die Aufsichtsbehörden im Düsseldorfer Kreis Kriterien zur angemessenen Wahrung der Interessen der Betroffenen im Rahmen der genannten Abwägung entwickelt. Diese Kriterien hat der Gesetzgeber mit der neuen Regelung des § 28 a Abs. 1 BDSG aufgegriffen. Die Vorschrift enthält eine abschließende Aufzählung aller Fallgruppen, in denen eine Datenübermittlung über Forderungen an Auskunfteien zulässig ist. Dies sind zunächst Forderungen, die durch ein rechtskräftiges oder für vorläufig vollstreckbar erklärtes Urteil festgestellt worden sind bzw. Schuldtitel nach § 794 ZPO. § 28 a Abs. 1 Satz 1 Nr. 4 BDSG betrifft nicht titulierte (also nicht gerichtlich bestätigte) Forderungen und listet folgende Voraussetzungen auf, die erfüllt sein müssen, um eine solche Forderung bei einer Auskunftei einmelden zu dürfen:

- der Betroffene muss nach Eintritt der Fälligkeit der Forderung mindestens zwei Mal schriftlich gemahnt worden sein,
- zwischen der ersten Mahnung und der Übermittlung müssen mindestens vier Wochen liegen,
- der Gläubiger muss den Betroffenen rechtzeitig vor der Übermittlung der Angaben, jedoch frühestens bei der ersten Mahnung, über die bevorstehende Übermittlung unterrichten und
- die Forderung darf durch den Betroffenen nicht bestritten worden sein.

Eine weitere Neuregelung enthält § 28 a Abs. 2 BDSG, der festgelegt, unter welchen Voraussetzungen Kreditinstitute personenbezogene Daten über Vertragsverhältnisse mit ihren Kunden an Auskunfteien übermitteln dürfen. Hierbei handelt es sich um sogenannte „Positivdaten“ (im Gegensatz zu „Negativdaten“, also Daten über Zahlungstörungen etc.).

Die spezielle Übermittlungsregelung war erforderlich, da nach der bisherigen Praxis Kreditinstitute zur Abfrage von Kunden bei einer Auskunftei mangels einer speziellen gesetzlichen Grundlage regelmäßig die Einwilligung der Betroffenen einholten. Dabei war jedoch die nach § 4 a BDSG erforderliche Freiwilligkeit der Einwilligung von Kunden faktisch nicht gegeben, weil es in der Regel nicht möglich ist, ein Girokonto zu eröffnen oder einen Kredit zu erhalten, ohne die genannte Einwilligungsklausel zu unterschreiben.

§ 28 a Abs. 2 Satz 4 BDSG legt nunmehr ausdrücklich fest, dass Kundendaten, die lediglich dazu dienen, sich über Kreditkonditionen bei Banken zu informieren, nicht in den Auskunftsbestand von Auskunfteien übermittelt werden dürfen. Begrüßenswert sind auch die Neuregelungen in § 28 a Abs. 3 BDSG (Nachberichtspflicht des einmeldenden Unternehmens zur Gewährleistung eines aktuellen Datenbestandes) und in § 35 Abs. 1 Satz 2 BDSG (Kennzeichnungspflicht für Daten, die auf bloßen Schätzungen beruhen).

Der neue § 28 b BDSG regelt die Anforderungen an die Zulässigkeit von Scoring-Verfahren. Der Begriff „Scoring“ umschreibt die Berechnung eines Wahrscheinlichkeitswertes für ein bestimmtes zukünftiges Verhalten eines Betroffenen (§ 28 b Abs. 1 Satz 1 BDSG). Nach § 28 b Satz 1 Nr. 2 BDSG dürfen insbesondere keine Daten zur Erstellung des Scores verwendet werden, die nicht auch sonst durch die Auskunftfeier oder das Unternehmen zulässigerweise nach § 28 bzw. § 29 BDSG übermittelt oder genutzt werden.

Bedauerlicherweise hat der Gesetzgeber das sogenannte „Geosoring“ (Scoreberechnung aufgrund von Anschriften bzw. Daten über das Wohnumfeld) nicht generell verboten. Allerdings dürfen gemäß § 28 b Satz 1 Nr. 3 BDSG Scores nicht ausschließlich aufgrund von Anschriftendaten erstellt werden.

Flankierend wurden in § 34 Abs. 2 BDSG entsprechende Auskunftsrechte für die vom Scoringverfahren Betroffenen aufgenommen. Diese können Auskunft verlangen über die innerhalb der letzten sechs Monate erhobenen Wahrscheinlichkeitswerte und über die der Berechnung zugrundeliegenden Datenarten sowie über das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte (bezogen auf den Einzelfall und in allgemein verständlicher Form). Außerdem können Betroffene nunmehr bei Auskunftfeiern einmal im Jahr eine kostenlose Auskunft verlangen (§ 34 Abs. 8 BDSG).

3.2.3 Novellierung des Internetrechts erforderlich

Das Internet wird zunehmend zum festen Bestandteil unserer alltäglichen Verrichtungen. Aufgrund der Eigenart der Technik und der auch daraus folgenden häufigen relativen Anonymität der im Internet Agierenden ist das Gefährdungspotential hinsichtlich möglicher Straftaten bzw. Verstöße auch gegen das informationelle Selbstbestimmungsrecht im Internet besonders groß. So wäre zu vermuten, dass in Deutschland gerade dieses Handlungsfeld (ähnlich wie der Straßenverkehr oder der Baubereich) relativ exakt und verständlich rechtlich geregelt ist. Bei genauer Betrachtung ergeben sich jedoch erstaunliche Regelungslücken auf allen Rechtsetzungsebenen.

Das Internetrecht stellt sich derzeit nicht als wünschenswert überschaubares Rechtsgebiet, sondern als Schnittstelle vieler - geradezu unüberschaubarer - nationaler und europäischer Rechtsgebiete dar. So finden sich vereinzelt und teilweise veraltete Regelungen im Urheberrecht, im Wettbewerbsrecht, im Namens- und Markenrecht, im internationalen Privatrecht, im Medienrecht, im Telekommunikationsrecht, im Rundfunkrecht, im internationalen Zivilverfahrensrecht, im allgemeinen und besonderen Zivilrecht und nicht zuletzt im Datenschutzrecht. Ergänzt wird diese verwirrende Vielfalt durch die EG-E-Commerce-Richtlinie und der E-Privacy-Richtlinie der EU.

Vor dem Hintergrund dieser verbesserungswürdigen Situation stellte das Bundesinnenministerium (BMI) schon im Dezember 2010 ein Maßnahmenpaket in Aussicht, das unter anderem einen Datenschutz-Kodex als ein Zeichen für funktionierende Selbstregulierungskräfte der IKT-Branche und einen Gesetzentwurf enthielt.

Dieser Gesetzentwurf sollte als „Rote-Linie-Gesetz“ Regelungen zur Stärkung der Selbstbestimmung durch eine Ergänzung des Bundesdatenschutzgesetzes (BDSG) und des Telemediengesetzes (TMG) enthalten.

Als notwendig wurde dabei ein breiter Ansatz erachtet, der das gesamte Internet einbezieht und sich nicht nur auf einzelne Teilaspekte wie Geodaten oder gar nur auf Google Street View etc. beschränkt. Eine gezielte Verbreitung von Persönlichkeitsprofilen sollte nach Ankündigung des BMI deshalb nur mit Einwilligung des Betroffenen erfolgen dürfen oder aber wenn ein klar überwiegendes Interesse an der Veröffentlichung besteht.

Als Diskussionsgrundlage enthielt der Entwurf zudem erste Regelungsvorschläge zu bestimmten Internetdiensten, die für die Integrität des Persönlichkeitsrechts von besonderer Bedeutung sind. Im Einzelnen waren dies (im Wesentlichen zitiert aus der Pressemitteilung des BMI vom 1. Dezember 2010):

Gesichtserkennungsdienste: Gemeint waren Fälle, in denen eine Person allein anhand eines Gesichts oder biometrischen Merkmals über Internetrecherchen identifiziert werden kann. Es wird zunehmend technisch möglich sein, über eine integrierte Kamera eines internetfähigen Handys jedermann auf der Straße oder in einem Café aufzunehmen und anhand des Fotos eine Sofortrecherche im Internet durchzuführen. Sofern dort Bildmaterial und weitere Angaben zu der betreffenden Person vorhanden sind, könnten diese angezeigt und die Person auf diese Weise (in Echtzeit) identifiziert werden. Durch entsprechende Anwendungen droht ein weit größerer Verlust an Anonymität im öffentlichen Raum als durch die Abbildung von Häuserfassaden.

Profilbildungen anhand von Suchmaschinenanfragen: Die Inhalte von Suchanfragen können den Kernbereich persönlicher Lebensgestaltung betreffen. Der Nutzer muss darauf vertrauen können, dass diese Daten nicht gesammelt, ausgewertet und dem Betroffenen zugeordnet werden. Aus den Inhalten der Suchanfragen können mitunter intime Erkenntnisse oder (vermeintliche) Rückschlüsse über Nutzer generiert werden.

Erhebung von Standortdaten: Standortdaten von Mobiltelefonen dürfen durch den Telekommunikationsanbieter an Dritte bereits jetzt nur übermittelt werden, wenn der Betroffene eine ausdrückliche und gesonderte Einwilligung erteilt hat (§ 98 Telekommunikationsgesetz). Durch die Verbreitung von GPS-Smartphones findet mittlerweile eine Erhebung des Standorts auch durch Diensteanbieter statt, die nicht dem TKG unterworfen sind. Das Erheben und Übermitteln von Standortdaten ist als Vorstufe zur Erstellung von Bewegungsprofilen in besonderem Maße persönlichkeitsrechtsrelevant.

Immaterieller Schadensersatz (Schmerzensgeld): Als Sanktion schwerer Verletzungen des Persönlichkeitsrechts sollte im damaligen Entwurf ein neuer Schmerzensgeldanspruch im BDSG geschaffen werden. Einen Schmerzensgeldanspruch kennt das BDSG bisher nur in Bezug auf die automatisierte Datenverarbeitung öffentlicher Stellen. Der neue Anspruch richtet sich gegen private Unternehmen.

Die neue Regelung sollte zugleich Kriterien für die Bemessung der Höhe des immateriellen Schadensersatzes aufstellen. Die dort ausdrücklich genannten Kriterien betonten den Sanktionscharakter der Geldentschädigung. Die Geldentschädigung sollte so bemessen sein, dass sie einen angemessenen Hemmungseffekt entfaltet. Insoweit sollte sich die Höhe des immateriellen Schadensersatzes auch an der Höhe der tatsächlichen oder zu erwartenden Gewinne orientieren.

Trotz einzelner kritikwürdiger und im Sinne des Datenschutzes verbesserungswürdiger Regelungen des Entwurfes (soweit er überhaupt bekannt wurde), war dem Regelungsanliegen des BMI grundsätzlich zuzustimmen - wenngleich die ebenfalls vorgestellte „Selbstverpflichtung“ der IKT-Branche unter keinen Umständen ausreichend sein konnte. Bis zum Redaktionsschluss dieses Tätigkeitsberichtes wurden die angekündigten Regelungen jedoch nicht umgesetzt. Möglicherweise ist der richtige Zeitpunkt hierfür auch unwiderruflich verpasst, da die Aufmerksamkeit nun ganz dem entsprechenden neuen EU-Rechtsrahmen gilt und dieser (bis zu seiner Verwirklichung in zwei oder auch drei Jahren) letztlich über den dann noch verbleibenden nationalen Regelungsspielraum entscheidet. Jedenfalls die Zwischenzeit hätte für ein optimiertes „Rote-Linie-Gesetz“ genutzt werden können.

3.2.4 Änderung des Bundesverfassungsschutzgesetzes

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hat mich im September 2011 darüber informiert, dass im Bundesrat der Gesetzentwurf der Bundesregierung zur Änderung des Bundesverfassungsschutzgesetzes behandelt werden soll. Inhaltlich ging es um einen Antrag der Länder Nordrhein-Westfalen und Rheinland-Pfalz und einen Antrag Bayerns, auch den Landesverfassungsschutzbehörden die Befugnis zur Kontostammdatenabfrage zukommen zu lassen.

Ich habe mich daraufhin an den Staatssekretär unseres Innenministeriums gewandt und darauf hingewiesen, dass ich es aus datenschutzrechtlicher Sicht ablehne, dass der Verfassungsschutzbehörde unseres Landes eine derartige Befugnis eingeräumt wird. Dies habe ich wie folgt begründet:

Die Möglichkeit des Abrufs von Kontostammdaten wurde in den letzten Jahren ständig ausgebaut, sodass sich sowohl Strafverfolgungsbehörden als auch Finanz- und Sozialbehörden Kenntnis über das Bestehen von Konten und Depots verschaffen können.

Wird diese Möglichkeit nun auch noch den Verfassungsschutzbehörden der Länder eingeräumt, so stellt dies eine datenschutzrechtlich problematische Ausweitung des Zwecks, zu dem Kontostammdaten ursprünglich vorrätig gehalten wurden, dar. Auch bestätigen sich Befürchtungen, dass bei der Einführung neuer Dateien Begehrlichkeiten geweckt werden und der Kreis der Zugriffsberechtigten im Laufe der Jahre ständig erweitert wird.

Die Ermittlungen über Kontostammdaten können Maßnahmen vorbereiten, die ohne die erlangten Kenntnisse nicht ohne weiteres möglich sind und die die Belange der Betroffenen erheblich berühren. Kontenabrufe nach § 24 c Kreditwesengesetz (KWG) können damit Grundrechtseingriffe von großem Gewicht nach sich ziehen. Dies gilt umso mehr, wenn es sich um Ermittlungen durch Nachrichtendienste handelt. Insbesondere das Argument, ein Abruf der Kontostammdaten wäre der mildere Eingriff gegenüber der Ermittlung der kontoführenden Kreditinstitute mit nachrichtendienstlichen Mitteln, verfängt in diesem Zusammenhang nicht. Die bisherige Vorgehensweise bietet mehr Garantie dahingehend, dass aufgrund des ansonsten damit verbundenen Aufwandes die Erhebung von Kontodaten auf die Fälle beschränkt bleibt, in denen diese Kenntnis auch tatsächlich erforderlich ist.

Wird der Zugang zu den Kontostammdaten erleichtert, so besteht die Gefahr, dass von dieser Möglichkeit zunehmend Gebrauch gemacht wird und sich in der Folge der Kreis der Betroffenen einer solchen Maßnahme erhöht. Die Maßnahme wird lediglich dadurch eingeschränkt, dass es im Gesetzentwurf bisher heißt: „im Einzelfall“. Dies reicht aus meiner Sicht nicht aus.

Meinen Empfehlungen wurde im laufenden Gesetzgebungsverfahren nicht gefolgt. Die sogenannte Länderöffnungsklausel wurde in das Bundesverfassungsschutzgesetz aufgenommen.

3.2.5 Elektronischer Entgeltnachweis ELENA

Am 18. Juli 2011 hat das Bundesministerium für Arbeit und Soziales in einer Pressemitteilung bekannt gegeben, dass das automatisierte Verfahren zum Elektronischen Entgeltnachweis (ELENA) schnellstmöglich eingestellt werden soll. Mit dem am 3. Dezember 2011 in Kraft getretenen Gesetz zur Aufhebung von Vorschriften zum Verfahren des elektronischen Entgeltnachweises (BGBl. I 2011 S. 2298) wurden die ELENA betreffenden Passagen des Vierten Buches Sozialgesetzbuch (SGB IV) aufgehoben.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Peter Schaar informierte in einer Pressemitteilung vom 8. Dezember 2011 darüber, dass er den sogenannten Datenbankhauptschlüssel des Verfahrens gelöscht hat. Nur mit diesem digitalen Schlüssel war der Zugriff auf die verschlüsselt gespeicherten Entgeltdaten von mehr als 35 Millionen Arbeitnehmerinnen und Arbeitnehmern möglich.

Ich begrüße die Einstellung des Verfahrens ausdrücklich, weil damit endlich eine der größten und datenschutzrechtlich umstrittensten Datensammlungen der Bundesrepublik Deutschland gelöscht und ein Verfahren beendet wird, das von Anfang an verfassungsrechtlich äußerst bedenklich war. Das Bundesverfassungsgericht wurde mehrfach angerufen, lehnte einen Eilantrag gegen ELENA im September 2011 aber ab. Die Entwicklung und Einführung von ELENA habe ich seit vielen Jahren begleitet. Trotz dauerhaft bestehender datenschutzrechtlicher Kritikpunkte (siehe zuletzt Neunter Tätigkeitsbericht, Punkt 2.9.4) hatte der Bundestag das Gesetz zur Einführung des ELENA-Verfahrens (BGBl. I, S. 634) im Frühjahr 2009 verabschiedet. Das im April 2009 in Kraft getretene Gesetz besagt, dass fünf bisher Papier basierte Entgeltbescheinigungen durch elektronische Speicherungen ersetzt werden. Arbeitgeber waren seit dem 1. Januar 2010 verpflichtet, einen umfangreichen Katalog von Entgeltdaten an die sogenannte Zentrale Speicherstelle (ZSS) zu übermitteln, wo diese zum Abruf durch die Antrag bearbeitenden Stellen bereitgehalten werden. Die ZSS wurde bei der Datenstelle der Träger der Rentenversicherung eingerichtet.

Um eine missbräuchliche Nutzung des umfangreichen Datenbestandes der zentralen Speicherstelle zu verhindern, waren umfassende technische und organisatorische Maßnahmen getroffen worden. So waren die Daten pseudonymisiert und in verschlüsselter Form in der ZSS gespeichert. Der zur Entschlüsselung erforderliche und inzwischen gelöschte Datenbankhauptschlüssel (siehe oben) wurde vom Bundesbeauftragten für den Datenschutz verwaltet um sicherzustellen, dass keine unautorisierten Zugriffe auf die Datenbank möglich sind.

Der Zugriff auf die Daten und die Zuordnung der Datensätze zu einzelnen Beschäftigten war nur möglich, wenn der Betroffene im Rahmen der Beantragung von Sozialleistungen die dafür erforderlichen Daten durch die Vorlage seiner Signaturkarte freigibt. Zudem musste der Mitarbeiter der Antrag bearbeitenden Stelle ebenfalls durch Vorlage einer Signaturkarte seine Berechtigung zur Verarbeitung dieser Daten nachweisen. Auf diese Weise sollte das von Beginn an geforderte Zwei-Karten-Prinzip umgesetzt werden.

Obwohl die Zweifel an der Verfassungsmäßigkeit des Verfahrens nie ausgeräumt werden konnten, habe ich mich bereit erklärt, die Vorgehensweise für den Abruf der Daten durch öffentliche Stellen der Länder in der Arbeitsgruppe „Informationssicherheit und Datenschutz“ des Bund-Länder-Arbeitskreises „ELENA-Verfahrensgrundsätze“ zu begleiten und auf ein gesetzeskonformes Vorgehen und ein möglichst hohes Datenschutzniveau hinzuwirken. Aber nicht alle sicherheitstechnischen Aspekte des Verfahrens wurden so ausgestaltet, wie ich gemeinsam mit meinen Kollegen von Bund und Ländern empfohlen habe. So kam die ZSS ihrer gesetzlichen Pflicht (§ 97 Abs. 6 SGB IV), die abrufenden Behörden bei ihrer Zulassung zur Teilnahme an dem Verfahren auf die Gewährleistung von Datenschutz und -sicherheit zu überprüfen, nach meiner Auffassung nicht in angemessener Weise nach. Immerhin konnte ich die Verfahrensträger davon überzeugen, einen Maßnahmenkatalog zu erarbeiten und den abrufenden Stellen zur Verfügung zu stellen, dessen Umsetzung zumindest einen Grundschutz beim Datenabruf bewirken soll.

Völlig unbefriedigend war auch das gesetzlich verbrieftete Recht der Betroffenen auf Auskunft über die in der ZSS gespeicherten Daten gelöst (§ 103 Abs. 4 SGB IV). Eine solche Auskunftsmöglichkeit hätte mit Beginn der Datenspeicherung kostenlos angeboten werden müssen, wurde aber bis heute nicht umgesetzt. Das erst nach wiederholten Mahnungen konzipierte Auskunftsverfahren wäre mit erheblichen Kosten für die Betroffenen verbunden gewesen. Sie hätten sich eine Signaturkarte für derzeit etwa 50 Euro jährlich beschaffen und damit ihr Auskunftsersuchen elektronisch unterzeichnen müssen. Das Auskunftsrecht wäre damit de facto ausgehebelt worden.

Nach Auffassung der Bundesregierung führte die fehlende Verbreitung genau dieser Signaturkarten zur Einstellung des Verfahrens. Ich halte die Begründung für scheinheilig. Obwohl die Bundesregierung nie bezweifelt hat, dass der Einsatz qualifizierter elektronischer Signaturen für das ELENA-Verfahren zwingend geboten war, hat sie nie ernsthafte Bemühungen zur Förderung dieser Technologie unternommen und vergeblich darauf gehofft, dass der Markt das Erforderliche bewirken würde. Mit der Einstellung des ELENA-Verfahrens ist die Verbreitung der qualifizierten elektronischen Signatur wohl endgültig gescheitert (siehe dazu Achter Tätigkeitsbericht, Punkt 2.15.2). Ich befürchte, dass damit eine wesentliche Grundlage für rechtsverbindliche und datenschutzfördernde elektronische Transaktionen künftig nicht mehr zur Verfügung stehen wird.

Dass andere Verfahren wie der elektronische Identitätsnachweis des neuen Personalausweises (siehe Neunter Tätigkeitsbericht, Punkt 2.4.9) oder das De-Mail-Verfahren (siehe Punkt 3.2.6) einen gleichwertigen Ersatz liefern können, bezweifle ich, da die dort genutzten Authentisierungsverfahren ausschließlich zur Identifizierung von Personen geeignet sind, die Authentizität und Integrität von Dokumenten jedoch nicht sicherstellen können (siehe dazu Achter Tätigkeitsbericht, Punkt 2.5.7).

Mit dem Ende des Verfahrens stehen zunächst aber andere Fragestellungen im Raum. Unstrittig ist, dass alle Daten, die im Zusammenhang mit dem ELENA-Verfahren erhoben und gespeichert wurden (es handelt sich dabei um mehr als 700 Millionen Datensätze allein in der ZSS!), vollständig gelöscht werden müssen.

Dazu war die oben erwähnte Aufhebung der entsprechenden Regelungen des SGB IV (§§ 95 bis 103) erforderlich (siehe auch BR-Drs. 608/11 vom 14. Oktober 2011). In seiner Entschlieung vom 4. November 2011 (BR-Drs. 608/11 - Beschluss) hat der Bundesrat die Bundesregierung aufgefordert zu prufen, welche durch ELENA entstandenen Daten zu löschen sind, und die Vorlage entsprechender Gesetzentwürfe gefordert. Ausdrücklich hat der Bundesrat die Löschung der rund 120.000 Versicherungskonten gefordert, die für Beamte, Soldaten und Richter angelegt wurden.

Angesichts der erheblichen Investitionskosten ist auch der künftige Umgang mit der für ELENA beschafften IT-Technik zu klären. Inzwischen hat die Bundesregierung das ELENA-Nachfolgeprojekt „Projektorientiertes Meldeverfahren in der Sozialversicherung“ angekündigt, um zumindest Teile der ELENA-Infrastruktur weiter nutzen zu können. Ich unterstütze ausdrücklich die Forderungen des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, das neue Verfahren an den Grundsätzen der Erforderlichkeit und der Datensparsamkeit auszurichten, eine strikte Zweckbindung der neu zu erhebenden Daten zu gewährleisten, den Betroffenen die Kontrolle der Datenverarbeitung zu ermöglichen und ihnen umfassende Auskunftsansprüche zu gewähren sowie angemessene und dem Stand der Technik entsprechende IT-Sicherheitsmaßnahmen umzusetzen.

3.2.6 De-Mail: Vorsicht bei sensiblen Daten!

Eine E-Mail ist nach wie vor sicherheitstechnisch mit einer Postkarte vergleichbar. Um dies zu verbessern, hat bereits die vorige Bundesregierung den Entwurf eines Bürgerportalgesetzes vorgelegt, der jedoch zahlreiche Fragen offen ließ. Nach massiver Kritik auch seitens der Datenschutzbeauftragten des Bundes und der Länder hat sie diesen Gesetzentwurf zurückgezogen (siehe Neunter Tätigkeitsbericht, Punkt 2.14.7). Im Berichtszeitraum unternahm die Bundesregierung mit dem De-Mail-Gesetz einen neuen Anlauf. Am 3. Mai 2011 trat es in Kraft.

Der De-Mail-Dienst besteht mindestens aus einem Postfach- und Versanddienst, einer Komponente für die sogenannte sichere Anmeldung und einem Verzeichnisdienst. Er kann zusätzlich Identitätsbestätigungsdienste und Dokumentenablagendienste bereitstellen. Wer einen De-Mail-Dienst anbieten will, muss sich durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) akkreditieren und durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zertifizieren lassen. Erste Anbieter von De-Mail-Diensten werden nach eigenen Ankündigungen wahrscheinlich im Frühjahr 2012 an den Markt gehen.

Ein De-Mail-Benutzerkonto kann nur gegen Vorlage eines amtlichen Lichtbildausweises, mit dem Identifikationsnachweis des elektronischen Personalausweises (siehe Neunter Tätigkeitsbericht, Punkt 2.4.9) oder mit einer qualifizierten elektronischen Signatur eröffnet werden. Nach diesem einmaligen Identifizierungsvorgang kann sich der registrierte Nutzer dann bei seinem De-Mail-Konto anmelden. Dabei hat er die Auswahl zwischen einer „normalen“ Anmeldung mit Benutzernamen und Passwort und einer sogenannten sicheren Anmeldung, die noch eine unabhängige zweite Komponente, beispielsweise eine Chipkarte, erfordert. Mitunter ist eine sichere Anmeldung vorgeschrieben, etwa zum Empfang von Nachrichten, bei denen der Absender eine Empfangsbestätigung benötigt. Der Postfach- und Versanddienst ist eine spezielle Form der E-Mail, bei der mindestens zwei Diensteanbieter beteiligt sind. Die beteiligten Diensteanbieter müssen für eine Transportverschlüsselung der Mails sowohl untereinander als auch auf dem Weg vom Absender zum Anbieter und vom Anbieter zum Empfänger sorgen. Hierfür verwenden sie SSL bzw. TLS (siehe Punkt 4.2.6). Außerdem haben die Anbieter die De-Mails während der Zwischenspeicherung zu verschlüsseln. Mit dem Verzeichnisdienst können die Nutzer auf freiwilliger Basis ihre DeMail-Adressen, Namen und Anschriften sowie öffentliche Schlüssel veröffentlichen.

Mit dem Identitätsbestätigungsdienst kann ein Nutzer auf Wunsch in sicherer Weise einem anderen De-Mail-Nutzer seine beim Diensteanbieter gespeicherten Identitätsdaten senden. Mit dem Dokumentenablagedienst schließlich soll der Nutzer Dateien seiner Wahl sicher speichern und gezielt anderen Nutzern zugänglich machen können. Auch hier muss der Anbieter die Dokumente während des Transports und bei der Speicherung verschlüsseln.

Die vorgeschriebene Transport- und Speicherverschlüsselung von De-Mails führt zu einem besseren Schutz vor unbefugtem Mitlesen als bei normalen E-Mails. Für Nutzer, denen das vom De-Mail-Dienst gewährte Basis-Sicherheitsniveau für die jeweilige Anwendung ausreicht, ist die Installation zusätzlicher Verschlüsselungssoftware und Schlüssel nicht erforderlich. Jedoch kann der De-Mail-Dienst ohne Zusatzmaßnahmen der Kunden keine Ende-zu-Ende-Sicherheit bieten. Es ist nämlich vorgesehen, dass die Diensteanbieter alle DeMails nach jedem Transport- und Speicherschritt kurzzeitig entschlüsseln, um die Mails auf schädliche Inhalte wie Viren, Würmer und Trojanische Pferde untersuchen zu können. Dies ist sicherlich sinnvoll, es sollte die Nutzer aber nicht davon abhalten, eigene Schutzmaßnahmen zu ergreifen, in der Regel also eigene Antiviren-Programme zu installieren und aktuell zu halten. Angesichts dieser Zugriffsmöglichkeiten für die Diensteanbieter eignet sich der De-Mail-Dienst ohne weitere Schutzvorkehrungen wie nutzerseitige Verschlüsselung nicht zur Übertragung oder zur Speicherung sensibler personenbezogener Daten, beispielsweise medizinischer Daten. Immerhin bietet der De-Mail-Dienst gute Voraussetzungen für die zusätzliche Verwendung einer Ende-zu-Ende-Verschlüsselung. Als potenzieller Empfänger von De-Mails hat jeder Nutzer die Möglichkeit, den erforderlichen Verschlüsselungsschlüssel im Verzeichnisdienst des Diensteanbieters öffentlich zugänglich abzulegen, damit Absender diesen Schlüssel zur Verschlüsselung der De-Mails verwenden können.

Die vorgeschriebenen Verschlüsselungsverfahren führen zusammen mit der sicheren Anmeldung auch zu einer verbesserten Integrität und Authentizität (Unversehrtheit und Echtheit) der übertragenen Nachrichten. Wichtig ist aber, dass die sichere Anmeldung sich jeweils auf alle Aktivitäten in einer Sitzung auswirkt. Im Gegensatz zur qualifizierten elektronischen Signatur werden nicht einzelne Nachrichten zur Bestätigung angezeigt und dann nach Einstecken der Chipkarte in den Leser und Eingabe der PIN signiert. Daher ist es für böswillige Personen oder auch für Schadsoftware auf dem Computer des Nutzers möglich, De-Mails im Namen des Nutzers zu senden und zu empfangen.

Dies ist viel einfacher, als qualifizierte elektronische Signaturen zu fälschen. Daher ist De-Mail kein Ersatz für die qualifizierte elektronische Signatur. Der Vollständigkeit halber sei noch erwähnt, dass De-Mail-Diansteanbieter bestimmte Dokumente wie Versandbestätigungen und Identitätsbestätigungen selbst qualifiziert elektronisch signieren. Deren Aussagewert ist jedoch begrenzt; die qualifizierte elektronische Signatur des Nutzers ist dadurch nicht zu ersetzen.

Auch beim Dokumentenablagedienst kann sich der Diansteanbieter, bedingt durch die technische Ausgestaltung, Zugriff auf die Inhalte verschaffen. Deshalb gilt auch hier, dass die Kunden Nutzen und Risiken dieses Dianstes sorgfältig gegeneinander abwägen und gegebenenfalls eigene Sicherheitsmechanismen wie Verschlüsselung einsetzen müssen.

Problematisch ist darüber hinaus, dass sich Kunden bei De-Mail-Diansteanbietern nicht nur mit amtlichen Ausweisen, sondern auch anhand einer qualifizierten elektronischen Signatur registrieren lassen können. Dieses Verfahren liefert nämlich keine ausreichenden Informationen über die Identität des Nutzers. Zertifizierungsdiansteanbieter stellen ein Zertifikat für qualifizierte elektronische Signaturen zwar nur gegen Vorlage eines amtlichen Lichtbildausweises oder unter Nutzung der Identifikationsfunktion des neuen Personalausweises aus. Die Zertifizierungsdiansteanbieter nehmen in das Zertifikat aber keine ausreichenden Informationen auf, die eine zweifelsfreie Identifikation des Nutzers ermöglichen, und sie speichern diese Daten auch nicht in anderer Weise. Eine sichere Identifizierung des Signierenden anhand der Signatur ist somit nicht möglich. Auf dieses Problem habe ich bereits mehrfach hingewiesen, in diesem Bericht beispielsweise im Personenstandswesen (siehe Punkt 2.4.9) oder im Steuerbereich (siehe Punkt 5.7.3).

Im Berichtszeitraum hat das Innenministerium unseres Landes Anwendungsmöglichkeiten für den De-Mail-Dienst untersuchen lassen. Dabei sind umfangreiche Maßnahmekataloge entstanden, die das Ministerium interessierten Behörden auf Wunsch zur Verfügung stellt.

Ich empfehle der Landesregierung, den De-Mail-Dienst nur dann einzusetzen, wenn vorher geprüft wurde, ob ein ausreichendes Sicherheitsniveau erzielt werden kann. Insbesondere bei der Verarbeitung sensibler personenbezogener Daten sind zusätzlich Maßnahmen erforderlich, wie Ende-zu-Ende-Verschlüsselung und gegebenenfalls die qualifizierte elektronische Signatur.

3.2.7 IT-Planungsrat

Am 1. April 2010 trat mit der Hinterlegung von 17 Ratifikationsurkunden des Bundes und der Länder der IT-Staatsvertrag („Vertrag über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern – Vertrag zur Ausführung von Art. 91c GG“) in Kraft. Am 22. April 2010 trat der IT-Planungsrat zu seiner konstituierenden Sitzung zusammen.

Zunächst sah die Geschäftsordnung des IT-Planungsrates lediglich vor, dass der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit mit beratender Stimme an den Sitzungen teilnimmt. Nachdem die Datenschutzbeauftragten im Oktober 2009 auch die Beteiligung eines Landesdatenschutzbeauftragten gefordert hatten (siehe Neunter Tätigkeitsbericht, Punkt 2.1.3) und sich einige Landesparlamente mit entsprechenden Entschlüssen dieser Forderung angeschlossen hatten, beschloss der IT-Planungsrat in seiner 2. Sitzung am 2. Juli 2010 eine Änderung der Geschäftsordnung. Demnach nimmt an den Sitzungen auch ein Vertreter aus dem Kreis der Landesdatenschutzbeauftragten teil, soweit sich aus der Anmeldung zur Tagesordnung ergibt, dass die Länder betreffende datenschutzrelevante Belange erörtert werden sollen. Da die Datenschutzkonferenz beschlossen hatte, mich in meiner Eigenschaft als Vorsitzender des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ in den IT-Planungsrat zu entsenden, nahm ich erstmalig an der 3. Sitzung des IT-Planungsrates am 24. September 2010 teil.

Es zeigte sich sehr schnell, dass die in der Geschäftsordnung beschriebene Einschränkung für meine Teilnahme auf „die Länder betreffende datenschutzrelevante Belange ...“ keine praktische Relevanz hatte, da sämtliche Entscheidungen des IT-Planungsrates Datenschutzbezug auch auf der Ebene der Länder aufweisen. Vor diesem Hintergrund werde ich zu allen Sitzungen eingeladen und habe die Möglichkeit, datenschutzrelevante Aspekte bei allen Tagesordnungspunkten anzusprechen.

Inzwischen habe ich an vier Sitzungen des IT-Planungsrates teilgenommen. Von besonderer Bedeutung war die 3. Sitzung im September 2010. Der IT-Planungsrat beschloss die „Nationale E-Government-Strategie (NEGS)“, mit der sich Bund, Länder und Gemeinden zum ersten Mal gemeinsam darauf verständigt haben, wie die elektronische Abwicklung von Verwaltungsangelegenheiten über das Internet weiterentwickelt werden soll (Details zur NEGS unter www.it-planungsrat.de).

Die Strategie definiert sechs zentrale Ziele, an denen sich die Projekte des IT-Planungsrates ausrichten werden, etwa die maßgebliche Orientierung am Nutzen von Bürgern, Unternehmen und Verwaltung, die Erhöhung der Effizienz des Verwaltungshandelns, die Transparenz über Daten und Abläufe, Datenschutz sowie die Stärkung der gesellschaftlichen Teilhabe über Internetangebote des Staates.

Die 4. Sitzung des IT-Planungsrates fand im März 2011 auf der CeBIT in Hannover statt. Unter anderem wurde beschlossen, Leitlinien für IT-Sicherheit und Datenschutz zu erarbeiten, um eine gemeinsame Basis für die Informationssicherheit der öffentlichen Verwaltung in Deutschland zu schaffen. Während dieser Sitzung wurde auch der Aufbau der Koordinierungsstelle für IT-Standards (KoSIT) beschlossen. Der IT-Planungsrat reagierte auf die Forderung der Datenschutzbeauftragten und einiger Landesparlamente nach datenschutzkonformen Standards mit der Zusage, dass die KoSIT datenschutzrechtliche Aspekte selbstverständlich berücksichtigen werde.

In seiner 5. Sitzung am 30. Juni 2011 in Berlin verabschiedete der IT-Planungsrat ein Memorandum, in dem Schwerpunkte zur Umsetzung der NEGS formuliert wurden. In Berlin wurden auch die Weichen für die eID-Strategie der Bundesregierung gestellt. Die Teilnehmer konstatierten, dass die eCard-Strategie aus dem Jahr 2005 überholt sei, insbesondere weil die Erwartungen an die Qualifizierte Elektronische Signatur nicht erfüllt worden sind. Die eCard-Strategie soll daher zu einer Strategie für „Elektronische Identitäten und selbst bestimmtes Handeln im Netz“ weiter entwickelt werden.

In der 6. Sitzung am 13. Oktober 2011 in Stuttgart nahm der IT-Planungsrat das NEGS-Umsetzungskonzept zur Kenntnis und beschloss ein entsprechendes Schwerpunktprogramm. Als ersten Schritt zu verbindlichen Leitlinien nahm der IT-Planungsrat das Konzept zu „Ziel, Geltungsbereich und Inhalten einer Leitlinie für Informationssicherheit der öffentlichen Verwaltung“ zur Kenntnis. Die Mitglieder konnten sich allerdings nicht auf eine Forderung zur verbindlichen Umsetzung der Leitlinien in den Kommunen verständigen, weil damit nicht abschätzbare finanzielle Folgen verbunden wären. Stattdessen wird den Kommunen die Umsetzung der Leitlinien lediglich empfohlen.

Erfreulich ist die Tatsache, dass die Mitarbeit der Landesdatenschutzbeauftragten auch in den Arbeitsgremien des IT-Planungsrates gewünscht ist und ermöglicht wird.

Mit Blick auf meine Zuständigkeit für Informationsfreiheit wurde ich gebeten, in einer Arbeitsgruppe des IT-Planungsrates zum Thema Open Government teilzunehmen. In einer weiteren Arbeitsgruppe, die die Leitlinien für IT-Sicherheit und Datenschutz entwickeln soll, arbeitet mein Kollege aus Schleswig-Holstein erfolgreich mit. Im Dezember 2011 fand die konstituierende Sitzung des KoSIT-Beirates statt. Der IT-Planungsrat hatte die Datenschutzkonferenz ausdrücklich gebeten, einen Vertreter in das Gremium zu entsenden. Dies erscheint mir besonders wichtig, da sowohl von den Landesdatenschutzbeauftragten als auch von einigen Landesparlamenten gefordert wurde, nur solche Interoperabilitäts- und IT-Sicherheitsstandards festzulegen, die dem Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme genügen. Auch hier hat mein Kollege aus Schleswig-Holstein sich zur Mitarbeit bereit erklärt, sodass davon ausgegangen werden kann, dass Datenschutzaspekte in angemessener Form berücksichtigt werden.

3.2.8 Stiftung Datenschutz

Der Koalitionsvertrag der Regierungsparteien auf Bundesebene sieht die Errichtung einer Stiftung Datenschutz vor, die Produkte und Dienstleistungen auf Datenschutzfreundlichkeit prüfen, die Bildung im Bereich des Datenschutzes stärken, die Aufklärung zwecks Prävention verbessern und ein Datenschutzaudit entwickeln soll. Die Datenschutzbeauftragten des Bundes und der Länder haben im Ergebnis der 80. Datenschutzkonferenz im November 2010 klargestellt, dass ein Mehrwert der als Unterstützung grundsätzlich zu begrüßenden Stiftung nur gewährleistet ist, wenn die Stiftung ihre Aufgaben in personeller und finanzieller Unabhängigkeit von den Daten verarbeitenden Stellen wahrnimmt, zudem mit auskömmlichen finanziellen Mitteln versorgt ist, eng mit den Datenschutzbehörden kooperiert und etwaige alleinige oder vorrangige Länderkompetenzen - wie zum Beispiel im Bereich der Bildung - schon auf Grundlage ihrer entsprechend zu gestaltenden Satzung respektiert.

Entgegen vereinzelter Ankündigungen aus der Bundespolitik konnte die Stiftung jedoch im Jahr 2011 nicht mehr starten, sondern wird wohl erst im Jahr 2012 ihre Aufgaben aufnehmen. Offenbar ist die Verzögerung auf Unklarheiten hinsichtlich des Umfangs der finanziellen Ausstattung und der finanziellen Struktur der Stiftung sowie auf noch ungeklärte Probleme hinsichtlich des Standortes und des genauen Aufgabenprofils zurückzuführen. Insbesondere auch die Frage der Gütesiegelvergabe und der vergleichenden Tests wird derzeit noch besonders kontrovers diskutiert.

Bei allem Verständnis für die Erforderlichkeit einer gründlichen Analyse und Abwägung der potentiellen Wirkungsmöglichkeiten einer unabhängigen Stiftung wird die Politik darauf zu achten haben, dass schon durch die bisherige erhebliche Dauer der Diskussion das eigentliche Anliegen nicht zerredet wird. Ich betone an dieser Stelle unter Verweis auf den oben zitierten Beschluss, dass die Unabhängigkeit der Stiftung bei der Gütesiegelvergabe und der Durchführung von vergleichenden Tests sowie hinsichtlich einer unbedingt erforderlichen transparenten und auskömmlichen Finanzierung ohne jede Einschränkung gewahrt werden muss. Nur unter diesen Voraussetzungen kann und wird die Stiftung als Unterstützung bzw. Bereicherung der bisherigen Datenschutzstrukturen Positives (und nicht etwa Negatives) bewirken.

Ich empfehle der Landesregierung, sich für die personelle und finanzielle Unabhängigkeit der geplanten Stiftung Datenschutz einzusetzen und darauf hinzuwirken.

3.3 Neue Entwicklungen im Landesrecht

3.3.1 Landesdatenschutzgesetz

Mit der notwendig gewordenen Überarbeitung des Landesdatenschutzgesetzes Mecklenburg-Vorpommern (DSG M-V) im Mai 2011 erfuhr das Gesetz seit 2002 seine sechste Novellierung. Diese ungewöhnlich hohe Frequenz macht die ausgesprochene Aktualitätsbezogenheit und Dynamik der Rechtsmaterie des Datenschutzes deutlich, die sich wie kaum eine andere ständig verändernden Anforderungen zu stellen hat.

Dies liegt zum einen in den sehr schnell eintretenden technischen Entwicklungen insbesondere im IT- und Sicherheitsbereich, und zum anderen darin begründet, dass sich gelingender Datenschutz als Ausfluss des informationellen Selbstbestimmungsrechtes nicht als statische Ideologie, sondern als flexibler kontext- und erkenntnisabhängiger gesellschaftlicher Konsens immer wieder neu definieren und behaupten muss.

Gemäß § 1 DSG M-V gilt das Landesdatenschutzgesetz für Behörden und öffentlich-rechtliche Einrichtungen und Stellen des Landes, der Landkreise, der Ämter, der Gemeinden sowie für sonstige der Aufsicht des Landes unterstehende juristische Personen des öffentlichen Rechts (sog. öffentliche Stellen). Bei öffentlich-rechtlichen Wettbewerbsunternehmen gelten das DSG M-V und das Bundesdatenschutzgesetz (BDSG) jeweils eingeschränkt (siehe § 1 Abs. 5 DSG M-V).

Die auch von mir zum großen Teil unterstützten wesentlichen Neuerungen des Gesetzes betrafen vor allem:

- § 5 Abs. 2: Benehmensepflicht für Prüfung informationstechnischer Produkte
- § 27 Abs. 4 S. 1 und 2: Anpassung des Bußgeldrahmens an das BDSG (auf 130.000 €)
- § 29 Abs. 6 S. 2: Stärkung der Unabhängigkeit des Landesdatenschutzbeauftragten
- § 33a S. 2: Entfall der Rechtsaufsicht durch das Innenministerium
- § 33b: Einführung des Datenschutzbeirates
- § 42: Ordnungswidrigkeiten im öffentlichen Bereich

Die in § 5 Abs. 2 neu geregelte Benehmensepflicht für die Prüfung informationstechnischer Produkte war einer alternativen Genehmigungspflicht schon aus Bürokratierwägungen vorzuziehen. So wird der Landesbeauftragte für den Datenschutz in die Lage versetzt, konstruktiv und nicht schlicht restriktiv oder gar repressiv am Prüfverfahren mitzuwirken und durch die damit verbundene Sachverhaltskenntnis die förderlichen Beratungsprozesse kompetent sowie auf dem aktuellen Stand zu gestalten. Ein Audit-Verfahren ist durch diese Bestimmung noch nicht etabliert, könnte sich aber bei weiteren Novellierungen auf der Basis der hierdurch gewonnenen Erfahrungen als geeignete Zukunftsvariante herausstellen.

Die weitgehende Herstellung der Unabhängigkeit meiner Behörde und ihrer Aufgabenerfüllung durch die Neuerungen in den §§ 29 Abs. 6 S. 2 und 33a S. 2 (Einschränkung der Dienstaufsicht und Wegfall der Rechtsaufsicht) entsprechen dem Grunde nach bundesweitem sowie europaweitem Standard, der durch die aktuelle Rechtsprechung des EuGH begründet wurde. Der Landesgesetzgeber entschied sich hier nach dem Vorbild einiger Bundesländer für eine „Minimallösung“, die keine weitergehenden Regelungen etwa zum Status der Behörde des Landesbeauftragten (als oberster Landesbehörde) und zu Haushaltsbudgets etc. enthält und zudem eine „Restdienstaufsicht“ ohne fachliche Befugnisse weiter bestehen lässt. Ob diese Kompromisslösung Bestand haben kann, wird sich im Lichte des neuen Rechtsrahmens der EU zum Datenschutz erweisen, da in der geplanten Verordnung auch dezidierte Regelungen zur Unabhängigkeit der Aufsichtsbehörden vorgesehen sind.

Durch die Einfügung des neuen § 33b wird ein Datenschutzbeirat etabliert, der sowohl eine beratende als auch für die landesweite Einigung zu Datenschutzstandards unterstützende Funktion erfüllen soll. Der Beirat besteht aus zehn, für die Datenschutzthemen des DSGVO M-V besonders relevanten, Mitgliedern, die jeweils vom Landtag bestellt werden. Der Landesbeauftragte für den Datenschutz ist selbst kein reguläres Mitglied, nimmt aber gemäß § 33b Abs. 5 an den Sitzungen teil und informiert den Beirat zum Beispiel vor Beanstandungen nach § 32 Abs. 1. Der Beirat soll nicht auf eine Monofunktion und Einbahnstraße beschränkt sein, indem er den Datenschutzbeauftragten ausschließlich berät. Sondern er soll auch in umgekehrter Richtung als Multiplikatoren gremium die Anliegen und Themen des Datenschutzes nach außen transportieren und so die Gewährleistung und den Schutz des Rechtes auf informationelle Selbstbestimmung auf einen breiten Konsens hin orientieren.

Durch die Neuregelung des § 42 wurden letztlich auch für den öffentlichen Bereich Ordnungswidrigkeiten eingeführt - mit entsprechenden Rechtsfolgen bei etwaigen Verstößen. Gemäß § 42 Abs. 4 wurde als zuständige Behörde für die Verfolgung und Ahndung dieser Ordnungswidrigkeiten jedoch nicht die wohl naheliegende unabhängige Fachbehörde des Landesbeauftragten für den Datenschutz, sondern die jeweils zuständige Aufsichtsbehörde bzw. die verarbeitende Stelle selbst - wenn diese als oberste Behörde keiner behördlichen Aufsicht untersteht - bestimmt. Dies führt in bestimmten Situationen zu einer „Selbstbestrafung“ innerhalb einer Behörde - eine dem Datenschutz möglicherweise nicht förderliche Rechtsfolge. Ob sich diese Regelung im weiteren Verfahren bewährt, soll Gegenstand einer entsprechenden Auswertung sein, die ich in den kommenden Jahren als einen Beitrag zur Umsetzung der Koalitionsvereinbarungsziffern 390 und 391 plane.

Für zukünftige Anpassungen des DSG M-V an die Erfordernisse eines modernen Datenschutzes plane ich zudem eine genaue Auswertung der geänderten und noch unverändert weiter geltenden Regelungen des DSG M-V und des IFG M-V. Schon jetzt kristallisieren sich aber zwei Änderungsbedarfe heraus, auf die ich hinweisen möchte und die ich mit jeweils einer Empfehlung verbinde:

Zum einen stellt sich in der Praxis bei § 18 DSG M-V (Verfahrensverzeichnis) die exakte Definition der Formulierung „jedes eingesetzte Verfahren“ als im Rahmen des geltenden Wortlautes kaum praktikabel lösbares Problem dar. So stellt sich unter anderem die Frage, ob damit auch einfachste Word- bzw. Excel-Alltagstätigkeiten gemeint sein können.

Um diese rechtliche Unklarheit zu beseitigen, empfehle ich dem Gesetzgeber, die Anwendung dieses Begriffes auf automatisierte Verfahren zu beschränken, mit der Ausnahme bei allgemeinen und nur Verwaltungszwecken dienenden automatischen Verarbeitungen, bei denen das Auskunftsrecht nach § 19 Abs. 3 oder 4 eingeschränkt wird (siehe auch § 18 Abs. 2 BDSG).

Zum anderen deckten laufende Auseinandersetzungen zwischen Aufsichtsbehörden und vor allem multinationalen Unternehmen ungewollte Unklarheiten bzw. nicht sachgemäße Zuständigkeitsregelungen formaler Art bei der Durchführung von Ordnungswidrigkeitsverfahren auf. Dies ist auch in Mecklenburg-Vorpommern der Fall.

Ich empfehle zur Beseitigung dieser Gesetzesmängel daher eine Regelung innerhalb des § 42 Abs. 4 DSG M-V etwa mit dem Inhalt, dass für Ordnungswidrigkeiten nach § 85 SGB X und nach Abschnitt 4 des TMG der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern die Verwaltungsbehörde im Sinne des § 36 Abs. 1 Nr. 1 des Gesetzes über Ordnungswidrigkeiten (OWiG) ist.

3.3.2 Sicherheits- und Ordnungsgesetz

Das neue Sicherheits- und Ordnungsgesetz (SOG M-V) ist am 31. März 2011 in Kraft getreten. In meiner schriftlichen Stellungnahme und während der mündlichen Anhörung zum Entwurf des Gesetzes (LT-Drucksache 5/3735) habe ich mich im Wesentlichen wie folgt geäußert:

Videüberwachung

Die im Gesetzentwurf gewählte Formulierung ist aus datenschutzrechtlicher und aus verfassungsrechtlicher Sicht nicht zu befürworten. Die Formulierung „ein die öffentliche Sicherheit schädigendes Ereignis“ dürfte wohl kaum für eine an einem öffentlichen Ort einzurichtende Videobeobachtung ausreichen.

Eine Videüberwachung auch nur in Form der Beobachtung erfasst regelmäßig eine Vielzahl von Personen, die sich an einem Ort aufhält und sich überwiegend normenkonform verhält. Es bleibt unklar, ob ein einzelnes schädigendes Ereignis ausreichen soll, um eine Videobeobachtung rechtfertigen zu können. Zudem stellt sich die Frage, auf welcher Tatsachenbasis dazu eine entsprechende Prognoseentscheidung getroffen werden soll. Die Tatbestandsvoraussetzung „ein die öffentliche Sicherheit schädigendes Ereignis“ ist daher zu unbestimmt.

Auch halte ich die Maßnahme für nicht geeignet, da die Videobeobachtung voraussetzt, dass in einer Polizeidienststelle jemand ständig vor dem Monitor sitzt und gegebenenfalls sofort einen Streifenwagen zu dem betreffenden Ort hinschicken müsste. Durch den eintretenden Zeitverzug und die Tatsache, dass nach Satz 1 eine Speicherung der Bilder nicht zulässig ist, ist diese Alternative der Videobeobachtung unpraktikabel und daher schon nicht geeignet.

Verfahren beim Einsatz besonderer Mittel der Datenerhebung

Ich begrüße es ausdrücklich, dass die Landesregierung und dem folgend der Fraktionsentwurf meine dringende Anregung aus dem 8. Tätigkeitsbericht (LT-Drucksache 5/1440) aufgegriffen hat und dementsprechend die Regelungen zum Unterbleiben der Unterrichtung des Betroffenen insbesondere bei Observationen in § 34 Abs. 6 des Gesetzentwurfs neu gefasst hat.

In § 34 Abs. 5 SOG M-V ist die Frist für die Unterrichtung des Landesbeauftragten für den Datenschutz bei Observationen geregelt. Ich hatte bereits anlässlich der Novellierung des SOG M-V im Jahre 2006 empfohlen, die Frist für die Unterrichtung des Landesbeauftragten für den Datenschutz zeitlich früher zu setzen. Bisher lautet die Formulierung: Ist dies (gemeint ist die Unterrichtung des Betroffenen) fünf Jahre nach Abschluss der Maßnahme nicht möglich, ist der Landesbeauftragte für den Datenschutz zu unterrichten“. Diese Frist ist eindeutig zu lang bemessen. Wenn der Landesbeauftragte für den Datenschutz im Bereich der Observationen prüfen soll, muss er über die Zurückstellung der Unterrichtung früher informiert werden. Andernfalls besteht die Gefahr, dass sich eine datenschutzrechtliche Überprüfung durch Zeitablauf erledigt.

Datenerhebung zur Überwachung der Telekommunikation

Aus datenschutzrechtlicher Sicht sollte überlegt werden, die Datenerhebung zur Überwachung der Telekommunikation gänzlich zu streichen bzw. inhaltlich stark einzuschränken.

Für problematisch erachtete ich es insbesondere, Inhalte der Telekommunikation aufzuzeichnen. Vor dem Hintergrund der Rechtsprechung des Bundesverfassungsgerichts zur Vorratsdatenspeicherung (BVerfG, Urteil vom 2. März 2010 - 1 BvR 256/08), die schon die Speicherung von Verkehrsdaten (und demzufolge auch die Abfrage der entsprechenden Daten) für verfassungswidrig hielt, erscheint eine Abfrage der Inhaltsdaten erst recht als unverhältnismäßig. Bei einem Vergleich mit den Polizeigesetzen anderer Bundesländer, beispielsweise mit dem von Nordrhein-Westfalen, Brandenburg oder Hamburg, fällt auf, dass diese ganz ohne Abfrage der Telekommunikationsdaten im präventiven Bereich auskommen. Daher sollte auch in Mecklenburg-Vorpommern das Erfordernis dieser Norm gründlich überdacht werden.

Einsatz technischer Mittel zur Erkennung von Kraftfahrzeugkennzeichen

Der Einsatz technischer Mittel zur Erkennung von Kraftfahrzeugkennzeichen sollte nach dem vorliegenden Fraktionsentwurf neu gefasst werden. Ich bin ebenfalls der Auffassung, wie es der Entwurf in seiner Begründung darlegt, dass die entsprechende brandenburgische Regelung Vorbild sein sollte, da allein diese vom Bundesverfassungsgericht in seiner Entscheidung vom 11. März 2008 (1 BvR 2074/05) als verfassungskonform eingestuft wurde. Was die Voraussetzungen anbelangt, trifft dies auf die Nummern 1 bis 3 des Absatzes 1 des Entwurfs zu; die Nummern 4 und 5 gehen jedoch darüber hinaus, was gerade nicht den Ausführungen des Bundesverfassungsgerichts in seiner oben genannten Entscheidung entspricht.

Meine Bedenken sind im laufenden Gesetzgebungsverfahren - mit Ausnahme der Regelungen zum Unterbleiben der Unterrichtung des Betroffenen bei verdeckten Datenerhebungen - nicht berücksichtigt worden.

3.3.3 Landeskrankenhausgesetz

Am 20. Januar 2010 sandte mir das Ministerium für Soziales und Gesundheit den Entwurf des Landeskrankenhausgesetzes zu, durch den das bestehende Gesetz novelliert werden sollte. Bis zum 29. Januar 2010 sollte meine Stellungnahme beim Ministerium vorliegen. Bei der geplanten umfassenden Änderung des Gesetzes war dieser Zeitraum unangemessen kurz. In der Regel wird dadurch zweifellos vorhandenes datenschutzrechtliches Optimierungspotenzial verschenkt.

Der Entwurf sah vor, dass die Regelungen zum Patientendatenschutz an das Ende des Gesetzes verschoben werden, was mit systematischen Aspekten begründet wurde. Der Regelungsumfang sollte außerdem so knapp wie möglich gefasst werden. Das hat dazu geführt, dass wesentliche datenschutzrechtliche Regelungen zu dem damals bestehenden Gesetz nicht mehr vorhanden waren und damit das Recht der Patientinnen und Patienten auf informationelle Selbstbestimmung nach meiner Auffassung unzulässig verkürzt wurde. So war an zentraler Stelle des Entwurfs die Einwilligung der Patientin bzw. des Patienten, insbesondere hinsichtlich der Übermittlung ihrer bzw. seiner Daten, nicht mehr vorgesehen.

Begründet wurde dies damit, dass die Einwilligung im Landesdatenschutzgesetz geregelt ist und daher in diesem Gesetz darauf verzichtet werden kann. Wäre die Einwilligung nicht mehr im Landeskrankenhausgesetz ausdrücklich enthalten, hätte aber die Gefahr bestanden, dass dieses essenzielle Recht der Patienten nicht mehr angewendet werden würde. An der Systematik des Gesetzentwurfes habe ich auch kritisiert, dass die Abschnitte Patientenrechte und Patientendatenschutz getrennt an voneinander weit entfernten Orten im Gesetz platziert worden sind, obwohl sie zusammengehören. Schließlich ist der Patientendatenschutz ein wesentlicher Bestandteil der Patientenrechte, die seinerzeit meines Erachtens zu recht an den Anfang des Gesetzes gestellt worden sind.

Im Einzelnen habe ich an dem Gesetzentwurf weiterhin Folgendes bemängelt:

- Der Begriff „Patientendaten“ anstelle von „personenbezogenen Daten“ sollte wie bisher im Landeskrankenhausgesetz durchgängig erhalten bleiben.
- Bei der Wahrnehmung des Auskunftsrechts der Patientinnen und Patienten sollten auch die Bestimmungen des Landesdatenschutzgesetzes beachtet werden, was dazu geführt hätte, dass die dort festgelegten Einschränkungen, beispielsweise bei der Gefährdung der öffentlichen Sicherheit, ohne ersichtlichen Grund bei der Anwendung des Landeskrankenhausgesetzes beachtet werden müssten.
- Durch die Zusammenfassung der Regelungen zur Verarbeitung von Patientendaten und anonymisierten Daten für unterschiedliche Zwecke wäre die Anwendbarkeit des Gesetzes für die Krankenhausmitarbeiter unnötig erschwert worden.
- Die Systematik innerhalb der Normen zum Patientendatenschutz sollte erhalten bleiben. So sollte nach dem Entwurf die Norm zur Übermittlung von Patientendaten innerhalb eines Krankenhauses auf die Norm zur Übermittlung an Stellen außerhalb des Krankenhauses folgen, was die Anwendung nach meiner Auffassung ebenfalls erschwert hätte.

Der Gesetzentwurf wurde aufgrund meiner Kritik geändert. Die bewährten Regelungen zum Patientendatenschutz sind bis auf kleinere Änderungen erhalten geblieben. Leider wurde aber meiner Empfehlung nicht gefolgt, Patientenrechte und Patientendatenschutz in einem Abschnitt oder zusammenhängend zu regeln.

Eine aufgrund der Gesetzesänderung aktualisierte Version meiner Hinweise zum „Datenschutz im Krankenhaus“ steht auf meiner Internetseite zur Verfügung.

3.3.4 Klinisches Krebsregistergesetz

Im Dezember 2010 sandte mir das Ministerium für Soziales und Gesundheit den Entwurf eines Gesetzes zur Ergänzung und Änderung von Gesundheitsrecht und des Aufgabenzuordnungsgesetzes zur datenschutzrechtlichen Stellungnahme zu. Der Gesetzentwurf war als Artikelgesetz aufgebaut und enthielt als Artikel 1 den Entwurf eines Klinischen Krebsregistergesetzes.

Mit dem Gesetzentwurf verfolgte die Landesregierung das Ziel, die in den vier regionalen klinischen Krebsregistern in Greifswald, Neubrandenburg, Rostock und Schwerin gespeicherten Daten zu einem zentralen klinischen Krebsregister zusammenzuführen. Nach der Gesetzesbegründung solle der Vorteil für Patientinnen und Patienten unter anderem darin liegen, dass durch nahezu vollständige Meldungen der Informationsfluss zwischen den Behandlern optimiert und die Nachsorge gezielt gesteuert werden könne.

Die Patientinnen und Patienten würden mittelbar aus der Transparenz Nutzen ziehen können und somit bei ihrer Auswahlentscheidung für Behandlungsformen unterstützt werden. Die landesweiten Auswertungen sollen darüber hinaus zu Qualitätsverbesserungen der Diagnostik und der Therapie führen.

Die gesetzlichen Regelungen sehen eine Meldepflicht der Ärzte und ein Widerspruchsrecht der Patienten vor. Das zentrale klinische Krebsregister sollte die Identitätsdaten der Patienten verschlüsseln und unter einem Patientenidentifikator die klinischen Daten speichern.

Nach meiner Auffassung steht vor diesem Hintergrund die Datenverarbeitung in einem regionalen klinischen Krebsregister im Widerspruch zu der beabsichtigten Datenverarbeitung in dem zu bildenden zentralen klinischen Krebsregister. In einem regionalen klinischen Krebsregister werden Daten von Patientinnen oder Patienten nur dann gespeichert, wenn sie freiwillig in die Datenverarbeitung und Datennutzung eingewilligt haben. In dem zentralen Register sollen die Daten auf der Grundlage der neuen gesetzlichen Regelung gespeichert werden. Diese Regelung bedeutet, dass die Daten aller krebserkrankten Patientinnen und Patienten erfasst und solange gespeichert werden, bis gegebenenfalls ein Patient von dem Widerspruchsrecht Gebrauch macht. Deswegen habe ich mich dafür eingesetzt, auch in dem neu zu bildenden zentralen klinischen Krebsregister Daten von Anfang an auf der Grundlage der freiwilligen Einwilligung zu speichern. Zumindest sollten aber verfahrensrechtliche Vorkehrungen getroffen werden, die dazu beitragen, die Selbstbestimmung der Patienten zu wahren.

Die (Regierungs-)Fraktionen der SPD und der CDU haben schließlich einen Änderungsantrag in das Gesetzgebungsverfahren eingebracht, der zwar weiterhin die Widerspruchslösung gegen die Verarbeitung und Nutzung der Daten im zentralen klinischen Krebsregister vorsieht, nun aber das Datenmanagement ändert und eine Treuhandstelle vorschreibt, die aus den identifizierenden Daten der Patienten ein Pseudonym bildet, unter dem die klinischen Daten in dem zentralen klinischen Krebsregister gespeichert werden. Mit diesen verfahrensrechtlichen Vorkehrungen hat der Gesetzgeber das Gesetz beschlossen.

In den datenschutzrechtlichen Stellungnahmen habe ich eine Vielzahl von Detailfragen angesprochen, die hier nicht umfassend dargestellt werden können. Auch nach der Verabschiedung des Gesetzes habe ich das Ministerium für Arbeit, Gleichstellung und Soziales auf nach meiner Auffassung klarzustellende oder zu klärende Fragen hingewiesen. Dazu steht noch eine Antwort aus.

4. Technik und Organisation

4.1 Neue Technologien

4.1.1 Datenschutzgerechtes Cloud-Computing - geht das?

Ein Schwerpunktthema der Computermesse CeBIT des Jahres 2011 hieß „Work and Life with the Cloud“. Glaubt man den Werbebotschaften einiger Cloud-Befürworter, wird Cloud-Computing die gesamte IT-Welt revolutionieren. Cloud-Computing steht für „Datenverarbeitung in der Wolke“ und beschreibt eine über Kommunikationsnetze angeschlossene Rechnerlandschaft, in welche die eigene Datenverarbeitung teilweise oder vollständig ausgelagert wird. Cloud-Anwender können beliebige IT-Dienstleistungen bedarfsgerecht und flexibel nutzen, indem diese in Echtzeit als Service über das Internet bereitgestellt werden und nach dem individuellen Ressourcenverbrauch abgerechnet werden. Da diese Art der Datenverarbeitung auch personenbezogene Daten betreffen wird, ist vor dem Beginn der Verarbeitung zu klären, wie der Datenschutz gewährleistet werden kann.

Bei Cloud-Computing handelt es sich in den meisten Fällen um eine spezielle Form der Datenverarbeitung im Auftrag, wobei der Auftraggeber (Cloud-Anwender) eine IT-Dienstleistung (Cloud-Service) in Anspruch nimmt, die der Auftragnehmer (Cloud-Anbieter) zur Verfügung stellt. Das besondere Kennzeichen der Datenverarbeitung im Auftrag ist, dass der Auftraggeber, in diesem Fall der Cloud-Anwender, für die Einhaltung sämtlicher datenschutzrechtlicher Bestimmungen verantwortlich bleibt.

Für den Cloud-Anwender kann es jedoch mit erheblichen Schwierigkeiten verbunden sein, seinen gesetzlich vorgegebenen Pflichten als Auftraggeber nachzukommen. Einerseits hat er oftmals nur sehr beschränkte Einflussmöglichkeiten auf die Art und Weise der Datenverarbeitung, insbesondere dann, wenn die gleiche IT-Dienstleistung vielen verschiedenen Kunden am freien Markt angeboten wird. Andererseits kann er kaum nachvollziehen, wo „seine“ Daten zu bestimmten Zeitpunkten gerade verarbeitet werden, da die Cloud-Anbieter mitunter weltweit verteilte IT-Ressourcen nutzen, um die Dienstleistung möglichst kostengünstig anbieten zu können. Erschwerend kommt hinzu, dass bei bestimmten Formen des Cloud-Computing nicht etwa nur die Hardware-Komponenten der Cloud-Anbieter, sondern zusätzlich auch deren Betriebssysteme und Anwendungen genutzt werden, sodass der Cloud-Anwender keine administrativen, operativen oder kontrollierenden Zugriff mehr hat.

Zudem wurde im Laufe des Jahres 2011 bekannt, dass US-Behörden unter anderem auf der Grundlage des US-Patriot Act nicht nur auf personenbezogene Daten zugreifen, die in den Vereinigten Staaten gespeichert sind, sondern wohl auch auf Daten innerhalb der EU und des EWR (Europäischer Wirtschaftsraum). Große Unternehmen wie Google oder Microsoft hatten erklärt, dass sie entsprechenden Anforderungen von US-Behörden jedenfalls Folge leisten müssten. Vertreter deutscher Datenschutzaufsichtsbehörden haben darauf hingewiesen, dass ein solches Vorgehen ausländischer Behörden unter Missachtung des Territorialprinzips gegen europäisches und deutsches Datenschutzrecht verstößt. Die Europäische Kommission wurde aufgefordert zu klären, wie das in der Charta der Grundrechte der Europäischen Union garantierte Grundrecht auf Datenschutz im Hinblick auf die genannten Herausforderungen gemeistert werden kann.

Um dennoch den Datenschutz bei der Verarbeitung personenbezogener Daten in der Cloud zu gewährleisten, ist eine Reihe organisatorischer und technischer Maßnahmen erforderlich. In jedem Fall ist ein schriftlicher Vertrag zwischen Cloud-Anwender und Cloud-Anbieter erforderlich, der die Anforderungen des § 4 DSGVO M-V bzw. des § 11 BDSG erfüllt. Dazu gehört unter anderem, dass sich der Cloud-Anwender vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Cloud-Anbieter getroffenen technischen und organisatorischen Maßnahmen zu überzeugen hat. Für den Fall, dass Kontrollen vor Ort nicht möglich sind, können aktuelle und aussagekräftige Nachweise (bspw. Zertifikate anerkannter und unabhängiger Prüfungsorganisationen) über die Infrastruktur den Nachweis über die Datenschutzkonformität erbringen. Solche Zertifikate entbinden den Cloud-Anwender jedoch nicht vollständig von seinen weiteren Kontrollpflichten.

Da die Cloud nicht an geographische Grenzen gebunden und die darin stattfindende Datenverarbeitung gerade nicht ortsgebunden ist, ist es wichtig, dass der Cloud-Anwender über sämtliche möglichen Verarbeitungsorte vorab informiert wird. EU-Recht ist in diesem Zusammenhang bereits dann anwendbar, wenn personenbezogene Daten in einer in der EU gelegenen Niederlassung verarbeitet oder wenn die für die Verarbeitung verwendeten Mittel im Hoheitsgebiet der EU gelegen sind. Für Clouds im innereuropäischen Raum, bei denen die Datenverarbeitung ausschließlich innerhalb des EWR stattfindet, ergeben sich - abgesehen von den oben erwähnten umstrittenen Zugriffsbefugnissen amerikanischer Behörden infolge des US-Patriot Act - keine Besonderheiten, da die datenschutzrechtlichen Anforderungen der Europäischen Datenschutzrichtlinie 95/46/EG gelten. Cloud-Anbieter sollten daher verpflichtet werden, nur technische Infrastrukturen zu verwenden, die sich physikalisch auf dem Gebiet des EWR befinden.

Werden jedoch Daten außerhalb der EU und des EWR verarbeitet, was bei weltweit agierenden Anbietern wie Amazon, Google oder Microsoft regelmäßig der Fall sein dürfte, gelten die besonderen Anforderungen der §§ 4b, 4c BDSG für den sogenannten Drittstaatentransfer. Falls in dem Drittstaat kein angemessenes Datenschutzniveau besteht, müssen ausreichende Garantien zum Schutz des allgemeinen Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorgewiesen werden. Die Garantien können sich aus den sogenannten Standardvertragsklauseln der EU-Kommission vom 5. Februar 2010 ergeben. Bei konzernangehörigen Auftragnehmern, wenn also Cloud-Anwender und Cloud-Anbieter derselben Unternehmensgruppe angehören, können die erforderlichen ausreichenden Garantien zum Schutz der Persönlichkeitsrechte durch Binding Corporate Rules geschaffen werden. Werden personenbezogene Daten durch einen Cloud-Anbieter mit Sitz in den USA verarbeitet, können die EU-Standardvertragsklauseln ebenso wie Binding Corporate Rules entbehrlich sein, wenn sich der Cloud-Anbieter zur Einhaltung der Safe-Habor-Grundsätze verpflichtet hat. Bei allen genannten Regelungen werden die spezifischen Anforderungen der Auftragsdatenverarbeitung aber nicht vollständig abgebildet. Aus diesem Grunde muss der Cloud-Anwender zusätzlich die Anforderungen nach § 11 Abs. 2 BDSG erfüllen und entsprechend vertraglich abbilden. Dies kann durch Regelungen in den Anlagen zum Standardvertrag, durch ergänzende geschäftsbezogene Klauseln oder durch separate vertragliche Regelungen erfolgen.

Für die Cloud-Computing-Systeme der Cloud-Anbieter müssen technische und organisatorische Maßnahmen getroffen werden, deren Umsetzung die Verfügbarkeit, Vertraulichkeit, Integrität, Revisionssicherheit und Transparenz der Datenverarbeitung sowie die ordnungsgemäße Löschung und Trennung von Daten gewährleisten. Die Details dieser Maßnahmen hängen sowohl von den Betriebsmodellen und Typen des gewählten Cloud-Verfahrens als auch von der Sensibilität der verarbeiteten Daten ab. Aber auch Cloud-Anwender sind in der Pflicht, entsprechende Vorkehrungen zu treffen. So kann etwa Zugriffen von US-Behörden auf in der Cloud gespeicherte Daten nur begegnet werden, wenn der Cloud-Anwender seine Daten bereits vor der Übertragung in die Cloud selbst verschlüsselt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im September 2011 eine Orientierungshilfe zum Thema Cloud-Computing verabschiedet, in der ausführlich beschrieben wird, welche Maßnahmen bei welchen Cloud-Typen erforderlich sind. Die Orientierungshilfe kann aus meinem Internetangebot heruntergeladen werden (http://www.datenschutz-mv.de/dschutz/informat/cloud/oh_cloud.pdf).

Erste Reaktionen aus der Wirtschaft zeigen, dass die Orientierungshilfe als geeignetes Hilfsmittel zur datenschutzkonformen Ausgestaltung von Cloud-Diensten anerkannt wird. So hat die Firma Microsoft im Dezember 2011 angekündigt, die Vertragsbestimmungen für seinen Cloud-Dienst Office 365 in Anlehnung an die Empfehlungen der Orientierungshilfe zu ändern, um auf diese Weise seine Kunden in ihren Datenschutzpflichten zu unterstützen.

Ich empfehle der Landesregierung, Cloud-Dienste allenfalls von solchen Cloud-Anbietern in Anspruch zu nehmen, die dem europäischen Datenschutzrecht unterliegen und die Vorgaben der Orientierungshilfe Cloud-Computing vollständig berücksichtigen. Die Landesregierung sollte zudem prüfen, ob der IT-Landesdienstleister DVZ M-V GmbH mit der Schaffung einer Cloud für die Landes- und Kommunalverwaltung beauftragt werden kann.

4.1.2 IPv6 - neue Adressen für das Internet

„Das Internet“ ist genau genommen eine Zusammenschaltung von Netzen vieler verschiedener Betreiber. Alle nutzen dieselben Kommunikationsregeln, nämlich die Familie von Netzwerkprotokollen, die auf dem Internet Protocol (IP) basiert. Die meisten Nutzer und Betreiber verwenden heute die Version 4 dieses Protokolls (IPv4).

Computer, die über das Internet miteinander kommunizieren sollen, benötigen eine Adresse. Das Internet Protokoll hat bisher 32 Bit lange Adressen definiert. Dieser Adressraum reicht für ca. 4 Milliarden Adressen. Seit Anfang 2011 sind nun alle verfügbaren Adressen aufgeteilt und für Internet-Provider und viele andere Akteure ist es Zeit, Alternativen zu planen und zu realisieren.

Mit dem Internet Protocol Version 6 (IPv6) gibt es eine solche Alternative.

Der Adressraum dieses Protokolls ist bei 128 Bit langen Adressen sehr viel größer und umfasst unvorstellbare 10^{38} Adressen. Das sind 340 Sextillionen Adressen, mit denen man in der Lage wäre, jedem Quadratmillimeter der Erdoberfläche inklusive Ozeanen rund 600 Billionen Adressen zuzuweisen. Theoretisch könnte man jedem Sandkorn auf der Erde mehrere Internetadressen zuweisen. Durch den Umstieg auf IPv6 wird der heute bestehende Adressmangel damit mehr als behoben. Somit ist die heute bei Endkunden übliche dynamische Adresszuweisung - also die temporäre Zuweisung von Adressen - nicht mehr erforderlich, weiterhin möglich bleibt sie aber. Jedem Gerät kann nicht nur eine einzelne Adresse statisch zugeteilt werden, sondern ein ganzer Adressbereich. Dies hat auch Auswirkungen auf den Datenschutz, sowohl negative als auch positive.

Als negative Auswirkung ist festzustellen, dass sich durch die Vergabe statischer Adressen das Risiko erhöht, dass Internetnutzer identifiziert und ihre Aktivitäten auf einfache Weise zu individuellen Profilen zusammengeführt werden können. Sowohl der von den Internet-Providern bereitgestellte Adressanteil (Präfix) als auch gerätespezifische Anteile im hinteren Teil der IPv6-Adressen (Interface Identifier) machen eine dauerhafte Identifizierung möglich. Um einen konstanten und somit leicht wieder erkennbaren Interface Identifier zu vermeiden, kann man die sogenannten Privacy Extensions von IPv6 einsetzen. Sie sorgen für eine zufällige Vergabe und einen regelmäßigen Wechsel dieses Adressteils.

Positiv kann sich die Tatsache auswirken, dass bei statischer Adressierung jedes einzelne Gerät nicht nur Dienste nutzen, sondern auch bereitstellen kann. Auf diese Weise lassen sich datenschutzfreundliche, dezentrale Applikationen für Soziale Netzwerke, Telefonie und viele andere Anwendungsgebiete herstellen. Dezentrale Kommunikation ermöglicht es den Nutzern, ihre Daten selbst zu verwalten und ihre Erreichbarkeit selbst zu steuern. Beobachtungs- und Einflussmöglichkeiten durch zentrale Einrichtungen wie Portale werden so wirksam eingeschränkt. Die direkte, gleichberechtigte Kommunikation (das sogenannte Peer-to-Peer-Prinzip) ist schon immer eine wesentliche Eigenschaft des Internet gewesen. Erst durch Geschäftsmodelle der Telekommunikationsdienstleister, bei denen der Zugang zum Internet mit dynamischen Adressen preiswerter als der Zugang mit statischen Adressen angeboten wurde, wurde dieses Prinzip zurückgedrängt. Die oben beschriebene Adressknappheit bei IPv4 beschleunigte diesen Verdrängungsprozess weiter.

Sowohl die deutschen Datenschutzbeauftragten als auch ihre Kollegen weltweit untersuchen seit geraumer Zeit, welche Chancen und Risiken für den Datenschutz mit dem Umstieg auf IPv6 verbunden sind.

So hat die Internationale Datenschutzkonferenz am 1. November 2011 in Mexico City eine Entschließung gefasst, die im Wesentlichen folgende Empfehlungen enthält (siehe <http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/IntDSK/2011InternetIPv6.html>):

Nutzer sollten von ihren Providern weiterhin dynamische Adressen erhalten können und sie sollten auch innerhalb einer laufenden Sitzung die Möglichkeit zum Wechsel der Adresse erhalten.

Dynamische Adressen sollen gemeinsam mit den Privacy Extensions genutzt werden können. Zusätzlich werden die Gerätehersteller aufgefordert, die Privacy Extensions in ihre Produkte einzubauen und standardmäßig zu aktivieren.

Außerdem soll, wann immer passend, die Sicherheitserweiterung IPsec benutzt werden, die IPv6-fähige Geräte gemäß den einschlägigen Standards beherrschen muss.

Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich mit diesem Thema befasst. Ihre Entschließung vom 28./29. September 2011 (siehe <http://www.datenschutz-mv.de/dschutz/beschlue/ipv6.pdf>) geht stärker auf die Chancen von IPv6 ein und empfiehlt zusätzlich beispielsweise:

Access Provider sollten den Kunden jeweils dynamische und statische Adressen zuweisen, damit sie den für ihre Anwendung jeweils passenden Adresstyp auswählen können.

Hard- und Softwarehersteller sollten den Kunden dezentrale Kommunikationsmöglichkeiten anbieten (Peer-to-peer-Dienste).

Content Provider dürfen zur Reichweitenmessung nur die ersten vier Bytes der IPv6-Adresse heranziehen und müssen den Rest löschen. Dieses Verfahren ermöglicht eine grobe Geolokalisierung und anonymisiert die Adressen gleichzeitig ausreichend.

Erste Erläuterungen zu diesen Thesen finden sich in einem Positionspapier des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ (AK Technik, siehe Punkt 6), das die Konferenz der Datenschutzbeauftragten von Bund und Ländern im Zusammenhang mit der Verabschiedung der oben genannten Entschließung zur Kenntnis genommen hat (siehe http://www.datenschutz.rlp.de/downloads/oh/Positionspapier_IPv6.pdf). Der AK Technik wird sich auch weiterhin mit dem Thema befassen. Zurzeit wird eine Orientierungshilfe zu Datenschutzaspekten von IPv6 erarbeitet, deren Fertigstellung für Anfang 2012 geplant ist.

4.1.3 Smart Meter - Energieverbrauchsmessung der Zukunft

Mit einem Richtlinienentwurf (2009/28/EG) zur Förderung erneuerbarer Energien hat die EU-Kommission das Ziel ausgegeben, bis zum Jahr 2020 den CO₂-Ausstoß um 20 % zu reduzieren und die Energieeffizienz und den Anteil erneuerbarer Energien auf 20 % anzuheben. Dazu bedarf es einer nachhaltigen Energieversorgung, die in der Lage ist, intelligente Verknüpfungen zwischen ihrer Erzeugung und Speicherung sowie ihrem Transport und Verbrauch herzustellen.

Mit Hilfe „intelligenter“ Stromnetze, den sogenannten Smart Grids, und intelligenter Mess- und Steuerungstechnik, den sogenannten Smart Metern, soll sichergestellt werden, dass stets die jeweils notwendige Energie zum gewünschten Zeitpunkt beim Verbraucher bereitgestellt werden kann.

Entsprechend verpflichtet das Energiewirtschaftsgesetz (EnWG) in § 21c die Betreiber von Energieversorgungsnetzen seit dem 1. Januar 2010 dazu, bei Neubauten, größeren Renovierungen oder bei Verbrauchern, die einen Jahresverbrauch von 6000 Kilowattstunden überschreiten, „intelligente“ Zähler einzubauen. Zudem müssen die Stromlieferanten gemäß § 40 EnWG lastvariable oder tageszeitabhängige Tarife anbieten, die dem Verbraucher einen Anreiz zur Energieeinsparung oder Steuerung des Energieverbrauchs liefern.

Im Vergleich zu den bisher üblichen (Ferraris-)Zählern können intelligente Stromzähler den Verbrauch sekundengenau erfassen und an zentrale Stellen weiterleiten. Mit Hilfe dieser Verbrauchsinformationen können Last- und Nutzungsprofile erstellt werden, aus denen ganze Tagesabläufe und damit auch Verhaltensprofile der Verbraucher abgeleitet werden können.

Wissenschaftliche Untersuchungen haben ergeben, dass aus derartigen Verbrauchsprofilen die Einschaltzeiten verschiedener elektrischer Geräte wie Herd, Kühlschrank, Wasserkocher, Waschmaschine oder Fernsehgerät ablesbar sind. Bei typischen Fernsehgeräten konnte darüber hinaus sogar nachvollzogen werden, welche Programme eingeschaltet bzw. welche Filme gesehen worden waren. Damit ist nicht nur das Recht auf informationelle Selbstbestimmung bedroht, sondern es besteht auch die Gefahr, dass es zum „gläsernen“ Energieverbraucher kommt. Damit genau dies nicht geschieht, sind datenschutzkonforme Konzepte für die neuen Mess- und Kommunikationseinrichtungen sowie gesetzliche Regelungen für die Erhebung, Verarbeitung und Nutzung der Verbrauchsinformationen unabdingbar.

In Zusammenarbeit mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und den Kolleginnen und Kollegen aus den anderen Bundesländern ist es gelungen, genau solche gesetzlichen Regelungen in die Novellierung des Energiewirtschaftsgesetzes vom 11. Juli 2011 einzubringen. Damit existiert nun ein Rechtsrahmen für den datenschutzgerechten Einsatz von Smart Metern. Besonders hervorzuheben ist dabei die Datenhoheit der Verbraucher. Beispielsweise darf künftig die Energielieferung nicht von der Offenlegung detaillierter Verbrauchsprofile abhängig gemacht werden. Gesetzlich verankert sind auch eine enge Zweckbindung für sensible Verbrauchsdaten sowie verbindliche Standards für die Datensicherheit. So dürfen zur Datenerhebung, -verarbeitung, -speicherung, -prüfung und -übermittlung ausschließlich solche technischen Systeme und Bestandteile eingesetzt werden, die den Anforderungen von sogenannten Schutzprofilen genügen. Gemeinsam mit einigen Kollegen von Bund und Ländern habe ich die Entwicklung dieses Schutzprofils durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) begleitet.

Das Schutzprofil beschreibt insbesondere technische Details der Kommunikationseinheit (Gateway) von Smart Metern. Das Gateway muss dem Verbraucher stets die Möglichkeit bieten, datenschutzfreundliche Einstellungen bei der Verbrauchsmessung zu wählen, ohne dass er dadurch Nachteile befürchten muss. So ist es durchaus wünschenswert, dass er seinen Energieverbrauch im Rahmen einer Visualisierung verfolgen und „Stromfresser“ identifizieren kann. Eine sekundengenau Übermittlung dieser Verbrauchsdaten an Dritte darf daran jedoch nicht gekoppelt sein. Im Schutzprofil wurde daher mit einer lokalen, kryptographisch gesicherten Schnittstelle, durch welche die Verbrauchsdaten ohne Umwege direkt abgerufen werden können, eine alternative Lösung verpflichtend festgeschrieben.

Tageszeit- und lastvariable Tarife sollen einen Anreiz für eine Energieeinsparung liefern. Jedoch ist es nicht erforderlich und darf daher nicht verlangt werden, dass Verbrauchsdaten im 15-Minuten-Takt übermittelt werden. Das Gateway soll daher für jeden Tarif ein separates Register vorsehen, das Verbrauchswerte der einzelnen Stromzähler sammelt und je nach gewähltem Tarif zu einem entsprechenden Summenwert zusammenfasst. Dieser Wert kann dann monatlich vom Gateway an den Lieferanten übermittelt werden.

Ebenfalls im Fokus des Schutzprofils stehen die im Datenschutz fest verankerten Schutzziele Authentizität, Vertraulichkeit und Integrität der Daten. So übernimmt ein Sicherheitsmodul die Verschlüsselung und Signierung der Verbrauchsdaten, um sicherzustellen, dass Verbrauchsdaten einerseits nur von den jeweils berechtigten Stellen eingesehen und verarbeitet und andererseits sicher einem Verbraucher zugeordnet und unverfälscht übermittelt werden können.

Die Einführung von Smart Meter und Smart Grid werde ich auch weiterhin beratend begleiten, denn die Entwicklung des Schutzprofils für die Kommunikationseinheit in Smart Metern ist nur der erste Schritt zu einem datenschutzgerechten Einsatz intelligenter Verbrauchsmesstechnik. Einerseits müssen weitere Schutzprofile entwickelt werden, andererseits ist eine technische Richtlinie erforderlich, welche beispielsweise die Interoperabilität der verschiedenen Komponenten in einem Smart Metering System gewährleistet.

4.1.4 Smartphone & Tablet PC im professionellen Einsatz

Mobile Endgeräte wie die sogenannten Smartphones (z. B. BlackBerry und iPhone) oder die Tablet PC wie iPad und Co. erreichen schon seit langem die Rechenleistung und Komplexität von handelsüblichen Personalcomputern und stehen deren Möglichkeiten daher in nichts mehr nach. Beliebige Anwendungen können überall und jederzeit, in der Regel auch mit einer Anbindung an das Internet, ausgeführt werden. Inzwischen hat nicht nur die Wirtschaft die vielfältigen und flexiblen Möglichkeiten für sich entdeckt, auch aus der öffentlichen Verwaltung erreichen mich immer mehr Nachfragen zum datenschutzgerechten Einsatz dieser Geräte. So hat der Landtag Mecklenburg-Vorpommern seine Abgeordneten beispielsweise mit „lüfterlosen Lesegeräten“ - so die offizielle Gerätebezeichnung, gemeint sind iPads der Firma Apple - ausgestattet, damit sie etwa während der Landtagssitzungen auf Landtagsdokumente online zugreifen können.

Sehr häufig enthalten die mobilen Endgeräte eine Vielzahl personenbezogener Daten, in der Regel werden dabei auch Daten Dritter (z. B. Kontaktdaten, E-Mails oder Bilder) erfasst. Die auf den Endgeräten gespeicherten Daten werden oft in intransparenter Weise und weitgehend unkontrollierbar an weitere Nutzer verteilt. Zudem entziehen sich die besonders einfach installierbaren Applikationen, die sogenannten Apps, oftmals der Kontrolle des Nutzers und machen beispielsweise Kontaktdaten sehr schnell für andere Anwendungen zugänglich. Andere Apps wiederum erzwingen einen weitgehenden Zugriff auf die Nutzerdaten und Rechte des Endgerätes. Zwar informieren diese in der Regel vor der Installation über die benötigten Zugriffsrechte und Ressourcen, echte Wahlmöglichkeiten hat der Nutzer jedoch kaum. Er muss diese Rechte meist vollständig gewähren, um die Applikation sinnvoll verwenden zu können. Die Apps erhalten - mit mehr oder weniger informierter Einwilligung des Nutzers - Zugriff auf im Gerät verwendete Sensoren (z. B. GPS) und gespeicherte Daten wie Kontakte oder E-Mails und können diese Daten unbemerkt beispielsweise zum Hersteller der Anwendung übertragen. Hinzu kommt die zunehmende Verlagerung der auf den mobilen Endgeräten gespeicherten Daten ins Internet (siehe auch Cloud-Computing, Punkt 4.1.1), um von verschiedenen Quellen auf diese zugreifen zu können, wie es beispielsweise mit der von der Firma Apple angebotenen und ausschließlich für den privaten Gebrauch vorgesehenen iCloud ermöglicht wird.

Für den Einsatz mobiler Endgeräte im Bereich der öffentlichen Verwaltung bedarf es deshalb einer vorherigen Risikoanalyse und der Umsetzung konkreter Schutzmaßnahmen, um einerseits zu verhindern, dass die Sicherheit der angeschlossenen Systeme im lokalen Netz nicht durch unsichere Endgeräte korrumpiert wird, und um andererseits beurteilen zu können, wer unter welchen Umständen Zugang zu den mit den Endgeräten verarbeiteten Daten erlangen kann.

Um den immer häufiger werdenden Anfragen zu diesem Thema gerecht zu werden, untersuche ich aktuell in einer Projektarbeit die Gefahren und Möglichkeiten für Datenschutz und Datensicherheit, welche von mobilen Endgeräten ausgehen. Aus den Ergebnissen dieser Studie soll eine Orientierungshilfe zum Thema „Datenschutzgerechter Einsatz von Smartphones und -pads in Unternehmen und Dienststellen der öffentlichen Verwaltung“ entstehen. Die bisherigen Ergebnisse zeigen, dass der sichere Einsatz der neuen Technik eine äußerst anspruchsvolle Aufgabe für die IT-Fachleute in Wirtschaft und Verwaltung ist.

Beim Umgang mit den mobilen Geräten sind verschiedene Herausforderungen zu meistern. So ist die Einbindung in vorhandene Infrastrukturen abhängig von der Einsatzstrategie. Mit Sorge beobachte ich, dass die Art der einzusetzenden Geräte nicht mehr von der Leitung des Unternehmens oder der Dienststelle oder den IT-Verantwortlichen bestimmt wird, sondern dass in zunehmendem Maße die Mitarbeiter Forderungen stellen. Diese „Bring Your Own Device“-Strategie (BYOD) führt zu erheblichen Sicherheitsrisiken und ist daher eine schwere Aufgabe für die verantwortlichen Abteilungen.

Ein typisches Szenario, das insbesondere Arbeitnehmer in der Management- und Leitungsebene einfordern, ist die parallele private und dienstliche Nutzung derartiger Geräte. Dies erfordert eine klare Trennung zwischen den privaten und geschäftlichen bzw. dienstlichen Datenbeständen auf den Geräten. Diese Trennung ist nach dem Stand der Technik aber auf keinem der verbreiteten Geräte ohne weitere Einschränkungen möglich. Bei privaten Geräten sind solche Einschränkungen nicht immer möglich, ohne die privaten Interessen des Arbeitnehmers zu beschneiden. Die Vielfalt der verschiedenen Gerätehersteller und Betriebssystemhersteller erweitert die Problematik der Einbindung um eine weitere Facette. Selbst, wenn es gelingt, diese Art von Geräten in die geschäftliche bzw. dienstliche IT-Infrastruktur einzubinden, bleibt als weitere Herausforderung die Administration einer Vielzahl von verschiedenen Geräten im Unternehmen bzw. in der Dienststelle. Jeder Hersteller von Smartphones und -pads hat seine eigenen Apps und Voreinstellungen, welche nicht immer mit den Sicherheitskonzepten der Betriebssysteme harmonieren. Inzwischen existieren zwar verschiedene Administrationsumgebungen (Mobile Device Management - MDM) für mobile Geräte, welche einen regelgerechten Einsatz in Unternehmen und Dienststellen teilweise unterstützen. Nach wie vor stoßen aber selbst solche Werkzeuge auf Grenzen, wenn die Smartphones und -pads auch privat genutzt werden sollen.

Für iPads und iPhones sind insbesondere bei den aktuellen Betriebssystemversionen verschiedene Beschränkungen konfigurierbar und sollen damit auch in Unternehmen und in Dienststellen einsetzbar sein. Dennoch können Handlungsoptionen der Besitzer des Gerätes nicht beliebig eingeschränkt werden.

Entscheiden sich die Nutzer beispielsweise, für den Abgleich der Daten verschiedener Apple-Geräte die zentralen Datenspeicher von Apple (die sogenannte iCloud) zu nutzen, verlieren die Geräte bezogenen Einschränkungen jegliche Wirkung.

Daraus macht Apple auch gar kein Geheimnis. Ein Blick in Apples allgemeine Geschäftsbedingungen für die iCloud zeigt, dass Apple sich nicht nur volle Zugriffsrechte auf die in der iCloud abgelegten Daten einräumt. Apple räumt sich auch das Recht ein, Daten an „... Strafverfolgungsbehörden, andere Behörden und/oder sonstige Dritte weiterzugeben, wenn Apple der Meinung ist, dass dies vernünftiger Weise erforderlich oder angemessen ist ...“. Dass damit die dienstliche Nutzung der iCloud datenschutzrechtlich unzulässig ist, liegt auf der Hand (weitere Hinweise zum Thema Cloud-Computing unter Punkt 4.1.1). Immerhin weist Apple in den Geschäftsbedingungen für die iCloud darauf hin, dass der Dienst nur für den privaten Gebrauch bestimmt ist. Aber auch private Nutzer sollten sich im Klaren darüber sein, dass das Hochladen von Daten in die iCloud praktische einer Veröffentlichung dieser Daten gleich kommt.

Neben der iCloud sind weitere Risiken zu bedenken. Die Benutzer können beispielsweise bereits mit wenig technischen Kenntnissen die Sicherheitsstrategien des Betriebssystem- und Geräteherstellers unterwandern und so zu einem hohen Risiko für die IT-Infrastruktur werden. Das sogenannte „Jailbreaking“ auf iPhones und iPads sowie das „Rooten“ von Geräten mit Android-Betriebssystem nutzen Anwender mitunter, um auch solche Apps installieren zu können, die normalerweise durch Sicherheitsvorkehrungen oder infolge fehlgeschlagener Signaturüberprüfungen blockiert werden. Diese Umgehung von Sicherheitsmechanismen öffnet die Systeme aber auch für verschiedenste Arten von schädlicher Software. Die Erkennung von solchen „geknackten“ Geräten ist möglich, allerdings noch nicht zuverlässig und schnell genug, um daraus resultierenden Risiken für den Datenschutz und die Datensicherheit ausreichend vorzubeugen.

Die Anfragen zur Integration von mobilen Geräten in Unternehmen und Dienststellen der öffentlichen Verwaltung nehmen ständig zu. Weiterentwicklungen der Betriebssysteme und Geräte werden weitere Probleme aufwerfen, die auch aus datenschutzrechtlicher Sicht neu bewertet werden müssen. So ist die Entwicklung von Siri (Sprachunterstützung des iPhone und iPad mit dem Betriebssystem iOS 5) einerseits eine große Hilfe für die Benutzer, insbesondere für Personen mit Behinderungen. Andererseits sind mit diesem Dienst völlig neue Risiken verbunden, da die gesamten Daten zunächst in die USA übermittelt und dort verarbeitet werden. Aus anderen Bereichen bereits bekannte Verfahren wie die biometrischen Erkennungsverfahren halten nun auch auf Smartphones und -pads Einzug.

Die Sicherheitsmechanismen derartiger Verfahren müssen im Umfeld von iPad und Smartphone völlig neu bewertet werden, um Risiken für den Datenschutz und die Datensicherheit einschätzen zu können.

Ich empfehle der Landesregierung, die Erforderlichkeit des Einsatzes von Smartphones und Tablet PC eingehend zu prüfen und die damit einhergehenden Risiken detailliert zu bewerten. In keinem Fall sollten diese Geräte ohne geeignete Administrationsumgebungen eingesetzt werden, die einerseits eine klare Trennung zwischen dienstlicher und privater Nutzung ermöglichen und andererseits die Administrationsmöglichkeiten der Nutzer wirkungsvoll verhindern oder zumindest erheblich einschränken. Die Anbindung solcher Geräte an Cloud-Strukturen ist allenfalls unter den Bedingungen möglich, die ich in Punkt 4.1.1 beschrieben habe.

4.1.5 Sicheres Löschen von Daten

Das Nutzen personenbezogener Daten ist zulässig, wenn und soweit es zur Erfüllung einer in der Zuständigkeit der verarbeitenden Stelle liegenden Aufgabe erforderlich ist. Der Umkehrschluss aus dieser Regelung in § 10 Abs. 1 DSGVO ist die Pflicht zur Löschung von Daten, die nicht mehr gebraucht werden. Und auch hier weiß das Landesdatenschutzgesetz Rat: Löschen ist das dauerhafte Unkenntlichmachen gespeicherter Daten (§ 3 Abs. 4 Nr. 6).

Was „dauerhaftes Unkenntlichmachen“ aber nun heißt, wird unter Fachleuten seit Jahren diskutiert. Bis Anfang des Jahres 2011 war in meinem Internetangebot eine Orientierungshilfe zum sicheren Löschen magnetischer Datenträger wie Festplatten zu finden, die der Arbeitskreis Technik (siehe Punkt 6) bereits im Jahr 2004 erarbeitet hatte. Dort wurde unter anderem empfohlen, personenbezogene Daten mit hohem Schutzbedarf mit mindestens 33 Überschreibzyklen zu löschen. Schon im Jahr 2008 hatten hingegen anerkannte Experten behauptet, dass einmaliges Überschreiben völlig ausreichend wäre, um die Rekonstruktion von Daten auf Festplatten zu verhindern.

Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat sich mit dem Thema Löschen befasst und im Jahr 2009 eine neue technische Leitlinie „Anforderungen zum Überschreiben von Datenträgern“ herausgegeben (BSI TL-03423). Das BSI empfiehlt ein 5-stufiges Verfahren aus Überschreib- und Prüfschritten.

Derzeit existiert jedoch noch kein Produkt, das die Anforderungen dieser BSI-Leitlinie umfassend erfüllt. Diese Situation führt zu erheblichen Schwierigkeiten bei der Beratung von Behörden und Unternehmen zum Thema datenschutzgerechtes Löschen. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat daher im Sommer 2011 das BSI um Stellungnahme gebeten.

Das BSI teilte daraufhin mit, dass das Open-Source-Produkt DBAN (Darik's Boot and Nuke) als brauchbare Alternative anzusehen ist (www.dban.org). Durch das Überschreiben mit Zufallszahlen wird ein Löschvorgang realisiert, der die Anforderungen der BSI-Leitlinie TL-03423 offenbar weitgehend erfüllt. Bei Redaktionsschluss des Zehnten Tätigkeitsberichts empfahl das BSI die Version 2.2.6. Diese Version unterstützt auch das Löschen sogenannter HPA-Bereiche von Festplatten. Host Protected Area (HPA), auch bekannt als Hidden Protected Area oder ATA-geschützter Bereich, ist ein reservierter Bereich für die Speicherung von Daten außerhalb des normalen Dateisystems. Dieser Bereich wird vor dem Dateisystem und dem Betriebssystem - und somit auch vor Formatierungs- und Partitionierungsprogrammen - versteckt und ist für diese normalerweise nicht erreichbar.

Detaillierte Informationen zum sicheren Löschen von Festplatten sind einem Hinweisblatt des BSI zu entnehmen, das regelmäßig aktualisiert wird und im Internetangebot des BSI veröffentlicht ist (www.bsi.bund.de/DE/Themen/ProdukteTools/VSClean/vsclean_node.html).

In zunehmendem Maße werden personenbezogene Daten aber auch auf anderen Speichermedien gesichert. Digitalkamera, Smartphone, MP3-Player oder USB-Stick - die Zahl der Geräte, die sogenannte Flash-Speicher verwenden, nimmt rasant zu. Das mehrfache Überschreiben sämtlicher Daten, was bei herkömmlichen magnetischen Datenträgern als sicheres Lösungsverfahren angesehen wird, funktioniert bei diesen Speichermedien nicht zuverlässig, da hier völlig andere physikalische Prinzipien wirken.

Aber auch hier spricht das BSI Empfehlungen aus: Zum sicheren Löschen speziell von sensiblen Daten auf USB-Sticks empfiehlt das BSI das kostenlose Produkt Eraser sowie das anschließende Überschreiben mit einer Datei in der Größe des Speichervolumens auf dem USB-Stick.

Eraser ist ebenfalls ein Open-Source-Produkt. Informationen zu diesem Produkt sowie der entsprechende Download dazu können unter der Internetadresse www.heidi.ie/eraser/ bezogen werden.

Die gesamte Problematik des Löschens kann von vornherein wesentlich entschärft werden, indem insbesondere sensible Daten ausschließlich verschlüsselt gespeichert werden. Dann ist nämlich ein sicheres Löschen einfach und schnell dadurch möglich, dass der zuvor verwendete kryptographische Schlüssel rückstandslos gelöscht wird. Und auch hier kann man sich an Empfehlungen des BSI orientieren: Das BSI empfiehlt das kostenlose Produkt TrueCrypt zur Grundverschlüsselung von sensiblen Daten. Auch TrueCrypt ist ein Open-Source-Produkt (Details hierzu unter www.truecrypt.org).

4.1.6 Biometrische Authentisierung mit Augenmaß

Anfang des Jahres 2010 erreichte meine Kollegen vom Hessischen Datenschutzbeauftragten eine Anfrage vom TeleTrusT Deutschland e. V. mit der Bitte um Mitarbeit an der Broschüre „Biometrische Authentisierung“. TeleTrusT ist ein Sicherheitsverband, der rund 100 Mitglieder aus Industrie, Wissenschaft und Forschung sowie öffentlichen Institutionen mit dem Ziel vertritt, einen vertrauenswürdigen Einsatz von Informations- und Kommunikationstechnik zu schaffen.

Die Kollegen aus Hessen baten mich daraufhin im Rahmen meines Vorsitzes des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ (AK Technik - siehe Punkt 6) um eine offizielle Beauftragung unter Mitarbeit der Kollegen vom Berliner Beauftragten für Datenschutz und Informationsfreiheit.

Gern bin ich dieser Bitte nachgekommen. Im Zeitalter des E-Government und des E-Business gewinnen zuverlässige Verfahren zur sicheren Identifizierung und Authentisierung von Personen ständig an Bedeutung, sodass verlässliche Informationen zu geeigneten Verfahren immer wichtiger werden. Auch mich erreichen regelmäßig Fragen zur Zulässigkeit von biometrischen Verfahren zur Authentisierung von Personen (siehe Neunter Tätigkeitsbericht, Punkt 2.14.8). Zusätzliche Relevanz erhält das Thema auch mit Blick auf den neuen Personalausweis (siehe auch Punkt 5.4.7) oder den elektronischen Reisepass (siehe Neunter Tätigkeitsbericht, Punkt 2.4.8), welche beide biometrische Daten in Form von Fingerabdrücken und digitalem Lichtbild enthalten.

Grundsätzlich versteht man unter der biometrischen Authentisierung den Nachweis der eigenen Identität mit Hilfe eines oder mehrerer unverwechselbarer körperlicher Merkmale. Geeignete Merkmale können beispielsweise Fingerabdrücke, die Unterschrift, das Gesichtsbild oder die Stimme sein. Die Merkmale eines Menschen werden mit einem entsprechenden Sensor erfasst (wie Fingerabdruckleser, berührungsempfindliches Display, Kamera, Mikrofon). Die mit dem Sensor erfassten Daten werden mit einem bereits gespeicherten Referenzmuster verglichen. Das Ergebnis ist nie die vollständige Übereinstimmung, sondern immer ein Wahrscheinlichkeitswert.

Bereits im Jahr 2009 hat sich der AK Technik mit diesem Thema befasst und die Orientierungshilfe „Biometrische Authentisierung - Möglichkeiten und Grenzen“ herausgegeben (abrufbar unter: <http://www.datenschutz-mv.de/dschutz/informat/biometrie/oh-biometrie.pdf>). Die Inhalte und Empfehlungen dieser Orientierungshilfe wurden in der TeleTrust-Broschüre unter dem Punkt „Biometrische Authentisierung - Möglichkeiten und Grenzen“ berücksichtigt.

In der Broschüre werden einige besondere Vorkehrungen bei biometrischer Authentisierung gefordert, die den Schutz der besonders sensiblen biometrischen Daten gewährleisten sollen:

- Die Verbindung zwischen biometrischen und anderen Identitätsdaten muss sicher geschützt werden.
- Der Schutz des Speichersystems der biometrischen Referenzdaten ist für Datensicherheit und Datenschutz des Verfahrens von grundlegender Bedeutung. Dabei sollte keine zentrale, sondern eine dezentrale Speicherung der Referenzdaten, z. B. auf einer Chipkarte, realisiert werden.
- Speicherung und Übertragung der biometrischen Daten müssen gegen Abhören, unbefugte Offenbarung und Modifikation geschützt werden. Dies erfordert den Einsatz kryptographischer Verfahren. Die biometrischen Daten sind nicht geheim und sie können nach Bekanntwerden oder Missbrauch nicht verändert oder gesperrt werden. Deshalb ist Folgendes wichtig:
- Die biometrischen Daten dürfen nicht allein zur Authentisierung herangezogen werden, sondern sie sind mit sperr- und veränderbaren Daten wie Besitz und Wissen wirksam zu koppeln.

Neben der Formulierung von Forderungen aus datenschutzrechtlicher Sicht gibt die Broschüre einen guten Überblick über die Funktionsweise biometrischer Erkennung und untersucht auch, ob die Biometrie eine sinnvolle und geeignete Alternative zum Passwort darstellen kann und welches dieser beiden Verfahren das sichere ist.

Die Broschüre „Biometrische Authentifizierung“ kann auf der Webseite der TeleTrust Deutschland e. V. (abrufbar unter: http://www.teletrust.de/uploads/media/TeleTrust-Biometrische_Authentisierung.pdf) heruntergeladen werden.

Ich empfehle der Landesregierung, die Hinweise der Broschüre bei der Planung und beim Einsatz biometrischer Verfahren zu berücksichtigen. Vor dem Einsatz biometrischer Verfahren zur Authentisierung und Identifizierung von Personen sollte allerdings sorgfältig geprüft werden, ob nicht Verfahren mit geringerer Eingriffstiefe den gleichen Zweck erfüllen.

4.2 Internet und E-Mail

4.2.1 Google Street View / Microsoft Streetside

Google Street View ist ein Internetdienst, der es Nutzern ermöglicht, Straßenpanoramen aus dem Blickwinkel von Passanten zu betrachten. Die Fotos werden von speziellen Pkw beim Befahren öffentlicher Straßen mit Kameras aus ca. 2,9 Meter Höhe aufgenommen. Für den Nutzer ist es auf diese Weise möglich, eine Strecke virtuell zu befahren. In der Bundesrepublik Deutschland ist der Internetdienst seit November 2010 für die 20 größten deutschen Städte online. Vor und während seiner Einführung wurde er in der Bevölkerung und in den Medien sehr kontrovers diskutiert.

Die deutschen Datenschutzaufsichtsbehörden haben sich von Beginn an sehr intensiv mit Street View befasst. Sie stellten hierzu bereits im November 2008 durch einen Beschluss des Düsseldorfer Kreises¹ fest, 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 die Möglichkeit einzuräumen, der Veröffentlichung der sie betreffenden Bilder zu widersprechen. Hierzu hatte die federführende Datenschutzaufsichtsbehörde Hamburg in schwierigen Verhandlungen mit dem Unternehmen insbesondere erreicht, dass Google Gesichter und Kfz-Kennzeichen verpixelt und bei Widersprüchen von Betroffenen entsprechende Bilder vor der Veröffentlichung unkenntlich macht.

Die Beantwortung einer Vielzahl von Anfragen und die Beratung der von den Kamerafahrten Betroffenen stellte im Jahre 2010 zeitweise einen Aufgabenschwerpunkt der Datenschutzaufsicht Mecklenburg-Vorpommern dar. Im April 2011 hat das Unternehmen mitgeteilt, sich bei der Veröffentlichung der bundesweit aufgenommenen Bilder auf die 20 größten deutschen Städte beschränken zu wollen.

Bereits Ende April 2010 musste Google zudem einräumen, bei seinen Fahrten für Street View nicht nur fotografiert zu haben, sondern auch Daten von WLAN-Netzen zu scannen. Auf Intervention des Hamburgischen Datenschutzbeauftragten hat das Unternehmen die entsprechenden Geräte aus seinen Fahrzeugen entfernt. Der Hamburgische Datenschutzbeauftragte hat wegen des vorliegenden Verstoßes des Unternehmens außerdem Strafantrag gestellt. Die entsprechenden Ermittlungen der Staatsanwaltschaft Hamburg dauern an.

Im Frühjahr 2011 hat auch die Firma Microsoft mit den Vorbereitungen für einen vergleichbaren Panoramadienst unter dem Namen „Bing Maps Streetside“ und entsprechenden Kamerafahrten in Süddeutschland begonnen. Die zuständige bayerische Datenschutzaufsichtsbehörde hat die Vorbereitungen zu diesem Projekt aus datenschutzrechtlicher Sicht begleitet und insbesondere sichergestellt, dass betroffenen Bürgerinnen und Bürgern auch bei „Streetside“ ein Vorabwiderspruchsrecht eingeräumt wird.

¹ Beschluss des Düsseldorfer Kreises vom 13./14. November 2008 „Datenschutzrechtliche Bewertung von digitalen Straßenansichten insbesondere im Internet“ <http://www.datenschutz-mv.de/dschutz/beschlue/digistra.pdf>

Vorabwiderspruch konnte (deutschlandweit) ausschließlich in der Zeit vom 1. August 2011 bis zum 30. September 2011 eingelegt werden, um sicherzustellen, dass alle eingegangenen Widersprüche noch vor der Veröffentlichung der Bilder berücksichtigt werden können. Eine Widerspruchsmöglichkeit besteht jedoch auch noch nach Veröffentlichung der Bilder im Internet.

Die Erfahrungen mit Google Street View und Microsoft Streetside beweisen erneut, dass die derzeitigen Bestimmungen des Bundesdatenschutzgesetzes für die datenschutzrechtliche Beurteilung von internetspezifischen Projekten nur bedingt geeignet sind. Die Grundstruktur des Bundesdatenschutzgesetzes stammt aus dem Jahre 1977. Im heutigen weltweit vernetzten Zeitalter muss der Einzelne sein Recht auf informationelle Selbstbestimmung auch im Internet durchsetzen können. Ein modernes Datenschutzrecht muss internetfähig sein. Einen Gesetzentwurf zur Novellierung des Bundesdatenschutzgesetzes und speziell zur Regelung georeferenzierter Panoramadienste hatte der Bundesrat im Sommer 2010 beschlossen (BR-Drs. 259/10). Die Bundesratsinitiative wurde von den Justizministern des Bundes und der Länder ausdrücklich begrüßt. Sie scheiterte jedoch an der Ablehnung der Bundesregierung und insbesondere deshalb, weil das Bundesinnenministerium eine Selbstregulierung durch die Internetwirtschaft präferiert.

In diesem Zusammenhang hat der Branchenverband BITKOM am 1. März 2011 im Rahmen einer Selbstverpflichtung einen Datenschutz-Kodex für Geodatendienste vorgelegt. Das Bundesinnenministerium hatte zuvor der Internetwirtschaft in Aussicht gestellt, bei Vorlage einer angemessenen und mit den Datenschutzbehörden abgestimmten Selbstverpflichtung auf gesetzliche Spezialregelungen zu verzichten. Die Datenschutzaufsichtsbehörden haben sich mit Beschluss vom 8. April 2011 zu diesem Datenschutzkodex geäußert und festgestellt, dass die angestrebte Selbstregulierung der Internetwirtschaft mit dem von BITKOM vorgelegten Datenschutzkodex nicht gelingt. Der Kodex entspricht in wesentlichen Bereichen nicht den datenschutzrechtlichen Anforderungen und ist nicht mit den Datenschutzbehörden abgestimmt. Er sieht zwar ein Widerspruchsrecht gegen die Veröffentlichung von Gebäudeansichten im Internet vor - allerdings kann dieser Widerspruch erst nach der Veröffentlichung eingelegt werden. Doch schon mit der Veröffentlichung der Bilder wird das Recht auf informationelle Selbstbestimmung verletzt! Außerdem soll der Datenschutzkodex nur für diejenigen Unternehmen bindend sein, die ihn unterzeichnet haben.

Die Aufsichtsbehörden haben deshalb in dem oben genannten Beschluss den Gesetzgeber zu einer umfassenden Regelung aufgefordert, die das Recht auf informationelle Selbstbestimmung im Internet schützt und dem besonderen Gefährdungspotenzial für das Persönlichkeitsrecht im Internet Rechnung trägt. Hierzu zählt insbesondere ein gesetzlich verbrieftes Widerspruchsrecht sowohl vor der Veröffentlichung personenbezogener Daten im Internet als auch die Möglichkeit, nach der Veröffentlichung Widerspruch einlegen zu können. Außerdem müssen die geplante Datenerhebung und die Widerspruchsmöglichkeit rechtzeitig in der Öffentlichkeit bekanntgegeben werden.

Maßstab für die Mindestanforderungen an einen Selbstverpflichtungskodex muss der von der hamburgischen Aufsichtsbehörde zu Google Street View festgelegte Anforderungskatalog² sein. Ein entsprechender Kodex muss zudem wirksame Sanktionsmöglichkeiten enthalten und für alle deutschen Internetunternehmen verbindlich sein.

² http://www.datenschutz-hamburg.de/uploads/media/13_Zusagen_von_Google.pdf

4.2.2 Google Analytics - Wo warst Du surfen?

Viele Web-Seitenbetreiber analysieren zu Zwecken der Werbung und Marktforschung oder bedarfsgerechten Gestaltung ihres Internet-Angebotes das Surf-Verhalten der Nutzerinnen und Nutzer. Zur Erstellung derartiger Nutzungsprofile verwenden sie vielfach Software bzw. Dienste zur sogenannten Reichweitenanalyse, die von Dritten kostenlos oder gegen Entgelt angeboten werden.

Bei der Erstellung von solchen Nutzungsprofilen sind die Bestimmungen des Telemediengesetzes (TMG) zu beachten. § 15 Abs. 1 TMG legt fest, dass ein Diensteanbieter personenbezogene Daten eines Nutzers ohne dessen Einwilligung nur erheben und verwenden darf, „soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen“. Die Verwendung dieser Daten über das Ende des Nutzungsvorgangs hinaus ist gemäß § 15 Abs. 4 TMG nur erlaubt, „soweit sie für Zwecke der Abrechnung mit dem Nutzer erforderlich sind“. Zudem dürfen Diensteanbieter für die angesprochenen Zwecke „der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien“ gemäß § 15 Abs. 3 TMG Nutzungsprofile nur unter „Verwendung von Pseudonymen erstellen, sofern der Nutzer nicht widerspricht“. In diesem Zusammenhang möchte ich auf die Feststellung der Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich verweisen, dass IP-Adressen kein Pseudonym im Sinne des TMG darstellen (vgl. Beschluss des Düsseldorfer Kreises vom 26./27. November 2009 in Stralsund - www.datenschutz-mv.de/dschutz/beschlu/Analyse.pdf).

Bei stichprobenartigen Kontrollen von Webseiten sowohl im öffentlichen als auch im nicht-öffentlichen Bereich habe ich im Laufe des Jahres 2010 festgestellt, dass die von der Firma Google zur Verfügung gestellte Software zur Reichweitenanalyse Google Analytics sehr häufig zum Einsatz kam.

Den Webseitenbetreibern war häufig nicht bewusst, dass dieses Tool damals nicht den gesetzlichen Anforderungen an den Umgang mit personenbezogenen Daten entsprach. Daraufhin forderte ich die Webseitenbetreiber in Mecklenburg-Vorpommern auf, ein Analysetool einzusetzen, das den Anforderungen des Datenschutzes gerecht wird.

Als Reaktion auf die anhaltende Kritik der Datenschutzbeauftragten des Bundes und der Länder gegenüber Google hat der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit Gespräche mit Google geführt und die erforderlichen Änderungen eingefordert, die zum gesetzeskonformen Einsatz von Google Analytics führen. Als Basis für die Verhandlungen diente der oben genannte Beschluss des Düsseldorfer Kreises zur datenschutzkonformen Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internetangeboten.

Mitte September 2011 hat Google verschiedene Änderungen an dem Produkt Google Analytics abgeschlossen und erfüllt seitdem weitgehend die Anforderungen der Datenschutzaufsichtsbehörden. Diese Änderungen betreffen sowohl die internen Verarbeitungsprozesse bei Google als auch die Einflussmöglichkeiten der Besucher von Webseiten, auf denen Google Analytics eingesetzt wird. Den Nutzern wird nun eine Möglichkeit zum Widerspruch gegen die Erfassung von Nutzungsdaten eingeräumt. Google stellt hierfür ein sogenanntes Deaktivierungs-Add-On für Web-Browser zur Verfügung (<http://tools.google.com/dlpage/-gaoptout?hl=de>).

Dieses Add-On war bisher für die besonders stark verbreiteten Browser Internet Explorer, Firefox und Google Chrome verfügbar. Jetzt steht das Add-On auch für die Browser Safari und Opera zur Verfügung, sodass alle gängigen Browser berücksichtigt sind.

Weiterhin garantiert Google nun, dass auf Verlangen des Webseitenbetreibers das letzte Oktett der IP-Adresse der Seitenbesucher vor jeglicher Speicherung gelöscht wird, sodass darüber keine Identifizierung einzelner Nutzer mehr möglich ist. Die Löschung erfolgt dabei innerhalb Europas.

Zudem stellt Google einen mit den deutschen Datenschutzaufsichtsbehörden abgestimmten, vorformulierten Vertragstext zur Auftragsdatenverarbeitung nach § 11 BDSG zur Verfügung. Webseitenbetreiber, die Google Analytics verwenden wollen und die dem deutschen Datenschutzrecht unterliegen, müssen einen solchen Vertrag mit Google abschließen.

Detaillierte Hinweise für den datenschutzgerechten Einsatz von Google Analytics sind in meinem Internetangebot zu finden (http://www.datenschutz-mv.de/dschutz/informat/google-analytics/G_A_Hinweise.pdf). Auch der oben erwähnte Vertragstext für die Auftragsdatenverarbeitung nach § 11 BDSG kann dort heruntergeladen werden (http://www.datenschutz-mv.de/dschutz/informat/google-analytics/G_A_Nutz.pdf).

Mein Kollege aus Hamburg wird die Gespräche mit Google fortsetzen, damit die oben beschriebenen Widerspruchsmöglichkeiten beispielsweise auch Nutzern beim Surfen mit Smartphones eingeräumt werden können.

4.2.3 Das Internet vergisst nicht

Im Januar 2011 meldete sich die Bundesverbraucherschutzministerin Ilse Aigner mehrfach zum Thema „Löschen im Internet“ zu Wort. Sie warb für eine technische Lösung, die Wissenschaftler der Universität des Saarlandes entwickelt hatten. Künftig solle es möglich sein, dass jeder seine Dateien mit einem Verfallsdatum versehen kann, bevor er sie ins Internet stelle. Das komme dem vielfach geforderten „digitalen Radiergummi“ sehr nahe und ließe sich weltweit verkaufen.

Die Idee hinter dieser Lösung ist, Text- oder Bilddateien nur noch verschlüsselt beispielsweise in soziale Netzwerke hochzuladen. Zum Ansehen eines solchen Bildes benötigt man ein Zusatzprogramm für seinen Browser, ein sogenanntes Browser-Plugin, das den Schlüssel von einem zentralen Server abrufen und die Bilddatei entschlüsselt. Nach einem einstellbaren Zeitraum wird der zentral gelagerte Schlüssel dann gelöscht, sodass die Bilder oder Texte nicht mehr abgerufen werden können.

Die Lösung wurde von renommierten Informatikern vehement kritisiert. Schon kurz nach dem Start des vorgeblichen Internet-Radiergummis wurde demonstriert, welche Schwächen das Konzept hat. Durch Modifikationen des für die Entschlüsselung notwendigen Browser-Plugins ließen sich Schlüssel sammeln und auf einem separaten Server ablegen.

Zum Ansehen der verschlüsselten Bilder war es dann nicht mehr erforderlich, auf den originalen Schlüsselserver zuzugreifen. Stattdessen konnten die zeitlich unbegrenzt verfügbaren Schlüssel des separaten Servers verwendet werden, wodurch sämtliche Verfallsdaten umgangen wurden.

Es ist anzuerkennen, dass sich die saarländischen Wissenschaftler eines gravierenden Problems angenommen haben. Nicht nur Nutzer sozialer Netze haben oft wenig Bedenken, Privates im Internet dem - oft sehr unbestimmten - Bekanntenkreis und teilweise sogar der Öffentlichkeit zugänglich zu machen (siehe Punkt 2.2). Auch öffentlichen Stellen fehlt hier mitunter die erforderliche Sensibilität und die Kenntnis der Mechanismen des Internet (siehe Punkt 5.4.5). Obwohl die Lösung der saarländischen Wissenschaftler keine neuen Möglichkeiten zum vollständigen und dauerhaften Löschen im Internet aufgezeigt hat, war sie für die Sensibilisierung des Problems hilfreich. Im Ergebnis der zahlreichen Diskussionen (siehe dazu auch Punkt 6.1) wurde erneut klar herausgestellt, dass das von Politikern erhoffte und vorschnell propagierte „Vergessen im Internet“ mit technischen Mitteln nicht zuverlässig realisiert werden kann. Selbst die Entwickler der oben genannten Lösung räumten ein, dass ihre oder andere technische Lösungen keinen Verfall garantieren können.

Umso wichtiger ist die Schulung und Sensibilisierung aller Nutzer moderner Medien. Solange ein zuverlässiger Schutz vor missbräuchlicher Verwendung von einmal im Internet veröffentlichten Daten zumindest technisch nicht möglich ist, muss jeder für sich selbst genau abwägen und entscheiden, welche Informationen er dem Internet und damit der weltweiten Öffentlichkeit zugänglich machen will. Das betrifft nicht nur eigene Daten und Bilder. Noch sorgfältiger muss die Veröffentlichung von Daten Dritter geprüft werden. Diese Pflicht trifft nicht nur Private, sondern genauso Wirtschaft und Verwaltung.

4.2.4 Kontrolle des E-Mail-Verkehrs durch eine Gemeindevertretung

Eine Gemeindeverwaltung hat mich gefragt, inwieweit Gemeindevertreter im Rahmen des ihnen zustehenden Kontrollrechtes gegenüber der Verwaltung den dortigen E-Mail-Verkehr einsehen können.

Aus meiner Sicht ist hier zu unterscheiden, ob ein genereller Zugriff auf den E-Mail-Verkehr in der Verwaltung oder ob die Einsicht in einen konkreten Vorgang begehrt wird.

Genereller Zugriff

Das Ausmaß und die Art der Nutzung von E-Mail und Internet am Arbeitsplatz durch die Beschäftigten unterliegen dem Weisungsrecht des Arbeitgebers beziehungsweise des Dienstherrn. Lediglich für den Arbeitgeber beziehungsweise den Dienstherrn besteht unter bestimmten Voraussetzungen ein mögliches Kontrollrecht.

Aus datenschutzrechtlicher Sicht wird dabei empfohlen, über die Nutzung von E-Mail und Internet mit dem Personalrat eine Dienstvereinbarung abzuschließen, in der auch die Fragen der Protokollierung, Auswertung und Durchführung von Kontrollen eindeutig geregelt werden (siehe hierzu auch Orientierungshilfe „Datenschutzgerechte Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz“ und „Musterdienstvereinbarung zur Nutzung von Internetdiensten“ unter www.lfd.m-v.de/download.html).

Ich habe der Verwaltung mitgeteilt, dass aus meiner Sicht für Gemeindevertreter keine generelle Möglichkeit besteht, in den E-Mail-Verkehr der Verwaltung Einsicht zu nehmen. Dieses ergibt sich auch aus dem Wortlaut des § 34 Abs. 4 der Kommunalverfassung Mecklenburg-Vorpommern (KV M-V). Nach dieser Vorschrift ist in Einzelfällen auf Antrag eines Viertels aller Gemeindevertreter oder einer Fraktion einzelnen, von den Antragstellern jeweils zu benennenden Gemeindevertretern Akteneinsicht zu gewähren, soweit dem nicht schutzwürdige Belange Betroffener oder Dritter oder zu schützende Interessen des Landes oder des Bundes entgegenstehen.

Diese Einsichtsrechte beziehen sich lediglich auf Akten. Unter dem Begriff einer Akte versteht man die in einer bestimmten Angelegenheit von einer Behörde gesammelten und geordneten Schriftstücke (siehe Kreifels, Rechtswörterbuch, 16. Auflage, S. 33). Elektronische Medien, wie beispielsweise eine E-Mail, fallen nicht hierunter. Sollte eine E-Mail indes als ausgedrucktes Schriftstück Inhalt einer Akte sein, unterliegt es (sofern nicht die in § 34 Abs. 4 KV M-V genannten Ablehnungsgründe zutreffen) dem gesetzlich geregelten Akteneinsichtsrecht. Zu beachten ist dabei allerdings, dass das in § 34 Abs. 4 KV M-V ausgedrückte Akteneinsichtsrecht nur in Einzelfällen zur Anwendung kommt. Das bedeutet, dass nach einem konkreten Vorgang gefragt werden muss, nicht aber eine Durchsicht „aller Bauakten des letzten Jahres“ oder ähnliches verlangt werden kann (siehe Schweriner Kommentierung der Kommunalverfassung des Landes Mecklenburg-Vorpommern, Darsow/Gentner/Glaser/Meyer, 3. Auflage, S. 209).

Konkrete Akteneinsicht

Eine konkrete Akteneinsicht in Schriftstücke ist (wie oben bereits beschrieben) nach § 34 Abs. 4 KV M-V möglich. Ferner haben Gemeindevertreter nach § 34 Abs. 2 KV M-V gegenüber dem Bürgermeister und den Beigeordneten einen Anspruch auf Auskunftserteilung. Darüber hinaus besteht nach dem Gesetz zur Regelung des Zugangs zu Informationen für das Land Mecklenburg-Vorpommern (IFG M-V) auch für Gemeindevertreter die Möglichkeit, nach dem vorgenannten Gesetz einen möglichen Informationszugang in Anspruch zu nehmen. Nach § 10 Abs. 2 IFG M-V sind die begehrten Informationen in dem Antrag zu umschreiben, wobei der Behörde im Bedarfsfall eine Beratungsfunktion obliegt.

Nach § 2 IFG M-V gelten auch E-Mails als Informationen im Sinne des vorgenannten Gesetzes. Zu beachten ist dabei allerdings, dass gemäß § 4 Abs. 1 IFG M-V die Behörde dem Antragsteller gegebenenfalls technische Möglichkeiten zur Sicherstellung des Informationszugangs zur Verfügung stellen muss.

Da der Informationszugang nach dem IFG M-V aber nicht schrankenlos besteht, wäre im Einzelfall zu prüfen, ob Ablehnungstatbestände der §§ 5 bis 8 IFG M-V dem möglichen Informationszugang ganz oder teilweise entgegenstehen.

4.2.5 Umgang mit E-Mails am Arbeitsplatz

In der Praxis treten immer wieder Fragen auf, die den Umgang mit E-Mails am Arbeitsplatz betreffen. In einem Fall hat mir eine Datenschutzbeauftragte geschildert, dass in der Kommunalverwaltung die private Internet- und E-Mail-Nutzung per Dienstanweisung ausdrücklich verboten sei. Die Beschäftigten seien aufgefordert worden, ihren jeweiligen Fachvorgesetzten den Zugriff auf ihr E-Mail-Postfach zu eröffnen. Die Fachvorgesetzten sollten ihrerseits dem Behördenleiter den Zugriff auf ihre E-Mail-Postfächer eröffnen. Es stellte sich die Frage, ob die Beschäftigten die Eröffnung des Zugriffs auf ihre E-Mail-Postfächer wegen der Beeinträchtigung ihres Rechts auf informationelle Selbstbestimmung verweigern können. Der Arbeitgeber hat natürlich ein Kontrollinteresse daran, den dienstlichen Charakter der E-Mail-Nutzung festzustellen, das heißt, unerlaubte Nutzung zu verhindern. Es ist jedoch immer darauf hinzuweisen, dass eine automatisierte Vollkontrolle durch den Arbeitgeber nicht zulässig ist und eine Protokollierung sowie Nutzung der Daten zur Verhaltens- und Leistungskontrolle einen Eingriff in das Persönlichkeitsrecht der Beschäftigten darstellen würde.

Die Beschäftigten sollten auf jeden Fall darüber informiert werden, auf welche Weise der Arbeitgeber die Einhaltung der Nutzungsbedingungen kontrolliert. Daher sollten in einer Dienstvereinbarung neben den Nutzungsbedingungen von Internet und E-Mail auch Fragen der Protokollierung und einzelfallbezogenen Überprüfungen und Kontrollen bei Missbrauchsverdacht transparent geregelt werden. Da solche Maßnahmen dazu geeignet sind, das Verhalten oder die Leistungen der Beschäftigten zu überwachen, unterliegen sie laut Personalvertretungsgesetz/Betriebsverfassungsgesetz der Mitbestimmung des Personalrates/des Betriebsrates. Im vorliegenden Fall hatte ich auch empfohlen zu regeln, wie mit irrtümlich zugegangenen offenkundig privaten E-Mails umzugehen ist.

Eine weitere Anfrage betraf die Regelung des E-Mail-Verkehrs in einer Behörde bei Abwesenheit. Es stellte sich dort die Frage, ob ein Mitarbeiter die eingehenden Mails an den Vertreter weiterleiten muss oder ob die Aktivierung eines Abwesenheitsassistenten ausreicht.

Selbst, wenn klar geregelt sein sollte, dass die E-Mail-Nutzung nur dienstlich erfolgen darf, ist aus datenschutzrechtlicher Sicht eine automatische Weiterleitung von E-Mails im Falle der Abwesenheit nicht empfehlenswert. Es kann niemals ausgeschlossen werden, dass ein Mitarbeiter private E-Mails erhält, die dann im Falle einer einfachen Weiterleitung dem Vertreter zur Kenntnis gegeben werden. Ich hatte daher die Aktivierung des Abwesenheitsassistenten mit Hinweis auf die Nichtweiterleitung und auf den Vertreter mit Telefonnummer und E-Mail-Adresse empfohlen.

Hingewiesen hatte ich ergänzend auch darauf, dass der Absender trotz Abwesenheitsnachricht nicht im Unklaren darüber gelassen werden sollte, wie mit seiner Mail weiter umgegangen wird, ob sie also bis auf Weiteres unbearbeitet bleibt oder ob sie an den Vertreter zur Beantwortung weitergeleitet wird oder ob der Vertreter selbst kontaktiert werden muss. Allerdings sollten nicht zu viele Informationen preisgegeben werden, um mögliche Angriffe (unbenutzter Account ist unbeobachtet) weitestgehend auszuschließen.

In der Dienstvereinbarung sollte hierzu immer auch geregelt werden, ab welchem Zeitpunkt einer Abwesenheit, gegebenenfalls unter Zuhilfenahme weiterer Personen und unter Einhaltung welcher Mitteilungspflichten, die Öffnung von E-Mail-Postfächern erfolgt.

Neues zur privaten E-Mail-Nutzung von Arbeitnehmern gibt es aus der Rechtsprechung. Das Landesarbeitsgericht Berlin-Brandenburg hat mit Urteil vom 16. Februar 2011 entschieden, dass ein Arbeitgeber auf dienstliche E-Mails seiner Mitarbeiter zugreifen darf, sofern die eingehenden E-Mails im Posteingang- bzw. die versendeten im Postausgangsfach belassen werden und dieses zulässigerweise auch für den Empfang und die Versendung privater E-Mails verwendet wird. Der Zugriff werde in diesem Fall nicht durch das Fernmeldegeheimnis beschränkt, da der Arbeitgeber, auch wenn er den Mitarbeitern die private E-Mail-Nutzung gestatte, kein Diensteanbieter im Sinne des Telekommunikationsgesetzes (TKG) sei. Dies ist eine bisher oft widersprochene Ansicht. Das Gericht geht jedoch davon aus, dass jedenfalls das Fernmeldegeheimnis gemäß § 88 Telekommunikationsgesetz (TKG) hier nicht gelte, da es im Ergebnis die Nachricht nur auf dem Übertragungsweg bis zum Eintreffen in den Herrschaftsbereich des Arbeitgebers grundgesetzlich schütze.

Nach diesem Urteil verhindert die erlaubte Nutzung dienstlicher bzw. geschäftlicher E-Mail-Accounts zu privaten Zwecken also nicht, dass ein Arbeitgeber bei Abwesenheit und einem dienstlichen bzw. geschäftlichen Bedürfnis auch zufällig Kenntnis vom Inhalt privater E-Mails erhält. Das dienstliche bzw. geschäftliche Interesse am Erhalt dienstlicher oder geschäftlicher Informationen soll im Ergebnis das private Geheimhaltungsinteresse immer dann verdrängen, wenn gleichzeitig private und dienstliche bzw. geschäftliche Kommunikation stattfindet.

Probleme können meines Erachtens dadurch vermieden werden, wenn dienstliche bzw. geschäftliche und private E-Mail-Nutzungen getrennt voneinander stattfinden. Bei erlaubter privater Nutzung empfehle ich, für den privaten E-Mail-Verkehr ausschließlich einen Webmail-Dienst zu verwenden. Dadurch wird ausgeschlossen, dass Arbeitgeber von Inhalten und von Absendern oder Empfängern privater Nachrichten Kenntnis nehmen.

4.2.6 Fragwürdige Sicherheit mit SSL-Verschlüsselung

Bei vielen Internet-Diensten werden die Sicherheits-Protokolle SSL oder TLS verwendet. Prominentestes Beispiel ist sicher HTTPS zur sicheren Übertragung von WWW-Inhalten. Viele Inhaltsanbieter verlassen sich auf den von SSL bzw. TLS verheißenen Schutz. Dank SSL bzw. TLS sollen sich die Anwender sicher sein können, mit der richtigen Website zu kommunizieren und dass die übertragenen Inhalte nicht abgehört oder verfälscht wurden.

Es soll ganz einfach sein: Man muss einfach auf den grün oder blau hinterlegten Domain-Namen im Adressfeld des Browsers und auf ein Schlosssymbol in einem Anzeigefeld des Browsers achten (die genaue Anzeige variiert je nach Browsertyp) und schon kann man sicher surfen, einkaufen, Home-Banking betreiben und sogar medizinische Daten übertragen.

Was sind SSL und TLS?

SSL (Secure Socket Layer) und TLS (Transport Layer Security) sind Protokolle, die die Sicherheit von Internet-Übertragungen mit kryptographischen Mitteln gewährleisten sollen. Es handelt sich um eine einheitliche Protokollfamilie. TLS ist die neuere Bezeichnung und SSL 3.1 entspricht TLS 1.0. Die neueste Version ist TLS 1.2. Begann die Entwicklung von SSL beim früheren Browser-Hersteller Netscape, so hat inzwischen das Internet-Standardisierungs-Gremium IETF die Normierung von TLS übernommen. TLS 1.2 ist beispielsweise im Internet-Standard RFC 5246 definiert.

SSL und TLS sind Protokolle, die zwischen TCP und Anwendungsprotokollen wie HTTP zur Übertragung von Web-Inhalten, FTP zur Dateiübertragung oder SMTP zum Mailversand angesiedelt sind. Sie sorgen mit symmetrischen und asymmetrischen kryptographischen Verfahren für eine Verschlüsselung und Integritätssicherung der Inhalte. Auf Serverseite und mitunter auch auf Clientseite kommen sogenannte Zertifikate zum Einsatz, in denen die verwendeten öffentlichen Schlüssel einem Eigentümer zugeordnet werden. Die Zertifikate werden von verschiedenen in- und ausländischen Zertifizierungsstellen ausgestellt.

SSL und TLS sind in Web-Servern, Web-Browsern, Mail-Clients und etlichen anderen Programmen implementiert, die der Kommunikation über das Internet dienen.

Aber es ist offenbar doch nicht ganz so einfach, denn im Berichtszeitraum sind einige neue Sicherheitsprobleme im Umfeld von SSL bzw. TLS bekannt geworden. 2011 musste der niederländische Zertifizierungsdiensteanbieter Diginotar auf behördliche Weisung seinen Betrieb einstellen. Vorausgegangen waren massive Manipulationen an den Systemen des Anbieters, die zur Ausstellung gefälschter Zertifikate führten. Aber auch davor gab es bereits Meldungen, wonach es Unbefugten gelang, sich Zertifikate unter dem Namen bekannter Unternehmen zu beschaffen. Mittlerweile akzeptieren viele Browser Zertifikate von Diginotar nicht mehr. Dennoch sind vergleichbare Angriffe auch künftig nicht auszuschließen.

Da in gängigen Browsern die Zertifikate sehr vieler verschiedener Zertifizierungsdiensteanbieter hinterlegt sind, gibt es auch viele potenzielle Angriffsziele, denn grundsätzlich kann jeder Anbieter Zertifikate für jede Domain ausstellen.

Empfehlung 1: Nutzer sollten daher auch die Daten zum Aussteller des Zertifikats prüfen und sich bei unplausiblen Angaben beim Betreiber der Website rückversichern. Institutionen, die viele Arbeitsplätze mit Browsern zu verwalten haben oder web-basierte Fachanwendungen nutzen, sollten sich nicht auf vorinstallierte Zertifikate verlassen, sondern die benötigten Zertifikate oder zumindest die Zertifikate der von ihnen genutzten Zertifizierungsstellen selbst einspielen und aktuell halten.

Überdies sind die Identitätsprüfungen, die die Anbieter vornehmen, bevor sie ein Zertifikat ausstellen, mitunter sehr lax. Es sind Fälle bekannt geworden, in denen Zertifikate ausgestellt wurden, obwohl nur geprüft wurde, dass die im Antrag genannte Mail-Adresse erreichbar ist. Diesem Missstand versuchen die Anbieter zu begegnen, indem sie eine neue Klasse von Zertifikaten eingeführt haben, die sogenannten Extended-Validation-Zertifikate (EV).

Das CA/Browser Forum, ein freiwilliger Zusammenschluss von Browserherstellern und Zertifizierungsdiensteanbietern, verlangt, dass sich die Anbieter selbst einer Prüfung unterziehen und dass sie nur dann EV-Zertifikate ausstellen, wenn sie die Identität und die Adresse des Antragstellers, die Verfügungsberechtigung des Antragstellers für die Domain und die Berechtigung der Personen, die den Antrag stellen, überprüft haben. Verwendet ein Inhaltsanbieter ein solches Zertifikat, so wird die Domain in der Adresszeile des Browsers grün (anstatt blau) dargestellt, wobei die genaue Darstellung je nach Browsertyp abweichen kann.

Empfehlung 2: Nutzern ist daher zu raten, Anbieter zu bevorzugen, die EV-Zertifikate bereitstellen. In web-basierten Fachanwendungen sollte die Art des Zertifikats im Rahmen der zentralen Verwaltung (siehe weiter oben) geprüft werden.

Darüber hinaus ist ein Sicherheitsproblem in dem Standard TLS 1.0 bekannt geworden: Im Rahmen der Verschlüsselung von Inhaltsdaten werden sogenannte Initialisierungsvektoren benutzt. Wichtig ist, dass diese Zahlen in einer Verbindung nie mehrfach benutzt werden, da die Verbindungsinhalte sonst entschlüsselt werden können. Genau dies ist aber im Standard TLS 1.0 nicht hinreichend berücksichtigt worden, sondern erst in der Version 1.1.

Obwohl dieser Standard bereits im Jahr 2006 verabschiedet wurde, beherrschen ihn viele moderne Browser noch nicht. Im Übrigen wirft dieses Sicherheitsproblem ein Schlaglicht auf die Komplexität der TLS-Standard-Familie.

Führende Kryptologen wie Bruce Schneier halten diese Standards für so kompliziert und unübersichtlich, dass sie weitere, noch unentdeckte sicherheitskritische Mängel nicht nur bei der technischen Umsetzung (Implementation einschließlich der Programmierung), sondern auch in den Standards selbst für wahrscheinlich halten.

Da zum Ende des Berichtszeitraumes kaum Browser zur Verfügung stehen, die die neue Protokoll-Version unterstützen, ist ein Wechsel oder eine Aktualisierung des Browsers oft keine Lösung. In Fachanwendungen besteht unter Umständen eher die Möglichkeit, den Hersteller zum Umstieg auf eine höhere Protokoll-Version ohne die bekannten Schwächen zu bewegen.

Empfehlung 3: Insbesondere Betreiber von Systemen zur Verarbeitung sensibler personenbezogener Daten sollten den Einsatz anderer Verschlüsselungsverfahren erwägen. Eine mögliche Alternative oder Ergänzung kann IPsec sein (siehe auch Punkt 4.1.6).

In diesem Zusammenhang sei auch noch auf eine weitere Unsitte bei Betreibern von Websites hingewiesen: Viele Betreiber gestatten den Zugriff auf personenbezogene Daten von Benutzern zwar nur nach Eingabe von Benutzername und Passwort und übertragen die personenbezogenen Daten auch mit SSL oder TLS verschlüsselt, jedoch wird die Seite mit der Passwortabfrage selbst nicht gesichert. So können die Login-Eingabefelder gleich auf der Einstiegsseite platziert werden und die Bedienung wird vereinfacht. Auf die Einstiegsseite wird jedoch häufiger als auf andere Seiten zugegriffen, und jede verschlüsselte Verbindung erzeugt Last auf den Servern des Anbieters. Ein Angreifer kann nun eine echt aussehende Website nachbauen, Nutzer auf diese Website locken und sich Benutzernamen und Passwörter übermitteln lassen. Da sich die Nutzer nicht mit SSL oder TLS davon überzeugen können, wer ihr Kommunikationspartner ist, können sie sehr leicht auf eine solche Täuschung hereinfallen.

Empfehlung 4: Wer auf seiner Web-Page personenbezogene Daten anfordert, sollte deshalb bereits das Formular mit SSL bzw. TLS verschlüsseln. Einen zusätzlichen Klick, der auf eine spezielle Anmeldeseite führt, nehmen die Nutzer bestimmt gern hin, wenn ihre Daten dann sicherer sind.

4.3 IT-Verfahren der Landesverwaltung

4.3.1 IP-Telefonie - Organisation verbesserungswürdig

Dem von der DVZ M-V GmbH (DVZ) betriebenen Verfahren IP-Telefonie konnte ich in der Vergangenheit ein hohes Datenschutzniveau bescheinigen (siehe Neunter Tätigkeitsbericht, Punkt 2.14.1). Während dieses Berichtszeitraumes musste ich jedoch einen schwerwiegenden Datenschutzverstoß feststellen.

Im Rahmen einer Kontrolle habe ich den Umgang mit den Verkehrsdaten (Begriff des TKG für Verbindungsdaten) der IP-Telefonie geprüft. Diese werden mit zwei verschiedenen Systemen verarbeitet. Der Call Manager der Firma Cisco übernimmt die von klassischen Telefonanlagen bekannten Steuerungs- und Vermittlungsfunktionen. Dort fallen die Verkehrsdaten an und werden zwischengespeichert. Für die weitere Verarbeitung dieser Daten sorgt dann die Software Alwin Pro der Firma Aurenz. Sie trennt beispielsweise die kostenfreien von den kostenpflichtigen Verbindungen, ordnet die Kosten den Dienststellen zu und ermöglicht Berechtigten eine Kontrolle der Kosten.

Bei meiner Kontrolle stellte ich fest, dass im Call Manager entgegen der geltenden Rechts- und Vertragslage sämtliche Verkehrsdaten eingehender und ausgehender Verbindungen für 60 Tage gespeichert wurden.

Die unterschiedslose Speicherung sämtlicher Verkehrsdaten kann nicht auf Vorschriften zur Abrechnung gestützt werden, denn kostenlose Verbindungen, wie solche zu 0800-Nummern oder kommende Verbindungen, werden nicht abgerechnet. Als Rechtsgrundlage in Betracht kommt allenfalls § 100 Abs. 1 TKG: „Soweit erforderlich, darf der Diensteanbieter zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden.“ Gerichte räumen den Providern hierfür maximal eine Woche ein. Bei der Bewertung des Einzelfalls ist wichtig, ob die Daten für die genannten Zwecke tatsächlich erforderlich sind. Da das DVZ von eventuellen Störungen üblicherweise spätestens am folgenden Werktag erfährt, sind vier Tage Speicherfrist für die Rohdaten im Call Manager ausreichend. Das Restrisiko, dass eine später bemerkte Störung nicht mehr aufgeklärt werden kann, ist hinzunehmen.

In Verträgen mit dem DVZ und in Dienstvereinbarungen zur IP-Telefonie gibt es klare Vorgaben zum Umfang und zur Dauer der Speicherung, die diesen gesetzlichen Rahmenbedingungen genügen. Demnach sind Daten von kostenfreien Verbindungen nicht zu speichern. Dies betrifft beispielsweise alle kommenden Verbindungen sowie Verbindungen zu Rufnummern, die mit 0800 beginnen. Gespräche innerhalb des IP-Telefonienetzes sind in der Regel ebenfalls kostenlos und daher nicht zu registrieren. Bestimmten Nutzern wie Personalräten oder meinen Mitarbeiterinnen und Mitarbeitern und mir wird in der Dienstvereinbarung darüber hinaus zugesichert, dass die Zielrufnummern ihrer Verbindungen nicht gespeichert werden.

Diese Regelungen hat das Innenministerium mit der Arbeitsgemeinschaft der Hauptpersonalräte ausgehandelt und sie sind vom Innenministerium in die Verträge mit dem DVZ aufgenommen worden. Im DVZ war jedoch bekannt, dass der Call Manager bei der Speicherung von Verkehrsdaten nicht nach den genannten Kriterien unterscheiden kann. Vorgesehen ist dort lediglich, die anfallenden Datensätze nach einer einstellbaren Anzahl von Tagen komplett zu löschen. Dieser Umstand spiegelte sich in den Verträgen und Dienstvereinbarungen jedoch nicht wider. Umgekehrt waren die letztlich vereinbarten Fristen und Modalitäten offenbar nicht allen fachlich Zuständigen im DVZ bekannt.

Nach meiner Kontrolle wurde die Speicherfrist im Call Manager auf vier Tage verkürzt. Die Dienstvereinbarung wurde so angepasst, dass sie die Verarbeitung der Verkehrsdaten in diesem System korrekt beschreibt.

Bei der weiteren Verarbeitung der Verkehrsdaten mit Alwin Pro habe ich keine Datenschutzverstöße festgestellt. Dieses System erhält vom Call Manager im Vier-Stunden-Rhythmus die neu angefallenen Verkehrsdaten überspielt. Danach filtert es sofort die benötigten Daten heraus, wie im oben erwähnten Regelwerk definiert, und übernimmt die übrigen gar nicht erst in seine Datenbank. Es ist auch sichergestellt, dass Auswertungen strikt nach Mandanten, hier den Auftrag gebenden Behörden, getrennt sind.

Ich empfehle der Landesregierung, regelmäßig zu prüfen, ob alle Details von Verträgen, die mit IT-Dienstleistern ausgehandelt wurden, eingehalten werden. Ebenso sollte regelmäßig geprüft werden, ob die in Dienstvereinbarungen festgeschriebenen Rechte und Pflichten vollständig umgesetzt werden.

4.3.2 Elektronisches Dokumentenmanagement in der Landesverwaltung (DOMEA®)

Bereits seit 2008 berate ich die Landesregierung bei der Einführung des einheitlichen elektronischen Dokumentenmanagement- und Vorgangsbearbeitungssystems DOMEA® in den Ministerien und der Staatskanzlei (siehe dazu auch Neunter Tätigkeitsbericht, Punkt 2.14.2). Betroffen sind von diesem Projekt in etwa 2.400 Arbeitsplätze. Die Federführung des Projektes wurde dem Finanzministerium übertragen. Die zentralen IT-Komponenten des Verfahrens betreibt die Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH (DVZ M-V GmbH) im Auftrag der Landesregierung.

Während der letzten zwei Jahre konnte das von mir geforderte Verfahren zur datenschutzgerechten Protokollierung fast vollständig umgesetzt werden. Die Protokollierung setzt nun die Vorgaben des § 21 Abs. 2 Nr. 5 DSGVO M-V bezüglich der Revisionsfähigkeit in vorbildlicher Weise um. Mit Hilfe aussagekräftiger Protokolleinträge ist nunmehr jederzeit feststellbar, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat.

Die realisierte Protokollierungslösung genügt nunmehr ebenfalls den Anforderungen des § 22 Abs. 2 DSGVO M-V. Die Vorschrift verlangt, dass es nur berechtigten Personen - in der Regel den Administratoren - möglich sein darf, Änderungen an einem automatisierten Verfahren durchzuführen, und dass diese Zugriffe protokolliert und kontrolliert werden müssen.

Die Protokollierung dient dabei nicht nur der Kontrolle der Einhaltung der Datenschutzvorschriften durch die Administratoren, sondern auch dem Schutz dieses Personenkreises. Nur mit einer angemessenen Protokollierung können sich Administratoren vor unberechtigten Vorwürfen hinsichtlich eines Missbrauches ihrer administrativen Rechte schützen.

Das DSG M-V fordert die Beteiligung der Personalvertretung bei der Festlegung des Protokollierungsverfahrens, um eine missbräuchliche Verwendung der Protokolle zu verhindern (§ 21 Abs. 2 Nr. 5). Durch den Abschluss einer Dienstvereinbarung wird der Personalvertretung dieses Mitbestimmungsrecht eingeräumt. Die Erstellung der Dienstvereinbarung über die Nutzung von DOMEA® habe ich beratend begleitet. Ich konnte mich frühzeitig davon überzeugen, dass die Kontroll- und Protokollierungsergebnisse nur zu Zwecken des Datenschutzes, der Datensicherung oder zur Sicherung des ordnungsgemäßen Betriebs des Dokumentenmanagementsystems (§ 10 Abs. 6 DSG M-V) und nicht zu einer Leistungs- und Verhaltenskontrolle (§ 35 Abs. 7 DSG M-V) verwendet werden dürfen.

Revisionsfähigkeit beinhaltet auch die Forderung, nachvollziehen zu können, welche personenbezogenen Daten wann und von wem gelöscht wurden. Damit die Löschprotokolle nicht selbst zu löschende Sachverhalte enthalten, muss sichergestellt werden, dass weder Inhalte noch der Betreff der gelöschten Akte oder des gelöschten Dokuments und damit möglicherweise personenbezogene Daten ersichtlich sind. Das Finanzministerium ist daher meinen Empfehlungen gefolgt, die ich für die Erstellung des Löschkonzeptes eingebracht habe. Das Löschen ist beispielsweise erst dann möglich, wenn ein Löschgrund angegeben wurde und wenn die Abfrage des Löschgrundes mit einem Hinweis versehen ist, dass vor dem Löschen eventuelle personenbezogene Daten in den Metadaten zu anonymisieren sind.

4.3.3 EPOS - Personaldatenverarbeitung in der Landesverwaltung

Die Einführung des elektronischen Personal-, Organisations- und Stellenmanagementsystems EPOS wurde bereits am 27. Januar 2004 durch das Kabinett beschlossen. Das landesweit als zentrale Lösung eingeführte Verfahren soll die Personalsachbearbeiter bei der Stellenplanverwaltung, der Mittelkalkulation, der Materialverwaltung sowie der Darstellung von Organisationsstrukturen entlasten und unterstützen. Von Beginn an habe ich das Projekt begleitet (siehe Neunter Tätigkeitsbericht, Punkt 2.11.6) und zahlreiche Empfehlungen zum Datenschutz und zur IT-Sicherheit ausgesprochen.

Nach Vorlage des Abschlussberichtes und mit dem Beschluss zur Kabinettsvorlage 53/10 vom 20. April 2010 wurde das Pilotprojekt EPOS 2.0 offiziell beendet und das Innenministerium gebeten, die Einführung von EPOS 2.0 in der Landesverwaltung fortzusetzen.

Um den hohen Schutzbedarf von Personaldaten auch in den EPOS-nutzenden Behörden zu gewährleisten, wurde ein spezieller Maßnahmenkatalog entwickelt, der natürlich von besonderer datenschutzrechtlicher Brisanz ist. Anfang des Jahres 2011 bat mich das Innenministerium, eine vorgesehene Änderung des EPOS-Maßnahmenkatalogs aus datenschutzrechtlicher Sicht zu bewerten. Mitarbeitern der Herstellerfirma sollte durch eigene, zeitlich begrenzte Kennungen der Zugriff auf das EPOS-Echtssystem und damit Zugriff auf die Echt-daten ermöglicht werden.

Die bisher erforderliche Einwilligung der betroffenen Verfahrensbetreuer für jeden Einzelfall sollte dann nicht mehr eingeholt werden. Ich habe darauf hingewiesen, dass in jedem Fall das Vier-Augen-Prinzip gewahrt bleiben muss, indem für administrative Zugriffe Externer geteilte Passwörter verwendet werden, deren zweite Hälfte nur die zentrale Fachadministratorin kennt.

Damit wären nur kontrollierte Zugriffe möglich und die Revisionsfähigkeit bliebe gewahrt. Ich habe auch darauf hingewiesen, dass eine Fernwartung auch weiterhin ausgeschlossen sei und administrative Zugriffe nur in den Räumen des Innenministeriums stattfinden können.

Die erweiterten Zugriffsmöglichkeiten sollten insbesondere deshalb ermöglicht werden, damit eine Vielzahl unterschiedlicher, ressortbezogener Vorlagen erstellt und getestet werden. Angeblich wäre dies aus Kompatibilitätsgründen abschließend nur im Echtssystem mit Echt-daten möglich. Nach Ansicht des Innenministeriums sei der dadurch entstehende hohe Zeitaufwand von der zentralen Fachadministratorin nicht allein zu bewältigen, sodass die Unterstützung Externer als notwendig angesehen wurde. Ich wies auf die damit zusammenhängenden Datenschutzfragen hin: Der Test (von Vorlagen) mit Echt-daten (siehe Orientierungshilfe Datenschutz und Datensicherheit in Projekten: Projekt- und Produktivbetrieb; abrufbar unter http://www.datenschutz-mv.de/dschutz/informat/projekt/oh_projekt.pdf) ist nicht zulässig und der damit verbundene Zugang zu Echt-daten durch Externe daher nicht zu rechtfertigen. Vorlagen müssen folgerichtig im Test- oder ggf. im Referenzsystem erstellt und getestet werden. Die Einbeziehung Externer wäre hier unkritisch. Ein abschließender Funktionstest im Echtssystem könne dann durch die Verfahrensbetreuer erfolgen.

Dieser Empfehlung folgte das Innenministerium. Bis auf Weiteres werden die Vorlagen nun im Test- bzw. Referenzsystem entwickelt und getestet. Der abschließende Funktionstest wird von den Verfahrensbetreuern im Echtssystem durchgeführt. Ergibt sich bei diesen Tests weiterer Änderungs- oder Anpassungsbedarf, erfolgt die erforderliche Nacharbeit nicht im Echt-system, sondern die Vorlagen gehen zur weiteren Bearbeitung wieder zurück in die Testumgebung.

Weiterhin gab es Überlegungen, ob eine Schnittstelle zu dem einheitlichen Zeiterfassungssystem ZEUS (siehe auch Punkt 4.3.4) eingerichtet werden soll, um damit einen Datenaustausch von Fehlzeiten zwischen ZEUS und EPOS zu realisieren. Mit Blick auf den für EPOS ermittelten hohen Schutzbedarf hat man jedoch sehr schnell festgestellt, dass so tiefgreifende Sicherheitsmaßnahmen notwendig wären, dass der Aufwand hierfür in keinem angemessenen Verhältnis zum erwarteten Nutzen stehen würde. Die Schnittstelle wurde daher nicht eingerichtet.

Auch weiterhin werde ich die Entwicklung und den Betrieb von EPOS begleiten, nicht zuletzt deshalb, weil zumindest eine wesentliche Forderung nach wie vor nicht umgesetzt ist. Von Beginn an werden sowohl der gesamte Datenverkehr zwischen den EPOS-nutzenden Behörden und den Applikationsservern in der Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH (DVZ M-V GmbH) als auch die Datensicherungen durch kryptographische Verschlüsselung wirksam gegen die Kenntnisnahme Unbefugter geschützt. Die im EPOS-Sicherheitskonzept geforderte und auch aus datenschutzrechtlicher Sicht notwendige Verschlüsselung der EPOS-Datenbank ist jedoch nach wie vor nicht umgesetzt (siehe Neunter Tätigkeitsbericht, Punkt 2.11.6).

Das Innenministerium stellte in der Stellungnahme zu meinem Neunten Tätigkeitsbericht (LT-Drs. 5/4145) zwar in Aussicht, die Möglichkeiten der Verschlüsselung gemeinsam mit dem Softwarehersteller und der DVZ M-V GmbH zu prüfen. Das Ergebnis dieser Prüfung lag mir bis zum Redaktionsschluss dieses Berichtes jedoch noch nicht vor.

4.3.4 Anlasslose Kontrolle der Arbeitszeit durch Vorgesetzte

Über die Kontrollmöglichkeiten elektronisch verarbeiteter Daten von Arbeitszeiterfassungssystemen durch Vorgesetzte habe ich mich bereits im Neunten Tätigkeitsbericht geäußert (siehe Neunter Tätigkeitsbericht, Punkt 2.11.7). Jedoch haben sich diese Hinweise und Empfehlungen offensichtlich nicht überall durchgesetzt, denn das Innenministerium hat mit der Personalvertretung eine Dienstvereinbarung geschlossen, die eine regelmäßige und anlasslose Vorlage des vom Beschäftigten auszudruckenden Monatsjournals der Arbeitszeiten an den Vorgesetzten vorsah. Weil dies bei der vorhergehenden Aufschreibung der Arbeitszeiten durch jeden Beschäftigten so üblich war, hat man diese Praxis offensichtlich fortgeführt.

Es ist aber ein qualitativer Unterschied, ob die Arbeitszeiten aufgeschrieben oder elektronisch erfasst und verarbeitet werden. Wird die tägliche Arbeitszeit von den Beschäftigten aufgeschrieben, ist gegen die Vorlage des Monatsjournals an den Vorgesetzten nichts einzuwenden, damit dieser zum Beispiel bestätigen kann, dass die notierten Zeiten plausibel sind. Anders verhält es sich aber, wenn die Arbeitszeitdaten auf der Grundlage einer Gleitzeitvereinbarung elektronisch erfasst und verarbeitet werden. In diesem Fall steht die Frage, zu welchem Zweck es erforderlich sein soll, dass der Vorgesetzte das Monatsjournal jedes einzelnen Beschäftigten regelmäßig zur Kenntnis nehmen soll. Zumal hier das System die Kontrolle der Plausibilität der Arbeitszeit übernehmen kann.

Das Innenministerium hat argumentiert, die Vorlage des Monatsjournals sei aus Fürsorgegesichtspunkten notwendig; so müsse der Vorgesetzte rechtzeitig erkennen können, ob beispielsweise ein Beschäftigter überlastet ist und deswegen keine gesetzlich vorgeschriebene Arbeitspause (siehe § 4 Arbeitszeitgesetz) einlegt. Dieser Argumentation konnte ich mich nicht anschließen. In den Gleitzeitregelungen ist auch die Gestaltung der Arbeitspause geregelt; üblicherweise kann danach eine Mittagspause innerhalb des Zeitraums von 11:30 bis 13:30 Uhr eingelegt werden, die mindestens 30 Minuten dauern soll. Ob diese Vorgabe eingehalten wird, kann durch die Software zur Verarbeitung der Gleitzeitdaten geprüft werden. Hält ein Beschäftigter eine entsprechende Vorgabe der Gleitzeitregelung, wie die zur Arbeitspause, nicht ein, kann dies erfasst und sofern der Verstoß personalrechtlich relevant ist, dem Vorgesetzten mitgeteilt werden. Es ist jedoch nicht erforderlich, dass regelmäßig und anlasslos ein Beschäftigter dem Vorgesetzten auch die Arbeitszeiten zur Kenntnis geben muss, die innerhalb der Gleitzeitregelungen liegen. Sofern ein konkreter Verdacht auf Manipulation der Erfassungsdaten durch einen Beschäftigten vorliegt, beispielsweise durch unerlaubtes Verlassen des Arbeitsplatzes oder der Arbeitsstelle, können selbstverständlich Kontrollen der erfassten und verarbeiteten Zeitdaten aus diesem Anlass durchgeführt werden.

Das Innenministerium hat zum Ende des Jahres 2011 signalisiert, die Gleitzeitverarbeitung entsprechend ändern zu wollen und die Vorlagepflicht des Monatsjournals zu streichen. Bis zum Redaktionsschluss lag jedoch noch keine geänderte Fassung vor.

4.3.5 Das Elektronische Gerichts- und Verwaltungspostfach EGVP

Schon seit längerer Zeit wird bundesweit der elektronische Rechtsverkehr zwischen der Justiz und deren „Kunden“ sowie innerhalb der Justiz über das Elektronische Gerichts- und Verwaltungspostfach (EGVP) abgewickelt. Technische Basis des Verfahrens ist der von mir wiederholt empfohlene E-Government-Standard Online Services Computer Interface - OSCI (siehe Achter Tätigkeitsbericht, Punkt 2.4.3), mit dem unter anderem Sicherheitsmechanismen wie Signatur und Verschlüsselung bei der Datenübertragung realisiert werden. Entgegen einer weit verbreiteten Meinung ist das EGVP keinesfalls ein Verfahren, das auf Anwendungen in der Justiz beschränkt ist. Die Lizenz für die Client-Software steht fast allen Verwaltungen in Deutschland zur Verfügung. So können etwa Kommunalverwaltungen mit dem EGVP die elektronische Zugangseröffnung gemäß § 3a des Verwaltungsverfahrensgesetzes realisieren. Das EGVP ist in der Lage, die geforderte Rechtssicherheit unter anderem durch qualifizierte elektronische Signaturen zu garantieren.

Die Landesverwaltung strebt eine breite, über die Justizverwaltung hinausgehende, Nutzung des EGVP an. Gemeinsam mit ihrem IT-Dienstleister DVZ M-V GmbH und der BOS GmbH Bremen hat sie im Juni 2011 ein Projekt gestartet, mit dem die Inbetriebnahme des EGVP innerhalb der Landesverwaltung und der kommunalen Verwaltungseinheiten des Landes vorbereitet werden soll. Ziel ist die Bereitstellung eines sicheren und verbindlichen Kommunikationsraumes für Behörden untereinander und die Öffnung auch für Kommunikationsprozesse mit den Bürgerinnen und Bürgern.

Geplant ist die Nutzung des sogenannten Office-Plug-In's für Microsoft Office, das die BOS GmbH entwickelt hat und für das das Zulassungsverfahren 2010 erfolgreich abgeschlossen wurde. Durch die Integration der Funktionalitäten der OSCI-Kommunikation in die vertraute Microsoft Office Umgebung besteht die Möglichkeit, OSCI-Nachrichten im EGVP-Format aus Microsoft Outlook und anderen gängigen Office-Anwendungen zu versenden und zu empfangen. Der Funktionsumfang umfasst unter anderem das Anbringen einer fortgeschrittenen oder einer qualifizierten elektronischen Signatur.

Mecklenburg-Vorpommern bietet sehr gute Voraussetzungen für den landesweiten Betrieb des EGVP, weil wesentliche zentrale Komponenten bereits vorhanden sind. So betreibt die DVZ M-V GmbH bereits einen sogenannten OSCI-Manager, der schon als Intermediär für andere Verfahren genutzt wird. Allen potenziellen EGVP-Nutzern kann dort das erforderliche elektronische Postfach zur Verfügung gestellt werden, über das die gesamte Kommunikation abgewickelt wird.

Ich unterstütze das Projekt ausdrücklich, weil hier - entgegen der Entwicklung in vielen anderen Bereichen (siehe Punkte 3.2.5, 3.2.7 und 5.4.7) - die Nutzung der qualifizierten elektronischen Signatur gefördert und somit ein Beitrag zur rechtsverbindlichen und vertraulichen elektronischen Kommunikation geleistet wird.

4.3.6 IT-Management für die Landesverwaltung

In meinem Neunten Tätigkeitsbericht hatte ich die Notwendigkeit eines einheitlichen IT-Managementsystem für die Landesverwaltung erläutert und die zögerliche Realisierung des Systems kritisiert (siehe dort Punkt 2.14.4). In ihrer Stellungnahme zu meinem Bericht (LT-Drs. 5/4145) hat die Landesregierung den „Schwarzen Peter“ dem IT-Landesdienstleister, der DVZ M-V GmbH, zugeschoben.

Die DVZ M-V GmbH hätte trotz vielfacher Bemühungen keine adäquate Lösung bereitstellen können, die die erforderlichen Funktionalitäten bietet und den Anforderungen der Landesverwaltung gerecht wird. Zudem wären umfangreiche Tests und Pilotierungen notwendig gewesen, die sich als zeitaufwändig erwiesen hatten.

Tatsächlich mussten zunächst eine Reihe technischer und lizenzrechtlicher Fragen geklärt sowie umfangreiche Tests durchgeführt werden, die offensichtlich mehr Zeit als zunächst geplant in Anspruch genommen haben. Darüber hinaus wurden die Anforderungskataloge auch mehrfach von der Landesregierung überarbeitet, sodass eine zügige Realisierung des Projektes durch den Dienstleister erschwert wurde. Nun ist jedoch ein erfreulicher Fortschritt des Projektes festzustellen. Inzwischen wurden die Teilprojekte Netzwerk- und Systemmanagementsystem, IT-Service-Managementsystem und Bestandsverwaltung definiert. Schon der Sachstandsbericht zum Projekt vom März 2010 wies aus, dass die technische Basis für die Teilprojekte aufgesetzt wurde.

Inzwischen wurden mit der DVZ Mecklenburg-Vorpommern GmbH, dem Innenministerium Mecklenburg-Vorpommern und dem Justizministerium Mecklenburg-Vorpommern die ersten drei Mandanten mit unterschiedlichem Leistungsspektrum realisiert. Die DVZ M-V GmbH nutzt bereits alle drei Komponenten, wobei das Netzwerk- und Systemmanagementsystem in der DVZ M-V GmbH die IT-Services IT-Grundsystem, IP-Telefonie, CN-LAVINE, Firewall und BK-Service umfasst und alle Informationen sammelt, die vom IT-Service-Management benötigt werden. Für das Innenministerium wurde zunächst das Netzwerk- und Systemmanagementsystem zur Überwachung der entsprechenden Komponenten eingerichtet. Das Justizministerium nutzt in einer ersten Stufe das IT-Service-Managementsystem. Nach einem Bericht der DVZ M-V GmbH vom Oktober 2011 werden durch das Managementsystem inzwischen 2.200 Komponenten überwacht, unter anderem Router, Switches, Firewalls, Server und Storage- sowie Virtualisierungsinfrastruktur-Komponenten.

Für die Optimierung und serviceorientierte Gestaltung von IT-Prozessen wendet die DVZ M-V GmbH die international anerkannten Richtlinien der IT Infrastructure Library (ITIL) an. Ich unterstütze dieses Vorgehen ausdrücklich, weil auf diese Weise auch grundlegende Datenschutzerfordernungen umgesetzt werden können (siehe Achter Tätigkeitsbericht, Punkt 5). Das Teilprojekt IT-Management-System dient der Umsetzung solcher ITIL-Prozesse.

Damit die laufenden IT-Management-Prozesse auf aktuelle Bestandsdaten zurückgreifen können, wurden inzwischen auch die erforderlichen Schnittstellen zwischen Systemmanagementsystem, Bestandsverwaltung und IT-Service-Management-Lösung geschaffen. Um die Akzeptanz für die Management-Lösungen in allen Ressorts zu verbessern, soll die ursprünglich englischsprachige Bedienoberfläche umgestaltet werden, sodass künftig verständlichere und vorzugsweise deutsche Texte angeboten werden.

Leider befindet sich das gesamte Projekt nach wie vor in der Pilotphase. Angesichts der Bedeutung des gesamten Projektes für den Datenschutz und die Datensicherheit halte ich es für dringend erforderlich, den Pilotbetrieb in einen stabilen Produktivbetrieb zu überführen. Dafür ist es sicher auch erforderlich, dass vorrangig die wesentlichen Kernprozesse einer solchen Management-Lösung einheitlich für die gesamte Landesverwaltung realisiert werden.

Ein weiterer wichtiger Schritt zu einer landesweit einheitlichen Bearbeitung von IT-Projekten wurde im März 2011 abgeschlossen. Das Innenministerium des Landes legte das Projektmanagementhandbuch als Leitfaden für die Durchführung von IT-Projekten in der Landesverwaltung Mecklenburg-Vorpommern vor. Das Handbuch beschreibt die notwendigen Grundanforderungen zum Management, zur Steuerung und zur Organisation von Projekten. Es wurde mit dem korrespondierenden Dokument der DVZ M-V GmbH abgestimmt, sodass einheitliche Begriffsbestimmungen und Rollenbeschreibungen angewendet werden können. Mit dem Handbuch wird nicht nur das generelle Vorgehen bei der Umsetzung ressortspezifischer, sondern auch ressortübergreifender Projekte des Landes beschrieben. In einem separaten Kapitel des Handbuches werden datenschutzrechtliche Anforderungen erläutert. Erfreulicherweise wird ausdrücklich auf meine Empfehlungen zu Datenschutz und Datensicherheit im Projekt- und Produktivbetrieb verwiesen (siehe Neunter Tätigkeitsbericht, Punkt 2.14.8), wo für jede Phase eines Projektes erläutert wird, ob und unter welchen Rahmenbedingungen personenbezogene Daten verarbeitet werden dürfen.

Ich empfehle der Landesregierung, das IT-Managementsystem auf die gesamte Landesverwaltung auszudehnen, um auf der Basis geordneter und transparenter Managementprozesse auch ein zuverlässiges und robustes Datenschutzmanagement realisieren zu können. Der Pilotbetrieb sollte schnellstmöglich in einen stabilen Produktivbetrieb überführt werden. Vorrangig sollten die wesentlichen Kernprozesse einer solchen Management-Lösung einheitlich für die gesamte Landesverwaltung realisiert werden.

4.3.7 Einsicht in die Protokolldaten bei Internetverkehr

Vertreter eines Ministeriums wollten die Protokolldaten des Proxy-Servers kontrollieren. Dieser Server wird im Auftrag des Ministeriums vom IT-Landesdienstleister, der DVZ M-V GmbH (DVZ), betrieben. Die Beteiligten wandten sich an mich mit der Frage, wann und in welchem Umfang solche Auswertungen zulässig sind.

Ein Proxy-Server nimmt Internet-Verbindungen aus einem Netz (hier: LAN des Ministeriums) entgegen und gibt sie unter eigener Adresse an den eigentlichen Zielservers weiter. Oft speichert ein Proxy Inhalte von Websites zwischen, um sie ohne Anfrage an den Zielrechner sofort an den anfragenden Rechner ausliefern zu können. Außerdem kann ein Proxy-Server die übertragenen Daten auf unerwünschte oder schädliche Inhalte (beispielsweise bekannte Viren, Würmer, Trojanische Pferde) untersuchen. Viele Proxy-Systeme können die Zeitpunkte, Quelladressen und Inhalte von Anfragen, deren Ergebnisse und eventuell aufgetretene Probleme, wie Verbindungsabbrüche, protokollieren.

Ich habe dem Ministerium und dem DVZ mitgeteilt, dass ich sowohl stichprobenartige Kontrollen ohne konkreten Anlass als auch Anlass bezogene, gezielte Auswertungen unter bestimmten Voraussetzungen für zulässig halte. Dies sind insbesondere:

Der Auftragnehmer muss die Protokolldaten so verarbeiten, dass die gewünschten Daten selektiert werden können und keine zusätzlichen Daten, womöglich von anderen Auftragnehmern, mitgelesen werden können.

Es muss gewährleistet sein, dass die Protokolldaten nur der Datenschutzkontrolle oder der Sicherstellung des ordnungsgemäßen Betriebes des IT-Systems dienen (§ 10 Abs. 6 DSGVO M-V). Behördliche Datenschutzbeauftragte sollten in etwaige Kontrollen einbezogen werden.

Häufig können aus Protokolldaten Rückschlüsse auf die Arbeitsleistung oder das Verhalten von Beschäftigten gezogen werden. Dies gilt auch für Protokolle an Proxys einer Behörde. Daher sind die Mitbestimmungsrechte der jeweiligen Personalvertretung zu beachten und eine Dienstvereinbarung abzuschließen oder eine Dienstanweisung mit Zustimmung des Personalrates zu erlassen. Diese Dokumente machen das Verfahren auch gegenüber der Belegschaft transparent.

Diese und weitere Fragen werden auch in der Orientierungshilfe „Datenschutzgerechte Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz“ des Arbeitskreises Medien der Ständigen Konferenz der Datenschutzbeauftragten des Bundes und der Länder behandelt. Ich halte dieses Material gemeinsam mit einer Musterdienstvereinbarung zur Nutzung von Internetdiensten auf meinem Internetangebot zum Download bereit.

Dem Ministerium habe ich empfohlen, seine Dienstanweisung nach diesen Dokumenten zu überarbeiten, da die bestehende Regelung veraltet war. Das Ministerium ist dieser Empfehlung teilweise gefolgt.

4.3.8 Flüssiger Verkehr dank Bluetooth-Sensoren

Ein Straßenbauamt will den Autoverkehr zu einer beliebten Urlaubsinsel unseres Landes flüssiger gestalten. Um den Verkehr besser auf die beiden Zufahrten zur Insel verteilen zu können, möchte das Amt die Reisezeiten zwischen bestimmten Punkten auf der Insel und auf dem Festland messen. Aus den Daten sollen Routenempfehlungen für Kraftfahrer errechnet und über Hinweistafeln an den Straßen, Meldungen für Navigationssysteme, Rundfunk und Internet verbreitet werden. Das Straßenbauamt hat mich vorab um Beratung zu diesem Vorhaben gebeten und mir das System näher vorgestellt.

Technische Basis sind Geräte mit Bluetooth-Schnittstelle, die mittlerweile in vielen Fahrzeugen installiert oder von den Insassen mitgeführt werden. Die Sensoren des Straßenbauamtes fragen Bluetooth-Adressen von „sichtbar“ (discoverable) gestellten Geräten in einem Umkreis von 250 Metern ab. Diese Adressen werden zunächst pseudonymisiert, indem sie zusammen mit einer weiteren Zahl (der sogenannte Salt) mit Hilfe einer kryptographischen Einwegfunktion (Hash-Funktion) verschlüsselt werden. Das Pseudonym wird zusammen mit einer Zeitmarke gespeichert. Wird dasselbe Pseudonym an einer anderen Messstelle ermittelt, kann aus der Differenz der Zeitangaben die Reisezeit berechnet werden.

Aus dem vorderen Teil einer Bluetooth-Adresse lässt sich zunächst der Gerätehersteller ermitteln, da die verfügbaren Adressen den Herstellern blockweise zugeteilt werden. Manchmal kann man auch Rückschlüsse auf das Modell ziehen. Selbst bei auf „unsichtbar“ geschalteten Geräten ist dies oft möglich, weil bei der Datenübertragung 24 Bit der Adresse einer der beteiligten Bluetooth-Bausteine in jedem Datenpaket unverschlüsselt mitgesendet werden.

Die Zuordnung einer Adresse zu einem Nutzer ist dann recht einfach, da Bluetooth-fähige Geräte häufig nur von einer Person benutzt werden. Daher sind Bluetooth-Adressen als personenbezogene Daten zu bewerten.

Das beschriebene Verfahren kann zur Bildung von Bewegungsprofilen führen, denn so lange derselbe Salt-Wert benutzt wird, entsteht aus einer Bluetooth-Adresse immer dasselbe Pseudonym. Durch probeweises Verschlüsseln von Adressen könnte man außerdem feststellen, ob ein Bewegungsprofil zu diesen Adressen vorhanden ist. Deshalb habe ich dem Amt empfohlen, den Salt-Wert täglich zu löschen und durch eine neue zufällig erzeugte Zahl ausreichender Länge zu ersetzen. Außerdem sollten die pseudonymisierten Rohdaten bereits dann gelöscht werden, wenn sie nicht mehr zur Bestimmung von Reisezeiten erforderlich sind. Dies ist nach Angaben des Amtes spätestens nach sechs Stunden der Fall. Anschließend liegen nur noch anonymisierte Daten vor.

Im Ergebnis konnte ich feststellen, dass das vorgestellte System in hervorragender Weise nach dem Prinzip der Datensparsamkeit (§ 5 Abs. 1 DSGVO) entworfen ist, indem die Bluetooth-Adressen frühzeitig pseudonymisiert und danach anonymisiert werden. Da diese Adressen wie beschrieben als personenbezogen anzusehen sind, ist dennoch eine Rechtsgrundlage zu deren Verarbeitung notwendig. Außerdem ist für ausreichende Transparenz zu sorgen. Deshalb habe ich empfohlen, auf die Messungen durch Veröffentlichungen in der Tagespresse und auf der Website des Amtes hinzuweisen, für Interessierte Merkblätter bereitzuhalten und an den Messstellen Hinweistafeln aufzustellen.

Bluetooth

ist ein Standard zur drahtlosen digitalen Übertragung von Daten und Sprache. Bluetooth-Schnittstellen sind in vielen elektronischen Geräten wie Smartphones und anderen Mobiltelefonen, tragbaren und fest installierten Freisprecheinrichtungen sowie in vielen Notebooks und Navigationsgeräten eingebaut. Die Reichweite von Bluetooth beträgt je nach Einsatzbedingungen und Sendeleistung mehrere Meter bis etwa mehrere hundert Meter. Jeder Bluetooth-Baustein hat eine fest einprogrammierte, weltweit eindeutige Adresse, eine Zahl mit 48 Bit Länge. Diese wird vor allem zum Aufbau von Funkverbindungen benutzt und stets unverschlüsselt gesendet.

Man kann jedes Bluetooth-Gerät auf „sichtbar“ (englische Bezeichnung: discoverable) schalten. Dann identifiziert es sich auf Anfrage auch gegenüber Unbekannten, indem es unter anderem seine vollständige Bluetooth-Adresse aussendet. Ein Gerät muss aber nur dann „sichtbar“ sein, wenn ein anderes Gerät zum ersten Mal Verbindung zu ihm aufnehmen soll. Um der Bildung von Bewegungsprofilen entgegenzuwirken, sollte man Bluetooth-fähige Geräte immer nur dann auf „sichtbar“ schalten, wenn dies notwendig ist.

4.4 Service Internet

4.4.1 Gewerbedienst online

Der Zweckverband „Elektronische Verwaltung in Mecklenburg-Vorpommern“ (eGO-MV) bat mich im Mai 2011 um eine datenschutzrechtliche Stellungnahme zum vorgesehenen Aufbau eines Online Gewerbedienstes einschließlich eines zentralen Gewerberegisters für Mecklenburg-Vorpommern.

Mit dem Online Gewerbedienst soll Unternehmen die Möglichkeit geboten werden, das Anzeigeverfahren nach der Gewerbeordnung komplett online abwickeln zu können und die Daten medienbruchfrei bis in die Fachverfahren der Behörden zu übermitteln. Nach Abschluss der Bearbeitung der Anzeigen in den Fachverfahren sollen die Daten dann an eine Datenbank übermittelt werden, damit sie für einfache und erweiterte Gewerbeauskünfte zur Verfügung stehen. Unkritisch ist die einfache Auskunft über Name und Anschrift des Betriebes sowie die angezeigte Tätigkeit, weil diese Daten nach der Rechtsvorschrift in § 14 Abs. 5 Satz 2 Gewerbeordnung (GewO) allgemein zugänglich gemacht werden dürfen. Anders verhält es sich jedoch für erweiterte Auskünfte auf der Grundlage von § 14 Abs. 7 GewO: Daten, die über den Namen, die Anschrift und die Tätigkeit eines Gewerbetreibenden hinausgehen, dürfen an öffentlich-rechtliche Wettbewerbsunternehmen und an nicht-öffentliche Stellen übermittelt werden, wenn ein rechtliches Interesse an der Kenntnis der Daten glaubhaft gemacht wird und das schutzwürdige Interesse des Gewerbetreibenden nicht überwiegt. Es war geplant, diesen Abwägungsprozess auf den Zweckverband über das Rechtsinstitut der Datenverarbeitung im Auftrag (§ 4 DSGVO M-V) zu übertragen.

In meiner Stellungnahme habe ich darauf hingewiesen, dass die Abwägung keine Datenverarbeitung im Auftrag sein kann, weil der Zweckverband dann einen Bewertungs- und Ermessensspielraum hätte, der aber nach dieser Rechtsvorschrift nicht gegeben sein dürfte. Die Entscheidungsbefugnis muss bei einer Auftragsdatenverarbeitung bei dem Auftraggeber liegen, ein Auftragnehmer darf nur nach den Weisungen des Auftraggebers handeln. Der Abwägungsprozess kann daher nicht über die Auftragsdatenverarbeitung in zulässiger Weise durchgeführt werden.

Der Zweckverband hat daraufhin mitgeteilt, dass er rechtlich prüfen wolle, ob die Gewerbeämter den Abwägungsprozess und damit die Entscheidungsbefugnis auf den Zweckverband übertragen können, wenn dieser durch eine entsprechende Satzungsänderung die Voraussetzung dafür schafft, die Aufgabe übernehmen zu können.

Nach meiner Auffassung sollte eine mandantenfähige Datei eingerichtet werden, die in der Lage ist, die Vorgaben des § 14 Abs. 11 Gewerbeordnung umzusetzen. Danach müssen Datenempfänger und Verwendungszwecke für zugelassene Abrufe durch den Leiter des jeweiligen Gewerbeamtes schriftlich festgelegt und Abrufe protokolliert werden, wobei es möglich sein muss, die für einen Abruf verantwortliche Person festzustellen. Außerdem ist durch die speichernde Stelle zu gewährleisten, dass die Protokolle stichprobenweise ausgewertet und nach sechs Monaten gelöscht werden.

Ich habe den Zweckverband gebeten, mich über die weitere Entwicklung auf dem Laufenden zu halten.

4.4.2 Beschäftigtendaten im Internet

Nach wie vor erreichen mich Anfragen, unter welchen Voraussetzungen welche personenbezogenen Daten von Beschäftigten im Internet veröffentlicht werden dürfen. Dieses Thema ist bereits in meinen vorhergehenden Tätigkeitsberichten behandelt worden, siehe zum Beispiel Neunter Tätigkeitsbericht, Punkt 2.11.3.

Zu Beginn des Jahres 2011 bin ich gefragt worden, ob es zulässig sei, den Stellenplan einer Kommune im Internet zu veröffentlichen. Gegner dieser Veröffentlichung wandten ein, dass es unter Umständen leicht sei, aus dem Stellenplan eine Verbindung zu dem Inhaber einer Stelle herzustellen, was dazu führe, dass dann bekannt sei, wie hoch das Gehalt, der Lohn oder die Besoldung des Beschäftigten sei.

Nach meiner Auffassung enthält ein Stellenplan per se keine personenbezogenen Daten, denn er weist in der Regel ein knappes Anforderungsprofil einer Stelle aus, z. B. Techniker mit Fachhochschulabschluss, und gibt deren Dotierung an, beispielsweise Besoldungsgruppe A10. Dies sind keine personenbezogenen Daten nach den datenschutzrechtlichen Vorschriften. Ähnliche Angaben findet man auch in der Anlage zum Landesbesoldungsgesetz oder in der Kommunalbesoldungslandesordnung (siehe z. B. www.landesrecht-mv.de). Außerdem muss die angegebene Lohn-, Gehalts- oder Besoldungsgruppe nicht mit der tatsächlichen Eingruppierung übereinstimmen, weil die Angabe häufig die zu erzielende Endstufe ist, die der Stelleninhaber aber noch nicht erreicht haben muss. Schließlich hängt der gezahlte Lohn, das gezahlte Gehalt oder die gezahlte Besoldung von weiteren individuellen Faktoren des Stelleninhabers ab, sodass aus Stellenplanangaben nur eine grobe Orientierung hinsichtlich des gezahlten Betrages abgeleitet werden kann. Gleichwohl können aber Stellenplandaten bei Verknüpfung mit personenbezogenen Daten, wie beispielsweise einem auf der Homepage der Behörde oder des Arbeitgebers veröffentlichten Organigramm, zu Informationen werden, die eine betroffene Person als schutzwürdig betrachtet, sodass die Veröffentlichung nur zulässig wäre, wenn das öffentliche Interesse an der Kenntnis der Daten das schutzwürdige Interesse der betroffenen Person erheblich überwiegt. Um diesen Abwägungsprozess zu vermeiden, sollte kein detaillierter Stellenplan im Internet veröffentlicht werden. Es empfiehlt sich, Lohn-, Gehalts- und Besoldungsgruppen zusammengefasst und nur die Anzahl der jeweils darin eingruppierten Beschäftigten anzugeben. Für herausgehobene Funktionen ist dies allerdings nicht möglich, denn eine Stadt hat üblicherweise nur einen Oberbürgermeister. Vor dem Hintergrund der Kommunalbesoldungslandesverordnung muss er es hinnehmen, dass die Besoldungsgruppe von der Öffentlichkeit zur Kenntnis genommen werden kann. Das trifft im Übrigen auch auf den Landesbeauftragten für Datenschutz und Informationsfreiheit zu, dessen Besoldungsgruppe dem Anhang des Landesbesoldungsgesetzes entnommen werden kann.

Im Ergebnis habe ich auf die Anfrage mitgeteilt, dass gegen die Veröffentlichung von zusammengefassten Stellenplandaten keine datenschutzrechtlichen Bedenken bestehen. Sollte beabsichtigt werden, einen detaillierten Stellenplan zu veröffentlichen, aus dem Daten zu einzelnen Personen gewonnen werden können, die nicht der Leitungsebene angehören, ist vorher zwischen dem schutzwürdigen Interesse der Betroffenen und einem eventuell berechtigten Interesse der Öffentlichkeit an der Kenntnis der Daten abzuwägen. Nur bei Überwiegen des öffentlichen Interesses dürfen die erforderlichen Daten im Internet bekannt gegeben werden.

4.4.3 Wohngeldantrag online

Der Zweckverband „Elektronische Verwaltung in Mecklenburg-Vorpommern“ (eGO-MV) informierte mich im Juli 2010 über das Projekt Online-Wohngeldantrag, für das eine Förderung durch den Europäischen Fonds für regionale Entwicklung (EFRE) bewilligt worden ist. Die zu entwickelnde Software sollte es den Antragstellern auf Wohngeld künftig ermöglichen, durch Eingabe ihrer Daten in einen sogenannten Antragsassistenten zunächst unverbindlich zu prüfen, ob und in welcher Höhe ein Anspruch auf Wohngeld bestehen könnte. Sofern sich der Antragsteller entschließt, einen Antrag zu stellen, sollen die bereits in den Antragsassistenten eingegebenen Daten dafür genutzt und gegebenenfalls durch weitere vom Antragsteller einzugebende Daten ergänzt werden. Die elektronisch gespeicherten Daten können dann an die zuständige Wohngeldstelle übermittelt und dort verarbeitet werden oder der Antragsteller löscht seine Daten bzw. legt eine in seinem Ermessen liegende Speicherfrist fest.

Die Arbeitsprozesse in den Wohngeldstellen können dadurch ebenfalls optimiert werden, was dazu führt, dass die Betroffenen ihre Wohngeldbescheide schneller als bisher erhalten. Darüber hinaus sollen sich die Antragsteller regelmäßig über den Bearbeitungsstand ihres Antrages informieren können. Der eGO-MV geht davon aus, dass ca. 80 % der Wohngeldstellen das gleiche Fachverfahren nutzen, sodass der überwiegende Teil auch das Online-Verfahren nutzen werde.

Die Projektgruppe Online-Wohngeldantrag hat mich von Beginn an zu ihren Beratungen eingeladen, um frühzeitig datenschutzrechtliche Hinweise umsetzen zu können. Ein Schwerpunkt betraf beispielsweise die Identifizierung der Antragsteller. Nach den Bestimmungen des § 36a Sozialgesetzbuch Erstes Buch (SGB I) können Dokumente elektronisch erstellt und bearbeitet werden, wenn keine Zweifel an der Identität der wohngeldberechtigten Person bestehen. In der Regel bestehen diese Zweifel nicht, wenn elektronische Anträge mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen sind oder unter Verwendung des elektronischen Identitätsnachweises nach dem Gesetz über Personalausweise (siehe auch Punkt 5.4.7) gestellt werden. Es ist jedoch davon auszugehen, dass gegenwärtig nur wenige Bürger über eine qualifizierte elektronische Signatur verfügen und auch der elektronische Identitätsausweis noch nicht so verbreitet ist, dass das Verfahren allein auf diese beiden Varianten gestützt werden kann.

Von den Entwicklern war ursprünglich erwogen worden, dass die Identität des Antragstellers gegenüber der Wohngeldstelle durch eine einzureichende Kopie des Personalausweises nachgewiesen werden kann. Ich habe darauf verwiesen, dass das Bundesministerium des Innern die Nutzung von Ausweiskopien als unzulässig ansieht bzw. dies nur für bestimmte gesetzlich geregelte Anwendungen bei Schwärzung der Zugangsnummer als zulässig betrachtet. Außerdem wäre damit keine eindeutige Identifizierung möglich, weil eine solche Kopie leicht manipuliert werden kann, wenn kein Vergleich mit dem Original stattfindet. Es ist deswegen vorgesehen, dass neben den oben genannten elektronischen Identifizierungsverfahren das PostIdent-Verfahren geprüft wird oder der Antragsteller in der Wohngeldstelle seine Identität nachweist. Darüber hinaus wird geprüft, ob ein vom Betroffenen unterschriebener und eingesandter Antrag anerkannt wird. In den Wohngeldstellen wird für den Abruf des elektronischen Bescheids die qualifizierte elektronische Signatur genutzt.

Es ist vorgesehen, dass die Daten über das Internet mittels Hyper Text Transfer Protocol Secure (HTTPS) mit der Verschlüsselung Secure Sockets Layer (SSL) übertragen werden. Der Zugang für Antragsteller ist über ein Login mit einer passwortgeschützten Registrierung möglich. Das System verfügt über eine demilitarisierte Zone (DMZ), das heißt, vor und nach dem Wohngeldassistenten ist jeweils eine Firewall eingerichtet, die die Daten zum Fachverfahren und zur Datenbank filtert. Es werden Firewalls von unterschiedlichen Herstellern eingesetzt.

Insgesamt ist das Verfahren aus datenschutzrechtlicher Sicht auf einem guten Weg. Es soll in naher Zukunft von den Wohngeldstellen, die sich daran beteiligen, für die Nutzer/innen in ihrem Zuständigkeitsbereich in Betrieb genommen werden.

4.4.4 Geburtsurkunden aus dem Rechner

Im Januar 2009 ist das neue Personenstandsrecht in Kraft getreten. Seitdem können in den Standesämtern elektronische Personenstandsregister eingerichtet werden, ab dem 1. Januar 2014 sind sie zwingend vorgeschrieben. Nach § 67 des Personenstandsgesetzes (PStG) haben die Länder die Möglichkeit, zentrale Personenstandsregister einzurichten. Mecklenburg-Vorpommern hat hiervon selbst keinen Gebrauch gemacht. Ein zentrales Register wird es dennoch geben.

Damit nicht jedes Standesamt ein eigenes Register betreiben muss, richtet der Zweckverband „Elektronische Verwaltung in Mecklenburg-Vorpommern“ (ZV eGo-MV) derzeit ein zentrales elektronisches Personenstandsregister ein und bietet es allen Standesämtern des Landes zur Nutzung an. Mit der technischen Umsetzung wurde der IT-Landesdienstleister (DVZ M-V GmbH) beauftragt.

Der ZV eGo-MV betreibt das zentrale Personenstandsregister als ein gemeinsames Verfahren nach § 3 Abs. 10 DSGVO M-V. Gemeinsame Verfahren sind solche automatisierten Verfahren, die aus mindestens zwei eigenständigen automatisierten Teilverfahren bestehen, für die verschiedene Daten verarbeitende Stellen verantwortlich sind. Die Verantwortung für die zentralen Verfahrensbestandteile liegt beim ZV eGo-MV. Die Standesämter hingegen sind aus datenschutzrechtlicher Sicht für die dezentralen Komponenten (Anwendungen vor Ort) verantwortlich.

Die einzelnen Standesämter übermitteln somit personenbezogene Daten an den ZV eGo-MV. Da die gesetzlichen Anforderungen an die Zulässigkeit der Datenverarbeitung bei den gemeinsamen Verfahren unberührt bleibt (§ 17 Abs. 1 Satz 2 DSGVO M-V), ist auch für diese Datenübermittlung eine Rechtsvorschrift erforderlich. Ausreichend wäre beispielsweise eine entsprechende Regelung in der Verbandssatzung des ZV eGo-MV. Der Zweckverband hat bereits zugesagt, seine Satzung entsprechend anzupassen. Da diese Satzung aber nur für die Mitglieder des Zweckverbandes gilt, müssen alle übrigen Kommunen, die das zentrale Personenstandsregister nutzen wollen, mit dem ZV eGo-MV einen Vertrag zur Auftragsdatenverarbeitung (§ 4 DSGVO M-V) schließen.

Der Zweckverband befindet sich gerade in der Umsetzung des Projektes. Für die zentralen Verfahrensbestandteile wurde bereits eine Vorabkontrolle (§ 19 Abs. 2 DSGVO M-V) durchgeführt und die datenschutzrechtliche Freigabe erteilt (§ 19 Abs. 1 DSGVO M-V). Mit Stand Dezember 2011 sollen bereits 14 Standesämter das zentrale Personenstandsregister nutzen können.

Um der Gefahr eines möglichen Datenverlustes entgegenzuwirken, sind nach § 4 Abs. 1 PStG die Beurkundungen nach ihrem Abschluss in einem weiteren elektronischen Register (Sicherungsregister) zu speichern.

§ 3 Abs. 6 des Landespersonenstandsausführungsgesetzes (LPStAG M-V) ermächtigt das Innenministerium, ein zentrales Sicherungsregister zu errichten. Die Rahmenbedingungen hierfür sind in der Sicherungsregisterverordnung (SiRegVO M-V) geregelt. Diese Verordnung verpflichtet alle Standesämter, die beurkundeten Daten an das Sicherungsregister zu übermitteln.

Während der Beratungen zur technischen Umsetzung der Forderungen des PStG und der PStV sind mir insbesondere zwei Teilaspekte zur datenschutzrechtlichen Bewertung vorgelegt worden.

Die erste Frage betraf die Gewährleistung der Vertraulichkeit und der Integrität bei der Übermittlung von Daten in das elektronische Sicherungsregister. Die PStV verlangt hierfür gesicherte Verfahren, die eine Verschlüsselung nach dem Stand der Technik beinhalten (§ 63 Abs. 1) und fordert den Einsatz des Datenaustauschformats XPersonenstand und des Übertragungsprotokolls OSCI-Transport (§ 63 Abs. 2). Die Verordnung lässt jedoch Ausnahmen zu, wenn die Daten innerhalb von Rechenzentren und in besonders gesicherten verwaltungseigenen Netzen übertragen werden. Dann darf auf die Verwendung von OSCI-Transport verzichtet werden. Es müssen aber technische und organisatorische Maßnahmen getroffen werden, die die gleichen Sicherheitseigenschaften wie OSCI-Transport haben.

Ich habe akzeptiert, dass von der Ausnahmeregelung Gebrauch gemacht wird, da die Voraussetzungen hierfür gegeben waren. In die Sicherungsregisterverordnung des Landes sind auf meine Anregung hin jedoch zwei zusätzliche Forderungen aufgenommen worden. Bei der Übermittlung sind die Daten nach dem Stand der Technik zu verschlüsseln (§ 1 Abs. 2 Satz 3) und vor Eintragung in das Sicherungsregister ist die durch den Standesbeamten angebrachte qualifizierte elektronische Signatur zu prüfen (§ 1 Abs. 2 Satz 4). Zudem musste klargestellt werden, dass die ebenfalls übertragenen sogenannten Hinweise (vgl. § 18 PStV) rechtlich nicht relevant sind, somit im Gegensatz zu den Urkundsdaten nur geringen Schutzbedarf aufweisen und nicht gesondert signiert werden müssen. Für die Verschlüsselung wurde das weit verbreitete TLS-Protokoll (Transport Layer Security) gewählt. Mit Blick auf die inzwischen bekannt gewordenen Sicherheitsmängel dieses Protokolls (siehe Punkt 4.2.6) werden sich die Verfahrensbetreiber in absehbarer Zeit jedoch eine Alternative für dieses Verfahren suchen müssen.

Der zweite zu bewertende Aspekt betraf eine rechtliche Anforderung des PStG. Nach § 3 Abs. 2 Satz 2 PStG sind die Beurkundungen im elektronischen Personenstandsregister mit der Angabe des Familiennamens des zugriffsberechtigten Standesbeamten abzuschließen. Die Identität der Person, die die Eintragung vornimmt, muss jederzeit erkennbar sein (vgl. § 3 Abs. 2 Satz 3 PStG). Das Innenministerium war zunächst davon ausgegangen, dass diese Forderung allein dadurch erfüllt sei, dass der eintragende Standesbeamte den Eintrag mit einer qualifizierten Signatur versieht und somit der Urheber des Eintrags zweifelsfrei feststellbar sei. Zum wiederholten Mal musste ich jedoch darauf hinweisen, dass qualifizierte elektronische Signaturen allein nicht geeignet sind, die Identität des Zertifikatsinhabers nachzuweisen, in diesem Fall die des beurkundenden Standesbeamten (siehe Achter Tätigkeitsbericht, Punkt 2.5.7 und Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Oktober 2006, abrufbar unter <http://www.datenschutz-mv.de/dschutz/beschlue/ent2006.html#nr.1>). Die qualifizierte elektronische Signatur ist ausschließlich dazu geeignet, die Authentizität und Integrität des Registereintrags nachträglich überprüfen zu können.

Ich habe daraufhin vorgeschlagen, Attribute im Signaturzertifikat oder Attribut-Zertifikate zu verwenden. Wenn diese Attribute nachweisen, dass der Signierende ein Mitarbeiter des Standesamtes ist und zur Nutzung der Signaturkarte autorisiert wurde, könnte - zusammen mit weiteren organisatorischen Vorkehrungen - der vom PStG geforderte Identitätsnachweis erbracht werden. Diese Lösung hätte den Vorteil, dass weitere Anforderungen beim Umgang mit Signaturkarten umgesetzt werden können. Unter anderem muss nämlich auch die Sperrung von qualifizierten Signatur- bzw. Attribut-Zertifikaten durch die Behörde möglich sein. Dass eine solche Sperrmöglichkeit im Standesamt bezüglich des Personenstandsregisters auf jeden Fall gegeben sein muss, ist wohl unstrittig (z. B. bei Versetzung, Beurlaubung usw.). Diese Sperrung muss auch kurzfristig erfolgen können. Eine solche Sperrung von Signaturkarten ist nur durch vorherige Vergabe eines berufsbezogenen Attributs oder Attribut-Zertifikats durch das Standesamt möglich.

Ich empfehle der Landesregierung, sich dafür einzusetzen, dass eine einheitliche Handhabung beim Aufbau und der Formulierung der Attribute für elektronische Personenstandsregister oder sogar für alle behördlichen Signaturen realisiert wird. Darüber hinaus sollte geprüft werden, wo in Anlehnung an die Definition der Elektronischen Form in § 126 a BGB eine einheitliche Festlegung aufzunehmen ist, dass und wie in dem zu signierenden Personenstands-Dokument der Name des Standesbeamten (und ggf. der Behörde) hinzugefügt wird.

4.5 Technologischer Datenschutz in der Medizin

4.5.1 Telemedizin

In der 5. Legislaturperiode (2007 bis 2011) wurde beim Ministerium für Soziales und Gesundheit Mecklenburg-Vorpommern ein Beirat für Telemedizin eingerichtet. Aufgabe dieses Beirates war es, Entscheidungen zur Förderung von Projekten auf dem Gebiet Telemedizin vorzubereiten, um dadurch Aktivitäten zu koordinieren und Schwerpunkte zu setzen. Zu den Sitzungen des Beirates wurde ich als Sachverständiger eingeladen, um bereits in den frühen Projektstadien die Verantwortlichen datenschutzrechtlich zu beraten und mögliche nachträgliche Aufwendungen zur Erfüllung der datenschutzrechtlichen Bestimmungen zu vermeiden.

Die Teilnahme an den Sitzungen des Beirates ermöglichte es mir, einen umfassenden Überblick über die telemedizinischen Projekte unseres Bundeslandes zu erhalten. Bei diesen Sitzungen zeigte sich, dass insbesondere das Universitätsklinikum/die Universitätsmedizin Greifswald viele Projekte initiiert und damit eine maßgebliche Rolle in der Telemedizin unseres Landes spielt. Daraus resultierten wiederum mehrere datenschutzrechtliche Beratungen an der Universität und in meiner Dienststelle. Da ich bereits von Beginn an in die Projektentwicklung einbezogen worden bin, konnten datenschutzrechtliche Hinweise frühzeitig umgesetzt werden, beispielsweise bei dem Rahmenkonzept Datenschutz und IT-Sicherheit des Instituts Community Medicine. Darüber hinaus habe ich auch andere Projekte, wie beispielsweise die elektronische Fallakte, die maßgeblich vom HELIOS-Klinikum Schwerin projektiert und umgesetzt wird, beratend begleitet.

Im September 2011 hat mir der Verein „Telemedizin Euroregion POMERANIA“ seine Planung zur weiteren Entwicklung der Zusammenarbeit von Krankenhäusern und Kliniken in der Region vorgestellt. Die Euroregion POMERANIA umfasst Teile Vorpommerns, nordöstliche Teile des Landes Brandenburg und westliche Teile Polens. Durch Arbeitsteilung und Konsultationen bei der Behandlung von Erkrankungen soll eine wohnortnahe Diagnostik und Therapie auf einem hohen Qualitätsniveau gewährleistet werden. Als erste Schritte werden Videokonferenzen und Tumorfall-Besprechungen geplant. Die Videokonferenzen sollen beispielsweise auch die Übertragung von Sprache und Bild aus dem Operationsaal ermöglichen und dabei die bildliche Diagnostik einschließen. In der ersten Beratung ging es um die wesentlichen datenschutzrechtlichen Rahmenbedingungen für die geplanten Anwendungen.

Für Patienten, die in Kliniken und Krankenhäusern der Euroregion POMERANIA unseres Bundeslandes behandelt werden, ist die wesentliche Rechtsgrundlage das Landeskrankenhausesgesetz (LKHG M-V, siehe Punkt 5.10.1). Danach ist beispielsweise die Übermittlung von Patientendaten an Stellen außerhalb des Krankenhauses zur Durchführung einer Mit- oder Nachbehandlung zulässig, soweit der Patient nichts anderes bestimmt hat (§ 35 Abs. 1 Nr. 2 LKHG M-V). Ein Patient ist demnach über eine Mitbehandlung aufzuklären und - sofern er keinen gegenteiligen Willen äußert - es können die Daten auf dieser Grundlage verarbeitet werden. Im Sinne der Datensparsamkeit habe ich empfohlen, dazu möglichst pseudonymisierte Daten der Patienten zu nutzen. Da ärztliche Behandlungen zu dokumentieren sind, müssen in jedem Fall Maßnahmen getroffen werden, um bei dieser Verarbeitung die Integrität und Authentizität der Daten zu gewährleisten (siehe § 21 Abs. 2 DSGVO).

Ein weiteres Ziel des Projektes ist es, das Krankenhäuser Facharztleistungen anderer Krankenhäuser in Anspruch nehmen können. Zu diesem Zweck müssen dann Daten über die telemedizinische Infrastruktur ausgetauscht werden, beispielsweise pathologische Befunde. Vorrangig sollten auch dazu pseudonymisierte Daten genutzt und die oben erwähnten Maßnahmen umgesetzt werden. Die Frage ist aber, ob hierzu die Einwilligung des Patienten erforderlich ist. Eine ähnliche Fragestellung besteht im Übrigen auch, wenn Laborleistungen von Dritten erbracht werden. Nach meiner Auffassung ist dies nicht durch eine Einwilligung des Patienten zu lösen, weil eine Freiwilligkeit nicht gegeben ist. Würde ein Patient die Einwilligung verweigern, könnte die Behandlung ohne die Dienstleistung des Facharztes in dem Krankenhaus nicht bzw. nicht erfolgreich durchgeführt werden.

Diese Datenverarbeitung sollte daher auf die Norm gestützt werden, die eine Übermittlung von Patientendaten zur Erfüllung des Behandlungsvertrages erlaubt (§ 35 Abs. 1 Nr. 1 LKHG M-V). Wichtig ist, dass die Patienten bei Abschluss des Behandlungsvertrages darüber informiert werden, welche Leistungen von Dritten erbracht werden. Mit dem Verein „Telemedizin Euroregion POMERANIA“ ist die weitere datenschutzrechtliche Beratung bei der Umsetzung des Projektes vereinbart worden.

4.5.2 Anforderungen an Krankenhausinformationssysteme

Im Jahr 2011 hat eine Arbeitsgruppe aus Vertretern der Arbeitskreise „Gesundheit und Soziales“ und „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie aus kirchlichen Datenschutzbeauftragten die Orientierungshilfe „Krankenhausinformationssysteme“ verfasst.

In der Prüfpraxis der Datenschutzbeauftragten hatte sich in den letzten Jahren gezeigt, dass Krankenhausinformationssysteme wichtige gesetzliche Schutzanforderungen nicht abbilden und dass Schutzvorkehrungen nicht eingesetzt oder umgangen werden, weil sie schlecht bedienbar sind. Dazu gehören mangelnde Protokollierung insbesondere lesender Zugriffe, zu weit gefasste Zugriffsrechte und der Einsatz von Benutzerkonten für ganze Gruppen von Mitarbeitern.

In der nun vorliegenden Orientierungshilfe sind grundlegende Anforderungen des Datenschutzes an Hersteller und Betreiber von Krankenhausinformationssystemen zusammengefasst. In einem Kommentierungsverfahren und bei Expertenanhörungen wurden Hersteller von Krankenhausinformationssystemen, Betreiber, Anwendervereinigungen und Datenschutzbeauftragte von Krankenhäusern mit einbezogen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Düsseldorfer Kreis haben die Orientierungshilfe zustimmend zur Kenntnis genommen.

Die Orientierungshilfe enthält einen rechtlichen und einen technischen Teil.

Im rechtlichen Teil geht es darum, unter welchen Voraussetzungen der Zugriff auf Patientendaten in einem Krankenhausinformationssystem zulässig ist. Aufnahme, Behandlung und Abrechnung sowie Qualitätssicherung werden getrennt untersucht. Außerdem spielen Fragen der Zusammenarbeit medizinischer Einrichtungen, beispielsweise in Konzernen, und der Zugriffsmöglichkeiten im Rahmen der technischen Administration eine Rolle.

Im technischen Teil werden aus diesen rechtlichen Anforderungen technische Kriterien abgeleitet und erläutert. Hierbei geht es zunächst um das Datenmodell und um System- und Anwendungsfunktionen sowie das Rollen- und Berechtigungskonzept. Wegen ihrer Auswirkungen auf die datenschutzgerechte Gestaltung eines Krankenhausinformationssystems werden auch Fragen der Ergonomie und der Datenpräsentation untersucht. Beendet wird der technische Teil mit Ausführungen zur Protokollierung und zur technischen Administration.

Die Orientierungshilfe „Krankenhausinformationssysteme“ wird den Datenschutzbeauftragten und den Datenschutzaufsichtsbehörden bundesweit als Bewertungsmaßstab dienen. Sie kann auf meiner Website abgerufen werden (http://www.datenschutz-mv.de/dschutz/informat/kis/OH_KIS.pdf).

Ich empfehle allen öffentlichen und privaten Krankenhäusern unseres Landes, diese Orientierungshilfe zu beachten. Soweit an bestehenden Systemen Änderungen erforderlich sind, müssen diese selbstverständlich mit der gebotenen Sorgfalt unter Berücksichtigung der Patientensicherheit ausgeführt werden.

4.5.3 KV SafeNet - eine Kommunikationslösung für Ärzte

Bereits im Juli 2008 informierte mich die Kassenärztliche Vereinigung Mecklenburg-Vorpommern (KV M-V) über das Verfahren KV-SafeNet, einer Lösung für die Online-Kommunikation für Ärzte. Diese von der Kassenärztlichen Bundesvereinigung (KBV) bundesweit angebotene Lösung sollte auch die Übermittlung der Abrechnungsdaten von Ärzten an die KV M-V unterstützen und gleichzeitig der elektronischen Kommunikation zwischen Ärzten dienen. Nach entsprechender Prüfung habe ich der KV M-V bestätigt, dass die in der Rahmenrichtlinie der Kassenärztlichen Bundesvereinigung beschriebenen Anforderungen die Sicherheit der Netzinfrastruktur zur Kommunikation zwischen Ärzten und KV M-V gewährleisten und dass KV-SafeNet diese Anforderungen umsetzt.

Im September 2010 behauptete ein Informatiker, der Computersysteme ärztlicher Praxen betreut, dass KV-SafeNet grobe Sicherheitsmängel enthalte. Er befürchtete, dass beim Einsatz von KV-SafeNet der interne Datenverkehr des Praxis-Computernetzwerks überwacht werden könne. Da KV-SafeNet bundesweit eingesetzt wird, habe ich in meiner Eigenschaft als Vorsitzender des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten von Bund und Ländern (siehe Punkt 6) sowohl Vertreter der KBV als auch der KV M-V eingeladen, um zu klären, ob die Vorwürfe des Informatikers berechtigt waren.

Das Gespräch offenbarte tatsächlich einige Unzulänglichkeiten des Verfahrens sowohl in technischer als auch in organisatorischer Hinsicht. Für den Zugang zum Netz der KBV ist ein Router erforderlich, der von verschiedenen Providern angeboten wurde. Die Konfiguration dieses Routers entsprach den Sicherheitsanforderungen nicht vollständig. Auch waren Mängel bezüglich der Transparenz von Fernwartungsprozeduren festzustellen. Beispielsweise fehlten Protokolle, mit denen die Administrationstätigkeiten nachträglich geprüft werden können. Unklar war auch, welche Aussagekraft Zertifikate hatten, mit denen Provider für sich und für die von ihnen angebotenen Router geworben hatten.

Im Ergebnis des Gesprächs übergab ich der KBV einen Katalog mit Forderungen, deren Umsetzung einen vollständig datenschutzkonformen Betrieb von KV-SafeNet sicherstellen sollte. Diesen Katalog hat die KBV in kürzester Zeit vollständig abgearbeitet. So hat die KBV die Provider verpflichtet, die Router entsprechend den Forderungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu konfigurieren. Die KBV hat unverzüglich die entsprechenden Rahmenrichtlinien überarbeitet. Auch die technischen Dokumentationen wurden überarbeitet, sodass die Ärzte in die Lage versetzt wurden, die Verschlüsselungsmethodik und die allgemeine Funktionsweise von KV-SafeNet nachzuvollziehen. Darüber hinaus wurden detaillierte Vorgaben zum Ablauf der Fernwartung gemacht und den Ärzten angemessene Mitwirkungsmöglichkeiten eingeräumt. Schließlich wurde das Zertifizierungs- und Auditierungsverfahren für die Provider und die von ihnen angebotenen Router überarbeitet.

Nachdem die KBV alle Forderungen umgesetzt hatte, befasste sich auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit dem Thema. In ihrer Entschließung vom März 2011 (siehe <http://www.datenschutz-mv.de/dschutz/beschlue/entsch81.html#nr5>) haben die Datenschutzbeauftragten darauf hingewiesen, dass an medizinische Netze hohe Anforderungen hinsichtlich der Vertraulichkeit und Integrität zu stellen sind, da sowohl in den Netzen selbst als auch auf den angeschlossenen Praxissystemen Daten verarbeitet werden, die der ärztlichen Schweigepflicht (§ 203 StGB) unterliegen. Die Konferenz hat empfohlen, bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze die „Technische Anlage zu den Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung (siehe Deutsches Ärzteblatt, Jg. 105, Heft 19 vom 9. Mai 2008) zu beachten. Für die verwendeten Verschlüsselungs- und Authentisierungskomponenten sollten vorzugsweise Hardware-Lösungen genutzt werden, da bei Software ein erhöhtes Manipulationsrisiko besteht.

4.6 Videüberwachung

4.6.1 Polizeiliche Videüberwachung in der Rostocker Innenstadt

Das Polizeipräsidium Rostock hat mich frühzeitig in sein Pilotprojekt zur Videüberwachung von Teilen der Rostocker Innenstadt einbezogen. Hinsichtlich einer ständigen Bildüberwachung der Bereiche Neuer Markt/Kröpeliner Straße/Universitätsplatz sind unterschiedliche Rechtsauffassungen vorgetragen worden. Die Videüberwachung in diesem Bereich der Fußgängerzone wird vom Polizeipräsidium Rostock vorerst zurückgestellt.

Hinsichtlich einer Videüberwachung für die Bereiche Doberaner Platz, Lange Straße, Konrad-Adenauer-Platz (Bahnhofsvorplatz Nordseite) und Albrecht-Kossel-Platz (Hauptbahnhof Südseite) habe ich eine lageabhängige, anlassbezogene Bildüberwachung grundsätzlich als zulässig erachtet. Als Anlass wurden hier Fußballspiele von Hansa Rostock benannt, bei denen es bekanntermaßen regelmäßig zu (häufig gewalttätigen) Ausschreitungen kommt. Geplant ist hier, dass von Seiten der Polizei vorbereitende Maßnahmen getroffen werden, die eine spätere Installation von Kameras erlauben. Die Kameras sollen nur für den bestimmten Anlass installiert und danach entweder vollständig abgedeckt beziehungsweise wieder abgehängt werden.

Über die Anordnung der Bildüberwachung gemäß § 32 Abs. 3 Satz 6 Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommern (SOG M-V) wird mich das Polizeipräsidium Rostock unverzüglich unterrichten.

4.6.2 „Spicken“ und „Schummeln“ verboten

Von der Presse wurde ich darauf aufmerksam gemacht, dass Studierende einer Universität während einer Klausur per Videokamera überwacht worden sind. Die Studierenden wussten nichts von der Videüberwachung.

Nach Auskunft der Universität ist in einem Hörsaal eine Kameraanlage installiert worden, um zum Beispiel medizinische Demonstrationen am Patienten für alle Studierenden auf einer großen Leinwand sichtbar zu machen. Neben der Wiedergabe über die große Leinwand ist auch eine Kontrollwiedergabe des Bildes auf den Monitoren im Rednerpult möglich.

Die Anlage ist jedoch technisch nicht geeignet, Bilder aufzuzeichnen. Diese Technik nutzte nun ein Professor bei einer schriftlichen Prüfung, um die Plätze in den schlecht einsehbaren hinteren Hörsaalbereichen besser zu überschauen und um damit auch das „Spicken“ und „Schummeln“ zu erschweren.

Grundlage für die Verarbeitung personenbezogener Daten an Hochschulen ist § 7 Landeshochschulgesetz (LHG M-V). Dort ist geregelt, dass Hochschulen auf der Grundlage des Landesdatenschutzgesetzes Mecklenburg-Vorpommern (DSG M-V) das Nähere über die Verarbeitung der Studentendaten in einer Satzung auf der Grundlage des Landesdatenschutzgesetzes zu regeln haben. Dies bedeutet auch, dass die Regelungen zur Videoüberwachung nach § 37 DSG M-V umzusetzen sind. Die Satzung der betreffenden Hochschule enthielt dazu keine Regelung, sodass die Vorschrift des DSG M-V anzuwenden ist. Nach dieser Rechtsvorschrift ist die Videoüberwachung nur zur Wahrnehmung des Hausrechtes zulässig. Eine Videoüberwachung zur Vermeidung oder Aufdeckung von Betrugshandlungen bei Prüfungen fällt nicht unter das Hausrecht und war somit nicht zulässig.

Die Universität versicherte, dass es sich hier um einen bedauerlichen Einzelfall handelte und der Professor seine aus der Situation heraus entstandene Idee im Nachhinein nun sehr kritisch betrachte. Der Vorfall wurde mit den Mitarbeiterinnen und Mitarbeitern ausgewertet und es wurde nochmals darauf hingewiesen, dass diese Form der Überwachung bei Prüfungsarbeiten nicht zulässig ist.

4.6.3 Videoüberwachung in der Psychiatrie

Von der Krankenhausgesellschaft Mecklenburg-Vorpommern e. V. wurde ich aufgrund der Anfrage eines Mitglieds gebeten zu prüfen, ob es zulässig sei, die Flure und die Patientenzimmer in einem psychiatrischen Krankenhaus mit einer Videokamera zu überwachen. Ein Krankenhaus hatte diese Möglichkeit in Betracht gezogen, um bei Gefährdungen schnell reagieren zu können.

Auch wenn der Schutzbereich des Artikels 13 Grundgesetz (GG; Unverletzlichkeit der Wohnung) nach herrschender Auffassung das Patientenzimmer nicht umfasst, ist ein grundrechtlicher Schutz des Betroffenen an der Ungestörtheit in seinem Wohnbereich anzuerkennen. Eine Videoüberwachung des Patientenzimmers stellt einen erheblichen Eingriff in dieses Grundrecht des Patienten dar.

Nach § 40 Abs. 1 Psychischkrankengesetz Mecklenburg-Vorpommern (PsychKG M-V) sind abweichend von § 22 Abs. 1 besondere Sicherungsmaßnahmen zulässig, sobald die Gefahr besteht, dass der Betroffene sich selbst tötet oder ernsthaft verletzt oder gewalttätig wird oder die Einrichtung ohne Erlaubnis verlassen wird, und dieser Gefahr nicht anders begegnet werden kann. Besondere Sicherungsmaßnahmen dürfen nur durch den Arzt der Einrichtung angeordnet werden. Die besonderen Sicherungsmaßnahmen wiederum sind in § 22 Abs. 2 PsychKG M-V benannt. Danach gehört die Videoüberwachung nicht zu diesem Maßnahmenkatalog.

Ich habe der Krankenhausgesellschaft mitgeteilt, dass ich die Videoüberwachung der Patientenzimmer vor diesem rechtlichen Hintergrund für nicht zulässig halte. Die Videoüberwachung des Flures könnte jedoch zulässig sein, wenn die gesetzlichen Voraussetzungen von § 37 Abs. 1 DSGVO (Videoüberwachung und -aufzeichnung) erfüllt sind.

4.6.4 Videoüberwachung in Unternehmen

In zunehmendem Maße werden Videokameras auch geschäftlich eingesetzt, zum Beispiel in Kaufhäusern oder an Gebäuden. Beabsichtigt ist meist der Schutz vor Diebstahl, Vandalismus oder Einbrüchen – teilweise jedoch auch die Überwachung der eigenen Mitarbeiter durch die Geschäftsleitung.

Die eingesetzte Videotechnik ist wesentlich preiswerter, als das noch vor wenigen Jahren der Fall war. Auch dadurch steigt die Zahl der Fälle, in denen diese Technik zur Anwendung kommt. Insbesondere im Jahr 2011 stellte der Bereich Videoüberwachung einen Schwerpunkt für die Datenschutzaufsichtsbehörde dar. Die Kontrollpraxis hat gezeigt, dass der Einsatz der Videoüberwachungstechnik sehr oft über das zur Erfüllung der genannten Zwecke Erforderliche hinausgeht. Er ist in einer Vielzahl der Fälle unzulässig. Das technisch Machbare in diesem Bereich ist durchaus faszinierend. Aber nicht alles, was technisch möglich ist, ist datenschutzrechtlich zulässig. Bereits bei der Planung, aber auch beim Betrieb von Videoüberwachungsanlagen müssen die hierfür geltenden Datenschutzvorschriften eingehalten werden. Betrifft die Überwachung Arbeitnehmer, so sind beschäftigungsdatenschutzrechtliche Vorschriften zu beachten - insbesondere § 32 BDSG.

Soweit öffentlich zugängliche Räume betroffen sind, richtet sich die Zulässigkeit nach § 6 b BDSG. Öffentlich zugängliche Räume sind Bereiche innerhalb oder außerhalb von Gebäuden, die frei oder nach allgemein erfüllbaren Voraussetzungen (zum Beispiel mit Eintrittskarte) betreten werden können. Hierzu zählen zum Beispiel Verkaufsräume von Warenhäusern, Cafés, Publikumsbereiche von Banken, Hotelfoyers, Museen und Kinos nach Lösen einer Eintrittskarte. Bis auf den öffentlichen Straßenraum, wo die Videoüberwachung in der Regel unzulässig ist, dürfen Videokameras eingesetzt werden, wenn eine vorherige Prüfung durch die verantwortliche Stelle ergeben hat, dass dies für einen festgelegten, konkreten Zweck erforderlich ist und insbesondere die schutzwürdigen Interessen der überwachten Personen nicht überwiegen.

Vor dem Einsatz der Technik ist deshalb festzulegen und in einer Verfahrensbeschreibung zu dokumentieren, welcher genaue Zweck und welches Ziel damit erreicht werden soll. Handelt es sich um unterschiedliche Zwecke, so müssen sie differenziert festgelegt und hinsichtlich der erforderlichen Maßnahmen differenziert geprüft werden (Schutz vor Diebstahl, Vermeiden von Vandalismusschäden, Verhindern von Straftaten etc.). Ferner ist zu prüfen, ob die Videoüberwachung in der Praxis wirklich geeignet ist, um den festgelegten Zweck zu erreichen und ob hierzu nicht andere, die Videoüberwachung vermeidende, Mittel zur Verfügung stehen (Scheinwerfer mit Bewegungsmelder, Wachdienste, Einsatz eines Pförtners etc.). Erforderlich ist die Videoüberwachung nämlich nur dann, wenn das festgelegte Ziel mit der Überwachung erreicht werden kann und wenn es dafür kein weniger einschneidendes Mittel gibt.

Die Kontrollpraxis hat gezeigt, dass diese Erforderlichkeitsprüfung in der Regel in vielen Fällen nicht durchgeführt wird und dadurch zu viele und falsch positionierte Videokameras eingesetzt werden. Auch das zeitliche Maß der erforderlichen Überwachung wird oft nicht bedacht. In vielen Fällen reicht es aus, die Kameras lediglich zur Nachtzeit zu aktivieren, wenn sich entsprechende Vorfälle nicht tagsüber ereignet haben.

Sofern nur die Videoüberwachung als geeignete und erforderliche Maßnahme in Betracht kommt, so muss vor deren Einsatz geprüft werden, ob und gegebenenfalls welche Personengruppe videoüberwacht wird und ob deren schutzwürdige Interessen höher zu bewerten sind. Dieses schutzwürdige Interesse überwiegt nahezu immer, wenn sensitive Daten (politische Meinungen, religiöse Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit etc.) erhoben werden oder die Intimsphäre verletzt wird. Die Überwachung von Toiletten oder Umkleidekabinen ist deshalb nicht erlaubt.

Beim Einsatz der Videoüberwachung ist zu beachten, dass die Tatsache der Überwachung und die verantwortliche Stelle gemäß § 6 b Abs. 2 BDSG durch geeignete Maßnahmen (in der Regel Beschilderung) für die Betroffenen erkennbar gemacht werden muss. Der Hinweis muss vor Betreten des überwachten Bereiches problemlos wahrnehmbar sein, damit die freie Entscheidung für oder gegen das Betreten möglich ist. Die technischen und organisatorischen Maßnahmen sollten in einem Sicherheitskonzept dokumentiert werden. Bei komplexen Videoanlagen ist in der Regel ein betrieblicher Datenschutzbeauftragter zu bestellen.

Entstehen durch die Videoüberwachung Bilder, die einer bestimmten Person zugeordnet werden, so ist diese gemäß § 6 b Abs. 4 BDSG darüber zu benachrichtigen. Eine Aufzeichnung ist nur rechtmäßig, wenn der mit der Videoüberwachung verfolgte Zweck dies erfordert. Wenn aufgezeichnet wird, ist das Videomaterial nach Erreichen des Aufzeichnungszwecks unverzüglich zu löschen. Praktikabel ist eine automatisierte Löschung durch Selbstüberschreiben zurückliegender Aufnahmen. So werden beispielsweise Videoaufzeichnungen zum Beweis von Einbrüchen oder Ladendiebstählen dann nicht mehr benötigt, wenn kein Ereignis festgestellt wurde. Die Aufzeichnungen eines Geschäftstages sollten daher möglichst am nächsten Tag, spätestens aber nach Ablauf von zwei bis drei Arbeitstagen gelöscht werden.

Nachfolgend nun einige Beispiele, die im Berichtszeitraum gehäuft aufgetreten sind:

4.6.5 „Nachbarschaftliche“ Videoüberwachung

Videokameras werden zunehmend auch im Rahmen von nachbarschaftlichen Auseinandersetzungen als technisches Hilfsmittel benutzt - entweder zur Einschüchterung oder um sich gegen tatsächliche oder vermeintliche Angriffe des Nachbarn zu wehren und diese zu dokumentieren. Die Installation von Videokameras ist dann in der Regel nicht die Ursache, sondern mehr eine weitere Eskalationsstufe dieser nachbarschaftlichen Auseinandersetzungen.

Die Videoüberwachung des eigenen privaten Grundstücks ist grundsätzlich möglich, solange kein öffentlich zugänglicher Raum und keine Nachbargrundstücke überwacht werden. Erfasst die Kamera jedoch das Nachbargrundstück, werden die Rechte des Nachbarn verletzt.

Das Bundesdatenschutzgesetz ist gemäß § 1 Abs. 2 Nr. 3 BDSG jedoch nicht anwendbar, da in diesem Fall die Datenverarbeitung in der Regel zu persönlichen oder familiären Zwecken erfolgt. Gegen die Überwachung von Privatgrundstücken, z. B. durch Nachbarn, bestehen allerdings für Betroffene in der Regel zivilrechtliche Unterlassungs- und Abwehransprüche nach den §§ 1004, 823 BGB. Diese Ansprüche müssen allerdings durch die Betroffenen selbst auf dem Zivilrechtsweg und gegebenenfalls unter Einschaltung eines Rechtsanwalts durchgesetzt werden.

Die Videoüberwachung von öffentlich zugänglichem Raum unterliegt demgegenüber den Zulassungsvoraussetzungen des § 6 b BDSG. Die Videoüberwachung öffentlich genutzten Straßenraums ist grundsätzlich unzulässig. Kameras zur Überwachung des eigenen Grundstücks müssen deshalb so ausgerichtet werden, dass der öffentlich genutzte Straßenraum vor dem Grundstück nicht erfasst wird. Mit Blick auf die oftmals gewünschte Überwachung der eigenen Hausfassade sind allerdings Ausnahmen möglich. So kann die Erfassung eines schmalen Streifens entlang der Hauswand unter bestimmten Umständen nach der Rechtsprechung ausnahmsweise zulässig sein (vgl. Urteil des AG Berlin-Mitte vom 18. Dezember 2003, Az.: 16 C 427/02).

4.6.6 Webcams

Bei einer Videoüberwachung unter Einsatz von Webcams ist zu berücksichtigen, dass die Bilder über das Internet einer nicht bestimmbar Anzahl von Personen zugänglich gemacht werden - und zwar in der Regel weltweit. Zunehmend werden Webcams auch im Tourismussektor eingesetzt, was im Tourismusland Mecklenburg-Vorpommern zu einem Anstieg der Fälle geführt hat. Hotels ermöglichen ihren potenziellen Kunden über das Internet gern schon vor der Reise einen Blick auf den eigenen Park mit angrenzendem Badestrand per Webcam, verlinkt von ihrer Homepage. Auch Fremdenverkehrsvereine binden Livebilder des Yachthafens eines Küstenortes per Webcam in ihre Homepage ein.

Datenschutzrechtlich zu bedenken ist, dass bei solchen Bildern nicht nur Strände, Häfen oder Bootsstege zu sehen sind, sondern dass auch die sich dort aufhaltenden Personen erfasst werden. Sobald ein Personenbezug möglich ist, also auf den Bildern Personen oder personenbeziehbare Daten (z. B. Kfz-Kennzeichen) identifizierbar sind, ist § 22 Kunsturhebergesetz (KunstUrhG – Recht am eigenen Bild) zu beachten.

Nach dieser Regelung ist die Veröffentlichung von Bildern mit personenbezogenen Daten in der Regel nur dann zulässig, wenn die ausdrückliche Einwilligung der Betroffenen vorliegt, was meist wegen der Vielzahl der potenziell betroffenen Personen nicht oder nur sehr schwer umsetzbar ist. Eng begrenzte Ausnahmen enthält § 23 KunstUrhG. Liegt eine Einwilligung nicht vor, so kann die Veröffentlichung der Bilder gemäß § 22 KunstUrhG in Verbindung mit § 33 KunstUrhG wegen der Verletzung des Rechts am eigenen Bild nicht nur unzulässig, sondern grundsätzlich sogar strafbar sein. Gegen die Zulässigkeit bestehen nur dann keine Bedenken, wenn die Bilder so unscharf sind, dass eine Identifizierbarkeit der abgebildeten Personen ausgeschlossen werden kann oder die Kamera so eingestellt ist, dass Personen und personenbeziehbare Merkmale von vornherein nicht erfasst werden.

4.6.7 Mitarbeiterüberwachung

Bei den überprüften Videoüberwachungsanlagen waren die Kameras von den Geschäftsführern der Betriebe nach ihren eigenen Angaben dazu installiert worden, um Straftaten (Diebstähle, Überfälle etc.) dokumentieren zu können. Bei der Überprüfung stellte sich jedoch nicht selten heraus, dass die Kameras gleichzeitig geeignet waren, auch eigene Mitarbeiter zu überwachen. Dies betraf in größerer Zahl insbesondere kleinere Ladengeschäfte (oft in Einkaufspassagen) und in vielen Fällen Bäckereifilialen oder kleinere Lebensmittelgeschäfte.

Wenn durch Videoüberwachungsmaßnahmen Arbeitnehmer betroffen sind, müssen beschäftigungsdatenschutzrechtliche Vorschriften und insbesondere § 32 BDSG beachtet werden. Dabei ist der Maßstab für die Erforderlichkeit des Einsatzes von Videotechnik im Arbeitsverhältnis hoch anzusetzen, da es sich um einen besonders intensiven Eingriff in die Persönlichkeitsrechte von Beschäftigten an ihrem Arbeitsplatz handelt. Eine Videoüberwachung, die nur dazu dient, die Effizienz und Sorgfalt der Beschäftigten zu gewährleisten, ist unzulässig - ebenso wie eine durchgängige Videoüberwachung während der gesamten Arbeitszeit. Toiletten und Sanitärbereiche sowie Umkleidekabinen und andere sensible Bereiche sind von der Beobachtung auszunehmen. Eine Videoüberwachung als Mittel zur Aufdeckung von Straftaten im Beschäftigungsverhältnis ist nur im Ausnahmefall als „letztes Mittel“ und nur unter den strengen Zulässigkeitsanforderungen des § 32 Abs. 1 Satz 2 BDSG zulässig. Danach müssen tatsächliche und zu dokumentierende Anhaltspunkte dafür vorliegen, dass eine Straftat durch den Betroffenen begangen worden ist. Bei der Erforderlichkeit der Maßnahme ist zu prüfen und sicherzustellen, dass alle anderen Mittel zur Aufklärung erfolglos geblieben sind. Ferner darf kein überwiegendes schutzwürdiges Interesse des Betroffenen am Ausschluss der Überwachung bestehen. Die Maßnahme darf insgesamt in Art und Ausmaß im Verhältnis zum Anlass der Überwachung nicht unverhältnismäßig sein. Der Betriebsrat muss vor der Überwachung beteiligt werden.

Im Ergebnis der datenschutzrechtlichen Prüfungen wurde eine Vielzahl von Kameras in Einstellung und Position entsprechend geändert, sodass diese nunmehr datenschutzgerecht betrieben werden. Diese Fälle betrafen keine verdeckten, sondern offene Videoüberwachungen. In einigen Fällen wurde die Deinstallation von rechtswidrig betriebenen Kameras durch die verantwortlichen Stellen (auch durch Einschaltung von Rechtsanwälten) in der Umsetzung verzögert.

4.6.8 Videoüberwachung in Einkaufszentren

Im Rahmen von umfangreichen Kontrollen wurden die in Mecklenburg-Vorpommern gelegenen Einkaufszentren einer bundesweiten Unternehmenskette in Hinblick auf die dort zahlreich installierten Videokameras kontrolliert. Teilweise überwachten Videokameras die Ladenpassagen und die dort gelegenen Cafés und Ruhebereiche, die Zugänge zu den Fahrstühlen, Rolltreppen, sowie Eingangsbereiche, Parkautomaten, Parkplätzen und Notrufsäulen etc.

Im Ergebnis der Kontrollen und der datenschutzrechtlichen Bewertung wurden Kameras in den Ladenpassagen, an Fahrstühlen, Rolltreppen und Eingängen/Drehtüren als unzulässig bewertet. Insbesondere in den von Videokameras überwachten großflächigen Ladenpassagen, in denen zum Teil auch Cafés, Espressobars, Eisdielen etc. angesiedelt sind, überwiegen die schutzwürdigen Interessen der Kunden und Angestellten, nicht ständig im Einkaufszentrum von einer Videoüberwachung erfasst zu werden, gegenüber dem Interesse des Einkaufszentrums an einer störungsfreien Atmosphäre.

Das Recht auf informationelle Selbstbestimmung schließt das Recht des Einzelnen ein, sich in der Öffentlichkeit frei bewegen zu können, ohne befürchten zu müssen, dass er ständig beobachtet wird. Die Schutzbedürftigkeit ist besonders in öffentlichen Räumen hoch, in denen sich Menschen typischerweise länger aufhalten oder miteinander kommunizieren.

Bei den Ladenstraßen in den Einkaufszentren handelt es sich nicht um Durchgangsbereiche, die man rasch durchquert und wieder verlässt. Einkaufszentren, in denen die Kunden ein breites Warenangebot vorfinden, ermöglichen es ihnen, zu verweilen und in Ruhe die Auslagen der Geschäfte anzusehen. Sitzgelegenheiten werden geschaffen und Gastronomie angesiedelt, um die Kunden zu einem längeren Aufenthalt zu motivieren. Kunden, die dies tun, können sich der umfassenden und ständigen Videoüberwachung jedoch nicht entziehen und werden dadurch in ihren Rechten unangemessen beeinträchtigt. Der bisherige Einsatz von insgesamt 28 Videokameras in diesen Bereichen war deshalb unzulässig.

Die Geschäftsleitungen aller Center waren ausnahmslos kooperativ. Die entsprechenden Kameras wurden abgebaut. Somit erfolgt der Einsatz von Videoüberwachungsanlagen in diesen Einkaufszentren nunmehr datenschutzgerecht.

5. Datenschutz in verschiedenen Rechtsgebieten

5.1 Rechtswesen

5.1.1 Handyortung und mehr

In Dresden hatten die Strafverfolgungsbehörden anlässlich einer Demonstration im Februar 2011 mit einer Funkzellenabfrage hunderttausende von Verkehrsdaten von Mobilfunkteilnehmern erhoben, darunter Rufnummern von Anrufern und Angerufenen in einer bestimmten Funkzelle. Die Datenschutzbeauftragten von Bund und Ländern haben daraufhin öffentlich gefordert, dass die nichtindividualisierte Funkzellenabfrage eingeschränkt wird und dem Grundsatz der Verhältnismäßigkeit in der Praxis mehr Rechnung getragen wird.

Vom Freistaat Sachsen ist aufgrund dieser Vorfälle eine Bundesratsinitiative auf den Weg gebracht worden (vgl. BR-Drs. 532/11), die die Voraussetzungen der nichtindividualisierten Funkzellenabfrage präzisiert. Die Thematik soll am 12. Januar 2012 auf der Tagesordnung der Sitzung des Bundesrates stehen. Der Sächsische Datenschutzbeauftragte hat in einem 53 Seiten umfassenden Bericht die Funkzellenabfragen gegenüber den zuständigen Behörden Polizeidirektion, Landeskriminalamt und Staatsanwaltschaft Dresden förmlich beanstandet. In der Folge ist in nicht nachvollziehbarer Weise die Kompetenz des Sächsischen Datenschutzbeauftragten zur Kontrolle von Polizei und Staatsanwaltschaften im Vorfeld einer bzw. nach einer richterlichen Anordnung in Frage gestellt worden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher in einer Entschließung der 82. Konferenz am 28./29. September 2011 in München die Auffassung vertreten, dass die gesetzliche Befugnis des Sächsischen Datenschutzbeauftragten zur Kontrolle aller polizeilichen und staatsanwaltschaftlichen Maßnahmen der Datenverarbeitung außer Frage steht. Es ist auch im Bereich der Strafverfolgung eine verfassungsrechtlich begründete Kernaufgabe der unabhängigen Datenschutzbeauftragten, einen vorgezogenen Rechtsschutz dort zu gewährleisten, wo einzelne aufgrund der verdeckten Datenverarbeitung des Staates nicht oder nicht ausreichend früh anderweitigen Rechtsschutz erlangen können, vergleiche hierzu: www.lfd.m-v.de/dschutz/beschlue/funkzell.html.

Fraglich ist, wie sich die Situation in Mecklenburg-Vorpommern darstellt. Bei einer Recherche im Internet bin ich auf einen Beschluss des Landgerichts Rostock vom 16. Oktober 2007 gestoßen.

Im Tenor hat das Gericht festgestellt, dass die Anordnung zur Auskunftserteilung von Telekommunikationsverbindungsdaten mit Beschluss des Amtsgerichts Rostock vom 21. Mai 2007 rechtswidrig war. Der Betroffene hatte in dem vorliegenden Verfahren Beschwerde gegen den Beschluss des Amtsgerichts eingelegt. Das Landgericht hatte dem Richter am Amtsgericht vorgeworfen, nicht geprüft zu haben, ob es sich tatsächlich um eine erhebliche Straftat handelt. Zudem sei nicht erkennbar gewesen, dass der Richter sich mit der Verhältnismäßigkeit der Maßnahme auseinandergesetzt habe.

Insofern zeigt sich, dass auch hier im Land die Funkzellenabfragen nicht immer korrekt als Mittel der Strafverfolgung eingesetzt werden. Daher hätte schon die Strafverfolgungsbehörde im vorliegenden Fall strenger prüfen müssen, ob überhaupt die Voraussetzungen des § 100g Strafprozessordnung (StPO) vorliegen, insbesondere hätte die Verhältnismäßigkeit der Maßnahme geprüft werden müssen.

Als Landesbeauftragter für Datenschutz und Informationsfreiheit bin ich der Auffassung, dass die Voraussetzungen für eine Funkzellenabfrage in der StPO besser geregelt werden müssen. Daher unterstütze ich die entsprechende Bundesratsinitiative des Freistaates Sachsen.

5.1.2 Überwachungskonzept für besonders rückfallgefährdete Sexual- und Gewaltstraftäter

Nach dem Erlass der Verwaltungsvorschrift zum Überwachungskonzept für besonders rückfallgefährdete Sexual- und Gewaltstraftäter „FoKuS“ („Für optimierte Kontrolle und Sicherheit“) hatte mich das Justizministerium um eine datenschutzrechtliche Bewertung gebeten.

Der Vergleich mit den Unterlagen ähnlicher Projekte anderer Bundesländer zeigte erhebliche Unterschiede aus datenschutzrechtlicher Sicht:

1. In das Überwachungskonzept wurde ein sehr weiter Kreis von Personen bzw. Personengruppen aufgenommen, ohne im Einzelfall nach Fallgruppen zu differenzieren.

Auch solche Straftäter sollten in die Zielgruppe fallen, die sich wegen Mordes oder Totschlags strafbar gemacht haben, ohne dass ein sexueller Hintergrund der jeweiligen Straftat vorhanden sein muss. Meines Wissens ist jedoch die besondere Rückfallgefährdung gerade bei diesen Delikten, soweit keine sexuellen Motive zugrunde liegen, nicht unbedingt gegeben.

Soweit mir der Stand der Forschung bekannt ist, handelt es sich bei den Delikten gemäß §§ 211, 212 Strafgesetzbuch (StGB) meistens um Beziehungsdelikte, bei denen eine Rückfallgefährdung nicht notwendigerweise vorliegt.

2. Deliktsgruppen, die in Betracht kommen, sind in anderen Bundesländern enger gefasst.

Kriterien für die Aufnahme der betroffenen Personen in das Konzept sind lediglich das Vorhandensein einer bestimmten Deliktsgruppe und die Tatsache, dass sie wegen dieses Deliktes unter Führungsaufsicht stehen bzw. stehen werden. Es werden keine Differenzierungen vorgenommen, die den Probanden als besonders rückfallgefährdet erscheinen lassen. Angesichts der Folgen, die die Aufnahme des Betroffenen in das Konzept haben kann (unter anderem kann dies zur Ausschreibung zur polizeilichen Beobachtung für einen Zeitraum von im Regelfall fünf Jahren führen), ist das Fehlen von differenzierenden Kriterien ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung. Ohnehin ist fraglich, ob die polizeiliche Beobachtung überhaupt eine zielführende Maßnahme darstellt. Sie wurde zur Bekämpfung des Terrorismus entwickelt und auf diese besonderen Kriminalitätsformen zugeschnitten und sollte der Erkennung von Organisationszusammenhängen, Reisetätigkeiten und Kurierdiensten einer sich professionell abschirmenden Szene dienen.

Die polizeiliche Beobachtung funktioniert nach dem Zufallsprinzip. Die zur Beobachtung ausgeschriebenen Personen werden gerade nicht - wie es der Name der Maßnahme nahelegen könnte - besonders beobachtet. Lediglich wenn sie zufällig aus anderen Gründen überprüft werden, etwa beim Grenzübertritt oder bei einer Straßenverkehrskontrolle, werden Daten des Betroffenen an die ausschreibende Stelle gemeldet. So kann es sein, dass ein Proband monatelang reist, ohne auch nur ein einziges Mal kontrolliert worden zu sein. Die polizeiliche Beobachtung eignet sich nicht zur Abwehr einer konkreten Gefahr sowohl wegen ihres Zufallscharakters als auch wegen der Tatsache, dass beim Antreffen im Rahmen einer Kontrolle außer dem Abfassen einer Meldung nichts weiter zu veranlassen ist.

Trotz meiner Hinweise wollte das Justizministerium an der Verwaltungsvorschrift vorerst nichts ändern, weil man die Verwaltungsvorschrift „schlank“ halten und die Risikogruppen noch genauer differenzieren wolle. Ich habe das Justizministerium gebeten, im Zuge der fortlaufenden Evaluation des Projektes auf die von mir angesprochenen Kritikpunkte zu achten und gegebenenfalls das Konzept zu ändern.

5.2 Polizei/Ordnungsbehörden

5.2.1 Ahndung bei unerlaubten Datenabfragen

Die unerlaubte Datenabfrage durch Polizeiangehörige ist bei den Datenschutzbeauftragten von Bund und Ländern immer wieder ein Thema. Einer meiner Kollegen hat angefragt, wie sich die Situation und Ahndungspraxis in den einzelnen Bundesländern darstellt. In Mecklenburg-Vorpommern ist die Rechtslage wie folgt:

Nach § 42 Abs. 1 Landesdatenschutzgesetz von Mecklenburg-Vorpommern (DSG M-V) handelt ordnungswidrig, wer unbefugt von diesem Gesetz geschützte Daten, die nicht offenkundig sind,

1. erhebt, speichert, verändert, übermittelt, zweckwidrig verarbeitet, zum Abruf bereithält oder löscht oder
2. abrufen, einsieht, sich verschafft oder durch Vortäuschung falscher Tatsachen ihre Übermittlung an sich oder andere veranlasst.

Der Bußgeldrahmen geht bis 50.000 Euro. Gemäß § 42 Abs. 4 DSG M-V ist das Innenministerium Mecklenburg-Vorpommern für den Bereich der unerlaubten Datenabfragen durch Polizeibeamte die zuständige Behörde für die Verfolgung und Ahndung von Ordnungswidrigkeiten. Diese Regelung ist jedoch erst durch das Gesetz zur Änderung des Informationsfreiheitsgesetzes und des Landesdatenschutzgesetzes vom 20. Mai 2011 eingeführt worden.

Das Innenministerium hat mir mitgeteilt, dass es seit diesem Zeitpunkt zwei Sachverhalte gibt, bei denen gegebenenfalls Bußgeldverfahren wegen unerlaubter Datenabfragen durch Polizeiangehörige durchgeführt werden.

Ich habe mich aktuell auch mit einer vermuteten unbefugten Datenabfrage zu befassen. Eine Petentin äußerte mir gegenüber die Befürchtung, dass ein Polizeibeamter, den sie kennengelernt hatte, unbefugt Daten zu ihrer Person in polizeilichen Informationssystemen abgefragt hat. Es hat sich auf meine Nachfrage hin herausgestellt, dass dieser Polizeibeamte keine INPOL-Berechtigung (INPOL ist das Informationssystem der Polizeien des Bundes und der Länder) hatte, jedoch möglicherweise einen Kollegen veranlasst hat, personenbezogene Daten zu der Petentin ohne dienstlichen Grund abzufragen. Die Angelegenheit wird zurzeit noch von der zuständigen Polizeidienststelle geprüft.

5.2.2 Zweifelsfälle bei der DNA-Analyse

Unter den Datenschutzbeauftragten von Bund und Ländern wird derzeit die Zulässigkeit der Verwertung von „Beinahetreffern“ beim Abgleich der DNA-Identifizierungsmuster von Tatortspur und freiwillig abgegebener Speichelprobe diskutiert. Anlass war ein konkreter Fall in einem der Länder. Es kam dort bei einem Reihengentest infolge einer Meldung des mit der Untersuchung beauftragten Labors über eine relativ hohe Übereinstimmung, die auf eine mögliche verwandtschaftliche Beziehung des Probanden mit dem Spurenverursacher hindeutete, zu Ermittlungsmaßnahmen im Verwandtenkreis des Probanden. Der Spurenverursacher wurde dabei aber nicht festgestellt.

Die Generalstaatsanwaltschaft des betreffenden Bundeslandes will „Beinahetreffer“ als Zufallsfunde nach § 477 Abs. 2 StPO nutzen. Aus (datenschutz-)rechtlicher Sicht ist darauf hinzuweisen, dass § 477 Abs. 2 StPO nur für andere Strafverfahren gilt. Auch eine allgemeine Ermittlungsbefugnis (§ 161 StPO) greift hier nicht. Aus datenschutzrechtlicher Sicht weist der Wortlaut „Abgleich“ in § 81h Strafprozessordnung (StPO) darauf hin, dass das Spurenmateriale lediglich auf Treffer/Nichttreffer untersucht wird. Darüber hinaus ist die Frage der richtigen Belehrung vor der Einwilligung der Probanden ungeklärt, da in den Belehrungsformularen nach der Gesetzeslage bisher nicht auf die Nutzung von „Beinahetreffern“ und die mögliche Belastung von Personen, bei denen Aussageverweigerungsrecht besteht, hingewiesen wird.

Das Landeskriminalamt Mecklenburg-Vorpommern (LKA M-V) hat auf meine Nachfrage hin mitgeteilt, dass es seitens der Behörde, Fachbereich DNA-Analytik, keine Mitteilungen zu „Beinahetreffern“ bei Reihengentests gegeben habe. Auch sei nicht die Übermittlung derartiger „Beinahetreffer“ veranlasst worden. Nach der rechtlichen Bewertung des LKA M-V sieht § 81h StPO einen automatisierten Abgleich und die Feststellung vor, ob das festgestellte DNA-Identifizierungsmuster mit den DNA-Identifizierungsmustern von Spurenmaterial übereinstimmt (Treffer: ja/nein). Die Einwilligung des Betroffenen umfasse ausschließlich die Untersuchung nach Abs. 1, also den Abgleich der DANN-Identifizierungsmuster. Die Übermittlung von „Beinahetreffern“ sei davon nicht umfasst.

Zusammenfassend ist festzustellen, dass das Landeskriminalamt Mecklenburg-Vorpommern die gleiche kritische Auffassung zu dieser Thematik vertritt wie die Datenschutzbeauftragten von Bund und Ländern.

5.2.3 Polizei: Uni soll Studenten erziehen

Der Direktor eines Instituts der Ernst-Moritz-Arndt-Universität Greifswald (EMAU Greifswald) informierte mich darüber, dass er durch ein Schreiben einer Polizeiinspektion darüber in Kenntnis gesetzt wurde, dass ein Student der EMAU Greifswald eine Ordnungswidrigkeit begangen habe. Der Student soll sich während einer polizeilichen Maßnahme sehr unkooperativ gezeigt haben und nach Auffassung der Polizei somit ein unrühmliches Bild auf die EMAU Greifswald geworfen haben. Die Universität wurde gebeten, den Studenten durch „entsprechende Auswertepersonen“ noch einmal auf sein Fehlverhalten hinzuweisen.

Auf Nachfrage gab die Polizei an, dass der betreffende Student bei der Personalienfeststellung freiwillig auf seinen Studentenstatus hingewiesen habe.

Die Übermittlung seiner Daten an die EMAU Greifswald begründete die Polizei mit den Vorschriften des § 14 Abs. 1 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V). Weiterhin wies sie darauf hin, dass gemäß § 17 Abs. 9 Nr. 2 Landeshochschulgesetz (LHG M-V) in Verbindung mit § 24 Abs. 2 der Immatrikulationsordnung der EMAU Greifswald ein Student unter gewissen Umständen exmatrikuliert werden kann. Hierzu war es nach Auffassung der Polizeiinspektion jedoch erforderlich, dass die EMAU Greifswald erst einmal Kenntnis von diesen Umständen erlangt.

Nach § 14 Abs. 1 DSG M-V dürfen personenbezogene Daten an Stellen innerhalb des öffentlichen Bereichs nur dann übermittelt werden, wenn dies zur Erfüllung einer in der Zuständigkeit der Daten verarbeitenden Stelle liegenden Aufgabe erforderlich ist oder wenn die Nutzung der Daten zur Erfüllung einer in der Zuständigkeit des Empfängers liegenden Aufgabe erforderlich und nach § 10 DSG M-V zulässig ist. An den Begriff „Erforderlichkeit“ sind dabei enge Maßstäbe zu setzen. Erforderlich sind personenbezogene Daten nur dann, wenn die Aufgabe sonst nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllt werden kann. Diese Voraussetzungen lagen hier nicht vor.

Nach § 24 Abs. 2 der Immatrikulationsordnung können Studierende exmatrikuliert werden, wenn sie Einrichtungen der Hochschule zu strafbaren Handlungen nutzen oder gegenüber Mitgliedern und Angehörigen der Hochschule strafbare Handlungen begehen. Diese Bedingungen trafen ebenfalls nicht zu.

Auch § 17 Abs. 9 Nr. 2 LHG M-V war vorliegend nicht einschlägig. Nach dieser Vorschrift soll eine Immatrikulation beendet werden, wenn nach dieser Tatsachen bekannt werden und noch fortbestehen, die zur Versagung der Immatrikulation führen können oder müssen. Dies wäre beispielsweise nach § 17 Abs. 6 Nr. 2 LHG M-V bei der Verbüßung einer Freiheitsstrafe der Fall.

Die Datenübermittlung, die aufgrund einer begangenen Ordnungswidrigkeit und nicht wegen einer Straftat erfolgte, war rechtswidrig. Ich habe deshalb der zuständigen Polizeidirektion empfohlen sicherzustellen, dass derartige Datenübermittlungen künftig nicht mehr durchgeführt werden. Die Polizeidirektion will künftig entsprechend meiner Empfehlung verfahren; sie nahm diesen Fall gleichzeitig zum Anlass, diese Thematik mit dem Leiter der verantwortlichen Polizeiinspektion sowie aller weiteren Dienststellen zu besprechen.

5.2.4 Übermittlung zusätzlicher Daten beim Lichtbildabgleich

Im Berichtszeitraum erreichten mich einige Anfragen, in denen die Zulässigkeit und Durchführung von Lichtbildabgleichen in Frage gestellt wurde. In einem Fall wurde mir berichtet, dass neben der Lichtbildkopie noch eine Kopie der Unterschrift der vermeintlichen Fahrzeugführerin übermittelt wurde. Sofern eine Ordnungsbehörde oder die Polizei die Verfolgung einer Verkehrsordnungswidrigkeit für geboten hält, prüft sie, ob der Fahrzeughalter nach dem Beweisfoto der Verkehrsüberwachung als Betroffener des Ordnungswidrigkeitenverfahrens in Betracht kommt. Der Betroffene ist bereits mit dem Verwarnungsgeldangebot/Anhörungsbogen darauf hinzuweisen, dass ein Beweisfoto mit dem Lichtbild des Pass- oder Personalausweisregisters verglichen werden kann, falls er sich nicht äußert oder keine Angaben zum Fahrzeugführer macht (Lichtbildabgleich).

Im Erlass zum Lichtbildabgleich bei der Verfolgung von Ordnungswidrigkeiten nach dem StVG vom 15. September 1998 (Lichtbildabgleichserlass) wird die Durchführung eines solchen Lichtbildabgleichs näher beschrieben. Nach diesem Erlass wird die Ausweisbehörde, bei der der Fahrzeughalter nach den Unterlagen des Kraftfahrtbundesamtes gemeldet ist, um Einsichtnahme in das Ausweisregister bzw. um Übermittlung einer Lichtbildkopie ersucht. Sofern nach dem Beweisfoto der Fahrzeughalter aufgrund des Alters oder Geschlechts offensichtlich nicht als Fahrzeugführer in Betracht kommt, kann die Ordnungsbehörde/Polizei die zuständige Ausweisbehörde um die Übermittlung von Lichtbildern anderer Personen als der des Fahrzeughalters ersuchen.

Das Übermittlungsersuchen darf sich nur auf Familienmitglieder beziehen, die unter derselben Wohnanschrift wie die des Fahrzeughalters im Familienverband gemeldet sind. Außerdem muss das Ersuchen durch Angabe des Geschlechts und des ungefähren Alters der Person oder vergleichbare Kriterien weiter eingegrenzt werden.

Neben der Lichtbildkopie dürfen ausschließlich folgende Daten aus dem Ausweisregister übermittelt werden: Name, Vorname, Doktorgrad, Ordens- und Künstlernamen, Anschrift und Geburtsdatum.

Im vorliegenden Fall ergab meine Recherche, dass die Ordnungsbehörde, der die Ahndung dieser Ordnungswidrigkeit oblag, nicht um die Übersendung dieser Unterschriftskopie gebeten hatte. Außerdem sieht der Lichtbildabgleichserlass eine derartige Übermittlung nicht vor. Der zuständigen Ausweisbehörde habe ich deshalb empfohlen, künftig hierauf zu verzichten und im berechtigten Anforderungsfall neben der Lichtbildkopie ausschließlich die oben genannten Daten zu übermitteln. Die betreffende Behörde hat zugesagt, meine Empfehlung umzusetzen.

In einem anderen Fall wurden neben der Lichtbildkopie des Fahrzeugführers noch Kopien der Lichtbilder seiner Ehefrau und seines Sohnes an die Ordnungsbehörde übermittelt, obwohl die Ordnungsbehörde lediglich eine Bildkopie des Fahrzeughalters angefordert hatte. Für mich entstand der Eindruck, dass die Ausweisbehörde hier nicht die erforderliche Sorgfalt hat walten lassen. Im Ergebnis sagte mir die Ausweisbehörde jedoch zu, derartige Datenübermittlungen künftig nur unter Berücksichtigung der Bestimmungen des Lichtbildabgleichserlasses durchzuführen.

5.2.5 Gemeinsame Telekommunikationsüberwachung der norddeutschen Bundesländer

Schon seit längerem planen die Innenministerien bzw. Innensenatoren der norddeutschen Bundesländer Bremen, Hamburg, Niedersachsen, Schleswig-Holstein und Mecklenburg-Vorpommern ein gemeinsames Telekommunikationsüberwachungszentrum. Begründet wird dies mit der rasanten technischen Entwicklung und der zunehmenden Verlagerung der Telekommunikation in das Internet. Es bestehe daher das dringende Erfordernis, die Instrumente für die Erkenntnisgewinnung der Sicherheitsbehörden den veränderten Gegebenheiten anzupassen.

Das Projekt ist in zwei Phasen aufgeteilt:

Die Phase 1 betrifft zunächst den Aufbau einer technischen Kooperation der Länder zur Schaffung von erforderlichen Kompensationsmöglichkeiten beim Ausfall der ländereigenen Telekommunikationsüberwachungs-Anlage (TKÜ- Anlage) und eines sofortigen Ausgleichs bei Lastspitzen eines Landes im Bereich der IP-basierten Telekommunikation (TKÜ). Die Telekommunikationsanlagen in den Ländern werden vorerst weiterbetrieben. Die Phase 1 soll laut Auskunft unseres Innenministeriums am 1. April 2012 beginnen. Anschließend soll mit der Erstellung eines Umsetzungskonzeptes zur vollständigen Zentralisierung der Telekommunikationsüberwachung in einem Rechen- und Dienstleistungszentrum an den Standorten Hannover und Hamburg für alle fünf norddeutschen Länder begonnen werden. Diese 2. Phase erstreckt sich über die Jahre 2013 bis 2016.

Bei einer ersten Vorstellung des Projektes im Innenministerium am 12. Dezember 2011 habe ich darauf hingewiesen, dass es aus datenschutzrechtlicher Sicht wichtig ist, den sogenannten Kernbereichsschutz durch die jeweils verantwortliche Stelle bestimmen zu lassen. Nach § 100a Abs. 4 Strafprozessordnung (StPO) dürfen Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Telekommunikationsüberwachungsmaßnahme erlangt worden sind, nicht verwertet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Das Innenministerium teilte mir mit, dass die einschlägigen Leitlinien der Generalstaatsanwälte zum Kernbereichsschutz in die Verträge mit einbezogen werden sollen.

In der Praxis würde das bedeuten, dass ausschließlich der Sachbearbeiter bei dem für das Ermittlungsverfahren zuständigen Landeskriminalamt hierüber entscheidet und gegebenenfalls die Administration im Rechenzentrum anweist, Datensätze zu sperren oder zu löschen.

Die Landesbeauftragten für den Datenschutz der fünf norddeutschen Länder werden das Projekt gemeinsam datenschutzrechtlich begleiten. Wegen der Komplexität der Materie wird voraussichtlich ein gemeinsamer Ansprechpartner in Sachen Datenschutz benannt werden.

5.3 Wer wird künftig sicherheitsüberprüft?

Das Innenministerium hat mir den Entwurf der Sicherheitsüberprüfungsfeststellungslandesverordnung zur Stellungnahme übersandt. Es geht darum, bestimmte sogenannte lebenswichtige Organisationseinheiten innerhalb bestimmter Geschäftsbereiche von öffentlichen Stellen zu bestimmen.

Eine Sicherheitsüberprüfung, die erlaubt, dass die Verfassungsschutzbehörde bei zahlreichen Stellen zu einer sicherheitszuüberprüfenden Person personenbezogene Daten abfragt oder personenbezogene Daten im Nachrichtendienstlichen Informationssystem (NADIS) abgleicht, greift in das Grundrecht der Betroffenen auf informationelle Selbstbestimmung ein und darf daher nur auf gesetzlicher Grundlage erfolgen. Das Sicherheitsüberprüfungsgesetz stellt die entsprechende gesetzliche Grundlage dar und ermächtigt die Landesregierung, die Feststellung lebenswichtiger Einrichtungen im Verordnungswege zu treffen.

Die letzte Entscheidung, welche Stelle zur Feststellung berechtigt ist, ob eine Einrichtung tatsächlich von der Verordnung erfasst ist, trifft die zuständige oberste Landesbehörde. Ich halte es aus datenschutzrechtlicher Sicht für richtig, dass nicht jede kleinste Organisationseinheit sich selbst als „lebenswichtige Einrichtung“ einstuft. Des Weiteren wird grundsätzlich begrüßt, dass die Feststellung, welche Einrichtung tatsächlich lebenswichtig ist, in schriftlicher Form erfolgt und die Gründe daher jederzeit für die Behörde und den Betroffenen selbst nachvollziehbar sind. In diesem Zusammenhang ist für mich der Satz in der Verordnungsbegründung: „In Anbetracht des Schutzziels der Verordnung ist die schriftliche Feststellung nach der Verschlussachenanweisung als VS-VERTRAULICH einzustufen“ nicht nachvollziehbar und verstößt meines Erachtens gegen das Transparenzgebot. Für die Betroffenen ist es gerade wichtig zu wissen, warum gerade die Organisationseinheit, in der sie beschäftigt sind, als „lebenswichtig“ eingestuft ist. Ich hatte daher vorgeschlagen, die Einstufung als „VS-VERTRAULICH“ aus der Verordnungsbegründung zu streichen.

Leider wurde meinem Vorschlag nicht gefolgt. Der Satz wurde lediglich dahingehend verändert, dass die schriftliche Feststellung nach der Verschlussachenanweisung „i. d. R.“ als VS-VERTRAULICH einzustufen ist.

5.4 Einwohnerwesen/Kommunales

5.4.1 Visa-Warndatei und Änderung des Aufenthaltsgesetzes

Die Bundesregierung hat den Entwurf eines Gesetzes zur Errichtung einer Visa-Warndatei und zur Änderung des Aufenthaltsgesetzes vorgelegt. Der Gesetzentwurf (BT-Drs. 17/6643) vom 20. Juli 2011 sieht neben der Errichtung einer Visa-Warndatei und getrennt von dieser ein neues Verfahren zum Abgleich von Daten aus dem Visumverfahren mit Daten aus der Antiterrordatei vor.

Die Bundesregierung begründet die Notwendigkeit des Gesetzentwurfs damit, dass deutsche Visumbehörden derzeit keine Möglichkeit hätten, bei allen Visumanträgen die an einem Visumantrag beteiligten Personen gezielt auf rechtswidriges Verhalten im Zusammenhang mit einem Visumverfahren zu überprüfen. Dadurch soll insbesondere auch Schleusung und Menschenhandel unterbunden werden.

Gegenüber unserem Innenministerium habe ich eine Stellungnahme abgegeben. Es wird anerkannt, dass die vorgesehene Visa-Warndatei in Zweck, Umfang und Zugriffsmöglichkeiten im Vergleich zu früheren Vorhaben erheblich reduziert und somit datenschutzrechtlich deutlich verbessert wurde. Trotzdem bleiben Zweifel, inwieweit es erforderlich ist, Daten zu speichern, die bereits in anderen Dateien (z. B. dem Bundeszentralregister oder dem künftigen europäischen Visa-Informationssystem) enthalten sind.

Datenschutzrechtliche Bedenken bestehen auch gegenüber dem in § 72a Aufenthaltsgesetz-Entwurf vorgesehenen Verfahren eines verdachtslosen Vollabgleichs von sämtlichen Visumantragstellern, Einladern, Verpflichtungsgebern und sonstigen Referenzpersonen mit Daten aus der Antiterrordatei. Hierbei handelt es sich um Personen, die sich überwiegend rechtstreu verhalten und somit keinen Anlass für eine Überprüfung geben. Die Erforderlichkeit eines derart umfassenden Abgleichverfahrens ist meines Erachtens nicht dargelegt. Da es bei Eintragungen in die Antiterrordatei gerade bei Ausländern wegen unterschiedlicher Schreibweisen des Namens leicht zu Verwechslungen kommen kann, besteht die Gefahr, dass unbescholtene Bürger mit Nachteilen zu rechnen haben.

Auch ist bislang weder die technische noch die organisatorische Ausgestaltung des beabsichtigten Abgleichverfahrens hinreichend dargestellt worden.

Es bleibt abzuwarten, wie der Innenausschuss des Deutschen Bundestages nach der Durchführung einer öffentlichen Anhörung mit dem Gesetzentwurf weiter verfährt.

5.4.2 Bioenergieverbund - Voraussetzungen für freiwillige Datenerhebungen

Ein Petent hatte mir mitgeteilt, dass in einigen Gemeinden alle Haushalte gebeten wurden, einen Erhebungsbogen auszufüllen zur Erarbeitung einer Machbarkeitsstudie zu einem Bioenergieverbund. Mit dem Erhebungsbogen wurde eine Reihe von personenbezogenen Daten erhoben, unter anderem Kontaktdaten wie Name und Anschrift sowie Informationen zum Energieverbrauch. Die zuständige Amtsverwaltung hatte ein Ingenieurbüro mit der Befragung und deren Auswertung beauftragt. Der Petent hat mich gebeten, diesen Sachverhalt datenschutzrechtlich zu prüfen.

Auf meine Nachfrage hin hat mir die Amtsverwaltung mitgeteilt, dass die Beteiligung an der Umfrage freiwillig sei. Um alle Betroffenen umfassend zu informieren, habe ich empfohlen, im Rahmen einer Veröffentlichung im amtlichen Bekanntmachungsblatt auf die Freiwilligkeit der Angaben hinzuweisen. In dieser Veröffentlichung wurde dann auch die Datenverarbeitung näher beschrieben und darüber hinaus zum Ausdruck gebracht, dass mit der Teilnahme an dieser Umfrage keinerlei Verpflichtungen verbunden seien. Weiterhin wurde in dieser Veröffentlichung darüber informiert, dass die Daten zu den Verbrauchswerten der Häuser und der Wohnungen anonymisiert straßen- und ortsweise zusammengefasst werden.

Für die Auswertung der Umfrage für einen Bioenergieverbund sollten die ausgefüllten Erhebungsbögen tabellarisch ohne Nennung des Eigentümers und der Hausnummer straßenweise zusammengefasst werden. Selbst, wenn aus dieser Zusammenfassung ein Rückschluss auf personenbeziehbare Daten möglich wäre, bestanden aus meiner Sicht keine datenschutzrechtlichen Bedenken gegen diese Verfahrensweise, insbesondere auch deshalb nicht, weil die Amtsverwaltung inzwischen mit dem beauftragten Ingenieurbüro einen Vertrag zur Verarbeitung personenbezogener Daten im Auftrag im Sinne des § 4 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) geschlossen hatte. Neben den grundsätzlichen und in § 4 DSG M-V festgelegten Bestimmungen wurden hier unter anderem auch Festlegungen zur Löschung der personenbezogenen Daten getroffen.

Dem Petenten habe ich im Ergebnis mitgeteilt, dass die Amtsverwaltung meine Empfehlungen zum Verfahren bei dieser Umfrage so umgesetzt hat, dass keine datenschutzrechtlichen Bedenken mehr bestanden. Bei künftigen Projekten sollte jedoch sichergestellt werden, dass insbesondere auf die Freiwilligkeit der Teilnahme an einer Befragung gleich bei Übersendung des Erhebungsbogens hingewiesen wird.

5.4.3 Personenbezogene Daten in einem Planfeststellungsbeschluss?

Ein Bürger machte mich darauf aufmerksam, dass in der Begründung zu einem Planfeststellungsbeschluss, welcher den Neubau einer Autobahnrastanlage zum Inhalt hatte, personenbezogene Daten über ihn enthalten waren. Konkret wurde er hier zusammen mit einem zweiten Inhaber einer Gesellschaft des bürgerlichen Rechts als Einwendungsführer gegen dieses Projekt namentlich aufgeführt. Der Planfeststellungsbeschluss enthielt außerdem noch Informationen zum Eigentum an Grundstücken sowie Betriebsangaben. Daneben waren in dem betreffenden Beschluss auch noch Informationen über Privatleute enthalten.

Ich hatte das für den Planfeststellungsbeschluss zuständige Ministerium für Energie, Infrastruktur und Landesentwicklung Mecklenburg-Vorpommern unter anderem nach der Rechtsgrundlage für diese Datenverarbeitung gefragt. Als Rechtsvorschrift wurde mir § 17 b Abs. 1 Bundesfernstraßengesetz (FStrG) genannt. Diese Vorschrift wiederum verweist auf § 74 Verwaltungsverfahrensgesetz (VwVfG).

Nach § 74 Abs. 4 Satz 2 VwVfG ist die Ausfertigung eines Planfeststellungsbeschlusses mit einer Rechtsbehelfsbelehrung und einer Ausfertigung des festgestellten Plans zwei Wochen in den Gemeinden zur Einsicht auszulegen; Ort und Zeit der Auslegung sind ortsüblich bekannt zu machen. Diese Bekanntmachung erfolgte im vorliegenden Fall ordnungsgemäß. Damit hatten während des zweiwöchigen Zeitraums Dritte die Möglichkeit, in den Beschluss und somit auch in die hierin enthaltenen personenbezogenen Daten einzusehen.

Nach § 74 Abs. 1 VwVfG erfolgt die Planfeststellung durch einen Verwaltungsakt. Die Adressaten müssen dabei aber nicht namentlich bezeichnet werden. Vielmehr genügt eine pauschale Bezeichnung (z. B. als „Grundstückseigentümer in einem bestimmten Gebiet“). Entsprechendes gilt auch für die Bezeichnung der Einwendungsführer. Dieses stimmt mit dem in § 15 Abs. 1 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) festgeschriebenen Grundsatz, wonach personenbezogene Daten an inländische Stellen außerhalb des öffentlichen Bereichs nur dann übermittelt werden dürfen, wenn dies zur Erfüllung einer in der Zuständigkeit der Daten verarbeitenden Stelle liegenden Aufgabe erforderlich ist, überein. Ich habe dem Ministerium mitgeteilt, dass diese Anforderlichkeit meiner Ansicht nach nicht gegeben ist, da das Interesse des Einzelnen auf Schutz seiner personenbezogenen Daten einem möglichen Interesse der Allgemeinheit auf Offenbarung dieser Daten überwiegt.

Eine pauschale Bezeichnung des Betroffenen genügt, da dieser somit weiß, dass er vorliegend Adressat des Planfeststellungsbeschlusses ist, ohne das Dritte Näheres über seine Identität erfahren.

Ergänzend hierzu habe ich das Ministerium für Energie, Infrastruktur und Landesentwicklung Mecklenburg-Vorpommern auf die Beschlüsse des Bundesverfassungsgerichts vom 24. Juli 1990 und vom 14. Oktober 1987 (Aktenzeichen: 1 BvR 1244/87) hingewiesen. Das Bundesverfassungsgericht hat hier die Veröffentlichung von personenbezogenen Daten, die ein Einwendungsführer der Planfeststellungsbehörde preisgibt, um ihr eine sachgerechte Beurteilung der geltend gemachten Einwendungen zu ermöglichen, für verfassungswidrig erklärt.

Das Bundesverfassungsgericht ging in diesen Beschlüssen davon aus, dass der Bürger der Behörde seine personenbezogenen Daten nur zu einem bestimmten Zweck offenbart. Dieser Zweck ist die sachgerechte Entscheidung im Planfeststellungsverfahren. Durch die öffentliche Bekanntmachung der nicht anonymisierten Daten sah das Gericht diese Zweckbindung als unterlaufen und im Ergebnis als aufgehoben an. Das Bundesverfassungsgericht wies darauf hin, dass keine Gründe ersichtlich sind, warum eine ordnungsgemäße Begründung des Planfeststellungsbeschlusses notwendig voraussetzt, dass sachbezogene Erwägungen zu Beurteilung und Gewichtung der geltend gemachten Einwendungen personenbezogen in die Begründung aufgenommen und mit dieser veröffentlicht werden müssen. Die sachliche Zuordnung kann hier auch durch die Vergabe von Betriebsnummern erfolgen.

Im Ergebnis hat mir das Ministerium für Energie, Infrastruktur und Landesentwicklung Mecklenburg-Vorpommern mitgeteilt, dass das straßenrechtliche Planfeststellungsverfahren in Mecklenburg-Vorpommern durch das Landesamt für Straßenbau und Verkehr als Anhörungsbehörde geführt wird. Mit diesem Landesamt hat das Ministerium vereinbart, dass künftig den Einwendungsführern zu Beginn des Verfahrens grundsätzlich eine Kennziffer zugeteilt wird, die dann im weiteren Verfahren bis zum Abschluss beibehalten wird.

5.4.4 MfS-Überprüfung von Gemeindevertretern und kommunalen Wahlbeamten

Nach wie vor spielt das Thema der Überprüfung von Gemeindevertretern und kommunalen Wahlbeamten in einigen kommunalen Vertretungskörperschaften eine wichtige Rolle. Offensichtlich auch aus diesem Grunde hat der Gesetzgeber die ansonsten Ende des Jahres 2011 ablaufenden gesetzlichen Überprüfungsfristen bis zum 30. Dezember 2019 verlängert. Im Berichtszeitraum und vor allem im Nachgang zur Kommunalwahl im Jahr 2009 lagen mir einige Anfragen vor, die sich mit der Durchführung von MfS-Überprüfungen auf der kommunalen Ebene beschäftigten. Dabei ging es vor allem um die grundsätzliche Frage, unter welchen Voraussetzungen derartige Überprüfungen durchgeführt werden dürfen und was dabei zu beachten ist.

§ 20 Abs. 1 Nr. 6 b bzw. § 21 Abs. 1 Nr. 6 b des Gesetzes über die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (StUG) eröffnen die Möglichkeit zur Überprüfung von Abgeordneten und Angehörigen kommunaler Vertretungskörperschaften sowie kommunalen Wahlbeamten. Nach dem StUG ergibt sich keine Verpflichtung für öffentliche Stellen, die Überprüfung auch durchzuführen. Den kommunalen Vertretungskörperschaften steht es deshalb frei, darüber zu befinden, ob eine Überprüfung auf freiwilliger Basis oder generell stattfinden soll.

Formale Anforderungen an das Ersuchen werden durch das StUG nicht gestellt. Aus einem im Internet veröffentlichten Merkblatt des Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (BStU), welches sich mit dem Ersuchen öffentlicher und nicht-öffentlicher Stellen zur Verwendung der Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR für die Überprüfung von Personen zur Feststellung, ob diese hauptamtlich oder inoffiziell für den Staatssicherheitsdienst tätig waren, beschäftigt, lassen sich einige formale Anforderungen entnehmen (siehe: <http://www.bstu.bund.de>). Danach sollen in einer Anfrage, welche sich auf ein Ersuchen von mehreren Personen bezieht, die Namen alphabetisch in Listenform geordnet werden. Für jede zu überprüfende Person sind alle Vor- und Familiennamen, auch solche aus früheren Ehen und gegebenenfalls der Geburtsname, die in der ehemaligen DDR verwendete Personenkennzahl bzw. das Geburtsdatum und der Geburtsort anzugeben. Darüber hinaus werden durch den BStU, soweit möglich, aus dem Zeitraum 1950 bis einschließlich 1989 alle Wohnanschriften (auch Nebenwohnungen) nach dem vollendeten 18. Lebensjahr unter Angabe der bis zum 3. Oktober 1990 gültigen Postleitzahl benötigt. Nach Darstellung des BStU sollte es auch im Interesse einer zu überprüfenden Person liegen, alle erforderlichen Angaben mitzuteilen, um eine Verwechslung mit einer eventuell in den Unterlagen erfassten Person mit gleichem Namen und Geburtsdatum auszuschließen.

Zur Übermittlung dieser personenbezogenen Daten an den BStU dürfen auch Informationen aus dem Melderegister für die MfS-Überprüfungen herangezogen werden. Nach § 31 Abs. 1 Landesmeldegesetz (LMG) darf die Meldebehörde einer anderen Behörde oder sonstigen öffentlichen Stelle aus dem Melderegister die dort aufgeführten Daten von Einwohnern übermitteln (Behördenauskunft), soweit dies zur Erfüllung einer in ihrer Zuständigkeit oder in der Zuständigkeit des Empfängers liegenden Aufgabe erforderlich ist. Die Erforderlichkeit ergibt sich in diesem Fall aus den oben genannten Bestimmungen im StUG.

Um den jeweiligen Gemeindevertreter oder Wahlbeamten für den BStU möglichst eindeutig identifizierbar angeben zu können, steht aus datenschutzrechtlicher Sicht einer Übermittlung folgender personenbezogener Daten aus dem Melderegister nichts entgegen:

1. Familienname,
2. früherer Name,
3. Vornamen,
4. Tag und Ort der Geburt und
5. gegenwärtige und frühere Anschrift (Haupt- und Nebenwohnung, bei Zuzug aus dem Ausland auch die letzte frühere Anschrift im Inland).

Datenschutzrechtlich nicht eindeutig geregelt ist hingegen der Umgang mit den vom BStU übermittelten personenbezogenen Daten. Im StUG ist lediglich normiert, dass Unterlagen durch öffentliche Stellen in dem erforderlichen Umfang zum Zwecke einer Überprüfung von Mitgliedern kommunaler Vertretungskörperschaften verwendet werden dürfen. In welcher Form jedoch eine Auswertung und Verwendung des Überprüfungsergebnisses erfolgen darf, ist dort nicht genannt.

Um die Informationen über die MfS-Tätigkeit eines gewählten Vertreters in öffentlicher bzw. nichtöffentlicher Sitzung bekannt zu geben, wäre es mangels spezifischer gesetzlicher Regelungen denkbar, hierzu hilfsweise die Grundsätze für die Veröffentlichung von personenbezogenen Daten durch Presse, Rundfunk und Film gemäß § 34 Abs. 1 i. V. m. § 32 Abs. 3 StUG heranzuziehen. Danach ist eine Veröffentlichung von Informationen über eine Mitarbeit beim MfS nur möglich, wenn diejenige Person, deren Daten veröffentlicht werden, eingewilligt hat oder aber durch die Veröffentlichung ihre überwiegenden schutzwürdigen Interessen nicht beeinträchtigt werden. Somit hat eine Abwägung zwischen dem öffentlichen Interesse an der Aufarbeitung der MfS-Vergangenheit einerseits und den schutzwürdigen Belangen der jeweiligen Person andererseits stattzufinden.

Sinnvoll ist es meiner Ansicht nach, parallel zu der Beschlussfassung einer möglichen MfS-Überprüfung gleich Regelungen zu der Bildung eines Gremiums (sogenannte Ehrenkommission), welches die Überprüfung für die kommunale Vertretungskörperschaft durchführt, sowie zum Umgang mit den personenbezogenen Daten mit zu treffen.

5.4.5 Löschen von Informationen im Google-Cache

Ein Petent teilte mir mit, dass einer Stadtvertretung eine Beschlussvorlage über eine Wahlprüfungsentscheidung zu einer durchgeführten Bürgermeisterwahl vorlag. In dieser Vorlage waren personenbezogene Daten derjenigen, die Einsprüche gegen diese Wahl erhoben haben, enthalten (Name und Vorname). Diese Beschlussvorlage wurde vollständig, also mit den darin enthaltenen personenbezogenen Daten, im Internet veröffentlicht, obwohl es hierfür weder eine Rechtsvorschrift gab, die dieses erlauben würde, noch die betroffenen Personen hierfür ihre Einwilligung gegeben haben. Somit lag offensichtlich ein datenschutzrechtlicher Verstoß vor.

Durch die Qualität der Veröffentlichung (Internet) war es einer breiten Öffentlichkeit möglich, Informationen über die Personen, die Einspruch gegen die Bürgermeisterwahl erhoben haben, zu erhalten. Ich habe der verantwortlichen Stadtverwaltung daher empfohlen, die in dieser Beschlussvorlage enthaltenen personenbezogenen Daten zu löschen. Dieser Empfehlung kam die Verwaltung nur in der Weise nach, indem sie eine anonymisierte Version online stellte. Die Verwaltung hatte allerdings nicht bedacht, dass die Suchmaschine Google im sogenannten Google-Cache eine Kopie von jeder Webseite speichert, die sie beim Erstellen des Suchindex durchsucht. Dazu verwendet Google ein Computerprogramm namens Google-bot, das Texte und Bilder im World Wide Web herunterlädt und diese über die Web- und die Bildsuche von Google auffindbar macht. Der Google-Cache zeigt eine Seite in dem Zustand an, wie sie der Googlebot in seinem letzten Besuch vorgefunden hat. Damit bestimmte Daten von der Suchmaschine Google nicht mehr angezeigt werden, reicht es daher nicht aus, die betreffende Seite entsprechend zu ändern und die neue Version auf den Server hochzuladen. Die zeitlichen Abstände, in denen Googlebot Webseiten besucht, sind völlig unterschiedlich und können von wenigen Stunden bis mehrere Monate reichen.

Der Google-Cache kann von jedem Nutzer betrachtet werden und ist vor allem dann relevant, wenn eine Webseite vom Betreiber gelöscht wurde. Die ursprüngliche Beschlussvorlage mit den darin enthaltenen personenbezogenen Daten war somit trotz Löschung des Originals noch im Google-Cache auffindbar. Die von der Verwaltung durchgeführte Einstellung der anonymisierten Beschlussvorlage im Internet reichte folglich nicht aus. Aus diesem Grund habe ich empfohlen, schnellstmöglich über das Google Webmaster Tool die eigenen, noch im Cache befindlichen Inhalte zu entfernen. Dieser Empfehlung ist die Stadtverwaltung gefolgt.

Weil eine nachträgliche vollständige Löschung von Inhalten im Internet grundsätzlich unmöglich ist (vgl. Punkt 4.2.3) beziehungsweise unkontrollierbar ist, ob nicht irgendwo noch Kopien gespeichert sind, dürfen personenbezogene Daten nur dann veröffentlicht werden, wenn eine Rechtsvorschrift dies zulässt oder der Betroffene eingewilligt hat. Zu bedenken gebe ich in diesem Zusammenhang, dass bei einer Veröffentlichung im Internet nicht ausgeschlossen werden kann, dass im Zeitraum von der Veröffentlichung der Informationen bis zur Löschung Dritte von diesen Daten Kenntnis genommen und gegebenenfalls sogar eine Weiterverwendung dieser Informationen vorgenommen haben. Dabei spielt auch keine Rolle, wie lange die Informationen im Internet vorhanden waren.

Ich empfehle daher jeder öffentlichen Stelle, vor einer geplanten Internetveröffentlichung sorgfältig zu prüfen, ob personenbezogene Daten mit veröffentlicht werden dürfen.

5.4.6 Meldedaten an die Polizei

Eine Kommunalverwaltung informierte mich darüber, dass eine Kriminalpolizeiinspektion ihr einen Vorschlag zur Übermittlung von Meldedaten unterbreitet hat. Nach Ansicht der Polizei sollte der Datenaustausch mit den Meldebehörden künftig über eine verschlüsselte Liste per E-Mail erfolgen.

§ 31 Landesmeldegesetz (LMG) regelt die Datenübermittlungen an andere Behörden oder sonstige öffentliche Stellen. Nach Abs. 4 dieser Vorschrift hat die Meldebehörde der Polizei auf Ersuchen jederzeit die dort aufgeführten personenbezogenen Daten aus dem Melderegister zu übermitteln. Voraussetzung hierfür ist, dass die Datenübermittlung für die rechtmäßige Aufgabenerfüllung der Polizei erforderlich ist.

Für derartige und andere automatisierte Datenübermittlungen (z. B. Behördenauskunft nach § 31 Abs. 1 LMG) ist nach § 31 Abs. 10 LMG eine Datenübermittlung aus dem Informationsregister (§ 3 a LMG) vorgeschrieben. Nach § 3 a LMG hat das Land für Datenübermittlungen im automatisierten Verfahren an andere Behörden oder sonstige öffentliche Stellen nach § 31 LMG, an öffentlich-rechtliche Religionsgesellschaften nach § 32 LMG und die automatisierte Erteilung von Melderegisterauskünften nach § 34 a LMG ein Informationsregister (ZIR) eingerichtet. Bei dem ZIR handelt es sich um ein zentrales Datenverarbeitungsverfahren, auf dem die Meldedaten mandantenfähig (für jede einzelne Meldebehörde getrennt) geführt werden.

Die betreffende Kriminalpolizeiinspektion hat nach meinen Hinweisen die zunächst über E-Mail vorgesehene Datenübermittlung gestoppt und gleichzeitig Kontakt zum Landesamt für zentrale Aufgaben der Polizei, Brand- und Katastrophenschutz Mecklenburg-Vorpommern aufgenommen und dieses gebeten zu prüfen, ob eine Auskunftserteilung über das ZIR möglich ist, und dann gegebenenfalls die erforderlichen Voraussetzungen hierfür zu schaffen. Bis dahin sollen die Datenübermittlungen in Schriftform durchgeführt werden.

Ich empfehle der Landesregierung, gegenüber den Behörden und öffentlichen Stellen im Land sowie der Landespolizei sicherzustellen, dass die automatisierte Datenübermittlung im Sinne des § 31 Abs. 10 LMG über das ZIR erfolgt, und gegebenenfalls die hierfür erforderlichen Schritte einzuleiten.

5.4.7 Der neue Personalausweis

Seit dem 1. Oktober 2010 erhalten Bürgerinnen und Bürger auf Antrag den neuen Personalausweis (nPA), dessen neue Funktionen ich im Neunten Tätigkeitsbericht (siehe dort Punkt 2.4.9) bereits ausführlich beschrieben und datenschutzrechtlich bewertet habe.

Dass es bei einem solchen komplexen IT-Projekt zu Startschwierigkeiten gekommen ist, kann nicht überraschen. Die von mir beschriebenen Risiken der PIN-Eingabe bei der Nutzung der eID-Funktion über die Tastatur des Computers hat der Chaos Computer Club mehrfach praktisch demonstriert. Nach wie vor gilt daher meine Empfehlung, nur Chipkartenleser mit eigenem Tastaturfeld zu verwenden. Unerfreulich war auch, dass die erste Version der sogenannten Ausweis-App erhebliche Sicherheitsrisiken mit sich brachte, da die automatische Update-Funktion das Laden von Schadsoftware ermöglicht hatte.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) brauchte einige Monate, um eine fehlerfreie Ausweis-App zur Verfügung zu stellen. Darüber hinaus verwundert es angesichts des stetig sinkenden Interesses der Bundesregierung an der Verbreitung der qualifizierten elektronischen Signatur (siehe Punkte 3.2.5 und 3.2.7) nicht sonderlich, dass der nPA nach wie vor nicht in der Lage ist, derartige Signaturen zu erzeugen. Die dafür erforderlichen Signaturzertifikate stehen noch immer nicht zur Verfügung.

Mit besonderem Interesse verfolge ich jedoch die Entwicklungen um die neue Funktion des elektronischen Identitätsnachweises (eID-Funktion), mit der ein sicherer Nachweis der eigenen Identität etwa in E-Government- oder in E-Business-Verfahren gewährleistet werden soll und somit die Grundlage für sichere und datenschutzgerechte Kommunikationsvorgänge über das Internet geschaffen werden kann.

Damit Behörden oder Unternehmen Dienstleistungen anbieten können, für deren Inanspruchnahme die eID-Funktion des neuen Personalausweises genutzt werden kann, ist ein sogenanntes Berechtigungszertifikat erforderlich. Das Bundesverwaltungsamt (BVA) erteilt dieses Zertifikat, in dem festgelegt ist, welche Daten der Anbieter einer Dienstleistung aus dem Personalausweis auslesen darf. Die Erteilung der entsprechenden Berechtigungen macht das BVA auch von der Einhaltung datenschutzrechtlicher Anforderungen abhängig. So müssen unter anderem ein rechtmäßiger Verarbeitungszweck und die Erforderlichkeit der ausgelesenen Daten nachgewiesen werden. Unter maßgeblicher Mitwirkung der Datenschutzbeauftragten von Bund und Ländern wurden datenschutzrechtliche Leitlinien erstellt, die dem Bundesverwaltungsamt eine sachgemäße Entscheidung über die Vergabe der Zertifikate ermöglichen.

Für Behörden oder Unternehmen, die Dienstleistungen unter Nutzung des neuen Personalausweises anbieten wollen, fallen erhebliche Kosten an. Die zuvor beschriebenen Berechtigungszertifikate sind kostenpflichtig, denn für die Bereitstellung eines Berechtigungszertifikats verlangt das Bundesverwaltungsamt eine Gebühr. Dabei handelt es sich nicht um einen einmaligen Betrag, sondern vielmehr um eine laufende Gebühr für einen festgelegten Zeitraum. Zu den Kosten für das Berechtigungszertifikat pro Jahr kommen weitere Kosten für die entsprechende Technik, deren Wartung sowie das erforderliche Know-how hinzu. Ein wesentlicher Kostenfaktor ist die Nutzung sogenannter eID-Services. Will beispielsweise ein Unternehmen auf eID-Daten des nPA zugreifen, muss es entweder selbst einen eID-Server mit der dazugehörigen Sicherheitstechnik beschaffen oder die Angebote eines eID-Dienstleisters in Anspruch nehmen.

Gerade für die finanzschwachen Kommunen stellen diese anfallenden Kosten eine erhebliche Hürde dar, um nPA-basierende Dienstleistungen anbieten zu können. Da überrascht es nicht, dass Kommunen Wege suchen, die Menge der erforderlichen Zertifikate auf ein Minimum zu reduzieren, um Kosten zu sparen.

So ziehen insbesondere kommunale Zweckverbände sowohl in Mecklenburg-Vorpommern als auch in anderen Bundesländern in Erwägung, anstelle der eigentlich erforderlichen Berechtigungszertifikate für jedes Verwaltungsverfahren lediglich ein Berechtigungszertifikat zu erwerben, mit dem an zentraler Stelle - etwa in einem E-Government-Portal - nur einmal Daten des nPA ausgelesen und an die jeweiligen Fachverfahren weitergeleitet werden. Damit würden jedoch zwei wesentliche Ziele dieser Zertifikate unterlaufen werden, die von erheblicher Datenschutzrelevanz sind: Einerseits führt ein „gemeinsames“ Zertifikat dazu, dass mehr als nur das verfahrensspezifisch erforderliche Minimum von nPA-Daten ausgelesen wird. Andererseits kann nicht mehr verhindert werden, dass einzelne Aktivitäten der Nutzung des nPA miteinander verknüpft und somit Nutzerprofile ermöglicht werden, die gerade durch eine differenzierte Zertifikatsvergabe verhindert werden sollten.

Das BVA hat zwar mitgeteilt, dass es nach wie vor an den Plänen festhalte, nur verfahrensspezifische Zertifikate zu erteilen. Angesichts der kritischen Finanzlage der Kommunen befürchte ich jedoch, dass unter dem stetigen Sparzwang dem BVA künftig doch Zugeständnisse abgerungen werden und die datenschutzrechtlichen Vorgaben unterlaufen werden könnten.

Hier sehe ich die Bundes- und Landespolitik gefordert. Wenn den neuen Personalausweis nicht das gleiche Schicksal wie die qualifizierte elektronische Signatur ereilen soll, bei der eine völlig verfehlte Förderpolitik der Bundesregierung nicht zu deren Verbreitung beigetragen hat (siehe Punkt 3.2.5), müssen insbesondere Kommunen bei der Einbindung des nPA in E-Government-Verfahren finanziell unterstützt werden.

Ich empfehle der Landesregierung, sich dafür einzusetzen, dass Berechtigungszertifikate für die Nutzung des neuen Personalausweises für Anwendungen im öffentlichen Bereich und insbesondere bei den Kommunen vom Bundesverwaltungsamt kostenlos erteilt werden.

5.4.8 Kopieren von Personalausweisen nur ausnahmsweise

Immer wieder erreichen mich Petitionen, die sich auf das Kopieren von Personalausweisen beziehen. Dieses Verfahren wird von vielen Firmen angewandt - bei der Paketabholung ebenso wie beim Altmetallhandel. Hierbei sind jedoch die Regelungen des Personalausweisgesetzes (PAuswG) zu beachten.

Der Ausweisinhaber kann gemäß § 20 Abs. 1 PAuswG seinen Personalausweis nicht nur gegenüber Behörden, sondern auch gegenüber nicht-öffentlichen Stellen (Firmen und Unternehmen) als Identitätsnachweis und Legitimationspapier verwenden. Der Personalausweis darf jedoch nach § 20 Abs. 2 PAuswG durch Firmen und Unternehmen weder zum automatischen Abruf personenbezogener Daten noch zu deren automatisierten Speicherung benutzt werden.

Die Seriennummern stehen gemäß § 20 Abs. 3 PAuswG unter besonderem Schutz und dürfen nicht so verwendet werden, dass mit ihrer Hilfe ein automatisierter Abruf personenbezogener Daten oder eine Verknüpfung von Dateien möglich ist. Gegen eine Vorlage und einen einfachen Sichtabgleich des Ausweises ist deshalb (zu Zwecken der Legitimation, der Einlasskontrolle, des buchhalterischen Rechnungsnachweises etc.) grundsätzlich nichts einzuwenden. Dabei können ggf. Name, Anschrift und ggf. das Geburtsdatum notiert werden, wenn dies im Rahmen des Geschäftszwecks gemäß § 28 BDSG erforderlich ist oder eine (freiwillige) Einwilligung des Betroffenen vorliegt. Nach dem anschließenden Sichtvergleich des Ausweisfotos mit dem betroffenen Ausweisinhaber ist die Legitimationsfunktion des Unternehmens jedoch erfüllt und abgeschlossen.

Eine zusätzliche generelle Speicherung bzw. das generelle Kopieren von Ausweisen (einschließlich aller Angaben - insbesondere der Personalausweisnummer) durch Unternehmen ohne Einwilligung der Betroffenen ist unzulässig. Will dieser selbst eine Kopie (etwa zum Identifikationsnachweis) verwenden, sind dazu in der Regel nur Name und Vorname, die Anschrift und ggf. das Geburtsdatum erforderlich. Alle anderen auf der Kopie befindlichen Daten (und das Bild) sollen geschwärzt werden - insbesondere alle Nummernangaben. Spezialgesetzliche Regelungen - etwa nach dem Geldwäschegesetz - sind hiervon unbenommen.

5.4.9 Kreismusikschule: Dissonanzen bei der IT-Sicherheit

Nach einem Hinweis habe ich in der Kreismusikschule und in dem Medienzentrum eines Landkreises kontrolliert, wie es dort um die Informationssicherheit und den Arbeitnehmerdatenschutz bestellt ist. Dabei musste ich insbesondere folgende Verstöße gegen geltendes Datenschutzrecht feststellen:

Es war nicht zu ermitteln, wer in welchem Umfang darüber entscheidet, wie personenbezogene Daten in der Kreismusikschule zu verarbeiten sind. Hierfür kommen in diesem Landkreis mehrere Stellen in Betracht, nämlich Kreismusikschule, Kreismedienzentrum oder aber der zuständige Fachdienst der Kreisverwaltung. Außerdem ist noch ein externer Dienstleister involviert. Das Gesetz verlangt aber eine klare Organisation mit eindeutiger Aufgabenverteilung (§ 21 Abs. 1 DSGVO M-V). Details sind den Beteiligten in geeigneter Form bekannt zu machen (Transparenz gemäß § 21 Abs. 2 Nr. 6 DSGVO M-V).

Außerdem soll das Kreismedienzentrum die Informationstechnik der Kreismusikschule und anderer Bildungseinrichtungen warten, teilweise auch mittels Fernwartung. Der hierfür nötige schriftliche Auftrag, der inhaltlich den Anforderungen des § 4 DSGVO M-V entsprechen muss, fehlte jedoch. Darüber hinaus lagen auch kein Sicherheitskonzept, welches § 22 Abs. 5 DSGVO M-V genügt, keine Freigabeerklärung und keine Verfahrensbeschreibung (§§ 18, 19 DSGVO M-V) vor.

Auch im technischen Bereich waren Defizite festzustellen. So arbeiteten Beschäftigte der Kreismusikschule mit Administratorrechten. Von Arbeitsplätzen der Kreismusikschule und der Kreisvolkshochschule im selben Hause konnte auf Datenbestände der jeweils anderen Einrichtung zugegriffen werden. Ferner gab es auch keine Datensicherung, die diesen Namen verdient. Kopien wichtiger Daten wurden lediglich auf eine transportable Festplatte geschrieben, die ständig mit dem zu schützenden Rechner verbunden war.

Ich habe diese Verstöße gegenüber der Landrätin beanstandet. Daraufhin wurden die Mängel weitgehend behoben. Es fehlt noch ein Sicherheitskonzept, in dem zu beschreiben ist, welche technischen und organisatorischen Datenschutzmaßnahmen in der Kreismusikschule erforderlich sind. Dies gilt auch für das Kreismedienzentrum. Der Landkreis hat mir jedoch zugesichert, dass dies kurzfristig behoben wird.

5.5 Zensus 2011

5.5.1 Anfragen und Petitionen

In meinem Neunten Tätigkeitsbericht hatte ich über meine datenschutzrechtlichen Bedenken zum Entwurf eines Gesetzes zur Anordnung des Zensus 2011 als Berichterstatter vor dem Innenausschuss des Deutschen Bundestages (BT-Drs. 16/12219) berichtet.

Und ich hatte angekündigt, dass ich die Vorbereitung und Durchführung der Volkszählung 2011 kritisch begleiten werde.

Zensusstichtag war der 9. Mai 2011. Zu diesem Stichtag wurden die aus den Registern übernommenen Daten aktualisiert und die Befragungen gestartet. Befragt worden sind alle Haus- und Wohnungsbesitzer bei der Gebäude- und Wohnungszählung, bis zu 10 % der Bevölkerung bei der Haushaltebefragung und auch Einwohner von Wohnheimen und Gemeinschaftsunterkünften wie Alten- und Pflegeheimen oder Studentenwohnheimen, aber auch sensible Gemeinschafts- bzw. Sondereinrichtungen (Erziehungsheime, Notunterkünfte für Obdachlose, Justizvollzugsanstalten). Zu den unterschiedlichen Befragungen habe ich verschiedene Anfragen und Petitionen erhalten.

Gebäude- und Wohnungszählung:

Zur Gebäude- und Wohnungszählung wurde in erster Linie die Frage gestellt, ob man verpflichtet sei, auf dem entsprechenden Fragebogen den Namen eines Mieters anzugeben bzw. ob entsprechende Einwilligungserklärungen einzuholen seien.

In § 18 Zensusgesetz 2011 (ZensG) ist geregelt, dass für die Erhebungen nach diesem Gesetz Auskunftspflicht besteht. Gemäß Absatz 2 dieser Vorschrift sind für die Erhebung zur Gebäude- und Wohnungszählung die Eigentümer, die Verwalter und die sonstigen Nutzungs- und Verfügungsberechtigten der Gebäude oder Wohnungen auskunftspflichtig. Sie haben unter anderem Auskunft über Namen und Vornamen von bis zu zwei Wohnungsnutzern je Wohnung (§ 6 Abs. 3 ZensG) zu geben. Diese Angaben sind jedoch als sogenannte Hilfsmerkmale erhoben worden. Das heißt, sie sind zum frühestmöglichen Zeitpunkt von den sogenannten Erhebungsmerkmalen (z. B. Gemeinde, Postleitzahl, Eigentumsverhältnisse) zu trennen und gesondert aufzubewahren, bevor sie zu einem genau definierten Zeitpunkt zu löschen sind. Diese gesetzliche Auskunftspflicht habe ich den Petenten erläutert und empfohlen, die Mieter hierüber entsprechend zu informieren.

Haushaltebefragung:

Den Bewohnern von großen Mietshäusern bzw. Hochhäusern war aufgefallen, dass die Mieter sehr vieler Wohnungen eines Hauseinganges befragt worden sind. Der Hinweis auf den Flyern, dass nach einem mathematisch-statistischen Zufallsverfahren Anschriften für die Haushaltebefragung ausgewählt worden seien, löste damit sehr großes Unverständnis aus. Die Bürger standen einer Volkszählung generell sehr offen gegenüber, zweifelten nun aber daran, dass die Befragung nach den gesetzlich vorgeschriebenen Methoden erfolgt sei.

Nach Rücksprache mit dem Statistischen Amt Mecklenburg-Vorpommern habe ich den Petenten mitgeteilt, dass dieses Verfahren so gestaltet ist, dass nicht einzelne Personen mit einer dazugehörigen Adresse ausgewählt worden sind, sondern lediglich eine Auswahl von Adressen erfolgt ist. Bei einem Einfamilienhaus verbirgt sich hinter einer Adresse meistens eine Person bzw. Personen einer Familie. Wenn ein Mehrfamilienhaus in die Auswahl fällt, hatte dies zur Folge, dass alle Bewohner des Hauses, also alle Bewohner, die unter dieser Adresse wohnhaft sind, befragt wurden. Hinzu kommt, dass, insbesondere bei Hochhäusern, auch sogenannte Hausnummernbereiche gebildet worden sind. Hatte ein Hochhaus zum Beispiel die Hausnummern 1a und 1b, wobei auch beide Bereiche durch Flure miteinander verbunden sein können, sind für diese Bereiche keine Trennungen vorgenommen, sondern alle Bewohner befragt worden.

In einer weiteren Petition beunruhigte eine Rentnerin die Frage, was der Erhebungsbeauftragte später mit Kenntnissen über zum Beispiel Details aus der Wohnung anfangen könnte. Sie fühlte sich ausgespäht und im Hinblick auf einen möglichen späteren Einbruch in die Wohnung auch bedroht.

Was den Einlass der Erhebungsbeauftragten angeht, habe ich schon im Vorfeld klargestellt, dass niemand dazu verpflichtet sei, einen Erhebungsbeauftragten in seine Wohnung zu bitten und dass das Statistische Amt lediglich anbiete, beim Ausfüllen der Fragebogen durch einen geschulten und auf die Wahrung des Statistik- und Datengeheimnis verpflichteten Erhebungsbeauftragten behilflich zu sein. Nach dem ZensG 2011 sind auch solche Tatsachen geheim zu halten, die im Zusammenhang mit der Erhebungstätigkeit bekannt werden. Diese Verpflichtung gilt auch nach Beendigung der Tätigkeit eines Erhebungsbeauftragten. Ebenso ist gesetzlich festgelegt, dass Erhebungsbeauftragte nicht eingesetzt werden dürfen, wenn aufgrund ihrer beruflichen Tätigkeit oder aus anderen Gründen zu befürchten ist, dass Erkenntnisse aus der Erhebungstätigkeit zum Schaden der auskunftspflichtigen Personen genutzt werden.

5.5.2 Prüfung von Erhebungsstellen

Zur Vorbereitung und Durchführung des Zensus 2011 wurden gemäß § 10 Abs. 1 Zensusgesetz (ZensG) in Mecklenburg-Vorpommern insgesamt 36 örtliche Erhebungsstellen eingerichtet. Sie sind von den Landkreisen und Städten bzw. Gemeinden als eigene Verwaltungseinheiten eingerichtet worden. Das bedeutet, dass sie zur Sicherung der statistischen Geheimhaltungspflicht räumlich, technisch, organisatorisch und personell von anderen Verwaltungsteilen getrennt bzw. abgeschottet sein müssen. Zu den Hauptaufgaben der Erhebungsstellen gehörte die Durchführung der Haushaltebefragung und die Befragung in Sondereinrichtungen. Auch wurde der Einsatz von Interviewern vor Ort organisiert und deren Schulung vorgenommen. Außerdem waren die Erhebungsstellen dafür verantwortlich, dass die von den Auskunftspflichtigen ausgefüllten Fragebogen rechtzeitig und vollständig eingehen.

Ich habe vier Erhebungsstellen kontrolliert. Diese Kontrollbesuche sollten in erster Linie darüber Aufschluss geben, ob die Einrichtung der Erhebungsstellen und die Auswahl der Erhebungsbeauftragten den daten- und statistikrechtlichen Anforderungen genügt. Dazu gehört auch die oben erwähnte Abschottung von anderen Dienststellen der Verwaltung und die Auswahl der Erhebungsbeauftragten. Maßstab für die Prüfung waren insbesondere die vom statistischen Amt vorgegebene „Organisationsanweisung zur Durchführung des Zensus 2011“ und das „Konzept zur IT-Ausstattung und Netzanbindung der Erhebungsstellen für den Zensus 2011“.

Technische Abschottung:

Das IT-Konzept schreibt für den Zensus-PC in den Erhebungsstellen verschiedene Maßnahmen zur Gewährleistung der Endgerätesicherheit vor. So ist sicherzustellen, dass nur benötigte Hardware angeschlossen werden kann. Zulässig waren nur Tastatur, Scanner, Maus, Drucker und LAN. Alle anderen Schnittstellen des so abgeschotteten PC mussten gesperrt sein. Demzufolge durfte es beispielsweise nicht möglich sein, einen USB-Stick an den abgeschotteten PC anzuschließen und betriebsbereit zu machen, sodass keine Daten vom USB-Stick auf den Zensus-PC der Erhebungsstellen und ebenso keine Daten von diesem auf den USB-Stick kopiert werden konnten. Die Kontrolle hat gezeigt, dass die Abschottung in dieser Hinsicht aufgrund fehlerhafter Konfiguration der Zensus-PC zum Teil nicht funktioniert hat. In mindestens einem Fall war es möglich, einen USB-Stick an den Zensus-PC anzuschließen und betriebsbereit zu machen. Anschließend waren sowohl Schreib- als auch Leseoperationen möglich.

Das Statistische Amt Mecklenburg-Vorpommern hat die Sicherheitslücke in der betroffenen Erhebungsstelle umgehend beseitigt und sofort in allen anderen Erhebungsstellen des Landes Kontrollen aller übrigen Erhebungsstellen-Laptops vor Ort durchgeführt. Zusätzlich ist eine stichprobenartige Überprüfung der PC im Zensusnetz des Statistischen Amtes erfolgt. Auch hatte die Datenverarbeitungszentrum Mecklenburg-Vorpommern (DVZ M-V) GmbH mit den Herstellern der Schnittstellen-, VPN-Software und des Betriebssystems Kontakt aufgenommen, um nach einer allgemeinen Lösung zu suchen, welche die aufgetretenen Probleme künftig verhindern soll. Die weiteren Sicherheitsüberprüfungen des Statistischen Amtes haben keine weiteren Mängel hinsichtlich der technischen Abschottung ergeben.

Erhebungsbeauftragte:

Vor dem Hintergrund möglicher Interessenkollisionen habe ich besonders die Kriterien hinterfragt, welche die Erhebungsstellenleitungen bei der Auswahl und Ablehnung der Erhebungsbeauftragten herangezogen haben. Die Erhebungsbeauftragten stammten aus verschiedenen Bevölkerungsgruppen, in erster Linie hatten sich jedoch Rentner bei den von mir kontrollierten Erhebungsstellen beworben. Hinweise auf mögliche Interessenkonflikte oder eine nicht ausreichend erforderliche Sorgfalt bei der Auswahl der Erhebungsbeauftragten waren nicht ersichtlich. Allerdings habe ich die Aufbewahrung der Erhebungsunterlagen in Pappkoffern nicht für ausreichend erachtet. Ich habe der betreffenden Erhebungsstellenleitung empfohlen, mit den Erhebungsbeauftragten in den Schulungen eindringlich über die Aufbewahrung/Sicherung der Bögen im häuslichen Bereich zu sprechen bzw. danach zu fragen, wie die Erhebungsunterlagen im häuslichen Bereich geschützt werden. Ich habe gefordert, dass die Pappkoffer mit den Erhebungsunterlagen bei den Erhebungsbeauftragten in einem abschließbaren Bereich aufbewahrt werden müssen, also unter persönlichem Verschluss gehalten werden müssen. Das Statistische Amt hat meine Hinweise berücksichtigt, indem die Organisationsanweisung entsprechend geändert worden ist und in weiteren Schulungen besonders auf diese Problematik eingegangen werden sollte.

5.6 Finanzwesen

5.6.1 Steuer-ID

Meine datenschutzrechtlichen Bedenken im Hinblick auf die Einführung der Steuer-ID (siehe Achter Tätigkeitsbericht, Punkt 2.5.1) haben sich bestätigt. Mit zunehmender Automatisierung von Datentransfers in Steuersachen nutzen inzwischen auch nicht-öffentliche Stellen die Steuer-ID als Identifizierungsmerkmal.

So hat der Gesetzgeber zum Beispiel mit dem Jahressteuergesetz 2010 (hier durch das „Bürgerentlastungsgesetz Krankenversicherung“) die Möglichkeit geschaffen, dass die Steuer-ID durch private Krankenversicherungsunternehmen in Zusammenhang mit der steuerlichen Geltendmachung von Vorsorgeaufwendungen durch die Versicherten erhoben und verarbeitet werden darf. Hinzu kommt, dass eine vollständige steuerliche Berücksichtigung der Vorsorgeaufwendungen nur dann erfolgt, wenn der Betroffene der Erhebung und Verarbeitung der Steuer-ID durch die Krankenversicherungsunternehmen zustimmt. Eine solche Einwilligung entspricht nicht den Anforderungen an eine datenschutzrechtlich wirksame Einwilligung. Der Betroffene kann nicht frei zwischen Einwilligung und Verweigerung der Datenübermittlung entscheiden, da er bei Verweigerung tatsächlich geleistete Beiträge nicht mehr steuerlich geltend machen könnte. Die Forderung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit nach einer anderen Form des Nachweises der gezahlten Beiträge blieb bislang vom Bundesministerium der Finanzen unbeachtet.

Die Steuer-ID wird auch in weiteren Lebensbereichen verwendet. Dies hat Bürgerinnen und Bürger veranlasst, sich an mich zu wenden, da sie die Zusammenhänge zwischen der Beantragung einer Leistung und der Angabe der Steuer-ID nicht nachvollziehen können. So muss die Steuer-ID zum Beispiel auch gegenüber Banken (Freistellungsanträge, Eröffnung eines Kontos) oder gegenüber Sozialbehörden angegeben werden. Die Steuer-ID wird in immer mehr Lebensbereichen verwendet, sodass das Risiko der Erstellung von Persönlichkeitsprofilen und die Gefahr einer zweckwidrigen Verwendung wächst. Auch ist abzusehen, dass die Betroffenen durch die Vielzahl von Verfahren den Überblick verlieren, welche Stellen über ihre Steuer-ID für welche Zwecke verfügen.

Es ist zu befürchten, dass die Verwendung der Steuer-ID immer mehr ausufern wird und künftig noch weitere Behörden und Stellen, zum Beispiel Gerichte, Gemeinden, Stiftungen oder auch öffentlich-rechtliche Rundfunkanstalten, die Steuer-ID erheben werden.

Entsprechend den Anforderungen des Bundesverfassungsgerichts aus dem Volkszählungsurteil muss gewährleistet werden, dass die in verschiedenen Datenbanken unter der Steuer-ID gespeicherten Daten nicht zur umfassenden Registrierung oder zur Erstellung von Persönlichkeitsprofilen zusammengeführt werden.

Die Steuer-ID ist grundsätzlich beim Betroffenen zu erheben. Im Hinblick auf das Recht auf informationelle Selbstbestimmung muss er gegebenenfalls zumindest darüber informiert werden, welche Stelle seine Steuer-ID erhebt und unter ihr gespeicherte Daten zu welchem Zeitpunkt an die Finanzverwaltung übermittelt.

5.6.2 Gemeinsame Steuerdatenverarbeitung der norddeutschen Bundesländer

Das im Dezember 2005 in Kraft getretene Gesetz zum Dataport-Staatsvertrag regelt die gemeinsame Steuerdatenverarbeitung der vier Bundesländer Bremen, Hamburg, Schleswig-Holstein und Mecklenburg-Vorpommern (siehe Sechster Tätigkeitsbericht, Punkt A.1.IV.1). Mit Änderung des Staatsvertrages vom 26. November 2010 wurde auch das Land Niedersachsen in die gemeinsame Steuerdatenverarbeitung einbezogen.

Die Landesdatenschutzbeauftragten der beteiligten Länder begleiten das Projekt Data Center Steuern (DCS) von Beginn an und konnten sich stets davon überzeugen, dass die Anforderungen an die Datensicherheit und den Datenschutz bei der Verarbeitung der sensiblen Steuerdaten erfolgreich umgesetzt wurden.

Bereits im Dezember 2009 bestand Einigkeit darüber, dass für DCS ein umfassendes Informationssicherheits-Managementsystem (ISMS) etabliert werden muss, um die Datenschutzanforderungen dauerhaft und überprüfbar ausgestalten zu können. Ziel war die Auditierung sowohl nach Vorgaben der Grundschutzmethodik des Bundesamtes für Sicherheit in der Informationstechnik (BSI) als auch nach den Datenschutz-Audit-Vorgaben des Landes Schleswig-Holstein (Datenschutzbehördenaudit gemäß § 43 Abs. 2 Landesdatenschutzgesetz Schleswig-Holstein). Über die ersten gemeinsamen Begehungen der Rechenzentren in Kiel-Altenholz, Hamburg, Rostock und Schwerin hatte ich bereits berichtet (siehe Sechster Tätigkeitsbericht, Punkt 2.5.9).

Inzwischen ist das Audit-Verfahren abgeschlossen. Am 20. Oktober 2010 übergab der Landesdatenschutzbeauftragte Schleswig-Holsteins das Datenschutzaudit-Zertifikat an Data-port. Das Konzept des ISMS für DCS umfasst auf der Grundlage einer umfangreichen Basisdokumentation der eingesetzten IT-Systeme und Programme technische und organisatorische Vorgaben für den Betrieb der Großrechnersysteme der Steuerdatenverarbeitung. Die Prüfungen ergaben, dass sowohl das Sicherheitsmanagement als auch das Sicherheitskonzept die Datenschutzerfordernisse erfüllen.

Das Kurzgutachten mit den Ergebnissen der Auditierung hat das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein veröffentlicht unter <http://www.datenschutzzentrum.de/audit/register.htm>.

5.6.3 Elektronische Kommunikation mit der Finanzverwaltung

Immer mehr Bürgerinnen und Bürger nutzen das elektronische Verfahren ELSTER für ihre jährliche Steuererklärung. Für diese elektronischen Kommunikationsvorgänge mit der Finanzverwaltung sind Verfahren erforderlich, die sowohl die Authentizität und Integrität der übermittelten Dokumente sicherstellen als auch den Nachweis der Identität des Absenders ermöglichen. § 87a Abs. 3 Abgabenordnung (AO) lässt zu, dass eine durch Gesetz für Anträge, Erklärungen oder Mitteilungen an die Finanzbehörden angeordnete Schriftform durch die elektronische Form ersetzt werden kann. In diesem Fall ist das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz zu versehen.

In meinem Achten Tätigkeitsbericht (siehe dort Punkt 2.5.7) hatte ich bereits kritisiert, dass mit dem Jahressteuergesetz 2007 das Sicherheitsniveau für elektronische Kommunikationsvorgänge mit der Finanzverwaltung gesenkt worden ist, da nun das Bundesministerium der Finanzen (BMF) anstelle der qualifizierten elektronischen Signatur auch ein sogenanntes anderes sicheres Verfahren zulassen darf. Allerdings wurde diese Regelung bis Ende 2011 befristet und eine Entscheidung über das weitere Vorgehen sollte nach Vorliegen eines Evaluierungsberichtes getroffen werden.

Im August 2010 legte das BMF den ersten Entwurf des Evaluierungsberichtes vor. Dieser Bericht sollte nachweisen, dass das ELSTER-Authentifizierungsverfahren, das vom BMF als „anderes sicheres Verfahren“ im Sinne der Abgabenordnung bewertet wird, die gleiche Sicherheit wie eine qualifizierte elektronische Signatur bietet. Der Bericht überzeugte die Datenschutzbeauftragten von Bund und Ländern jedoch nicht.

Es konnten keine belastbaren, statistisch aufgearbeiteten Angaben zu den Erfahrungen der fünfjährigen Praxis von ELSTER-Online präsentiert werden. Der Bericht enthielt zudem keine umfassende Analyse der Risiken und Schwachstellen des „anderen sicheren Verfahrens“ und berücksichtigte in keiner Weise die geänderte Bedrohungslage seit Inbetriebnahme des ELSTER-Online-Portals im Jahr 2006. Auf eine Risikobewertung nach einem international anerkannten Kriterienkatalog wie den Common Criteria hatte das BMF ganz verzichtet. Auch der notwendige sicherheitstechnische Vergleich zwischen der qualifizierten elektronischen Signatur und dem „anderen sicheren Verfahren“ fehlte.

Ungeachtet der Kritik der Datenschutzbeauftragten von Bund und Ländern wurde mit dem Steuervereinfachungsgesetz 2011 nun dauerhaft festgeschrieben, dass neben der qualifizierten elektronischen Signatur auch ein „anderes sicheres Verfahren“ zugelassen werden darf. Die Befristung und die Evaluierungspflicht wurden trotz der Mängel des vorliegenden Evaluierungsberichtes gestrichen. Immerhin wurde mit dem neu gefassten § 87a Abs. 6 AO zusätzlich festgelegt, dass das Verfahren den Datenübermittler (Absender der Daten) authentifizieren und die Integrität des elektronisch übermittelten Datensatzes gewährleisten muss. Wie sich der Gesetzgeber dies technisch vorstellt, wird leider nicht normenklar im Gesetz geregelt, sondern lediglich in der Begründung zum Gesetzentwurf angedeutet. Demnach soll die Vertraulichkeit und Integrität der zu übermittelnden steuerlichen Daten gewährleistet werden, indem diese mit den Authentifizierungsdaten verknüpft und verschlüsselt an die Steuerverwaltung übermittelt werden. Als neue Anforderung wird dort nochmals klargestellt, dass das andere sichere Verfahren „den Datenübermittler zu authentifizieren hat.“ Offen bleibt dabei jedoch, ob Datenübermittler und Steuerpflichtiger identisch sind.

Die Bundesregierung ist sich der Absenkung des Sicherheitsniveaus offensichtlich bewusst, denn in der Begründung zum Gesetzentwurf wird auf Folgendes hingewiesen: „Wird nicht die qualifizierte elektronische Signatur verwendet, gilt zugunsten der Steuerpflichtigen die Beweiskraftregelung des § 87a Absatz 5 Satz 2 AO nicht.“ Damit gesteht die Bundesregierung ein, dass das „andere sichere Verfahren“ eben doch kein gleichwertiger Ersatz für eine gesetzlich angeordnete Schriftform sein kann.

Eine solche Beweislastumkehr zu Gunsten des Steuerpflichtigen ist angesichts des geringeren Sicherheitsniveaus folgerichtig. Allerdings hätte die für die Rechtsposition der Steuerpflichtigen ganz wesentliche Bemerkung nicht in die Begründung gehört, sondern aus Gründen der Normenklarheit in das Gesetz. Im Übrigen darf sich diese Klarstellung nicht nur auf die in § 150 Abs. 6 und 7 beschriebenen Besteuerungsverfahren beziehen, sondern muss ausdrücklich alle elektronischen Kommunikationsvorgänge mit der Finanzverwaltung (§ 87a AO) abdecken. Ich werde aufmerksam beobachten, welche Auswirkungen die neuen Regelungen zur elektronischen Kommunikation mit der Finanzverwaltung haben und ob Steuerpflichtige nicht doch Nachteile in Kauf nehmen müssen.

5.6.4 Ablösung der Lohnsteuerkarte

Im Rahmen der Änderung des Jahressteuergesetzes 2008 ist mit der Neuregelung des § 39 e Einkommensteuergesetz (EStG) trotz datenschutzrechtlicher Bedenken der Wegfall der Papierlohnsteuerkarte beschlossen worden. Alle Lohnsteuerdaten werden jetzt zusätzlich in der beim Bundeszentralamt für Steuern eingerichteten Datenbank zur Steuer-Identifikationsnummer gespeichert. Zu diesen Elektronischen LohnSteuerAbzugsMerkmale (ELSTAM) gehören neben steuerrechtlich relevanten Daten (Steuerklasse) auch sehr sensible personenbezogene Daten zur Religionszugehörigkeit, zum Familienstand oder zu Angehörigen. Mit diesem neuen Verfahren sollen Arbeitgeber zu Beginn eines Beschäftigungsverhältnisses die Möglichkeit erhalten, die in der zentralen Steuerdatenbank gespeicherten Lohnsteuerabzugsmerkmale eines Arbeitnehmers elektronisch abzurufen.

Die Erweiterung der zentralen Datenbank birgt aus datenschutzrechtlicher Sicht nicht unerhebliche Risiken. Zum Beispiel besteht die Gefahr, dass Begehrlichkeiten anderer Stellen geweckt werden oder Arbeitgeber die Daten unberechtigt abrufen könnten. Letzterem ist inzwischen mit dem neu eingeführten § 52 b Abs. 8 Einkommenssteuergesetz entgegen gewirkt worden, wonach jeder Arbeitnehmer das Recht hat zu bestimmen, welcher Arbeitgeber auf seine Lohnsteuerdaten zugreifen darf (Positivliste) und wer dies ausdrücklich nicht darf (Negativliste).

Ebenso ist das Authentifizierungsverfahren der Arbeitgeber über das Elster-Online Portal kritisch einzuschätzen. Bisher sind die technischen Voraussetzungen für den Nachweis noch nicht geschaffen, dass die anfragende Stelle tatsächlich der Arbeitgeber des Betroffenen ist.

Auch im Hinblick auf die Steuerpflichtigen halte ich das Authentifizierungsverfahren nach wie vor für unbefriedigend. Zwar kann neben der elektronischen Signatur gemäß § 87 a Abs. 6 Abgabenordnung (AO) auch ein anderes sicheres Verfahren (siehe auch Punkt 5.6.3) zugelassen werden, das die Authentizität und Integrität des übermittelten elektronischen Dokuments sicherstellt. Im Hinblick auf die Authentizität und Integrität elektronisch übermittelter Dokumente muss jedoch das Verfahren der qualifizierten elektronischen Signatur maßgeblich sein. So müssen Steuerpflichtige im elektronischen Verfahren die Möglichkeit haben, ihre elektronische Kommunikation mit der Finanzverwaltung durch das hierfür geeignete Verfahren der qualifizierten elektronischen Signatur abzusichern.

Im Herbst 2011 sind in Mecklenburg-Vorpommern rund 640.000 Arbeitnehmer durch Informationsschreiben der Finanzämter über ihre in die Datenbank aufgenommenen persönlichen elektronischen Lohnsteuerabzugsmerkmale informiert worden. Daraufhin gab es viele Nachfragen bei den Finanzämtern, da eine große Anzahl (5 - 10 %) der aufgelisteten Steuermerkmale falsch war. Nach Aussage des Finanzministeriums Mecklenburg-Vorpommern sei der Datentransfer von den Meldebehörden an das Bundeszentralamt für Steuern fehlerhaft gewesen, was auch darauf zurückzuführen sei, dass die Meldebehörden mit unterschiedlicher Software gearbeitet hätten und es daher zu Schnittstellenproblemen gekommen sei.

Das vom Bundesministerium der Finanzen gegenüber dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) zugesagte IT-verfahrensspezifische Sicherheitskonzept liegt bislang noch nicht vor. Sobald dieses erstellt ist, wird es vom BfDI und den Landesbeauftragten für den Datenschutz geprüft werden.

Mittlerweile hat sich das geplante Verfahren aufgrund von Softwarefehlern verzögert, sodass die Arbeitgeber die Lohnsteuerdaten nicht wie geplant ab Januar 2012 abrufen können.

Hinsichtlich der in unserem Bundesland aufgetretenen Probleme, insbesondere bezüglich der in den Informationsschreiben aufgetretenen Fehler und des geplanten Einsatzes der Software für den Abruf der Lohnsteuermerkmale durch den Arbeitgeber, habe ich das Finanzministerium aufgefordert, mich über die Lösung der Probleme zu informieren bzw. mich entsprechend zu beteiligen.

5.7 Medien und Telekommunikation

5.7.1 Vorratsdatenspeicherung

In meinem letzten Tätigkeitsbericht (siehe neunter Tätigkeitsbericht, Punkt 2.8.1) hatte ich über die gegen die Vorratsdatenspeicherung eingelegten Verfassungsbeschwerden und die einstweiligen Anordnungen des Bundesverfassungsgerichts vom 11. März 2008 und vom 28. Oktober 2008 berichtet. Das Bundesverfassungsgericht hat in seinem Urteil vom 2. März 2010 (1BvR 256/08) die Verfassungswidrigkeit der Regelungen zur Vorratsdatenspeicherung festgestellt und diese für nichtig erklärt.

Es bewertet die anlass- und verdachtslose vorsorgliche Speicherung von Telekommunikationsdaten als einen schweren Eingriff in das Telekommunikationsgeheimnis, weil über den gesamten Zeitraum von sechs Monaten „sämtliche Telekommunikationsverhaltensdaten aller Bürger ohne Anknüpfung an ein zurechenbar vorwerfbares Verhalten“ erfasst werden. Allerdings betont das Bundesverfassungsgericht, dass die Einführung einer sechsmonatigen Speicherungspflicht verfassungsrechtlich nicht schlechthin verboten ist. Erfolgt die vorsorgliche Speicherung der Telekommunikationsverbindungsdaten zu bestimmten Zwecken und auf Grundlage einer Norm, die den verfassungsrechtlichen Anforderungen insbesondere hinsichtlich der Datensicherheit, des Umfangs der Datenverwendung, der Transparenz und des Rechtsschutzes entspricht, ist laut Bundesverfassungsgericht der in einer solchen Speicherung liegende Eingriff verhältnismäßig im engeren Sinne.

Aufgrund der Nichtigkeit der entsprechenden Normen waren alle auf der Grundlage der Anordnungen vom 11. März 2008 und vom 28. Oktober 2008 gespeicherten Daten unverzüglich zu löschen.

Seit dem Urteil des Bundesverfassungsgerichts wird in Deutschland ein heftiger politischer Streit über die Zukunft der Vorratsdatenspeicherung geführt. Die Befürworter einer möglichst umfassenden Vorratsdatenspeicherung halten ohne diese eine effektive Strafverfolgung im Internet nicht mehr für möglich. Die Bundesjustizministerin dagegen lehnt die Einführung von entsprechenden gesetzlichen Regelungen, aufgrund derer eine sechsmonatige Speicherung von Telekommunikationsverkehrsdaten durch Diensteanbieter möglich wäre, als nicht erforderlich ab.

Nach dem Entwurf eines Gesetzes „zur Sicherung vorhandener Verkehrsdaten und Gewährleistung von Bestandsdatenauskünften im Internet“ sollen Telekommunikationsdaten für einen Zeitraum von sieben Tagen gespeichert werden. Inhalt dieses Entwurfs ist vor allem das sogenannte Quick-Freeze-Verfahren, bei dem Telekommunikationsanbieter auf Anordnung der Strafverfolgungsbehörden die Telekommunikationsdaten, die zur Aufklärung einer Straftat erforderlich sein können, nicht löschen, sondern für einen gewissen Zeitraum „einfrieren“. Die bei den Telekommunikationsunternehmen vorhandenen Verkehrsdaten sollen also anlassbezogen gesichert werden und so den Ermittlern unter Richtervorbehalt eine begrenzte Zeit zur Verfügung stehen können.

Auch die 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer Entschließung vom 3./4. November 2010 auf das Quick-Freeze-Verfahren als Alternative zur Vorratsdatenspeicherung hingewiesen, da es in einem erheblich geringeren Maße in die Grundrechte der Telekommunikationsnutzer eingreift. Im Gegensatz zur Vorratsdatenspeicherung werden nur punktuell und verdachtsabhängig Telekommunikationsdaten gespeichert.

Die Europäische Kommission hat am 20. April 2011 den Evaluationsbericht über die Umsetzung der EU-Richtlinie über die Vorratsspeicherung von Daten vorgelegt. In diesem wurde unter anderem die Verhältnismäßigkeit der Richtlinie in Frage gestellt, das Bestimmtheitsgebot als verletzt gesehen und festgestellt, dass die Richtlinie zu keiner nennenswerten Verbesserung der europäischen Aufklärungsquoten bei der Verbrechensbekämpfung geführt hat. Trotz allem soll lediglich eine punktuelle Überarbeitung der Richtlinie beim Anwendungsbereich, bei den Zugriffsrechten und der Speicherdauer, der Datensicherheit und der statistischen Evaluierung erfolgen.

Vor diesem Hintergrund ist zu begrüßen, dass in Deutschland noch keine neuen gesetzlichen Regelungen zur Umsetzung der EU-Richtlinie zur Vorratsdatenspeicherung verabschiedet worden sind.

5.7.2 Recht am eigenen Bild

Zunehmend haben Petenten Fragen zum Recht am eigenen Bild in Zusammenhang mit foto-fähigen Smartphones. Häufig geht es darum, ob bewusst, beiläufig oder heimlich gemachte digitale oder digitalisierte Fotos von Personen ohne deren vorherige Zustimmung ins Internet (z. B. auch auf Schulhomepages) gestellt (also veröffentlicht) werden dürfen. Einige Antworten zu diesen Fragen finden sich im Faltblatt „Wer hat schon Angst vor Kameras?“, siehe auf der Internetseite unter www.datenschutz-mv.de. Darüber hinaus weise ich in dieser speziellen Problematik auf die folgenden datenschutzrechtlichen Grundsätze hin:

Das Recht am eigenen Bild ist eine Ausprägung des allgemeinen Persönlichkeitsrechts und ist konkret in den §§ 22 und 23 des Kunsturhebergesetzes (KunstUrhG) geregelt. Diese Vorschriften regeln das Recht, darüber zu bestimmen, was mit Fotografien oder anderen bildlichen Darstellungen der eigenen Person in der Öffentlichkeit (Verbreitung oder Zur-Schau-Stellung) geschieht.

Nach der Rechtsprechung des BGH können durch die Verletzung des Rechtes am eigenen Bild sowohl ideelle als auch materielle bzw. kommerzielle Interessen des Abgebildeten betroffen sein. Es gilt daher wie in anderen Bereichen des Datenschutzes auch hier die Grundregel der vorherigen Einwilligung des Betroffenen als wichtigste Voraussetzung. Selbstverständlich kann der Abgebildete nicht uneingeschränkt darüber bestimmen, was mit seinem Bild oder seinen Bildnissen geschieht. Das Recht am eigenen Bild des Abgebildeten findet seine Schranken dort, wo andere Grundrechte gleichberechtigt Platz beanspruchen können. Das können zum Beispiel die Pressefreiheit oder auch die Kunstfreiheit sein. Insbesondere das gezielte (und nicht beiläufige) Fotografieren anderer (erkennbarer) Menschen kann jedoch unter Umständen Unterlassungs- und Löschungsverpflichtungen sowie Schadensersatzforderungen begründen, wenn der oder die Fotografierte mit den Aufnahmen nicht einverstanden ist. Die Ausnahmen dazu sind in § 23 KunstUrhG geregelt.

Selbstverständlich stehen dabei auch Kindern Persönlichkeitsrechte zu - grundsätzlich mit den gleichen Einschränkungen wie bei Erwachsenen. Nach der Rechtsprechung des Bundesverfassungsgerichtes geht dieser Schutz bei Kindern jedoch noch weiter, wenn durch die Veröffentlichung des Bildes die Persönlichkeitsentwicklung des Kindes gefährdet sein kann (Stichwort: Cybermobbing). Die Persönlichkeitsrechte werden bei kleineren Kindern (noch) ohne ausreichende Einsichtsfähigkeit (bis zum 7. Lebensjahr) von den sorgeberechtigten Eltern wahrgenommen - also muss die Einwilligung der Eltern eingeholt werden. Bei Kindern mit einer angenommenen ausreichenden Einsichtsfähigkeit (i. d. R. spätestens etwa ab 14 Jahren) ist zudem noch nach dem in der Rechtsprechung bisher entwickelten Grundsatz der „Doppelzuständigkeit“ die Zustimmung des oder der Minderjährigen erforderlich.

Grundsätzlich muss sich der Fotografierende strikt an die Veröffentlichungs- und Verbreitungsverbote der §§ 22 und 23 KunstUrHG halten. Insbesondere dort, wo gezielt andere Menschen erkennbar abgelichtet werden, ist größte Sorgfalt bei der erforderlichen Einzelfallprüfung geboten - hier ist die vorherige Einwilligung des Betroffenen in der Regel obligatorisch. Über Prominente (hierzu gehören Personen der Öffentlichkeit) darf im Bild grundsätzlich berichtet werden, sofern ein allgemeines Informationsinteresse angenommen und gegebenenfalls begründet werden kann - dabei ist aber auch hier der Schutz der Privatsphäre streng zu beachten.

5.7.3 15. Rundfunkänderungsstaatsvertrag

Die Ministerpräsidenten der Länder haben am 15. Dezember 2010 den 15. Rundfunkänderungsstaatsvertrag unterzeichnet. Die Ratifizierung durch die Länderparlamente ist bis zum 31. Dezember 2011 erfolgt, sodass der Vertrag am 1. Januar 2013 in Kraft treten wird. Damit ist ein grundlegender Systemwechsel bei der Finanzierung des öffentlich-rechtlichen Rundfunks vollzogen worden. Ab 2013 erfolgt die Finanzierung nicht mehr durch eine gerätebezogene Abgabe, sondern durch einen haushaltbezogenen bzw. betriebsbezogenen Beitrag. Der Beitrag soll für jede Wohnung, unabhängig von der Art und Anzahl der betriebenen Empfangsgeräte, und für jeden Betrieb, gestaffelt nach der Anzahl der Beschäftigten, zu entrichten sein.

Die Datenschutzbeauftragten des Bundes und der Länder sind davon ausgegangen, dass dieser Systemwechsel neben einer höheren Beitragsgerechtigkeit auch für eine deutlich datenschutzgerechtere Beitragserhebung genutzt wird. Diese Erwartung wurde jedoch enttäuscht. Die Datenschutzbeauftragten haben ihre notwendige Kritik in einer umfassenden Stellungnahme zum Gesetzesentwurf sowie in einer Entschließung vom 11. Oktober 2010 (siehe Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Oktober 2010 auf www.datenschutz-mv.de) zum Ausdruck gebracht.

Auf diese Kritikpunkte habe ich die Landesregierung Mecklenburg-Vorpommern hingewiesen. Sie beziehen sich zum Beispiel auf die umfangreichen Datenerhebungsbefugnisse der Landesrundfunkanstalten, die nicht den datenschutzrechtlichen Grundsätzen der Erforderlichkeit, Verhältnismäßigkeit, Datensparsamkeit, Normenklarheit und Transparenz entsprechen. So dürfen beispielsweise bei öffentlichen und nicht-öffentlichen Stellen ohne Kenntnis der Betroffenen Daten erhoben werden, ohne dass exakt geregelt ist, um welche Stellen es sich handelt.

Außerdem ist vorgesehen, dass an die Rundfunkbehörden von allen Meldebehörden ein festgelegter Datensatz aller volljährigen Personen übermittelt wird. Ein weiterer Kritikpunkt ist, dass die Rundfunkanstalten berechtigt sind, sich bei Antrag auf Befreiung von der Beitragspflicht oder auf Ermäßigung des Rundfunkbeitrags neben einer Bescheinigung auch die Originalbescheide oder beglaubigte Kopien dieser Bescheide vorlegen zu lassen, sodass viele, auch besonders sensible personenbezogene Daten, gespeichert werden, obwohl diese zur Aufgabenerfüllung nicht erforderlich sind.

Ich empfehle der Landesregierung, sich dafür einzusetzen, dass für den praktischen Vollzug der Regelungen des 15. Rundfunkänderungsstaatsvertrages Konkretisierungen und Differenzierungen vorgenommen werden bzw. diese auf einer Ebene unterhalb des Staatsvertrages unter Berücksichtigung der genannten elementaren datenschutzrechtlichen Grundsätze geregelt werden. Auch im Hinblick auf die geplante Evaluierung des Modellwechsels empfehle ich der Landesregierung, darauf hinzuwirken, dass die vorgebrachten datenschutzrechtlichen Belange, insbesondere hinsichtlich der Erhebung und Verarbeitung personenbezogener Daten sowie der Einhaltung des Grundsatzes der Verhältnismäßigkeit, überprüft werden und ich hierbei mit einbezogen werde.

5.8 Soziales

5.8.1 Kinder- und Jugendhilfe

Darf ein Sozialleistungsträger Daten eines Hilfesuchenden gegenüber Dritten offenbaren?

Ein Vater wollte zum Beispiel wissen, ob es erlaubt ist, wenn Mitarbeiter des Jugendamtes sich bei anderen Hausbewohnern nach ihm erkundigen. Er bat mich, den Sachverhalt zu prüfen.

Vom Jugendamt habe ich erfahren, dass die Mitarbeiter im Rahmen eines unangemeldeten Hausbesuches Angaben zu einem Sorgerechtsstreit überprüfen wollten. Da der Petent nicht auf das Klingeln der Mitarbeiter an der Haustür reagierte und sie auch nicht sicher waren, ob die Klingel an der Haustür funktioniert, wollten sie das Haus betreten, um an der Wohnungstür zu läuten. Sie baten daher einen Bewohner des Hauses um Einlass, wobei sie sich als Mitarbeiter des Jugendamtes vorstellten und ihren Dienstausweis zeigten. Der Amtsleiter konnte bei dem geschilderten Vorgehen keinen Verstoß gegen sozialdatenschutzrechtliche Bestimmungen erkennen. In der Praxis würden sich die Mitarbeiter häufig der Hilfe von Nachbarn bedienen, um in ein Mehrfamilienhaus zu gelangen.

Ein Bewohner eines Hauses, in dem ein Sozialleistungsempfänger wohnt, ist im sozialdatenschutzrechtlichen Sinne Dritter (§ 67 Abs. 10 Satz 2 Sozialgesetzbuch Zehntes Buch (SGB X)). Dass hier der Petent in einer Beziehung zum Jugendamt steht, ist ein Sozialdatum, dessen Bekanntgabe an einen Dritten eine Übermittlung von Sozialdaten ist (§ 67 Abs. 6 Satz 2 Nr. 3 SGB X).

Eine Übermittlung ist nach den sozialdatenschutzrechtlichen Bestimmungen jedoch nur zulässig, soweit eine gesetzliche Übermittlungsbefugnis nach den §§ 68 bis 77 SGB X oder nach anderen Rechtsvorschriften im Sozialgesetzbuch vorliegt. Eine Rechtsgrundlage für die Übermittlung wurde mir vom Jugendamt nicht genannt und bestand nach meiner Auffassung auch nicht. Außerdem war die Bekanntgabe der Mitarbeiter des Jugendamtes an den Hausbewohner, dass sie den Petenten in einer Angelegenheit als Mitarbeiter des Jugendamtes sprechen wollen, für die Gewährung des Einlasses auch nicht erforderlich, denn der Anlass für den Besuch hätte auch neutral dargestellt werden können.

Ich habe dem Jugendamt empfohlen, die Mitarbeiter auf die Einhaltung des Sozialdatenschutzes hinzuweisen und Sozialdaten künftig nur auf rechtlicher Grundlage oder mit Einwilligung des Betroffenen zu übermitteln, wenn dies erforderlich ist, um eine gesetzliche Aufgabe zu erfüllen.

Dortmunder Entwicklungsscreening für den Kindergarten (DESK)

Eltern und Mitarbeiter freier Träger haben mich auf die Anwendung des Dortmunder Entwicklungsscreenings für den Kindergarten (DESK-Verfahren) hingewiesen und gebeten, das Projekt unter datenschutzrechtlichen Aspekten zu prüfen. Auch das Kinderzentrum Schwerin hat mich um eine datenschutzrechtliche Beratung zum DESK-Verfahren gebeten.

Diese Beratung, an der auch Erzieherinnen aus verschiedenen Kindertagesstätten teilgenommen haben, fand im Kinderzentrum Schwerin statt. Hier berichteten auch die Erzieherinnen über Vorbehalte von Eltern gegenüber dem DESK-Verfahren, die sich vor allem darauf richteten, dass die Persönlichkeit eines Kindes nicht schematisch abgebildet werden dürfe. Sie unterstrichen aber auch, dass das DESK-Verfahren eine gute Grundlage ist, um Defizite feststellen zu können und diesen dann frühzeitig mit geeigneten Hilfsangeboten entgegenwirken zu können. Dabei würden im Übrigen die Entwicklungsstärken von Kindern nicht unberücksichtigt bleiben.

Im Kindertagesförderungsgesetz Mecklenburg-Vorpommern (KiföG M-V) wird ein Rahmen für den Betreuungs-, Bildungs- und Erziehungsauftrag formuliert. Um diesen Auftrag altersgemäß und dem Entwicklungsstand entsprechend erfüllen zu können, ist anhand von möglichst regelmäßigen Beobachtungen der jeweilige Entwicklungsstand des Kindes einzuschätzen (§ 1 Abs. 5 und 6 KiföG M-V). Die dokumentierten Beobachtungen und die Anmerkungen dienen dazu, die Bildungs- und Entwicklungsverläufe der Kinder kontinuierlich zu begleiten und Kinder gegebenenfalls individuell zu fördern.

Aus datenschutzrechtlicher Sicht ist es wichtig, dass das gesamte Verfahren für die Eltern bzw. die Personensorgeberechtigten transparent gestaltet wird. Die Eltern bzw. die Personensorgeberechtigten sollten von Beginn an umfassend über das Projekt und den Inhalt der Bildungsdokumentation informiert werden. Die Ergebnisse sind regelmäßig mit ihnen auszuwerten. Grundsätzlich gilt: Mit der Bildungsdokumentation können die anspruchsvollen Ziele nur erreicht werden, wenn das Verfahren transparent ist und es den Eltern bzw. den Personensorgeberechtigten jederzeit möglich ist, Einsicht in die Entwicklungsberichte ihrer Kinder zu nehmen. Darüber hinaus sollten von der Kindertagesstätte personenbezogene Daten der Kinder an Dritte nur weitergegeben werden, wenn die Eltern bzw. die Personensorgeberechtigten damit einverstanden sind. Denkbar wäre, dass die Ergebnisse des DESK-Verfahrens zum Beispiel der Grundschule sowie den Horten für die weitere individuelle Förderung zur Verfügung gestellt werden.

Eine ausführliche datenschutzrechtliche Bewertung des DESK-Verfahrens steht in meinem Internetangebot unter <http://www.datenschutz-mv.de/dschutz/informat/desk/desk.pdf> zur Verfügung.

5.8.2 Zuständigkeit für Hartz IV neu geregelt

Mit dem Gesetz zur Weiterentwicklung der Organisation der Grundsicherung für Arbeitsuchende wurde festgelegt, dass ab Januar 2011 für die Datenschutzkontrolle der Arbeitsgemeinschaften nach dem Sozialgesetzbuch Zweites Buch (ARGen) bzw. der Jobcenter ausschließlich der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zuständig ist. Bis zu diesem Zeitpunkt haben der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und die Landesbeauftragten für den Datenschutz, außer Sachsen, gemeinsam die Einhaltung datenschutzrechtlicher Vorschriften bei den ARGen bzw. Jobcentern kontrolliert.

Die betroffenen Bürgerinnen und Bürger können diese Änderung nicht ohne Weiteres nachvollziehen. Dies zeigten vor allem die bei mir weiterhin eingehenden Eingaben von Empfängern des Arbeitslosengeldes II (ALG II) bzw. des Sozialgeldes. Aufgrund der bis zum 1. Januar 2011 praktizierten, aber rechtlich umstrittenen Zusammenarbeit der Datenschutzbeauftragten konnten diese Anfragen mit den Mitarbeitern in den ARGen in der Regel schnell geklärt werden. Mit der Neuregelung müssen sich die Hilfesuchenden nun an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wenden. Dort ist der Arbeitsanfall aufgrund der nunmehr aus dem gesamten Bundesgebiet eingehenden Anfragen um ein Vielfaches höher als bisher.

Ich kontrolliere die Einhaltung des Datenschutzes nur noch bei den sogenannten Optionskommunen im Land, das heißt bei Einrichtungen in ausschließlich kommunaler Trägerschaft. Das war bis zum 31. Dezember 2011 nur die Optionskommune Ostvorpommern (neu: Landkreis Vorpommern-Greifswald). Mit Inkrafttreten der Kommunalträger-Zulassungsverordnung vom 14. April 2011 (BGBl. I, Nr. 18, S. 645) werden ab dem 1. Januar 2012 in Mecklenburg-Vorpommern auch der Landkreis Mecklenburgische Seenplatte (alt: Mecklenburg-Strelitz) und der Landkreis Vorpommern-Rügen (alt: Nordvorpommern) Aufgaben nach dem SGB II in alleiniger Zuständigkeit wahrnehmen und damit meiner Kontrolle unterliegen.

5.8.3 Betriebliches Eingliederungsmanagement oder Fahrtauglichkeitsprüfung?

Der Betriebsratsvorsitzende eines Verkehrsunternehmens bat mich zu prüfen, ob der Arbeitgeber zur Vorbereitung und Durchführung des Betrieblichen Eingliederungsmanagements (BEM, siehe § 84 Abs. 2 Sozialgesetzbuch Neuntes Buch - SGB IX) berechtigt ist, die Mitarbeiterinnen und Mitarbeiter schriftlich aufzufordern, die sie behandelnden Ärzte von der Schweigepflicht zu entbinden sowie Medikamentenpläne, fachärztliche Vorbefunde und ihre Krankengeschichte gegenüber dem Betriebsarzt offenzulegen. Anlass dieser Anfrage war ein konkreter Vorfall im Betrieb.

Der Betriebsleiter teilte mir auf meine Anfrage hin mit, dass beabsichtigt war, mit einem Mitarbeiter ein BEM unter Einbeziehung des Betriebsarztes durchzuführen. Offensichtlich wurde in dem Betrieb das BEM nicht als eine Präventionsmaßnahme verstanden, die den Arbeitnehmern unter den gesetzlichen Voraussetzungen anzubieten ist und an der sie auf freiwilliger Basis teilnehmen können. Der Mitarbeiter war zunächst mit dem Vorgehen des Betriebsleiters einverstanden, sodass mit dem Betriebsarzt ein Termin vereinbart wurde. Der Mitarbeiter hat diesen Termin auch wahrgenommen, sich dann aber geweigert, an der weiteren medizinischen Untersuchung teilzunehmen.

Daraufhin wurde dem betroffenen Mitarbeiter von dem Betriebsleiter in einem weiteren Schreiben mitgeteilt, dass er sich einer Untersuchung durch den Betriebsarzt zur Entscheidung über seine Diensttauglichkeit (Fahrtauglichkeit) zu unterziehen hat. Für den Fall, dass er diesen Termin nicht wahrnimmt, wurde eine Abmahnung angedroht. Es ging also nicht um ein BEM, vielmehr sollte die Fahrtauglichkeit des Mitarbeiters geprüft werden. Der Betriebsleiter ging deshalb von einer Mitwirkungspflicht des Mitarbeiters aus und sah es als dessen Pflicht an, dem Betriebsarzt Auskünfte zu Art und Ursache von Erkrankungen zu geben. Dem Betriebsleiter habe ich mitgeteilt, dass das BEM und die Prüfung der Fahrtauglichkeit unterschiedliche Maßnahmen sind, die nicht im Zusammenhang durchgeführt werden dürfen.

Das BEM verfolgt das Ziel, Erkrankungen durch betriebliche Leistungen und Hilfen zu verhindern oder ihnen vorzubeugen, um damit den Arbeitsplatz für einen betroffenen Mitarbeiter zu erhalten. Für den Arbeitnehmer ist die Teilnahme an dem BEM freiwillig, deshalb ist er nicht verpflichtet, seine Gesundheitsdaten dafür zu offenbaren. Dies habe ich dem Betriebsleiter mitgeteilt und empfohlen, künftig die Vorgaben des § 84 Abs. 2 SGB IX zu erfüllen. Dies bedeutet auch, dass die Annahme des BEM für die Betroffenen als Angebot dargestellt werden sollte (siehe Achter Tätigkeitsbericht, Punkt 2.10.2).

Sofern aber geprüft werden muss, ob der Mitarbeiter fahrtauglich im Sinne der Fahrerlaubnisverordnung ist, ist dies dem Betroffenen vor einer Aufforderung zu einer ärztlichen Untersuchung zu erläutern. Er ist in diesem Fall auch darüber zu informieren, dass er gegenüber dem Betriebsarzt zu Angaben über die Gesundheit und gegebenenfalls Medikationen nur verpflichtet ist, wenn sich diese auf die Fahrtüchtigkeit auswirken oder auswirken können. Wenn Zweifel an der Fahrtauglichkeit eines Mitarbeiters bestehen, der ein Fahrzeug führen soll, ist er verpflichtet, an einer entsprechenden Untersuchung teilzunehmen.

Der Betriebsleiter wird die Hinweise künftig beachten und in jedem Einzelfall die jeweiligen Umstände mit der erforderlichen Sensibilität berücksichtigen.

5.8.4 Akte auf dem Postweg verschwunden

Ein Vater hatte sich an mich gewandt, weil die Schwerbehindertenakte seines Sohnes auf dem Weg vom Sozialleistungsträger (einem Versorgungsamt) an seinen Rechtsanwalt verschwunden war. Von dem Versorgungsamt erhielt er keine befriedigende Auskunft, deshalb bat er mich um Unterstützung.

Auf meine Anfrage an das Versorgungsamt, welche technischen und organisatorischen Maßnahmen zum Schutz und zur Sicherheit von Daten beim Postversand getroffen werden, teilte mir das Amt mit, dass die Akte in diesem Fall über die interne Poststelle an einen privaten Paket- und Postversanddienst zur Zustellung übergeben worden sei. Eine Nachfrage bei dem Zusteller habe ergeben, dass die Sendung ordnungsgemäß zugestellt worden sei. Damit war nach Auffassung des Versorgungsamtes die Angelegenheit erledigt. Mehr könne man in dem Falle nicht tun.

In meiner datenschutzrechtlichen Bewertung habe ich darauf hingewiesen, dass nach den gesetzlichen Bestimmungen der Sozialleistungsträger für die Verarbeitung von Sozialdaten nach dem Sozialgesetzbuch Neuntes Buch (SGB IX) verantwortlich ist. Das bedeutet, dass das Versorgungsamt die erforderlichen technischen und organisatorischen Maßnahmen nach § 78a Sozialgesetzbuch Zehntes Buch (SGB X) treffen muss, die in einem angemessenen Verhältnis zu dem Schutzzweck stehen. Wird wie in diesem Fall eine vollständige Sozialleistungsakte mit der Post versandt, so ist eine Versandart zu wählen, bei der dokumentiert wird, an welches Versandunternehmen zu welchem Zeitpunkt welche Sendung übergeben wurde und an wen diese Sendung zu welchem Zeitpunkt beim Empfänger ausgehändigt worden ist. Nach meiner Auffassung hat das Versorgungsamt die vollständige Sozialakte nicht mit der gebotenen Sorgfalt versandt. Es hätte hier eine höherwertige Versandform, z. B. Wertbrief, gewählt werden müssen, um Sendungsverlauf und Aushändigung nachvollziehen zu können.

Um künftig die erforderlichen Maßnahmen beim Versand von Sozialleistungsakten zu gewährleisten, habe ich auch die übergeordnete Behörde auf die datenschutzrechtliche Problematik aufmerksam gemacht. Diese hat daraufhin festgelegt, dass Sozialakten künftig nur in Ausnahmefällen und mit Postzustellungsurkunde versandt werden, beispielsweise wenn die Adresse des Empfängers weiter als 50 km vom Standort des jeweiligen Dezernats entfernt ist. In allen anderen Fällen kann die Akte gegen Empfangsquittung an die Betroffenen oder deren Rechtsvertreter herausgegeben werden. Gegen diese Vorgehensweise ist aus datenschutzrechtlicher Sicht nichts einzuwenden.

Es konnte jedoch nicht geklärt werden, wo die Akte des Petenten verblieben ist. Ich habe ihn daher auf die Möglichkeit hingewiesen, dass er nach § 82 Sozialgesetzbuch Zehntes Buch (SGB X) einen Anspruch auf Schadensersatz gegenüber dem Sozialleistungsträger hat, sofern ihm oder seinem Sohn ein Schaden durch den Verlust von Unterlagen entstanden ist.

5.9 Gesundheitswesen

5.9.1 Umgang mit Patientendaten

Die Übermittlung von Patientendaten von Krankenhäusern, Arztpraxen oder Rehabilitationseinrichtungen steht im Mittelpunkt vieler Anfragen aus dem Gesundheitsbereich. Die Datenverarbeitung in Rehabilitationskliniken kann ich im Übrigen nur als Aufsichtsbehörde nach dem Bundesdatenschutzgesetz kontrollieren, wenn sie nicht im Rahmen der gesetzlichen Kranken- oder Rentenversicherung tätig wird. Dies liegt daran, dass in unserem Bundesland keine gesetzliche Krankenkasse oder gesetzliche Rentenversicherung mehr ihren Sitz hat, die nur im Gebiet dieses Landes tätig wird.

Im Folgenden stelle ich einen Auszug der Anfragen und deren datenschutzrechtliche Bewertung vor:

Übermittlung einer Diagnose an den überweisenden Arzt

Ein Patient wandte sich an mich, weil ein Facharzt eine mit der Behandlung nicht im Zusammenhang stehende Diagnose an den Arzt übermittelt hat, der die Überweisung ausgestellt hatte. Der Patient sollte sich einem Facharzt für Innere Medizin vorstellen. Der Facharzt stellte bei der Untersuchung neben dem internistischen Befund eine psychotische Diagnose, die außerhalb seiner Facharztztätigkeit lag. Den Befund und diese Diagnose übermittelte er an den überweisenden Arzt. Der Facharzt hatte den Patienten zuvor zwar gefragt, ob das von ihm diagnostizierte Krankheitsbild behandelt wird, was dieser verneint hat, aber ihn nicht um seine Einwilligung zur Übermittlung der psychotischen Diagnose an den Kollegen gebeten. Als der Patient von dieser Übermittlung erfuhr, hat er dem Facharzt mitgeteilt, dass er damit nicht einverstanden ist, woraufhin der Facharzt die Diagnose in „Verdacht auf ...“ änderte.

Weil die (Verdachts-)Diagnose auf dem Befundbericht stand, der zur Behandlung durch andere Fachärzte erforderlich war, haben auch diese davon Kenntnis erhalten. Der Patient meinte auch, dass die Diagnose unzutreffend sei und er damit bei anderen Ärzten in ein falsches Licht gerückt würde.

Ich habe den Arzt darauf hingewiesen, dass die ärztliche Schweigepflicht auch unter Ärzten einzuhalten ist. Dies bedeutet, dass Patientendaten an andere Stellen nur übermittelt werden dürfen, wenn eine Rechtsvorschrift dies vorsieht oder der Patient eingewilligt hat.

Für den zuvor beschriebenen Fall hätten die Daten nur auf der Grundlage der Einwilligung des Patienten übermittelt werden dürfen. Bevor der Patient um die Einwilligung gebeten wird, hätte der Facharzt allerdings prüfen müssen, ob die Datenübermittlung zur Erfüllung einer Aufgabe des Arztes, der die Überweisung ausgestellt hatte, überhaupt erforderlich ist. Diese Voraussetzung hätte hier nicht vorgelegen, weil der Arzt, an den die Daten übermittelt worden sind, kein Facharzt für die Behandlung psychotischer Krankheitsbilder ist. Wäre der die Überweisung ausstellende Arzt jedoch der Hausarzt, hätte nicht geprüft werden müssen, ob die Datenübermittlung erforderlich ist, weil nach dem Willen des Gesetzgebers der Hausarzt die Rolle eines Lotsen im Gesundheitswesen erfüllen soll. In einem solchen Fall würde die Einwilligung ausreichen. Was hätte der Facharzt also tun müssen? Er hätte den Patienten gegebenenfalls davon überzeugen müssen, dass er einen auf die Behandlung der Verdachtsdiagnose spezialisierten Arzt aufsucht.

Nach einem umfangreichen Schriftwechsel ist der Facharzt schließlich meiner Empfehlung gefolgt und hat einen neuen Befundbericht gefertigt, der die Verdachtsdiagnose nicht mehr enthielt. Diesen Bericht hat er dem überweisenden Arzt mit der Bitte zugesandt, ihn gegen den alten auszutauschen und auch die weiteren behandelnden Ärzte entsprechend zu informieren sowie die ohne Einwilligung übermittelte Diagnose zu löschen bzw. zu vernichten. Den Patienten habe ich über das Ergebnis informiert.

Auflösung einer Gemeinschaftspraxis - Wer bekommt die Patientenakten?

Zwei Ärztinnen, die ihre Patienten in einer Gemeinschaftspraxis behandelten, entschieden sich, künftig getrennte Wege zu gehen, und wollten von mir wissen, was bei der Aufteilung der Patientenakten zu beachten ist. Bei einer Gemeinschaftspraxis besteht im Gegensatz zu einer Praxisgemeinschaft die Besonderheit, dass die Patienten von jedem Arzt in der Gemeinschaftspraxis behandelt werden können. Ein Patient, der eine Gemeinschaftspraxis aufsucht, kann daher in der Regel nicht wählen, von welchem Arzt er behandelt werden möchte. Daher war hier die Frage, ob die Patientenakten und -dateien kopiert werden können, damit jede Ärztin ein Exemplar hat.

Patientenakten und -dateien sind zur Behandlung erforderlich; darüber hinaus ist ein Arzt aber auch zur Dokumentation der Behandlung berufsrechtlich verpflichtet. Ein Arzt muss, beispielsweise wenn ein Patient den Vorwurf erhebt, falsch behandelt worden zu sein, sein ärztliches Tun nachweisen können. Weil eine umfassende Behandlungsdokumentation eines Patienten einer Gemeinschaftspraxis in der Regel nicht einem der dort tätigen Ärzte eindeutig zugeordnet werden kann, hätte es nahegelegen, die Unterlagen oder Dateien zu kopieren und jedem Arzt zur Verfügung zu stellen. Dem steht jedoch das datenschutzrechtliche Prinzip der Datenvermeidung und Datensparsamkeit nach § 3a Bundesdatenschutzgesetz (BDSG) entgegen. Durch das Kopieren würde der Datenbestand verdoppelt, was unstrittig nicht datensparsam ist.

Bei der Trennung einer Gemeinschaftspraxis sind die Patientenakten und -dateien aus datenschutzrechtlicher Sicht daher so zu behandeln, wie bei einer Praxisauflösung oder einem Praxisverkauf: Entscheidend dafür, welcher Arzt die Unterlagen oder Daten weiter aufbewahrt oder speichert, ist der Wille des Patienten. Wenn der Patient mitteilt, von welchem Arzt er künftig weiter behandelt werden möchte, ist die Patientendokumentation diesem zu übergeben. Aus haftungsrechtlichen Gründen ist zu empfehlen, dass protokolliert wird, welcher Arzt von welchem Patienten Unterlagen und Daten in welchem Umfang erhalten hat. Die Protokolle sollten von dem abgebenden und von dem übernehmenden Arzt solange aufbewahrt werden, wie dies für die ärztliche Dokumentation nach der ärztlichen Berufsordnung geregelt ist, also 10 Jahre.

Muss man für die Reparatur einer Zahnprothese umfangreiche Gesundheitsdaten offenbaren?

Eine Patientin teilte mir mit, dass ihre Zahnprothese zu reparieren war. Da ihre behandelnde Zahnärztin im Urlaub war, wandte sie sich an die Urlaubsvertreterin. Diese Zahnärztin verlangte von ihr aber, dass sie zunächst ein Formular ausfüllen sollte. Mit diesem Formular wurden verschiedene Krankheitsbereiche abgefragt, beispielsweise ob Funktionsstörungen des Herz-Kreislauf-Systems, der Leber, der Schilddrüse, der Lunge, der Blase oder der Nieren vorliegen. Die Patientin war mit dieser Datenerhebung wegen einer Reparatur der Prothese nicht einverstanden.

Die Zahnärztin hat in der von mir erbetenen Stellungnahme dargelegt, dass auch für ihre Tätigkeit vielfältige Gesundheitsinformationen erforderlich sind. Vorerkrankungen und durchgeführte Operationen seien eine wesentliche Basis für eine zielgerichtete Diagnose sowie eine effiziente und erfolgreiche Therapie.

Es steht außer Frage, dass auch für eine zahnärztliche Behandlung der Gesundheitsstatus des Patienten dem Zahnarzt bekannt sein sollte. Muss beispielsweise ein Abdruck des Gebisses angefertigt werden, sollte der Zahnarzt wissen, ob zum Beispiel eine Erkrankung des Herz-Kreislauf-Systems oder der Lunge vorliegt, weil der Patient dann besonders beobachtet oder behandelt werden muss. Allein für die durch den Zahnarzt zu veranlassende Reparatur der Zahnprothese, wie in dem vorliegenden Fall, war diese Datenerhebung aber nicht erforderlich. Im Übrigen ist ein Patient nicht verpflichtet, umfassend Auskunft über seinen Gesundheitszustand zu geben. Wichtig ist vielmehr, dass auch ein Zahnarzt den Patienten über die Datenerhebung aufklärt und auf die Bedeutung der Angaben für die zahnärztliche Behandlung hinweist, denn nur so kann das notwendige Vertrauensverhältnis hergestellt und der Patient dazu motiviert werden, in seinem eigenen Interesse mögliche Gesundheitsstörungen zu nennen.

Der Zahnärztin habe ich empfohlen, künftig Daten nur dann zu erheben, wenn sie erforderlich sind. Der Patientin habe ich meine datenschutzrechtliche Bewertung mitgeteilt und insbesondere auf die Freiwilligkeit der Angaben hingewiesen.

Datenerhebung vor Beginn einer Rehabilitationsbehandlung

Eine Petentin beschwerte sich über den Patientenfragebogen einer Rehabilitationsklinik, der einen Umfang von zehn Seiten hatte, mit dem daher in einem großen Umfang Gesundheitsdaten erhoben wurden und der mit einer Anreisebestätigung der Klinik zugesandt werden sollte.

In meiner Bitte an die Rehabilitationsklinik um Stellungnahme habe ich darauf hingewiesen, dass derartige Angaben der Freiwilligkeit unterliegen und die Patienten darüber aufzuklären sind. Die Klinik hat in ihrer Antwort ausgeführt, dass sie folgenden Hinweis künftig verwenden wolle:

„Meine persönlichen Angaben dienen in erster Linie klinikinternen Zwecken und sind für den planmäßigen Verlauf der Rehabilitationsmaßnahme sowie zur Erstellung des ärztlichen Entlassungsberichtes erforderlich, der an meinen Kostenträger weitergeleitet wird. Sie wurden von mir freiwillig gemacht. Mir ist bekannt, dass die Daten dem Sozialgeheimnis unterliegen und nach den Bestimmungen des Bundesdatenschutzgesetzes behandelt werden. Ich gebe meine Zustimmung zur Weitergabe an Dritte für besonders begründete Ausnahmefälle, die unzweifelhaft in meinem Interesse liegen.“

Dieser neue Hinweis war in mehrfacher Hinsicht datenschutzrechtlich zu kritisieren. Es wird zwar auf die Freiwilligkeit hingewiesen, aber in einer Art, die wohl eher als Forderung verstanden wird. Die Daten unterliegen auch nicht dem Sozialgeheimnis, sondern der ärztlichen Schweigepflicht. Das Sozialgeheimnis richtet sich an die in § 35 Abs. 1 Sozialgesetzbuch Erstes Buch (SGB I) genannten Stellen, sodass eine Rehabilitationsklinik nur als solche Stelle gelten würde, wenn sie originäre Aufgaben der gesetzlichen Kranken- oder Rentenversicherung wahrnehmen würde, was hinsichtlich der Erhebung medizinischer Daten nicht der Fall ist.

Im Übrigen wären dann auch die Bestimmungen der Bücher des Sozialgesetzbuches und nicht die Bestimmungen des Bundesdatenschutzgesetzes einzuhalten. Schließlich ist auch die Formulierung zur Weitergabe von Daten nicht hinreichend bestimmt, weil offensichtlich nicht die betroffene Person über ihre Interessen entscheiden soll bzw. es hier zumindest fragwürdig ist, ob die Klinik alle ihre Interessen berücksichtigen kann. Aufgrund dieser Passage wäre damit eine Übermittlung der Daten nicht zulässig.

Die Klinik hat die Formulierung schließlich nochmals geändert und erläutert, dass die Angaben für die medizinische Behandlung wichtig sind und damit die Rehabilitation zielgerichtet geplant werden kann, dass die Angaben der ärztlichen Schweigepflicht unterliegen und dass bei Datenübermittlungen zuvor die Einwilligung eingeholt wird.

Das Ergebnis habe ich der Petentin mitgeteilt.

Arbeitgeber erkennt Entlassungsschein einer Rehabilitationsklinik nicht an

Ein Petent hat mir mitgeteilt, dass er zur Rehabilitation in einer Klinik behandelt worden ist. Von der Klinik hat er einen Entlassungsschein erhalten, den der Arbeitgeber aber nicht anerkannt hat, weil die Adresse der Klinik auf dem Schein nicht aufgeführt war und weil er nicht unterschrieben war. Der Schein enthielt die Versicherungsnummer, ein Kennzeichen, eine Maßnahmenummer, das Datum der Ausstellung, die Adresse des Patienten, den Aufnahme- und Entlassungstag sowie die Aussage, dass der Patient weiter arbeitsunfähig ist. Am Ende des Belegs stand der Satz „Dieser Schein ist maschinell erstellt und ohne Unterschrift gültig.“ Gegenüber dem Patienten hat die Rehabilitationsklinik angegeben, dass der Entlassungsschein aus Datenschutzgründen in der beschriebenen Weise ausgestellt würde. Der Arbeitgeber hingegen hat von dem Patienten verlangt, dass die Bezeichnung und die Adresse der Rehabilitationsklinik angegeben und der Schein unterschrieben werden müsse.

Die Forderung des Arbeitgebers entspricht den Vorgaben des Vordrucks „Entlassungsschein“ (G9309) der Deutschen Rentenversicherung Bund, den die Rehabilitationsklinik aber nicht verwendet hat. Aufgrund des Hinweises erhielt der Patient einen von der Rehabilitationsklinik unterschriebenen und mit dem Namen und der Adresse der Klinik versehenen Entlassungsschein. Datenschutzgründe stehen dem Verlangen nach einer Unterschrift und diesen Angaben jedenfalls nicht entgegen.

5.9.2 Zentrales Klinisches Krebsregister

Nach dem abgeschlossenen Gesetzgebungsverfahren über das Zentrale Klinische Krebsregister (siehe Punkt 3.3.5) hat das Ministerium für Arbeit, Gleichstellung und Soziales Mecklenburg-Vorpommern ein Interessenbekundungsverfahren zum Betrieb des Zentralen Klinischen Krebsregisters ausgeschrieben und eine Expertenkommission gegründet, die die eingereichten Unterlagen bewerten und für die Auswahl vorschlagen sollte.

An den Sitzungen der Expertenkommission habe ich beratend teilgenommen. Die Kommission hat einen Bewerber empfohlen, der über ausgewiesene Erfahrungen in der Tumordokumentation und in der Auswertung von Tumordaten verfügt.

In der sich anschließenden Beratung in der Auswahlkommission, die unter anderem aus Mitgliedern des Ministeriums, der Selbstverwaltung in der gesetzlichen Krankenversicherung und der beiden Universitäten Rostock und Greifswald bestand, wurde die Aufgabenwahrnehmung der Treuhandstelle und der Registerstelle durch den von der Expertenkommission favorisierten Bewerber kritisch hinterfragt. Dabei stand im Mittelpunkt, dass in anderen gesetzlichen Regelungen über Krebsregister, wie beispielsweise dem nicht mehr in Kraft befindlichen Gesetz über Krebsregister vom 4. November 1994 (BGBl. I, 1994, 3351 ff.), geregelt ist, dass das Krebsregister aus einer selbständigen, räumlich, organisatorisch und personell voneinander getrennten Vertrauensstelle, hier gleichbedeutend mit Treuhandstelle, und einer Registerstelle besteht. Die Kritiker zogen in Zweifel, dass der favorisierte Bewerber diese Voraussetzungen gewährleistet.

Epidemiologische oder klinische Krebsregister weisen hinsichtlich der Gestaltung der Vertrauens- oder Treuhandstelle und Registerstelle tatsächlich Variationen auf.

Während bei einem bayerischen Krebsregister die Trennung dadurch realisiert worden ist, dass die eine Stelle an einer Universität und die andere Stelle an einer anderen Universität untergebracht ist, befinden sich Vertrauens- und Registerstelle des Gemeinsamen Krebsregisters der Länder Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und der Freistaaten Sachsen und Thüringen unter dem Dach eines Gebäudes. Dennoch ist hier die Trennung realisiert, weil die Stellen in getrennten Bereichen des Gebäudes untergebracht sind und jede Stelle von einer anderen Person geleitet wird. Diese Personen sind untereinander hinsichtlich der Aufgabenwahrnehmung weisungsfrei. Entscheidend ist daher vielmehr, dass die Selbständigkeit der beiden Stellen durch räumliche, organisatorische und personelle Trennung gewährleistet wird. Dies lässt sich selbst dann erreichen, wenn relativ kurze Entfernungen zwischen ihnen liegen. Es kommt also auf die konkrete Ausgestaltung der beiden Stellen an. Bewährt hat sich in diesem Zusammenhang auch, dass die Vertrauens- oder Treuhandstelle von einer Person geleitet wird, die ein sogenannter Berufsgeheimnisträger ist, wie beispielsweise ein Arzt, ein Notar oder ein Rechtsanwalt etc. Zum einen unterliegt eine solche Person der strafbewehrten Pflicht zur Wahrung von Privatgeheimnissen (§ 203 Strafgesetzbuch) und zum anderen besteht für diese Daten ein Schutz vor Beschlagnahme (§ 97 Strafprozessordnung).

Nach dem Gesetz über das Zentrale Klinische Krebsregister kann das zuständige Ministerium die Einrichtung der Treuhandstelle und der Registerstelle bestimmen. Ich werde es dabei beraten, dass die Stellen ihre Aufgaben selbständig und eigenverantwortlich durch eine ausreichende räumliche, organisatorische und personelle Trennung wahrnehmen können.

5.10 Verarbeitung von Personalaktendaten

Im Berichtszeitraum erreichten mich wieder die unterschiedlichsten Anfragen zu den Rechten der Beschäftigten beim Umgang mit ihren Personaldaten. Anhand der folgenden Beispiele möchte ich die Spannbreite der Anfragen darstellen.

Einsicht in Personalunterlagen durch Vorgesetzte

Ein Gerichtsvollzieher beschwerte sich darüber, dass sein Dienstherr, ein Oberlandesgericht, ohne seine Zustimmung Einsicht in seine Personalakte genommen hat. Er befürchtete, dass seinem Dienstherrn damit auch die Art seiner Erkrankung bekannt würde.

Der Dienstherr teilte mir dazu mit, dass er über einen Antrag des Petenten auf Übernahme der Kosten für die Unterhaltung seines Büros zu entscheiden hatte. Nach der Bürokostenentschädigungsverordnung Mecklenburg-Vorpommern kann ein Gerichtsvollzieher, der länger als zwei Wochen (zum Beispiel durch Krankheit) an der Ausübung seiner Tätigkeit gehindert ist, für die Dauer der Erkrankung eine Entschädigung für laufende notwendige Kosten erhalten. Um über diesen Antrag entscheiden zu können, waren die Angaben über den Beginn und die Dauer der Erkrankung erforderlich. Angaben über die Art der Erkrankung waren nicht in der Akte. Da die Beihilfeakten der Beamten beim Landesbesoldungsamt geführt werden, hatte das Oberlandesgericht auch keine Möglichkeit, diese einzusehen.

Gemäß § 88 Abs. 1 S. 1 Landesbeamtengesetz (LBG M-V) ist es zulässig, die Personalakte ohne Einwilligung des Beamten für Zwecke der Personalverwaltung oder Personalwirtschaft der obersten Dienstbehörde oder einer im Rahmen der Dienstaufsicht weisungsbefugten Behörde vorzulegen. Die Nutzung der An- und Abwesenheitszeiten war zur Entscheidung über den Antrag zulässig (§ 88 Abs. 1 S. 1 LBG M-V). Dies habe ich dem Petenten mitgeteilt. Einen Verstoß gegen datenschutzrechtliche Bestimmungen konnte ich nicht feststellen.

Herausgabe von Personalakten

In einem anderen Fall schilderte eine Petentin, dass sie ihren ehemaligen Arbeitgeber gebeten hatte, ihr die dort vorhandenen Personalunterlagen auszuhändigen. Der Arbeitgeber ist ihrer Bitte nicht nachgekommen und hat darauf hingewiesen, dass er keine Personalunterlagen mehr hat. Die Petentin bat mich, den Sachverhalt datenschutzrechtlich zu prüfen.

Ich habe den Arbeitgeber gebeten, mir mitzuteilen, ob und gegebenenfalls an wen und wann die Personalunterlagen übermittelt oder ob sie vernichtet worden sind. Meine Frage konnte nicht beantwortet werden, da dort keine Personalunterlagen der Petentin vorlagen. Aufzeichnungen, ob und wann die Personalunterlagen an die Petentin gesandt oder vernichtet wurden, existierten dort ebenfalls nicht, sodass der Sachverhalt nicht weiter aufgeklärt werden konnte. Eine Herausgabe von Personalunterlagen an ehemalige Beschäftigte ist nach den datenschutzrechtlichen Bestimmungen grundsätzlich nicht vorgesehen. Es gibt aber den datenschutzrechtlichen Auskunftsanspruch, nach dem beispielsweise auch die Herausgabe von Kopien möglich ist.

Arbeitgeber sind nach den Bestimmungen der §§ 27 ff. Bundesdatenschutzgesetz (BDSG) dazu verpflichtet, sorgsam mit den Personalunterlagen der Beschäftigten umzugehen. Dazu gehört auch die sichere Aufbewahrung sowie ein Nachweis darüber, wer die Personalunterlagen wann an wen übermittelt hat oder ob diese gelöscht bzw. vernichtet worden sind. Bei dem ehemaligen Arbeitgeber der Petentin war ein solcher Nachweis nicht vorhanden. Ich habe dem Arbeitgeber mitgeteilt, dass dieser Umgang mit Personalunterlagen nicht mit den datenschutzrechtlichen Bestimmungen vereinbar ist.

Inhalt des Personalfragebogens

Eine Stadtverwaltung beabsichtigte, einen Personalfragebogen herauszugeben, der künftig von den Bewerberinnen/Bewerbern bei Neueinstellungen und auch von den derzeit Beschäftigten ausgefüllt werden sollte. Die Datenschutzbeauftragte wollte von mir wissen, ob der Arbeitgeber auch nach der Schwerbehinderung von Bewerberinnen/Bewerbern oder von Beschäftigten fragen darf.

Nach den Bestimmungen des Allgemeinen Gleichbehandlungsgesetzes (AGG) ist die Benachteiligung unter anderem aus Gründen einer Behinderung zu verhindern oder zu beseitigen (§ 1 i. V. m. § 2 Abs. 2 Nr. 1 AGG). Daher ist die Frage nach der Schwerbehinderung im Bewerbungsverfahren unzulässig. Wenn eine solche Frage gestellt wird, kann die Bewerberin/ der Bewerber das Verfahren anfechten.

Im Bewerbungsverfahren darf ebenfalls nicht nach dem Familienstand, der Anzahl der Kinder, der Bankverbindung und Daten zur Sozialversicherung gefragt werden, da diese Angaben für die Auswahl nicht relevant sind. Erst, wenn eine Bewerberin/ein Bewerber eingestellt wird, dürfen weitere Daten erhoben werden, wie zum Beispiel Grad der Behinderung, Familienstand und Anzahl der Kinder, weil diese Angaben für Zwecke der Personalwirtschaft erforderlich sind.

Es ist jedoch nichts dagegen einzuwenden, wenn ein Arbeitgeber in einer Stellenanzeige darauf hinweist, dass Schwerbehinderte oder ihnen gleichgestellte Personen bevorzugt eingestellt werden. In diesem Fall liegt es an den Bewerberinnen/Bewerbern, ob sie mitteilen, dass eine Schwerbehinderung bzw. eine Gleichstellung vorliegt. Auch nach § 32 Abs. 3 des Entwurfs des Beschäftigtendatenschutzgesetzes darf ein Arbeitgeber im Bewerbungsverfahren keine Auskunft darüber verlangen, ob eine Schwerbehinderung oder eine Gleichstellung mit einer Schwerbehinderung nach § 68 des Neunten Buches Sozialgesetzbuch (SGB IX) vorliegt.

Angaben von Streikdaten auf Gehaltsmitteilungen

Von einem Kollegen wurde ich darauf aufmerksam gemacht, dass in den Gehaltsmitteilungen der Beschäftigten der dortigen Landesbehörden gegebenenfalls „Streik“ als Abwesenheitsgrund ausgewiesen wird. Zwar war der Grund für die taggenaue Unterbrechung (Beginn und Ende) auf der Gehaltsmitteilung verschlüsselt angegeben, die Erläuterungen dieser Schlüssel für das dort eingesetzte Entgeltberechnungsverfahren waren jedoch für jedermann zugänglich im Internet eingestellt. Sofern jemand die Gehaltsbescheinigung bei persönlichen Angelegenheiten Dritten vorzulegen hatte, bestand zumindest die Möglichkeit, dass diese Personen Informationen über die Streiktage des Betroffenen erhalten oder sich bei Schwärzung dieser Passage die Frage stellen, welche Daten eventuell verheimlicht werden.

Ich habe daher beim zuständigen Ministerium nachgefragt, wie in unserem Bundesland in dem beschriebenen Fall verfahren wird. Ich erhielt die Auskunft, dass bei streikbedingten Ausfalltagen und entsprechender Entgeltkürzung auf der ersten Seite des Abrechnungsblattes der Kürzungsbetrag mit dem Zusatz „Nettoüberzahlung“ sowie dem Hinweis „siehe Folgeblatt“ ausgewiesen wird. Für eine Vorlage der Gehaltsbescheinigung bei Dritten können Beschäftigte die erste Seite des Abrechnungsblattes nutzen. Dieses Verfahren ist aus datenschutzrechtlicher Sicht nicht zu beanstanden. Über dieses Verfahren habe ich auch die Kollegen informiert.

Amtsärztliche Bescheinigung über die Dienstfähigkeit

Im Mai 2011 wandte sich eine in der Landesverwaltung beschäftigte Mitarbeiterin an mich, weil ihr Arbeitgeber von einem Amtsarzt umfangreiche medizinische Daten über sie erhalten und in der Personalakte aufbewahrt hat. Ihr Arbeitgeber hatte sie zuvor aufgefordert, sich von einem Amtsarzt auf ihre Dienstfähigkeit untersuchen zu lassen.

Grundlage der Beschäftigung war neben dem Arbeitsvertrag der Tarifvertrag für den öffentlichen Dienst der Länder (TV-L). Der Arbeitgeber hatte sich bei seiner Aufforderung zur medizinischen Untersuchung durch den Amtsarzt auf § 3 Abs. 5 TV-L berufen. Die tarifvertragliche Regelung lautet: „Der Arbeitgeber ist bei begründeter Veranlassung berechtigt, Beschäftigte zu verpflichten, durch ärztliche Bescheinigung nachzuweisen, dass sie zur Leistung der arbeitsvertraglich geschuldeten Tätigkeit in der Lage sind. Bei dem beauftragten Arzt kann es sich um einen Amtsarzt handeln, soweit sich die Betriebsparteien nicht auf einen anderen Arzt geeinigt haben. Die Kosten dieser Untersuchung trägt der Arbeitgeber.“

Der Amtsarzt hatte in diesem Fall ein umfangreiches medizinisches Gutachten über die Mitarbeiterin erstellt, wie es bei Beamten üblich und nach den beamtenrechtlichen Regelungen zur Beurteilung der Dienstfähigkeit auch zulässig wäre. Der Amtsarzt hat im Gegensatz zu der behandelnden Therapeutin, die sie als wieder arbeitsfähig beurteilt hat, jedoch festgestellt, dass die Mitarbeiterin nicht dienstfähig sei. Außerdem hat er gefordert, dass bei einer erneuten Begutachtung ein Zeugnis der Therapeutin vorliegen müsse, das Aussagen zum Behandlungserfolg enthalte, gegebenenfalls müsse auch noch ein Zeugnis eines Facharztes eingeholt werden. Gegen die unterschiedliche Beurteilung hat sich die Mitarbeiterin durch einen Rechtsanwalt für Arbeitsrecht beraten lassen. Mich hat sie gebeten zu prüfen, ob das medizinische Gutachten des Amtsarztes Bestandteil der Personalakte sein darf. Diese Frage lässt sich nach dem Wortlaut des oben genannten Tarifvertrages klar mit nein beantworten, denn die Vertragsparteien haben sich verständigt, dass eine Bescheinigung über die Dienstfähigkeit eingeholt werden kann. Eine solche Bescheinigung darf daher nur die Aussage enthalten, dass ein Mitarbeiter dienstfähig oder nicht dienstfähig ist, gegebenenfalls auch noch eine Prognose, wie lange die Dienstunfähigkeit voraussichtlich andauern wird oder ob sie dauerhaft ist.

Auf meine Frage an die Landesregierung, ob es sinnvoll ist, die tarifvertragliche Regelung vor dem Hintergrund der Prüfung der Arbeitsfähigkeit eines Arbeitnehmers durch den Medizinischen Dienst der Krankenversicherung auf der Grundlage der gesetzlichen Krankenversicherung (z. B. §§ 275 ff Sozialgesetzbuch Fünftes Buch - SGB V) fortbestehen zu lassen, antwortete der Staatssekretär des Finanzministeriums unter Hinweis auf ein Urteil des Bundesarbeitsgerichts (BAG, Urteil vom 7. November 2002, 2 AZR 475/01), dass der öffentliche Arbeitgeber prüfen können muss, ob nicht nur Arbeitsunfähigkeit, sondern Dienstunfähigkeit vorliegt. Ein erwerbsunfähiger Arbeitnehmer handelt nämlich grob pflichtwidrig, wenn er die Stellung eines Rentenantrages schuldhaft verzögert. Aus diesem Grund muss der Arbeitgeber prüfen lassen können, ob Dienstfähigkeit oder Dienstunfähigkeit vorliegt.

In dem konkreten Fall habe ich dem Arbeitgeber empfohlen, das umfangreiche medizinische Gutachten aus der Personalakte zu entfernen und durch eine Bescheinigung über die Dienstfähigkeit zu ersetzen. Der Arbeitgeber hat die Empfehlung umgesetzt. Dem amtsärztlichen Dienst habe ich empfohlen, umfangreiche medizinische Gutachten über Mitarbeiter des öffentlichen Dienstes in der amtsärztlichen Dokumentation zu belassen und dem Arbeitgeber nur das Ergebnis in Form einer Bescheinigung mitzuteilen. Dazu liegt derzeit keine abschließende Entscheidung vor.

5.11 Verarbeitung von Schülerdaten

Schülerbefragung zur Berufsvorbereitung

Ein Lehrer hat mich auf eine umfangreiche Befragung von Schülerinnen und Schülern in einem Landkreis zum Zweck der Berufsvorbereitung aufmerksam gemacht. Er war sich nicht sicher, ob die 25 Seiten umfassende Datenerhebung mit den datenschutzrechtlichen Bestimmungen vereinbar ist, und hat mich gebeten, die Unterlagen zu prüfen.

Nach einer ersten Einschätzung habe ich festgestellt, dass die Befragung nicht die im Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) vorgegebenen Voraussetzungen erfüllt. So fehlte in den Unterlagen die erforderliche Aufklärung der betroffenen Schülerinnen und Schüler nach § 9 Abs. 3 DSG M-V. Auch die verwendete „Einverständniserklärung“, die eine Einwilligungserklärung nach § 8 DSG M-V hätte sein müssen, entsprach nicht den gesetzlichen Vorgaben. Darüber hinaus war fraglich, aus welchem Grund die Datenerhebung überhaupt personenbezogen und nicht anonymisiert erfolgte. Außerdem konnte ich den Unterlagen nicht entnehmen, welche technischen und organisatorischen Maßnahmen getroffen worden sind, um den Datenschutz und die Datensicherheit zu gewährleisten.

Wegen der offenen datenschutzrechtlichen Fragen habe ich dem Lehrer empfohlen, den Schülerinnen und Schülern vorläufig keine Teilnahme daran zu empfehlen. Darüber hinaus habe ich die für die Befragung zuständige Stelle um eine Stellungnahme und um Übersendung der Verfahrensbeschreibung nach § 18 DSG M-V, der Freigabeerklärung nach § 19 Abs. 1 DSG M-V sowie des Sicherheitskonzeptes nach § 22 Abs. 5 DSG M-V gebeten.

Der Projektleiter teilte mir daraufhin mit, dass er davon ausgegangen sei, dass die Befragung nicht gegen datenschutzrechtliche Bestimmungen verstößt. Er bat mich um ein Gespräch, um die offenen Fragen zu klären. Wir waren uns einig, dass die Rechtsgrundlage für die Datenverarbeitung die freiwillige Teilnahme der Schülerinnen und Schüler ist. Die Freiwilligkeit muss in der Information für Schülerinnen und Schüler sowie Eltern deutlich hervorgehoben werden. Außerdem ist darauf hinzuweisen, dass auch die Beantwortung jeder einzelnen Frage freiwillig ist, also der Fragebogen beispielsweise nicht vollständig beantwortet werden muss. Die Betroffenen müssen darüber hinaus umfassend über die Datenspeicherung und das Datenmanagement informiert werden. Es müssen Informationen gegeben werden, wie und durch welche Stellen die Daten verarbeitet werden, wie sie gegen Missbrauch geschützt sind. Diese Informationen sollten im Internet verfügbar sein. Darüber hinaus sollte das Datenmanagement so geändert werden, dass der Dienstleister, bei dem die Daten im Auftrag der Koordinierungsstelle des Landkreises gespeichert werden, nur pseudonymisierte Daten verarbeitet und die identifizierenden Daten zusammen mit dem Pseudonym auf einem Server der Koordinierungsstelle des Landkreises verarbeitet werden. Außerdem muss mit der speichernden Stelle ein Vertrag zur Datenverarbeitung im Auftrag geschlossen und ein Sicherheitskonzept erarbeitet werden, in dem Maßnahmen festzulegen sind, die verhindern, dass Daten zweckwidrig verarbeitet und genutzt werden.

Die besprochenen Hinweise für die Schülerbefragung wurden durch den Projektträger umgesetzt. Insbesondere das Datenmanagement ist geändert worden, sodass die Befragungsdaten unter einer Teilnehmernummer (Pseudonym) bei dem Dienstleister gespeichert werden. Aus den dort gespeicherten Daten kann eine natürliche Person ohne die Zuordnungsfunktion nicht mehr oder nur mit unverhältnismäßig hohem Aufwand bestimmt werden.

Die Zuordnungsliste zwischen Nummern und Namen der Teilnehmer wird in der Koordinierungsstelle sicher aufbewahrt. Die Schülerinnen und Schüler können auf der Grundlage der Hinweise und der Erläuterungen zur Datenverarbeitung entscheiden, ob sie an diesem Projekt zur Berufsvorbereitung teilnehmen oder nicht.

Über das Ergebnis meiner Beratung habe ich auch den Lehrer informiert und mich für den Hinweis bedankt, der wesentlich dazu beigetragen hat, dass die datenschutzrechtlichen Voraussetzungen bei der Umsetzung dieses Projektes berücksichtigt worden sind.

Veröffentlichung von Namen von Preisträgern an Schülerwettbewerben

Das Bildungsministerium bat mich um datenschutzrechtliche Beratung, ob datenschutzrechtliche Bedenken gegen eine Veröffentlichung einer Liste mit den Preisträgern bestehen, die an Schülerwettbewerben teilgenommen haben.

Die Teilnahme an einem Schülerwettbewerb dürfte immer freiwillig sein, sodass keine Schülerin und kein Schüler verpflichtet ist, sich einem solchen Wettbewerb zu stellen. In den Teilnahmebedingungen sollte daher auch beschrieben werden, in welcher Weise Daten der Teilnehmerinnen und Teilnehmer verarbeitet, insbesondere ob und in welcher Form sie gegebenenfalls veröffentlicht werden.

Dies vorausgesetzt, sind die Bestimmungen zur Datennutzung nach § 10 Abs. 2 Satz 2 und 3 DSGVO zu beachten. Danach dürfen, wenn keine Erhebung vorausgegangen ist, personenbezogene Daten für den Zweck genutzt werden, für den sie bei erstmaliger Speicherung bestimmt wurden. Empfänger übermittelter Daten dürfen diese dann nur für den bei ihrer Übermittlung bestimmten Zweck nutzen.

Die Daten der Preisträger, wie Name, Vorname, gegebenenfalls Klasse und Schule, dürfen unter diesen Voraussetzungen dann veröffentlicht werden.

5.12 Datenschutz im Verein

5.12.1 „Schwarzes Brett“ als Pranger

Regelmäßig erreichen mich Beschwerden und Anfragen, wenn insbesondere Kleingartenvereine quasi als „Strafmaßnahme“ am „Schwarzen Brett“ diejenigen Mitglieder öffentlich machen, die ihren Rasen nicht gemäht oder ihre Hecke nicht ordnungsgemäß geschnitten haben. Meist befindet sich das „Schwarze Brett“ auf dem Gelände des Gartenvereins und ist in erster Linie für Vereinsmitglieder bestimmt. Dennoch handelt es sich hier datenschutzrechtlich um eine Übermittlung dieser Angaben an einen nicht überschaubaren Kreis von Adressaten (Vereinsmitglieder und Besucher), die hiervon Kenntnis nehmen können, was „psychologisch“ ja auch beabsichtigt ist. Gegenüber den betreffenden Vorständen der Vereine ist meist schwer vermittelbar, dass dieses Verfahren datenschutzrechtlich unzulässig ist, auch wenn es in vielen Vereinen seit langer Zeit so praktiziert worden war.

Es handelt sich bei der Veröffentlichung um personenbezogene Daten, die nach § 28 Abs. 1 Nr. 1 und 2 BDSG nur übermittelt werden dürfen, wenn es für den Vereinszweck unbedingt erforderlich ist und zusätzlich vorher geprüft und abgewogen wurde, ob das schutzwürdige Interesse der betreffenden Vereinsmitglieder, das gegen die Veröffentlichung spricht, nicht überwiegt. Letzteres ist hier der Fall.

Auch wenn gemäß der Satzung des Vereins bestimmte Pflichten für die Vereinsmitglieder bestehen, so ist das geeignete Mittel des Vorstands bei Nichteinhaltung dieser Pflichten, sich direkt und ausschließlich mit den betreffenden Vereinsmitgliedern in Verbindung zu setzen. Dies gilt auch für die Erörterung und Durchsetzung entsprechender Konsequenzen bei nachhaltiger Pflichtverletzung. Die Kommunikation muss zwischen dem Vorstand und den Mitgliedern direkt erfolgen. Eine Veröffentlichung von personenbezogenen Angaben mit diskriminierendem Charakter an andere Vereinsmitglieder oder sonstige Dritte ist von der Rechtsgrundlage des § 28 Abs. 1 BDSG nicht gedeckt. Im Gegensatz dazu können beispielsweise Erreichbarkeitsdaten von bestimmten Funktionsträgern des Vereins in der Regel auf diese Weise bekannt gegeben werden. Auch persönliche Nachrichten mit einem Bezug zum Verein, wie Eintritte, Austritte etc. können in der Regel veröffentlicht werden, vorausgesetzt, dass dem Verein keine schutzwürdigen entgegenstehenden Interessen des Vereinsmitglieds bekannt sind, die einer solchen Veröffentlichung entgegenstehen.

Um datenschutzrechtliche Verstöße zu vermeiden, empfiehlt es sich deshalb für Vereine, bereits beim Eintritt eines neuen Mitglieds darauf aufmerksam zu machen, welche Ereignisse üblicherweise am Schwarzen Brett oder auch im Vereinsblatt veröffentlicht werden und die Einwilligung der Mitglieder zu solchen Mitteilungen einzuholen.

Durch ein transparentes Verfahren bei der Datenerhebung und bei der Datenübermittlung werden spätere Streitigkeiten vermieden und es wird Auseinandersetzungen vorgebeugt, die später nicht selten auch Behörden und Gerichte beschäftigen.

5.12.2 Gruppenversicherungsverträge

Im Berichtszeitraum bezogen sich mehrere Petitionen auf die Übermittlung von personenbezogenen Mitgliederdaten durch den Landesverband einer bundesweiten Hilfe- und Wohlfahrtsorganisation. Der Landesverband ist unter anderem Träger von Wohnheimen für ältere Menschen und von Anlagen für betreutes Wohnen. In einem Schreiben informierte er die Bewohnerinnen und Bewohner eines Altenwohnheimes (betreutes Wohnen) über die Möglichkeit des Abschlusses einer besonders günstigen Gruppenversicherung (Sterbegeld- und Unfallversicherung). Das Schreiben enthielt jedoch nicht nur die Information über einen besonders günstigen Versicherungsvertrag. Vielmehr wurde mitgeteilt, dass seitens des Verbandes beabsichtigt sei, dem Versicherungsunternehmen die für den Vertragsabschluss notwendigen Daten des jeweiligen Vereinsmitgliedes zu übermitteln, es sei denn, das Mitglied würde gegenüber dem Landesverband innerhalb einer Frist von vier Wochen einer solchen Übermittlung widersprechen. Falls kein Widerspruch eingehe, würden die Daten an die Versicherung weitergegeben. Außerdem würde das Vereinsmitglied in diesem Fall von einem Versicherungsvertreter kontaktiert werden.

Gruppenversicherungsverträge

sind Rahmenverträge zwischen Vereinen und Versicherungsunternehmen, die den Vereinsmitgliedern unter bestimmten Voraussetzungen den Abschluss von Einzelversicherungsverträgen zu günstigeren als den üblichen Konditionen ermöglichen. Ein Verein darf im Rahmen eines beabsichtigten Gruppenversicherungsvertrages dem Versicherungsunternehmen die personenbezogenen Daten der Mitglieder nur übermitteln, wenn eine ausdrückliche schriftliche Einwilligung der betreffenden Mitglieder vorliegt.

Ich habe dem Landesverband mitgeteilt, dass dieses Verfahren datenschutzrechtlich unzulässig ist. Dies gilt sowohl für Neu- als auch für Altmitglieder des Vereins, die bei Abschluss des Gruppenversicherungsvertrages bereits Vereinsmitglieder waren. Im vorliegenden Fall handelt es sich zudem um einen Verein, der als Landesverband einer großen Hilfe- und Wohlfahrtsorganisation im Gegensatz zu rein kommerziellen Vereinen einer besonderen ethischen Verpflichtung gegenüber seinen Mitgliedern unterliegt.

Hinsichtlich der Bewertung der schutzwürdigen Interessen der Mitglieder war ferner zu berücksichtigen, dass es sich im vorliegenden Fall um die Bewohner einer Anlage für betreutes Wohnen handelte. Somit waren neben dem Vereinszweck als Wohlfahrtsorganisation insbesondere die schutzwürdigen Interessen dieser hier betroffenen, vorwiegend alten (möglicherweise behinderten) Menschen zu berücksichtigen sowie die besondere Drucksituation beim Besuch dieser Menschen durch einen (geschulten) Versicherungsvertreter. Es kam hinzu, dass die Betroffenen im Anschreiben des Landesverbandes darum gebeten worden waren, sogenannte Überschussanteile (die den Abschluss der Versicherung voraussetzen) zugunsten der Wohlfahrtsorganisation zu spenden.

Der Landesverband wollte das beschriebene Verfahren zunächst nicht ändern und wies unter anderem auf seine Verpflichtung hin, seinen Mitgliedern eine kostengünstige und wirksame Unfallvorsorge zu ermöglichen. Ich habe die grundsätzlich positive Absicht des Verbandes nicht in Zweifel gestellt. Sie ersetzt jedoch nicht die Prüfung eines differenzierten Verfahrens zur Information und zur Einwilligung der Vereinsmitglieder bei der Vertragsanbahnung und rechtfertigt keinen Verstoß gegen die Vorschriften des Bundesdatenschutzgesetzes. Es ist grundsätzlich nichts dagegen einzuwenden, wenn ein Verein seine Mitglieder über eine kostengünstige und wirksame Unfallvorsorgemöglichkeit informiert.

Dennoch muss jedes Vereinsmitglied individuell entscheiden können, ob es aufgrund dieser Information der Weitergabe seiner Daten an eine Versicherung zustimmt und von einem Versicherungsvertreter aufgesucht werden möchte. Mit Beschluss vom 25./26. November 2010 haben die obersten Datenschutzaufsichtsbehörden festgestellt, dass für alle Mitglieder von Vereinen die vorherige Einholung einer informierten Einwilligungserklärung erforderlich ist.

Der Landesverband hat daraufhin sein Verfahren geändert und mitgeteilt, dass nunmehr auch bundesweit in allen Landesverbänden keine Mitgliederdaten mehr an Versicherungen oder für vergleichbare Zwecke weitergegeben werden.

6. Arbeitskreis „Technische und organisatorische Datenschutzfragen“

Hauptaufgabe des unter meiner Federführung tagenden Arbeitskreises „Technische und organisatorische Datenschutzfragen“ (AK Technik) ist die Beratung und Unterstützung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu datenschutztechnischen Fragen. Selbstverständlich unterstützt der AK Technik auch die Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich in gleicher Weise. Angesichts der zunehmenden Komplexität der in der öffentlichen Verwaltung und in der Wirtschaft genutzten Informations- und Kommunikationstechnik gewinnt diese Beratungsaufgabe ständig an Bedeutung.

6.1 Turnusmäßige Sitzungen

Im Berichtszeitraum habe ich wieder vier Sitzungen des Arbeitskreises organisiert.

Im Februar 2010 konnte ich meine Kollegen vom Bund und aus den Ländern zur **54. Sitzung** des AK Technik nach Berlin einladen. Die Vertretung des Landes Mecklenburg-Vorpommern beim Bund bot hervorragende Arbeitsbedingungen für die Mitglieder und Gäste des AK Technik. Ein Schwerpunkt dieser Sitzung betraf den Einsatz mobiler Endgeräte in der öffentlichen Verwaltung (siehe dazu auch Punkt 4.1.4). Ich hatte Vertreter der Firma Research in Motion Deutschland GmbH (RIM) eingeladen, um die Grenzen und Möglichkeiten des Einsatzes sogenannter BlackBerrys in der öffentlichen Verwaltung zu diskutieren. Eingeladen hatte ich auch Mitarbeiter des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Das BSI rät nach wie vor dringend vom Einsatz von Geräten der Firma RIM ab, obwohl inzwischen eine Reihe international anerkannter Institutionen die Technik positiv bewertet hat. Leider kam das BSI meiner Einladung nicht nach, sodass der Widerspruch zwischen diesen Bewertungen und den Empfehlungen des BSI nicht ausgeräumt werden konnte. Darüber hinaus befasste sich der AK Technik erstmals mit neuen elektronischen Messverfahren für Strom und Gas (Smart Meter und Smart Grid - siehe auch Punkt 4.1.3) und steckte den Rahmen für die weitere Behandlung des Themas ab.

Für die **55. Sitzung** des AK Technik im Oktober 2010 hatte ich angesichts der für das Jahr 2011 vorgesehenen Volkszählung den Zensus 2011 als Schwerpunkt gewählt (siehe Punkt 5.5.1). Das Statistische Amt unseres Landes hatte den AK Technik eingeladen, um gemeinsam mit Statistikvertretern des gesamten Bundesgebietes insbesondere die technischen Datenschutzfragen des bundesweiten Vorhabens zu beraten. Darüber hinaus spielten auf der Sitzung erneut die Datenschutzaspekte von Smart Metern eine wichtige Rolle. Der AK Technik formulierte eine EntschlieÙung zu diesem Thema, die von der Datenschutzkonferenz im November 2010 verabschiedet wurde (siehe <http://www.datenschutz-mv.de/dschutz/beschlue/entsch80.html#nr2>).

Zur **56. Sitzung** des AK Technik im Februar 2011 hatte die Saarländische Landesdatenschutzbeauftragte nach Saarbrücken eingeladen. Anlass dieser Einladung war unter anderem die Diskussion um Veröffentlichungen eines Wissenschaftlers der Universität des Saarlandes zu den Möglichkeiten des Löschens im Internet. Der betreffende Professor hatte sich bereit erklärt, sein Konzept den Mitgliedern des AK Technik vorzustellen und sich unter dem Dach des AK Technik einem wissenschaftlichen Streitgespräch mit einem prominenten Kritiker seiner Ideen (siehe <http://www-sec.uni-regensburg.de/research/streusand>) zu stellen.

Die Ergebnisse dieses Streitgespräches sind unter Punkt 4.2.3 ausführlich dargestellt. Die 56. Sitzung des AK Technik lieferte weitere wichtige Ergebnisse. So wurden die Orientierungshilfe zu Krankenhausinformationssystemen verabschiedet (siehe Punkt 4.5.2) und Mindestanforderungen an den technischen Datenschutz in medizinischen Netzen formuliert, die zu einer Entschließung der Datenschutzkonferenz führten (siehe Punkt 4.5.3).

Die **57. Sitzung** des AK Technik fand im September 2011 auf Einladung der SAP AG in Berlin statt. SAP hatte angeboten, den AK Technik über wichtige Datenschutzentwicklungen einiger Produkte zu informieren und die Position des Unternehmens zum Thema Cloud-Computing zu erläutern.

Um ein möglichst umfassendes Bild zu Datenschutzaspekten bei Cloud-Computing zu erhalten, hatte ich weitere Unternehmen eingeladen, ihre Cloud-Computing-Projekte vorzustellen. Während dieser Sitzung verabschiedete der AK Technik dann die Orientierungshilfe zum Thema Cloud-Computing (siehe Punkt 4.1.1), die von einer Arbeitsgruppe des AK Technik unter Federführung des Hessischen Datenschutzbeauftragten erarbeitet worden war. Der Arbeitskreis befasste sich in dieser Sitzung weiterhin mit Datenschutzfragen des neuen Internetprotokolls IPv6. Der Datenschutzkonferenz wurde ein Entschließungsentwurf mit ersten kurzen Erläuterungen vorgelegt (siehe Punkt 4.1.2).

Die Mitglieder des AK Technik beschlossen, angesichts der besonderen Bedeutung von IPv6 eine Arbeitsgruppe einzurichten, um die Risiken und Chancen dieses neuen Protokolls für den Datenschutz zu untersuchen und zu bewerten.

6.2 Workshops des AK Technik

Nachdem das Konzept der gemeinsamen Workshops für Techniker und Juristen der Datenschutzdienststellen von Bund und Ländern in den vergangenen Jahren auf breite Zustimmung gestoßen ist (siehe Neunter Tätigkeitsbericht, Punkt 4.2), habe ich auch in diesem Berichtszeitraum wieder zwei Workshops organisiert und durchgeführt.

Im Juni 2010 führte ich gemeinsam mit der Bundesdruckerei und dem Bundesinnenministerium einen Workshop zum neuen Personalausweis durch (siehe Neunter Tätigkeitsbericht, Punkt 2.4.9). In den Räumen der Bundesdruckerei in Berlin konnten wir uns detailliert über den Stand der Einführung des neuen Personalausweises informieren. Die Mitarbeiter berichteten über den Stand der Feldtests, das neu eingerichtete Serviceportal und die Durchsetzung datenschutzrechtlicher Vorgaben in der Bundesdruckerei. Der offene und konstruktive Meinungs austausch hat einerseits zu einem besseren Verständnis für die gesamten Abläufe bei der Beantragung, Produktion und Auslieferung des Personalausweises beigetragen, andererseits aber auch noch weitere Möglichkeiten zur Verbesserung des Datenschutzes im gesamten Verfahren aufzeigen können.

Der Workshop im Juli 2011 befasste sich mit den Datenschutzfragen von IPv6. Eingeladen waren renommierte Fachleute aus Wirtschaft und Verwaltung, um gemeinsam mit den Datenschützern die Chancen und Risiken des neuen Internetprotokolls zu beraten und die künftigen Tätigkeitsschwerpunkte für alle Beteiligten festzulegen.

Im Ergebnis wurde deutlich, welcher Handlungsbedarf vorhanden ist, um nicht nur die Risiken des neuen Protokolls beherrschen, sondern um insbesondere die Chancen der neuen Technologie nutzen zu können (siehe Punkt 4.1.2). Mit dem Bundesinnenministerium wurde eine engere Zusammenarbeit vereinbart und die vom AK Technik gegründete Arbeitsgruppe sprach sich für eine kontinuierliche Einbindung externer Fachleute aus.

6.3 Gemeinsame Weiterbildung

In meinem Neunten Tätigkeitsbericht (siehe dort Punkt 4.3) hatte ich bereits über die von mir organisierten gemeinsamen Weiterbildungsveranstaltungen für die Datenschutzbeauftragten von Bund und Ländern berichtet. Im laufenden Berichtszeitraum konnte ich eine weitere Veranstaltung anbieten. Auf Anregung des Beauftragten für den Datenschutz in der Bundeswehr konnte ich gemeinsam mit anderen Kollegen vom Bund und aus den Ländern im März 2010 in Bonn an einem Datenschutz-Workshop der Bundeswehr zum Thema „Datenschutz und IT-Sicherheit bei SAP“ teilnehmen. Die im SAP-Workshop des Vorjahres erworbenen Kenntnisse konnten weiter vertieft werden. Schwerpunktmäßig wurden in Bonn Datenschutzaspekte von SAP-Anwendungen im Personalbereich erläutert und Hinweise für die Sicherheitsinspektionen und die Datenschutzkontrollen solcher Systeme gegeben.

6.4 Technology Subgroup - Zusammenarbeit auf europäischer Ebene

Die Artikel-29-Gruppe wurde im Rahmen der Richtlinie 95/46/EG des Europäischen Parlaments als zentrales Koordinierungsgremium für die datenschutzrechtliche Aufsicht innerhalb der Europäischen Union eingerichtet. Ähnlich dem AK Technik auf nationaler Ebene dient dabei die „Technology Subgroup“ im internationalen Kontext als Beratungs- und Unterstützungsgremium für die Artikel-29-Gruppe. Um die Synergieeffekte der sich überschneidenden Themen in der Technology Subgroup und dem AK Technik sinnvoll zu nutzen, bin ich als ständiger Vertreter der deutschen Landesdatenschutzbeauftragten Mitglied der Technology Subgroup. So ist es mir einerseits möglich, den AK Technik über die laufenden Entwicklungen im europäischen Rahmen zu informieren, und andererseits erlaubt mir die Mitgliedschaft, wichtige nationale Themen und Standpunkte des AK Technik auf internationaler Ebene einzubringen bzw. zu vertreten.

7. Informationsfreiheitsgesetz Mecklenburg-Vorpommern (IFG M-V)

7.1 Novellierung des Informationsfreiheitsgesetzes Mecklenburg-Vorpommern

Das novellierte Gesetz zur Änderung des Informationsfreiheitsgesetzes und zur Änderung des Landesdatenschutzgesetzes ist am 28. Mai 2011 in Kraft getreten. Zum Änderungsentwurf des Informationsfreiheitsgesetzes (Drucksache 5/4191) bin ich angehört worden. Ich habe dazu wie folgt schriftlich Stellung genommen:

Die vorgeschlagenen Änderungen im Gesetzentwurf habe ich überwiegend begrüßt. Darüber hinaus hatte ich noch folgende Empfehlungen:

Veröffentlichungspflichten

Das Innenministerium Mecklenburg-Vorpommern hat auf seiner Seite im Internet bereits einige Verwaltungsvorschriften veröffentlicht. Dies könnte noch ausgebaut werden. Es sollte eine gesetzlich verankerte Veröffentlichungspflicht für sämtliche Verordnungen und Verwaltungsvorschriften geben, soweit diese nicht geheim zu halten sind. Aktenpläne, Informationssammlungen etc. sollten ebenfalls proaktiv auf den Internetseiten der jeweiligen Behörden veröffentlicht werden.

Herausgabepflicht von Kopien bei gleichzeitiger Akteneinsichtnahme

Aus informationsfreiheitsrechtlicher Sicht sollte das Recht auf Herausgabe von Kopien auch bei gleichzeitiger Akteneinsichtnahme eingefügt werden. Bisher ist die Rechtslage so, dass, wenn die Behörde ausreichende zeitliche, sachliche und räumliche Möglichkeiten für den Informationszugang zur Verfügung stellt, nicht gleichzeitig auch ein Anspruch auf Kopien besteht. In der Praxis hat sich herausgestellt, dass Antragsteller häufig, nachdem oder während sie Akteneinsicht nehmen, einen Teil oder Extrakt der Dokumente mitnehmen möchten. Es ist nicht einzusehen, dass sich Antragsteller bei umfangreichen Aktenvorgängen mühsam handschriftlich Notizen machen müssen. Das Verwaltungsgericht Schwerin hat wegen der gegenwärtigen Gesetzeslage in einem Fall entschieden, dass der Antragsteller einen Anspruch auf ermessensfehlerfreie Entscheidung der Behörde hat und danach die Kopien ggf. (zusätzlich) bekommt. Aus meiner Sicht ist jedoch nicht nachvollziehbar, dass ein Antragsteller stets erst im Klagewege sein Recht bekommt.

Abwägungsklausel beim Vorliegen von Betriebs- und Geschäftsgeheimnissen

Aus informationsfreiheitsrechtlicher Sicht ist eine Abwägungsklausel beim Vorliegen von Betriebs- und Geschäftsgeheimnissen dringend erforderlich. Die Beratungspraxis hat gezeigt, dass das Fehlen einer solchen zu einer reflexartigen Ablehnung schon bei der Behauptung des Vorliegens solcher Betriebs- und Geschäftsgeheimnisse führt. Es sollte eine Abwägung des öffentlichen Interesses mit dem schutzwürdigen Interesse des Betroffenen an der Geheimhaltung stattfinden, wie dies schon jetzt im Umweltinformationsgesetz Standard ist.

Offenlegung von Verträgen zwischen Staat und Unternehmen

Ich hatte vorgeschlagen, alle Verträge zwischen Staat und privaten Unternehmen offenzulegen. Verträge beinhalten Angaben, die für bestimmte Leistungen bezahlt werden. Erfahren zu können, ob die Leistungen mit den zuvor ausgeschriebenen Anforderungen übereinstimmen und in welcher Höhe Steuermittel dafür aufgewendet werden, dient der Haushaltstransparenz und der Verhinderung von Korruption. Das Interesse der Öffentlichkeit an den Verträgen ist groß, die Bereitschaft der Vertragspartner, sie offenzulegen, meist gering. Die pauschale Zurückweisung von auf solche Verträge gerichtete Auskunftsbegehren unter Hinweis auf Vertraulichkeitsabreden und Betriebs- und Geschäftsgeheimnisse ist nicht länger hinnehmbar. Daher hält es die Konferenz der Informationsfreiheitsbeauftragten für dringend geboten, den Zugang zu entsprechenden Verträgen in den Informationsfreiheitsgesetzen sicherzustellen, wie dies jüngst im Berliner Informationsfreiheitsgesetz (GVBl Berlin, Seite 358) geschehen ist, vergleiche hierzu: Entschließung der 21. Konferenz der Informationsfreiheitsbeauftragten Deutschlands am 13. Dezember 2010 in Kleinmachnow unter: www.informationsfreiheit-mv.de/inffrei/beschlu/entsch21.

Höchstrahmen für Gebühren nach der Informationskostenverordnung M-V senken

Bereits im Gesetzgebungsverfahren hatte ich darauf hingewiesen, dass der Gebührenrahmen der Anlage zum Gebühren- und Auslagenverzeichnis mit bis zu 1000 € zu hoch ist. Im Vergleich dazu beläuft sich bei der Informationsgebührenverordnung des Bundes der Gebührenrahmen bei vergleichbaren Gebührentatbeständen nur auf bis zu 500 €. Es ist nicht nachzuvollziehen, warum die Gebühren in Mecklenburg-Vorpommern höher sein sollen als beim Bund. Ich habe darauf hingewiesen, dass die Inanspruchnahme des Informationsfreiheitsgesetzes sich nicht abschreckend auf einkommensschwächere Bürgerinnen und Bürger auswirken darf.

Meine Empfehlungen zu den Punkten Veröffentlichungspflichten, Abwägungsklausel beim Vorliegen von Betriebs- und Geschäftsgeheimnissen, Offenlegung von Verträgen zwischen Staat und Unternehmen wurden nicht bzw. nur teilweise umgesetzt. Meine Empfehlung zu dem Punkt Herausgabepflicht von Kopien bei gleichzeitiger Akteneinsichtnahme, welcher in der Praxis große Relevanz hat, wurde umgesetzt. Hinsichtlich der Informationskostenverordnung hat das Innenministerium mir inzwischen einen Entwurf zukommen lassen, in dem mein Vorschlag zur Gebührenreduzierung und darüber hinaus auch weitere informationsfreundliche Änderungen berücksichtigt worden sind.

7.2 Fachtagung 2010: Informationsfreiheit - die nächste Generation

Auf der Fachtagung zum Thema „Informationsfreiheit - die nächste Generation“ diskutierten im Jahr 2010 in Schwerin rund 150 Teilnehmerinnen und Teilnehmer, unter anderem aus den Bereichen Verwaltung, Politik und Informationsfreiheit, über ihre Erfahrungen mit den Informationsfreiheitsgesetzen.

In seinem Grußwort zog Thomas Lenz, Staatssekretär im Innenministerium Mecklenburg-Vorpommern, eine Bilanz über vier Jahre Informationsfreiheitsgesetz in Mecklenburg-Vorpommern. Danach seien die Teilhabe der Bürgerinnen und Bürger am Verwaltungshandeln und die Transparenz von Verwaltungshandeln zentrale Voraussetzungen für die effektive Wahrnehmung demokratischer Mitwirkungsrechte. Die Gewährung des freien Zugangs zu Informationen der Verwaltung auf der Grundlage des Informationsfreiheitsgesetzes habe sich in der Praxis grundsätzlich bewährt. Die Befürchtungen einer Überlastung öffentlicher Stellen hätten sich bislang nicht bestätigt.

Prof. Dr. Winfried Hassemer widmete sich in seinem Vortrag dem prinzipiellen Verhältnis von Datenschutz und Informationsfreiheit. Scheinbar existiere ein Gegensatz zwischen Datenschutz und Informationsfreiheit. So bedeute Datenschutz zuerst einmal Verbergen, Zurückhalten von Informationen und Abwehr gegen Offenlegung. Informationsfreiheit jedoch besage das genaue Gegenteil, und zwar: Aufdecken, Zugang und Offenheit. Anhand des Volkszählungsurteils zeigte Professor Hassemer in gelungener Weise auf, dass der mündige Bürger beides brauche, sowohl Orientierung als auch Schutz. Insofern gehörten Informationsfreiheit und Datenschutz geschwisterlich zusammen.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Peter Schaar, berichtete über seine Erfahrungen seit Inkrafttreten des Informationsfreiheitsgesetzes des Bundes. Er kritisierte, dass Deutschland noch weit davon entfernt sei, den freien Informationszugang gegenüber öffentlichen Stellen als bedeutsame Flankierung demokratischer Entscheidungsprozesse zu begreifen, wie dies in anderen Staaten bereits der Fall sei. Die behördliche Praxis ermutige in vielen Fällen nicht gerade die Wahrnehmung des Rechts auf Informationszugang. Die Ausnahmetatbestände des IFG bedürften einer gründlichen Überarbeitung. Unbefriedigend sei auch das Nebeneinander verschiedener Informationsansprüche nach dem Umweltinformationsgesetz, dem Verbraucherinformationsgesetz und dem Informationsfreiheitsgesetz.

Der Landesbeauftragte (Information Commissioner) für die Informationsfreiheit (Freedom of Information) Westaustralien, Sven Bluemmel, erläuterte seine Erfahrungen mit dem dortigen Informationsfreiheitsgesetz, welches 1992 in Kraft gesetzt wurde. Pro Jahr würden dort rund 12.000 Anträge an Behörden gestellt, zwischen 100 und 200 kämen aufgrund eines Einspruchs vor den Landesbeauftragten, und diese seien rechtlich oft kompliziert.

Prof. Dr. Michael Rodi fasste die Ergebnisse der Evaluierung des Informationsfreiheitsgesetzes Mecklenburg-Vorpommern zusammen. Zwar habe sich das Informationsfreiheitsgesetz grundsätzlich bewährt. Zu kritisieren sei jedoch, dass eine proaktive Verbreitung von in den Behörden vorhandenen Informationen aufgrund fehlender gesetzlicher Verpflichtung nicht stattfinde. Auch sei problematisch, dass der Gesetzgeber der Verwaltung keine Maßstäbe vorgebe, ob und inwieweit zur Förderung des Informationszugangs vom Prinzip der vollen Kostendeckung abgewichen werden könnte.

Prof. Dr. Herbert Kubicek stellte die Evaluierung des bremischen Informationsfreiheitsgesetzes dar. Er kam zu dem Ergebnis, dass die statistische Berichtspflicht abgeschafft werden sollte, der Ausbau des zentralen Registers und der Veröffentlichungspflicht durch halbjährliche Veröffentlichungspläne der Dienststellen vorangetrieben werden sollten und die Rolle der IFG-Beauftragten als Vermittler bei Verweigerungen von Informationsbegehren konkretisiert werden sollte.

Prof. Dr. Wilhelm Mecklenburg führte in seinem Vortrag aus, warum das IFG seinen „Praxistest vor Gericht“ nicht bestanden habe. Informationen stellen ein leicht verderbliches Gut da und seien mit dem jetzigen Prozessrecht wegen der langen Dauer häufig nicht zeitnah zu erlangen. Er schlägt daher eine Korrektur sowohl des Prozessrechts als auch der Informationsfreiheitsgesetze vor. Bei den Informationsfreiheitsgesetzen gehe der Änderungsbedarf in die Richtung, dass bestimmte Kataloge von Dokumenten festgelegt werden sollten, die immer freizugeben sind.

Informationsanspruch auch gegenüber Privaten? - Diese Frage stellte Prof. Dr. Hansjürgen Garstka in seinem Vortrag. Er zog einen Vergleich zu den datenschutzrechtlichen Abwehrrechten, die im Laufe der Zeit auch auf den privaten Sektor („nicht-öffentliche Stellen“) ausgedehnt wurden. Vergleichbares müsse auch bei der Geltendmachung der Informationsrechte gelten. Er gab zu bedenken, dass zurzeit noch verfassungsrechtliche Bedenken geltend gemacht werden insofern, als im privaten Bereich Grundrechte von Informationsverpflichteten entgegenstehen würden.

Prof. Dr. Albert von Mutius befasste sich in seinem Beitrag mit der Frage, ob wir in Deutschland ein Informationsgrundrecht brauchen, und zeigte die verfassungsrechtlichen Möglichkeiten und Grenzen auf.

Die Beiträge der Fachtagung 2010 sind zu finden unter: www.datenschutz-mv.de/dschutz/veransta/inffrei/index-inf.html

7.3 Open Data/Open Government

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) hat auf ihrer 22. Sitzung im Mai 2011 auf Vorschlag des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit die Einsetzung einer Arbeitsgruppe beschlossen, die sich mit der Open Government Strategie der Bundesregierung befassen sollte. An der Arbeitsgruppe, die am 28. September 2011 in Schwerin getagt hat, haben unter der Federführung des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern die Kolleginnen und Kollegen aus dem Bund, aus Berlin, Brandenburg, Bremen und aus Schleswig-Holstein teilgenommen.

Die Bundesregierung, viele Landesregierungen und zahlreiche Kommunen haben sich ein offeneres Handeln nach den Prinzipien von Open Government zum Ziel gesetzt.

Open Government bedeutet die weitere Öffnung des Staates gegenüber Bürgerinnen und Bürgern, Wirtschaft und Wissenschaft. Dadurch soll mehr Transparenz und Teilhabe und somit mehr direkte Demokratie geschaffen werden. Über eine gemeinsame Plattform sollen Bürgerinnen und Bürger an die weiterhin dezentral gelagerten Informationen der öffentlichen Stellen über entsprechende Links gelangen.

Aus Sicht der Informationsfreiheitsbeauftragten wird dieses Projekt der proaktiven Veröffentlichung von staatlichen Informationen sehr begrüßt. Bisher verhält es sich so, dass zwar viele Landesregierungen, so auch Mecklenburg-Vorpommern, sogenannte Dienstleistungsportale auf ihren Internetseiten haben und dort die unterschiedlichsten Leistungen anbieten, wie den elektronischen Zugang zu Gesetzen, Verordnungen, Verwaltungsvorschriften und den Zugang zu „Lebenslagen“. Das Zur-Verfügung-Stellen von Informationen ist jedoch nicht verpflichtend, sondern erfolgt auf freiwilliger Basis.

Die Arbeitsgruppe der Informationsfreiheitsbeauftragten ist der Auffassung, dass es eine Verpflichtung aller öffentlichen Stellen auf den unterschiedlichen Ebenen geben muss, von sich aus Informationen zu veröffentlichen. Um dies umzusetzen, sollte die Verpflichtung durch ein Gesetz festgeschrieben werden. Aus informationsfreiheitsrechtlicher Sicht bieten sich hierzu die Informationsfreiheitsgesetze an. Vorbildhaft sind beispielsweise das Bremische Informationsfreiheitsgesetz und das Bremische Informationsregister. Bürgerinnen und Bürger können dort eine Vielzahl von Informationen aus allen Politikfeldern erlangen, zum Beispiel auch beschlossene Senatsvorlagen und Gutachten. Das zentrale Informationsregister verschafft einen erleichterten Zugang ohne großen Suchaufwand.

Da die meisten Gesetze proaktive Veröffentlichungspflichten nicht vorsehen, ist hier noch einiges an gesetzgeberischem Aufwand in den Ländern notwendig. Die Bundesländer, die noch kein Informationsfreiheitsgesetz haben, müssten entsprechend „nachziehen“. Die 22. Konferenz der Informationsfreiheitsbeauftragten Deutschlands hat dazu auf ihrer Sitzung am 23. Mai 2011 eine entsprechende Entschließung unter der Überschrift „Informationsfreiheit - Lücken schließen“ verabschiedet, siehe hierzu unter www.informationsfreiheit-mv.de/inffrei/beschlu/entsch22.html.

Ein weiterer Punkt der Open Government Strategie ist die Teilhabe. Darunter wird die Mitwirkung an staatlichen Entscheidungsprozessen durch Bürgerinnen und Bürger verstanden. Die Arbeitsgruppe versteht darunter beispielsweise auch das Zur-Verfügung-Stellen von Gesetzesvorhaben auf Online-Plattformen. In diesem Zusammenhang weise ich darauf hin, dass in der Vergangenheit auf Regierungsplattformen bestimmte Gesetzentwürfe, wie beispielsweise die Novellierung des Verbraucherinformationsgesetzes, veröffentlicht wurden. Dadurch wurde einer breiten Öffentlichkeit - nicht nur Verbänden oder anderen Organisationen - die Möglichkeit gegeben, aktiv mitzudiskutieren. Derartige Instrumente werden noch viel zu selten genutzt.

In diesem Zusammenhang ist auch die positive Entwicklung in der Rechtsprechung zu beobachten, welche der Informationsfreiheit - auch was die Kenntnisnahme von Regierungsinformationen anbelangt - den Rücken stärkt. So hat sich der 12. Senat des Oberverwaltungsgerichts Berlin-Brandenburg in seinem Urteil vom 5. Oktober 2010 (Aktenzeichen: OVG 12 B 5.08) mit der Frage auseinandergesetzt, ob und welche Regierungsinformationen unbedingt geheim bleiben müssen. Streitgegenstand war der Informationszugang zu Materialien zu einem Gesetzgebungsvorhaben. Das Gericht hat dort entschieden, dass das Bundesministerium der Justiz bei der Vorbereitung von Gesetzentwürfen im Rahmen des Initiativrechts der Bundesregierung nach Art. 76 Abs. 1 Grundgesetz als Behörde handelt und ministerielle Behördentätigkeit im Sinne von § 1 Abs. 1 Satz 1 IFG (Bund) ausübt. Das Bundesverwaltungsgericht hat diese Entscheidung bestätigt.

Ein weiterer wichtiger Punkt ist aus Sicht der Arbeitsgruppe das grundsätzlich kostenfreie Zur-Verfügung-Stellen von öffentlichen Daten. Auch darf die Absicht der Datenverwendung keine Rolle spielen. Es darf kein Ausforschen seitens der Behörden stattfinden.

Diese Auffassung ist von der für die digitale Agenda zuständigen EU-Kommissarin Neelie Kroes auf einer Pressekonferenz am 12. Dezember 2011 in Brüssel bestätigt worden. Die Kommissarin legte einen Novellierungsvorschlag der EU-Richtlinie von 2003 über die Weiterverwendung von Informationen des öffentlichen Sektors vor. Vorgesehen ist darin, dass grundsätzlich alle Informationen, die von öffentlichen Stellen zugänglich gemacht werden, zu beliebigen Zwecken weiterverwendet werden können, soweit nicht Urheberrechte Dritter geschützt sind.

Werden Gebühren für die Weiterverwendung von Dokumenten erhoben, so sollten diese grundsätzlich auf die durch die Vervielfältigung und Weiterverbreitung verursachten Zusatzkosten beschränkt sein, sofern nicht nach objektiven, transparenten und überprüfbaren Kriterien eine Ausnahme hiervon gerechtfertigt ist, vergleiche hierzu Erwägungsgrund 12 des Richtlinienentwurfs unter http://ec.europa.eu/information_society/policy/psi/index_en.htm.

Auch hat sich die EU-Kommissarin gegen teure Lizenzen ausgesprochen. Vielmehr spricht sie sich für offene Lizenzen aus.

So heißt es im Erwägungsgrund 13 der vorstehend genannten Richtlinie wörtlich: „Offene Lizenzen, die online erteilt werden, die umfangreichere Weiterverwendungsrechte ohne technische, finanzielle oder geografische Einschränkungen gewähren und die auf offenen Datenformaten beruhen, können in diesem Zusammenhang eine wichtige Rolle spielen. Deshalb sollten die Mitgliedstaaten die Verwendung offener behördlicher Lizenzen fördern“. Meiner Auffassung nach müssen daher auch die bisher überwiegend kostenintensiven Lizenzvereinbarungen zum Beispiel auf Geoportalen in Deutschland auf den Prüfstand gestellt werden.

Die Arbeitsgruppe wird dem Bundesinnenministerium über die Konferenz der Informationsfreiheitsbeauftragten Deutschlands eine Stellungnahme zu dieser Thematik zuleiten.

7.4 Verwaltungskosten für Auskünfte nach dem IFG M-V

Nach § 13 Abs. 1 des Informationsfreiheitsgesetzes Mecklenburg-Vorpommern (IFG M-V) sind für Amtshandlungen nach diesem Gesetz Gebühren und Auslagen zu erheben. Details und die Kostenhöhe hierzu regelt die Informationskostenverordnung (IFGKostVO M-V).

Obwohl einzuschätzen ist, dass aufgrund der zumeist erteilten einfachen Auskünfte in der Mehrzahl der Fälle keine Gebühren erhoben werden (nach § 13 Abs. 1 Satz 2 IFG M-V sind diese gebührenfrei), macht die Erhebung von Verwaltungskosten in der Praxis durchaus Probleme. Dies liegt aus meiner Sicht zum einen daran, dass die IFGKostVO M-V im kommunalen Bereich nur für die Erteilung von Auskünften, die dem Komplex der weisungsgebundenen Aufgaben entstammen, Anwendung findet (für Selbstverwaltungsangelegenheiten gilt kommunales Satzungsrecht).

Zum anderen entsteht bei mir der Eindruck, dass die Möglichkeit der Kostenerhebung durch einige Behörden augenscheinlich auch dafür genutzt wird, um mit der Androhung einer bestimmten Gebührenhöhe bei Antragstellern eine derartig abschreckende Wirkung zu erzielen, dass diese in der Folge von ihrem ursprünglich bestehenden Informationsbegehren Abstand nehmen.

Die IFGKostVO M-V sieht im Fall einer umfangreichen Auskunft eine Gebührenerhebung vor. Dies ist insbesondere dann der Fall, wenn Daten zum Schutz privater oder öffentlicher Interessen abgetrennt oder geschwärzt werden müssen. Aufgrund mir vorliegender Petitionen habe ich in mehreren Fällen Behörden empfohlen, die bereits veranlasste oder vorgesehene Gebührenerhebung unter Berücksichtigung dieses Aspektes noch einmal kritisch zu überprüfen.

Durch das Innenministerium wird derzeit die IFGKostVO M-V überarbeitet. Dabei ist neben dem aus meiner Sicht wesentlichen Punkt, dass sich die Maximalgebühren erheblich reduzieren, auch eine konkrete Formulierung der Gebührentatbestände mit vorgesehen. Aus dem mir vorliegenden Entwurf geht hervor, dass sich die Maximalgebühr auf meine Empfehlung hin von jetzt 1.000,00 Euro auf 500,00 Euro reduziert.

Dies entspricht unter anderem auch den Gebührensätzen, die der Bund für die Amtshandlungen nach dem Bundes-IFG vorsieht. Die damit einhergehende Harmonisierung der Gebührentatbestände begrüße ich. Dennoch sollte die Zielstellung (im Sinne der Informationsfreiheit) sein, so weit wie möglich auf eine Kostenerhebung zu verzichten beziehungsweise restriktiv von der Gebührenerhebung Gebrauch zu machen.

7.5 Muss jede Information herausgegeben werden?

Ein Petent informierte mich darüber, dass er beim Ministerium für Energie, Infrastruktur und Landesentwicklung Mecklenburg-Vorpommern einen Antrag auf Informationszugang zu verkehrsrechtlichen Sachverhalten gestellt hatte. Der Informationszugang zu Fragen, die in Verbindung mit einer Auskunft zu Straßenverzeichnissen standen, wurde durch das Ministerium nicht gewährt. Vielmehr wurde der Petent auf die zuständige Straßenaufsichtsbehörde, welche nicht das Ministerium war, verwiesen.

§ 10 Abs. 3 Satz 2 IFG M-V verpflichtet eine Behörde, dem Antragsteller unverzüglich die zuständige Behörde zu benennen. Voraussetzung hierfür ist allerdings, dass die Behörde, an die der Antragsteller sein Begehren gerichtet hatte, nicht über die begehrten Informationen verfügt.

Das Ministerium hat im vorliegenden Fall verkannt, dass es bei einem Informationszugang nach dem IFG M-V nicht darauf ankommt, welche Behörde für die eigentliche Aufgabenerfüllung (hier: Führen von Straßenverzeichnissen) zuständig ist. Das Gesetz stellt vielmehr auf das Vorhandensein von Informationen ab (§ 1 Abs. 1 und 2 IFG M-V).

Aus diesem Grund habe ich dem Ministerium für Energie, Infrastruktur und Landesentwicklung Mecklenburg-Vorpommern empfohlen, die begehrten Informationen, sofern sie dort vorhanden sind und keine Ablehnungsgründe im Sinne der §§ 5 bis 8 IFG M-V vorliegen, zugänglich zu machen. Dieser Empfehlung ist das Ministerium gefolgt.

7.6 Immer Ärger mit den Kosten!

Ein Bürger hatte bei einem Verwaltungsgericht die Einsicht in den beruflichen Lebenslauf eines Richters beantragt. Das Verwaltungsgericht leitete diesen Antrag an die personalaktenführende Stelle (Justizministerium) weiter.

Von dort erhielt der Antragsteller die Antwort, dass ihm keine Einsicht gewährt wird, da die Akte schutzwürdige personenbezogene Daten enthält. Hiergegen legte der Antragsteller Widerspruch ein. Dieser wurde durch das Ministerium zurückgewiesen. In dem Widerspruchsbescheid wurde dem Antragsteller mitgeteilt, dass er die Kosten des Verfahrens zu tragen habe, obwohl der Ursprungsbescheid kostenfrei ergangen ist.

Ich habe das Justizministerium darauf hingewiesen, dass nach § 13 Abs. 1 IFG M-V für Amtshandlungen nach diesem Gesetz Gebühren und Auslagen zu erheben sind. Nach der IFGKostVO M-V (Tarifstelle 4) kann bei einer Zurückweisung eines Widerspruchs gegen eine Sachentscheidung aber nur dann eine Gebühr erhoben werden, wenn für diese bereits eine Gebühr verlangt wurde.

Da im vorliegenden Fall für den Ursprungsbescheid keine Kosten festgesetzt wurden, kann auch für den Erlass eines Widerspruchsbescheides keine Gebühr erhoben werden. Ich habe dem Justizministerium deshalb empfohlen, vorliegend auf die Gebührenerhebung zu verzichten. Dieser Empfehlung ist das Justizministerium gefolgt und hat den Kostenfestsetzungsbescheid aufgehoben.

7.7 Auskunftsbegehren über Spenden an einen Sportverein

Ein Bürger wollte von einer Stadt Informationen haben über die Zahlungen einer Wohnungsgesellschaft an einen Sportverein. Die Stadt lehnte diesen Antrag ab und verwies den Antragsteller dabei auf ein Schreiben, welches er von der betreffenden Wohnungsgesellschaft bereits erhalten hatte. Aus diesem ging hervor, dass die betreffenden Informationen nicht herausgegeben werden, da es sich nach Auffassung der Wohnungsgesellschaft um Betriebs- oder Geschäftsgeheimnisse handeln würde.

Gegen diese Entscheidung legte der Petent Widerspruch ein. Diesem gab die Stadt nicht statt, sondern führte in ihrem Widerspruchsbescheid aus, dass es sich vorliegend um Betriebs- oder Geschäftsgeheimnisse handeln würde und die Offenbarung der begehrten Informationen sowohl auf Seiten der Wohnungsgesellschaft als auch bei dem Verein zu wirtschaftlichen Schäden führen könne.

Ein Betriebs- oder Geschäftsgeheimnis setzt neben dem Mangel an Offenkundigkeit der zugrundeliegenden Informationen ein berechtigtes Interesse des Unternehmens an der Nichtverbreitung voraus. Ein solches Interesse fehlt, wenn die Offenlegung der Information nicht geeignet ist, exklusives technisches oder kaufmännisches Wissen den Marktkonkurrenten zugänglich zu machen und so die Wettbewerbssituation des Unternehmers nachteilig zu beeinflussen (vgl. Urteil des Bundesverwaltungsgerichts vom 28. Mai 2009, BVerwG 7 C 18.08).

Auf Grundlage der oben genannten Begriffsdefinition habe ich die Stadt darüber informiert, dass für ein objektiv berechtigtes wirtschaftliches Interesse vor allem die wettbewerbsrechtliche Relevanz der Information maßgeblich ist. Es muss also geprüft werden, ob dem Unternehmen durch eine Offenbarung der Informationen tatsächlich ein wirtschaftlicher Schaden entstehen würde. Aus dem Widerspruchsbescheid ging für mich nicht hervor, worin dieser reale Schaden tatsächlich bestehen könnte. Aus diesem Grunde habe ich die Stadt gebeten, ihre Entscheidung noch einmal zu überdenken beziehungsweise das berechtigte wirtschaftliche Interesse näher zu begründen.

Die Stadt teilte mir anschließend mit, dass es sich vorliegend um einen Sponsorenvertrag handelt. Sponsoring soll nach ihrer Auffassung auch dazu dienen, die eigenen Kommunikations- und Marketingziele durch die gesponserten Personen, Organisationen, Veranstaltungen, Unternehmen etc. zu fördern. Als Form der Öffentlichkeitsarbeit fordert das Sponsoring in der Regel sogar die Offenlegung der Partnerschaft. Diesem habe ich zugestimmt, da das Ziel von Sponsoring regelmäßig auch darin besteht, auf das eigene Unternehmen aufmerksam zu machen.

Weiterhin führte die Stadt aus, dass die Kenntnis der Höhe der Leistung bei anderen gesponserten Partnern Erwartungen wecken beziehungsweise diesbezügliche Verhandlungen erschweren könnte. Nach Ansicht der Stadt besteht dadurch die Gefahr, dass Sponsoring als Instrument der Öffentlichkeitsarbeit beeinträchtigt wird und die gezielte Marketingpolitik nicht zum Erfolg führt.

Aus meiner Sicht hat die Stadt die entscheidende Frage, inwiefern das Bekanntwerden von Sponsoringleistungen zu einem konkreten wirtschaftlichen, insbesondere wettbewerblichen Nachteil des Sponsors führen könnte, nicht beantwortet. Ich habe deshalb empfohlen, die begehrten Informationen vollständig zugänglich zu machen.

Die Stadt hat mir daraufhin nicht mitgeteilt, ob sie meine Empfehlung umsetzen wird. Vielmehr wurde ich darüber informiert, dass in dieser Angelegenheit nunmehr eine Klage beim Verwaltungsgericht anhängig ist und man beabsichtigt, diese abzuwarten. Die Entscheidung des Verwaltungsgerichts hierzu steht bislang noch aus. Von daher ist in diesem Fall derzeit noch offen, ob der Antragsteller die von ihm begehrten Informationen tatsächlich erhält.

7.8 Einsicht in Zirkusunterlagen

Ein Antragsteller wollte beim Veterinäramt eines Landkreises Einsicht in Zirkusunterlagen nehmen. Die begehrten Unterlagen bezogen sich vor allem auf Informationen, die im Zusammenhang mit dem Tierschutz standen. Die Einsicht hierzu wurde dem Antragsteller im Jahr 2006 zugestanden. Im Nachgang hierzu stellte er bei der Behörde den Antrag auf Überlassung von Kopien dieser Unterlagen. Dieses wurde durch den Landkreis mit dem Hinweis abgelehnt, dass (nach dem damaligen Gesetzeswortlaut - siehe hierzu auch Punkt 6.1) kein genereller Anspruch auf Herausgabe von Kopien bestand. Der Antragsteller erhob daraufhin Klage. Das Verwaltungsgericht Schwerin entschied hierzu, dass zwar grundsätzlich kein Rechtsanspruch auf die Zur-Verfügung-Stellung von Kopien besteht, hierüber jedoch eine Ermessensentscheidung zu treffen ist. Der Landkreis wurde verurteilt, erneut über den Antrag zu entscheiden.

Der Landkreis entschied daraufhin, dem Antragsteller die begehrten Kopien nicht zu überlassen und begründete dieses damit, dass in den Unterlagen personenbezogene Daten (§ 7 IFG M-V) und Betriebs- oder Geschäftsgeheimnisse (§ 8 IFG M-V) enthalten sind, die dem Informationszugang entgegenstehen. Der Antragsteller legte gegen diese Entscheidung Widerspruch ein und bat mich parallel um eine außergerichtliche Prüfung.

Ich teilte dem Landkreis mit, dass ich das Argument, dass vorliegend personenbezogene Daten betroffen sind, nur bedingt teile. Meiner Ansicht nach wären Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person nur in den Fällen vorhanden, wenn es sich bei dem jeweiligen Zirkus um ein Einzelunternehmen handelt. Sofern dieses der Fall gewesen wäre, hätten diese Angaben, um nach § 11 Abs. 3 IFG M-V zumindest einen Teilzugang zu gewähren, geschwärzt oder anderweitig abgetrennt werden können.

Des Weiteren gab der Landkreis an, dass es sich vorliegend um Informationen handelt, deren Offenlegung geeignet ist, den Konkurrenten exklusives technisches oder kaufmännisches Wissen zugänglich zu machen, welches die Wettbewerbsposition des jeweiligen Zirkusunternehmens nachteilig beeinflussen könnte. Nach Meinung des Landkreises lag hier eine sonstige wettbewerbsrechtliche Information vor, die zur Ablehnung des Antrages führen musste.

Ich habe den Landkreis darauf hingewiesen, dass auch bei einer wettbewerbsrelevanten Information der Unternehmer ein schutzwürdiges wirtschaftliches Geheimhaltungsinteresse benötigt. Die Behörde muss also prüfen, ob ein solches berechtigtes Interesse anzuerkennen ist, ob also ohne die Geheimhaltung ein erheblicher wirtschaftlicher Schaden entstehen könnte. Ein Kriterium ist dabei auch die Bedeutung der Information für Konkurrenten.

Vorliegend wurden insbesondere Informationen zur Haltung von Zirkustieren begehrt. Der Tierschutz genießt nach Art. 20a Grundgesetz (GG) Verfassungsrang. Im Hinblick auf Grundrechte hat die Gewährleistung des Art. 20a GG die Bedeutung, dass sie Beschränkungen von Grundrechten legitimieren kann, so unter anderem die Eigentumsgarantie (siehe: Jarass/Pieroth, GG-Kommentar, 8. Aufl., Art. 20a, Rdnr. 15). Art. 20a GG kann somit Auswirkungen auf andere Grundrechte haben. Hierfür ist allerdings eine gesetzliche Grundlage erforderlich. Als solche könnte das IFG M-V in Betracht kommen.

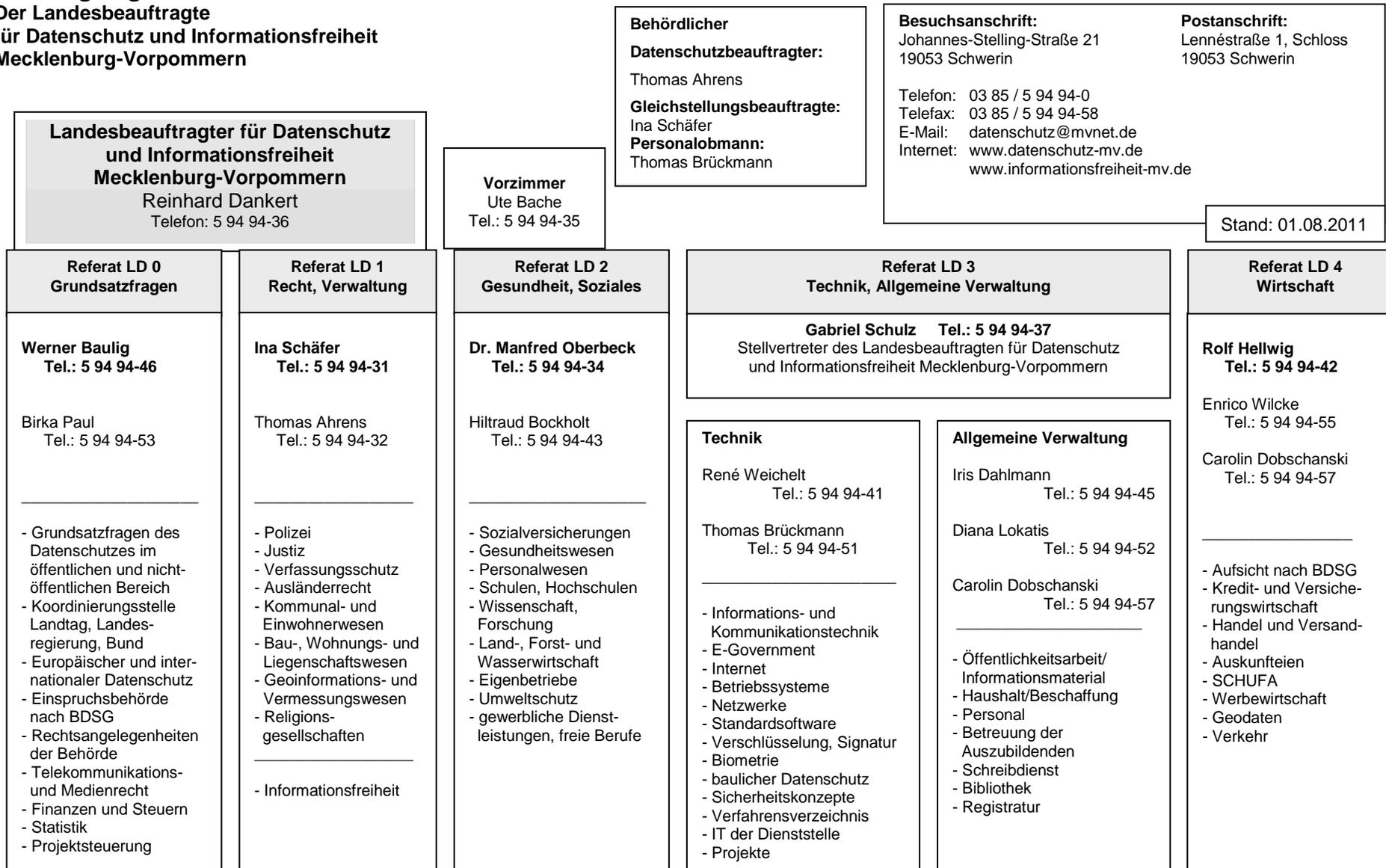
Meiner Ansicht nach hätte der Landkreis eine Abwägung des Art. 20a GG mit der in Art. 14 GG geschützten Eigentumsgarantie vorzunehmen müssen. Durch die in Art. 20a GG gewählte Formulierung „im Rahmen der verfassungsmäßigen Ordnung“ herrscht hierbei die prinzipielle Gleichordnung des Umweltschutzes wie des Tierschutzes mit anderen Verfassungsprinzipien und Verfassungsrechtsgütern (siehe hierzu auch oben erwähnten GG-Kommentar).

Aus vorgenannten Gründen habe ich dem Landkreis empfohlen, die dort getroffene Entscheidung noch einmal zu überdenken. Trotz meiner Hinweise blieb der Landkreis bei seiner Entscheidung, sodass in der Folge der Antragsteller beim Verwaltungsgericht Schwerin erneut Klage erhob.

Der Petent teilte mir abschließend mit, dass er das Verfahren gegenüber dem Verwaltungsgericht für erledigt erklärt hat, da er von dort zwischenzeitlich die betreffenden Kopien erhalten hat.

Erwähnen möchte ich in diesem Zusammenhang noch, dass der Gesetzgeber hinsichtlich der Frage, inwieweit auf Seiten der Antragsteller ein Herausgabeanspruch von Kopien besteht, meiner im Zuge der Novellierung des IFG M-V ausgesprochenen Empfehlung gefolgt ist und einen gesetzlichen Anspruch hierauf normiert hat (siehe hierzu auch Punkt 7.1).

**8. Organigramm
Der Landesbeauftragte
für Datenschutz und Informationsfreiheit
Mecklenburg-Vorpommern**



9. Abkürzungsverzeichnis

AK Technik	Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Ständigen Konferenz der Datenschutzbeauftragten des Bundes und der Länder
AO	Abgabenordnung
ARGE	Arbeitsgemeinschaft
BDSG	Bundesdatenschutzgesetz
BEM	Betriebliches Eingliederungsmanagement
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGBI.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BMF	Bundesministerium der Finanzen
BMI	Bundesministerium des Innern
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT	Bundestag
BT-Drs.	Bundestags-Drucksache
BVerfG	Bundesverfassungsgericht
CN-LAVINE	Corporate Network der Landesverwaltung
DNA	Desoxyribonukleinsäure - Träger der Erbinformationen
DSG M-V	Landesdatenschutzgesetz Mecklenburg-Vorpommern
DVZ M-V GmbH	Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH
EDV	elektronische Datenverarbeitung
EGVP	Elektronisches Gerichts- und Verwaltungspostfach
eID	elektronischer Identitätsnachweis
ELENA	elektronischer Einkommensnachweis
EnWG	Energiewirtschaftsgesetz
EPOS	Elektronisches Personal-, Organisations- und Stellenmanagementsystem
EU	Europäische Union
EWR	Europäischer Wirtschaftsraum
GG	Grundgesetz
HTTP	Hypertext Transport Protocol
HTTPS	Hypertext Transport Protocol Secure
ID	Identifikationsnummer
IFG M-V	Informationsfreiheitsgesetz Mecklenburg-Vorpommern
INPOL	polizeiliches Informationssystem
IP	Internet Protocol
IPsec	Internet Protocol Security
ITIL	IT Infrastructure Library
Kfz	Kraftfahrzeug
KunstUrhG	Kunsturhebergesetz
KV M-V	Kommunalverfassung des Landes Mecklenburg-Vorpommern
LBG M-V	Landesbeamtengesetz
LHG M-V	Landeshochschulgesetz
LKA M-V	Landeskriminalamt Mecklenburg-Vorpommern
LKHG M-V	Landeskrankenhausgesetz für das Land Mecklenburg-Vorpommern
LT-Drs.	Landtags-Drucksache
MfS	Ministerium für Staatssicherheit

OSCI	Online Services Computer Interface
OWiG	Gesetz über Ordnungswidrigkeiten
PDF	Portable Document Format - plattformunabhängiges Dateiformat für Dokumente
PIN	Persönliche Identifikationsnummer
RFID	Radio Frequency Identification
SAP	Systemanalyse und Programmentwicklung
SGB I	Sozialgesetzbuch Erstes Buch
SGB II	Sozialgesetzbuch Zweites Buch
SGB IV	Sozialgesetzbuch Viertes Buch
SGB V	Sozialgesetzbuch Fünftes Buch
SGB IX	Sozialgesetzbuch Neuntes Buch
SGB X	Sozialgesetzbuch Zehntes Buch
SOG M-V	Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommern
SSL	Secure Sockets Layer
Steuer-ID	Steueridentifikationsnummer
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TKG	Telekommunikationsgesetz
TLS	Transport Layer Security
TMG	Telemediengesetz
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
VPN	Virtual Private Network
VwGO	Verwaltungsgerichtsordnung
WLAN	Wireless Local Area Network - drahtloses lokales Netzwerk
ZIR	Zentrales Informationsregister
ZSS	Zentrale Speicherstelle

10. Stichwortverzeichnis

4-Augenprinzip.....	71	Auskunfteien.....	28
Abgabenordnung	115	Auskunftsanspruch	131
Abschottung	112	Auskunftsersuchen.....	33
Abwägungsklausel	141	Auskunftspflicht	111
Abwesenheitsassistenten	64	Auskunftsrecht	33, 41
Administratorrechte.....	110	Auslagen	146
Adresse	48	Ausweis-App	107
AK Technik	56, 138	Authentifizierungsverfahren	117
Akte	63	Authentisierung.....	56
Akteneinsicht.....	63, 141	Authentisierungsverfahren.....	33
Alwin Pro	68	Authentizität	33, 36, 52, 83, 115
Amtsarzt	132	automatisiertes Verfahren.....	69
Amtshandlungen.....	146	Banken	28
anderes sicheres Verfahren.....	115	BDSG.....	18, 61
angemessenes Datenschutzniveau.....	47	BDSG Novelle	28
Anitvirenprogramm.....	35	Beauftragter für den Datenschutz in der	
anonymisiert	102, 106	Bundeswehr	140
Anonymisierung	70, 76	Befund.....	126
Anordnung.....	87	Begutachtung	133
Antiterrordatei	101	Behörden.....	106
Antragsteller	141	Behördenauskunft.....	104
AO	115	behördlicher Datenschutzbeauftragter ...	76
Applikationen	52	Beihilfeakten.....	131
Apps	52	Beinahetreffer	96
Arbeitgeber.....	117	Beitrag.....	120
Arbeitnehmer.....	92, 117	Beitragserhebung	120
Arbeitnehmerdatenschutz.....	110	Bekanntmachung	102
Arbeitsgemeinschaften	123	Belehrung.....	96
Arbeitsgruppe	144	berechtigtes Interesse.....	150
Arbeitskreis "Technische und		Berechtigungskonzept.....	85
organisatorische Datenschutzfragen"	85	Berechtigungszeugnis.....	108
Arbeitskreis Technik	55	Beschäftigte	130
Arbeitskreis Technische und		Beschäftigtendatenschutz	27
organisatorische Fragen.....	138	Beschlussvorlage	105
Arbeitskreises Technik.....	86	Bestandsverwaltung.....	74
Arbeitslosengeldes II.....	123	Betrieblichen Eingliederungsmanagements	
Arbeitsplatz	62	123
Arbeitszeit	72	Betriebs- oder Geschäftsgeheimnis	148
Artikel-29-Gruppe	140	Betriebs- oder Geschäftsgeheimnisse ...	149
ärztliche Schweigepflicht	87, 128	Betriebs- und Geschäftsgeheimnisse ...	141
Attribut-Zertifikat.....	83	Betriebsnummer.....	103
Auditierung.....	114	Beurkundungen.....	83
Auditierungsverfahren.....	86	Bewegungsprofil.....	77
Aufenthaltsgesetz	101	Beweisfoto	98
Auftraggeber.....	46	Bewerbungsverfahren	132
Auftragnehmer	46	Bildüberwachung.....	87
Auftragsdatenverarbeitung	61	Bildungsaufgabe	15
Auzenz	68	Bildungsdokumentation.....	122

Bildungsoffensive.....	16	Daten verarbeitende Stelle.....	81
Binding Corporate Rules.....	47	Datenabfrage.....	95
Bing Maps Streetside.....	58	Datenbank.....	117
Bioenergieverbund.....	101	Datenbankverschlüsselung.....	71
Biometrische Authentisierung.....	56	Datengeheimnis.....	112
biometrische Daten.....	57	Datenschutz.....	134
biometrische Erkennung.....	54	Datenschutzaudit.....	38
biometrische Gesichtserkennung.....	18	Datenschutz-Audit.....	114
BITKOM.....	59	Datenschutzbeirat.....	40
BlackBerry.....	52, 138	Datenschutz-Kodex.....	59
Bluetooth.....	76	Datenschutzkonzept.....	23
BMF.....	115	Datenschutzrecht.....	23
Bonität.....	28	datenschutzrechtliche Überprüfung.....	42
Bring Your Own Device.....	53	Datenschutzrichtlinie.....	23, 24
Browser.....	61, 65	Datensicherheit.....	53, 134
BSI.....	34, 51, 55, 86, 107, 114, 138	Datensicherung.....	110
Bundesamt für Sicherheit in der Informationstechnik.....	34, 51, 55, 86, 107, 114, 138	Datensparsamkeit.....	34, 77
Bundesärztekammer.....	87	Datenübermittlung.....	81
Bundesbeauftragte für den Datenschutz.....	26	Datenverarbeitung.....	18
Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.....	117	Datenverarbeitung im Auftrag.....	46
Bundesdatenschutzgesetz.....	18	Datenverkehr.....	8
Bundesdruckerei.....	139	DCS.....	114
Bundesministerium der Finanzen.....	115	Deliktsguppe.....	95
Bundesministerium für Arbeit und Soziales	32	De-Mail.....	33, 34
Bundesrat.....	31	De-Mail-Gesetz.....	34
Bundesverfassungsgericht.....	43, 103, 118	Demonstration.....	93
Bundesverfassungsschutzgesetz.....	31	Diagnose.....	126
Bundesverwaltungsamt.....	108	Diensteanbieter.....	19, 60, 118
Bundeszentralamt für Steuern.....	116	Dienstfähigkeit.....	132, 133
Bürgerentlastungsgesetz Krankenversicherung.....	113	Dienstherr.....	131
Bürgermeister.....	105	Dienstleister.....	81
Bürgerportalgesetz.....	34	dienstliche Nutzung.....	53
Bußgeldrahmen.....	96	Diensttauglichkeit.....	124
Call Manager.....	68	Dienstvereinbarung.....	62, 64, 68, 70, 76
Chipkarte.....	35, 57	digitaler Radiergummi.....	61
Chipkartenleser.....	107	DNA-Identifizierungsmuster.....	96
Cisco.....	68	Dokumentenablagedienst.....	34
Cloud Computing.....	52, 54, 139	Dokumentenmanagementsystem.....	69
Cloud-Computing.....	46	DOMEA.....	69
CN-LAVINE.....	74	Dortmunder Entwicklungsscreenings... ..	122
Cookie.....	17	Drittstaat.....	47
Criteria.....	115	Drittstaatentransfer.....	47
Cybermobbing.....	120	Düsseldorfer Kreis.....	19, 60
Data Center Steuern.....	114	DVZ.....	68, 75
Dataport.....	115	DVZ M-V GmbH.....	10, 48, 68, 73, 74, 75, 81
Dataport-Staatsvertrag.....	114	E-Business.....	56
		eCard-Strategie der Bundesregierung.....	38
		Echtdaten.....	70, 71
		Echtssystem.....	71
		E-Government.....	56, 73
		E-Government-Portal.....	108

EGVP	73	Facebook-Fanpage	20
eID-Funktion	107	Fahrtauglichkeit	124
eID-Server	108	Fahrzeughalter	98
eID-Service.....	108	Familienverband	98
eID-Strategie der Bundesregierung	38	Fanpage.....	19
Eigentumsgarantie	150	Fan-Page	17
Einkaufszentren	92	Fernwartung.....	71, 86, 110
Einkommenssteuergesetz	116	Finanzverwaltung	115, 117
Einlader	101	Fingerabdruck	56
Einsicht.....	130	FoKuS	94
Einwendungsführer	102	Formatierungsprogramm	55
Einwilligung	18, 52, 71, 126	Foto	119
Elektronischer Entgeltnachweis	32	Fragebogen	112
elektronischer Identitätsnachweis	107	Freigabe	82, 110
elektronischer Personalausweis.....	35	Freiwilligkeit.....	102, 134
elektronischer Rechtsverkehr	73	Funktionstest.....	71
Elektronisches Gerichts- und Verwaltungspostfach.....	73	Funkzelle.....	93
ELENA.....	32	Funkzellenabfrage.....	93
ELSTAM.....	116	Gebäude- und Wohnungszählung.....	111
ELSTER	115	Gebühr	142, 147
Elster-Online Portal.....	117	Gebühren.....	145, 146
E-Mail.....	34, 62, 106	Gebührenrahmen.....	142
Ende-zu-Ende-Sicherheit	35	Gefällt-mir-Button	17
Ende-zu-Ende-Verschlüsselung	35	Geheimhaltungspflicht.....	112
Energiewirtschaftsgesetz	50	Gemeindevertreter	62, 104
Entgeltbescheinigung	32	Gemeinsames Verfahren.....	81
Entschließung	120	Gemeinschaftspraxis.....	127
Entschlüsselung	32, 61	Geolokalisierung.....	50
Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes.....	27	Geschäftsbereich.....	100
EnWG.....	50	Gesichtserkennungsdienst.....	30
EPOS	70	Gewerbeauskünfte	78
Eraser.....	56	Gleitzeitvereinbarung	72
Erforderlichkeit	34, 97, 103	Google.....	60, 106
Erhebungsbeauftragte.....	111	Google Analytics	60
Erhebungsbeauftragten.....	112	Google Street View.....	58
Erhebungsbogen	101	Google-Cache	106
Erhebungsmerkmalen.....	111	GPS	52
Erhebungsstelle	112	Grundschutzmethodik.....	114
Erkennung von Kraftfahrzeugkennzeichen	43	Grundsicherung.....	123
EU-Datenschutzverordnung	25	Gruppenversicherungsverträge	137
EU-Kommissarin.....	145	Gütesiegelvergabe.....	39
Europäische Datenschutzrichtlinie	47	Hash-Funktion	76
Europäische Parlament	8	Haushaltebefragung	111
Europäischer Wirtschaftsraum	46, 47	Hausnummern.....	58
Evaluierung	115	Herausgabepflicht	141
Extended Validation.....	66	Hilfsmerkmale	111
facebook	20	Hochschule	16, 88
Facebook	17	HTTPS	65
		iCloud	52, 53
		Identifizierung.....	33, 56, 61
		Identitätsbestätigungsdienst.....	34

Identitätsdaten	35	Kleingartenvereine.....	135
Identitätsnachweis	33, 83, 109	klinisches Krebsregistergesetz.....	44
Immatrikulation	98	Koalitionsvereinbarung.....	16
Informationsfreiheitsgesetz	140, 145	Koalitionsvertrag	38
Informationsinteresse	120	kommunaler Zweckverband	108
Informationskostenverordnung	142, 146	Kommunalverwaltung	106
Informationsregister	107, 144	Kommunikation	20
Informationssicherheit.....	110	Konferenz	19
Informationssicherheits-		Konferenz der Datenschutzbeauftragten.	23
Managementsystem	114	Konkurrenten	150
Informationszugang.....	63, 147	Kontostammdaten	31
informierte Einwilligung	52	Kontostammdatenabfrage	31
Innenministerium	31, 69, 74, 96, 99	Kontrollbesuch.....	112
Innenstadt	87	Kontrolle	94
INPOL-Berechtigung	96	Kontrollrecht.....	62
Integrität	33, 36, 48, 52, 83, 87, 115	Kontrollstelle	8
intelligentes Stromnetz.....	50	Koordinierungsstelle für IT-Standards ...	37
Interessenkonflikt	113	Kopie.....	109
Interface Identifier.....	49	Kopien.....	141, 149
Intermediär	73	KoSIT	37
Internet ...	17, 20, 29, 46, 48, 52, 61, 62, 79, 81, 91, 105, 119	Kraftfahrzeugkennzeichen	58
Internetrecht	29	Krankenhaus	88
iPad.....	52	Krankenhausinformationssystem.....	85
IP-Adresse	60	Krankenhausinformationssysteme	139
iPhone.....	52	Krebsregister.....	45, 129
IPSec.....	67	Kreditinstitut	31
IP-Telefonie.....	68, 74	Kreismusikschule.....	110
IPv6	139	Kriminalpolizeiinspektion	106
Irischer Datenschutzbeauftragter.....	19	kryptografischer Schlüssel.....	56
ISMS.....	114	kryptografisches Verfahren	57
IT Infrastructure Library	74	Kunsturhebergesetz.....	91, 119
ITIL	74	KV M-V	86
IT-Konzept	112	KV-SafeNet	86
IT-Managementsystem.....	74	Länderkompetenz	38
IT-Planungsrat	37	Landesamt.....	103
IT-Service-Managementsystem	74	Landesarbeitsgericht	65
Jahressteuergesetz 2010	113	Landesdatenschutzgesetz.....	8, 18, 39
Jahressteuergesetzes	116	Landeskrankenhausgesetz.....	43
Jailbreaking	54	Landeskriminalamt	100
Jobcentern.....	123	Landesregierung	10, 107, 120
Jugendamt.....	121	Landesrundfunkanstalt.....	120
Justizministerium	74, 95, 147	Landkreis	149
Kassenärztliche Bundesvereinigung	86	Last- und Nutzungsprofil	51
Kassenärztliche Vereinigung M-V	86	Lebenslauf.....	147
KBV	86	lebenswichtige Einrichtung	100
Kennziffer.....	103	Legitimation.....	109
Kernbereichsschutz	99	Leistungs- und Verhaltenskontrolle.....	70
Kindertagesstätte	122	Leitlinien für IT-Sicherheit und	
KinderUni	22	Datenschutz.....	37
kirchlicher Datenschutzbeauftragter	85	Lernspiel	22
		Lichtbild.....	99

Lichtbildabgleich.....	98	Nutzerdaten.....	19, 52
Lichtbildabgleichserlass	98	Nutzungsanalyse.....	17
Link	144	Nutzungsdaten	60
Lizenz	146	Nutzungsprofil	20, 60
Lohnsteuerabzugsmerkmale.....	116	Observation.....	42
Lohnsteuerdaten	116	öffentliche Sicherheit.....	42
Löschen	61	öffentliche Stelle.....	104
Löschen im Internet.....	138	öffentliche Stellen.....	106
Löschkonzept	70	Online Gewerbedienst	78
Löschprotokoll	70	Online Services Computer Interface.....	73
Löschung	48, 55, 106	Online-Wohngeldantrag	80
lüfterlose Lesegeräte	52	Open Government.....	38, 144
Machbarkeitsstudie.....	101	Open-Source-Produkt	56
magnetische Datenträger	55	Optionskommunen.....	123
mandantenfähig	107	Ordnungswidrigkeit	96
Mandantentrennung.....	69	Organisationsanweisung	112
Marktforschung	19, 60	Organisationseinheit	100
medizinische Netze	139	Orientierungshilfe	85
Medizinischen Dienst der		OSCI	73
Krankenversicherung	133	OSCI-Manager.....	73
medizinisches Gutachten.....	133	OSCI-Transport	82
Melddaten	106	Partitionierungsprogramm	55
Melderegister.....	104, 106	Passwort.....	35, 57, 71
Menschenrechtskonvention.....	24	Patientenakte.....	127
MfS-Überprüfungen	104	Patientendaten.....	126
Microsoft	48, 58	Patientenfragebogen	128
Ministerium	102, 147	Peer-to-peer-Dienst.....	50
Mitarbeiter.....	131	Personalakte.....	130
Mitarbeiterüberwachung	92	Personalausweis.....	56, 107, 108, 109
Mitbestimmungsrecht.....	70	Personalausweisgesetz.....	109
Mobile Device Management	53	Personaldaten	70, 130
mobile Endgeräte.....	52	Personalfragebogen.....	131
mobiles Endgerät.....	138	Personalrat	69
Mobilfunkteilnehmer.....	93	Personalsachbearbeitung.....	70
Mobiltelefon	77	Personalunterlagen.....	131
Musterdienstvereinbarung	76	Personalvertretung	70, 76
Nachbar	90	Personen der Öffentlichkeit	120
Nationale E-Government-Strategie	37	personenbezogene Daten	149
Navigationssystem	76	Personenstandsgesetz.....	82
NEGS	37	Personenstandsregister.....	81, 83
NEGS-Umsetzungskonzept.....	38	Personenstandsverordnung	82
Netzwerk- und Systemmanagementsystem		Persönlichkeitsrecht	47, 64
.....	74	Pilotbetrieb.....	75
Netzwerkprotokoll.....	48	Planfeststellungsbeschluss.....	102
Netzwerkstar.....	22	Plattform	144
neuer Personalausweis.....	33, 139	Polizei	18, 97
nichtöffentlicher Bereich.....	19	Polizeiangehörige	95
Nichttreffer	96	Polizeiliche Beobachtung	95
Normenklarheit.....	116	Polizeipräsidium	87
Novelle	8	Pranger.....	135
Novellierung.....	150	Praxis-EDV-System.....	87

private Nutzung	53	Schadensersatzanspruch	8
privater Gebrauch	54	schädigendes Ereignis	42
Privatsphäre	18	Schmerzensgeldanspruch	30
Proband	95, 96	Schriftform	115
Produktivbetrieb	75	Schüler	16
Profil	17	Schutzbedarf	70
Profilbildung	17, 23, 30	Schutzmaßnahmen	53
Projektmanagementhandbuch	75	Schutzprofil	51
Protokolldaten	75	Schwarzes Brett	135
Protokollierung	50, 64, 69, 85, 86	Schweigepflicht	123, 126
Provider	48	Schwerbehindertenakte	125
Proxy-Server	75	Schwerbehinderung	132
Pseudonym	19, 60, 134	Scoring	28
pseudonymisiert	134	Selbstverpflichtung	59
Pseudonymisierung	32, 76	Selbstverwaltungsangelegenheiten	146
PStG	82	sensitive Daten	90
PStV	82	Sexual- und Gewaltstraftäter	94
qualifizierte elektronische Signatur	73, 82, 115	SGB IV	34
Qualifizierte Elektronische Signatur	33, 35, 38, 107	Sicherheitskonzept	53, 71, 110, 115, 117
Quick-Freeze-Verfahren	118	Sicherheitsmanagement	115
Recht am eigenen Bild	119	Sicherheitsüberprüfung	100
Recht auf informationelle Selbstbestimmung	18	Sicherheitsüberprüfungsfeststellungslandes verordnung	100
Rechts auf informationelle Selbstbestimmung	20	Sicherungsregister	82
Rechtsprechung	65	Sicherungsregisterverordnung	82
Rechtsschutz	94	Signatur	52, 73
Regierungsinformation	145	Signaturkarte	33
Rehabilitation	129	Signaturprüfung	54
Reichweitenanalyse	17, 60	Signaturzertifikat	83, 107
Reichweitenmessung	50	Smart Grid	50, 138
Reihengentest	96	Smart Meter	50, 138
Reisepass	56	Smartphone	52, 61, 77
Revisionsfähigkeit	69, 71	Social-Plugin	17
Revisionssicherheit	48	Sondereinrichtungen	112
Richtlinie	8	Sozialdaten	121
Richtlinie 95/46/EG	23, 24, 140	soziales Netzwerk	61
Richtlinienentwurf	145	Soziales Netzwerk	17
RIM	138	Sozialleistung	33
Risikoanalyse	53	Speichelprobe	96
Risikogruppe	95	SSL	35, 65
Rostock	87	Staatssicherheitsdienst	104
Rote-Linie-Gesetz	29	Standardvertragsklauseln	47
Routenempfehlungen	76	Standesämter	81
Rückfallgefährdung	94	Standesbeamter	83
Rundfunkänderungsstaatsvertrag	120	Statistischen Amt	111
Safe-Habor-Grundsätze	47	Statistisches Amt	138
SAP AG	139	Stellenplan	79
		Steuerdatenverarbeitung	114
		Steuererklärung	115
		Steuer-ID	113
		Steuervereinfachungsgesetz 2011	116

Stiftung	23, 38, 39	Verarbeitung personenbezogener Daten im Auftrag	102
Stiftung Datenschutz	23, 38	Verbindungsdaten	68
Störung	68	Verbrauchsprofil	51
Strafverfolgungsbehörde	93	Verein	137
Straßenaufsichtsbehörde.....	147	Verfahren	41
Straßenverzeichnissen	147	Verfahrensbeschreibung	110
Streikdaten.....	132	Verfallsdatum	61
Student.....	97	Verfassungsbeschwerde.....	118
Subsidiaritätsprinzip.....	24	Verfassungsprinzipien	150
Suchmaschine.....	17	Verfassungsrang	150
Surf-Verhalten	60	Verfassungsrechtsgütern.....	150
Systemwechsel	120	Verfassungsschutzbehörde	100
Tablet PC.....	52	Verfügbarkeit.....	48
Tatortspur	96	Verhaltensprofil	51
TCP.....	66	Verhältnismäßigkeit.....	94
Technologieneutralität.....	25	Verkehr	76
Technology Subgroup	140	Verkehrsdaten	68, 93
Teilzugang.....	149	Verkehrsordnungswidrigkeit	98
Telekommunikation	43, 68	Veröffentlichungspflicht.....	145
Telekommunikationsdaten	118	Veröffentlichungspflichten.....	141
Telekommunikationsgeheimnis	118	Verordnungen	141
Telekommunikationsüberwachungs- Anlage	99	Verpflichtungsgeber	101
Telekommunikationsüberwachungszentru m.....	99	Verschlüsselung. 32, 35, 56, 61, 71, 73, 82, 86	
Telemedien	19, 60	Verschlussachenanweisung.....	100
Telemediengesetz.....	18, 60	Versicherung.....	136
Telemedizin.....	83	Versorgungsamt.....	125
TeleTrusT	56	Vertraulichkeit	48, 52, 87
Tierschutz	149	Verwaltung	62
TLS.....	35, 65	Verwaltungsakt	103
TLS-Protokoll.....	82	Verwaltungsgericht.....	147, 149
TMG.....	18, 60	Verwaltungskosten	146
Transparenz	48, 52, 77, 110	Verwaltungsverfahrensgesetz.....	73
Treffer.....	96	Verwaltungsvorschriften.....	141
Trojanisches Pferd.....	35	Verzeichnisdienst.....	34
TrueCrypt	56	Video.....	92
Übermittlung	121	Videokamera.....	87, 88, 89, 92
Überschreiben.....	55	Videouberwachung... 42, 87, 88, 90, 91, 92	
ULD.....	18	Viertes Buch Sozialgesetzbuch.....	34
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein.....	18	Viren	35
Unabhängigkeit	25, 40	Visa-Warndatei	101
Universität	87, 97	Visumantrag.....	101
Unkenntlichmachen.....	55	Visumantragsteller.....	101
Unterrichtung	42	Visumbehörde.....	101
Unterschrift.....	98	Vollabgleich.....	101
Urkundensdaten	82	Vorabkontrolle.....	82
USA.....	17	Vorgangsbearbeitungssystem	69
USB-Stick.....	55, 112	Vorgesetzter	72
		Vorratsdatenspeicherung	118
		Vorratsdatenspeicherung.	26

VS-VERTRAULICH	100	Zeiterfassungssystem	71
Wahlbeamte.....	104	Zensus 2011	110, 112, 138
Webcam.....	91	Zensusgesetz	112
Webseite	17	Zensusgesetz 2011	111
weisungsgebundenen Aufgaben	146	Zensus-PC.....	112
Weiterverwendung	145	Zentrale Speicherstelle.....	32
Werbung	17, 19, 60	Zertifikat	47, 66
Wettbewerbsposition	150	Zertifizierung	34, 86
Widerspruch	60	Zertifizierungsdiensteanbieter	36, 66
Widerspruchsrecht.....	19	Zugriffsberechtigte	31
WLAN-Netze	58	Zugriffsrecht	85
Wohngeldantrag	80	Zustellung	125
Wohngeldstelle.....	80	Zweckverband.....	81
XPersonenstand	82	Zwei-Karten-Prinzip.....	33
zahnärztliche Behandlung	128		

11. 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 Medizinetze -
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)