LANDTAG MECKLENBURG-VORPOMMERN **Drucksache 6/2810**
6. Wahlperiode **19.03.2014**

UNTERRICHTUNG

durch den Landesbeauftragten für Datenschutz und Informationsfreiheit

Elfter Tätigkeitsbericht gemäß § 33 Absatz 1 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V)

Sechster Tätigkeitsbericht gemäß § 38 Absatz 1 Bundesdatenschutzgesetz (BDSG)

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

Berichtszeitraum: 1. Januar 2012 bis 31. Dezember 2013

Zugeleitet mit Schreiben des Landesbeauftragten für Datenschutz und Informationsfreiheit vom 17. März 2014.

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 Elfte Tätigkeitsbericht gemäß § 33 Absatz 1 des Landesdatenschutzgesetzes Mecklenburg-Vorpommern (DSG M-V), der Sechste Tätigkeitsbericht gemäß § 38 Absatz 1 des Bundesdatenschutzgesetzes (BDSG) und der Vierte Tätigkeitsbericht nach dem Informationsfreiheitsgesetz Mecklenburg-Vorpommern (IFG M-V) umfassen den Zeitraum vom 1. Januar 2012 bis zum 31. Dezember 2013. Da es bei etlichen Sachverhalten fachliche Überschneidungen gibt, sind die Beiträge nach dem DSG M-V und nach dem BDSG nicht separat aufgeführt, weil die Themen häufig im Zusammenhang zu betrachten sind.

Die hier dargestellten Vorgänge sollen einen Eindruck von der breit gefächerten Tätigkeit der Behörde als Beratungs-, Aufsichts- und Kontrollbehörde vermitteln. Einige Beiträge schließen an Sachverhalte aus den Tätigkeitsberichten der vorherigen Berichtszeiträume 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	6
1	Empfehlungen	11
1.1	Zusammenfassung aller Empfehlungen	11
1.2	Umsetzung der Empfehlungen des Zehnten Tätigkeitsberichtes	13
2	Bildungsprojekte	17
2.1	Ausgangspunkt	17
2.2	Projekt „Medienscouts MV“	18
2.3	Schulungen für Lehrerinnen und Lehrer, Schulsozialarbeiterinnen und Schulsozialarbeiter sowie Fachkräfte der Jugendhilfe	20
2.4	Landesweite Netzwerke für Medienkompetenz	20
2.5	„TEO - Tage ethischer Orientierung“	22
2.6	Veranstaltungen an Schulen	22
2.7	Projekt „Medientango“	23
2.8	Projekt „Netzwerkstar II“	23
2.9	Projekt „PeerCon“	24
2.10	Ausblick	27
3	Entwicklung des Datenschutzrechts	29
3.1	Die EU-Datenschutz-Grundverordnung	29
3.2	Förderung der elektronischen Verwaltung	31
3.3	Datenschutz-Beirat	35
4	IT-Planungsrat	36
4.1	Beratung des IT-Planungsrates durch die Datenschutzbeauftragten von Bund und Ländern	36
4.2	Soziale Netze in der Verwaltung	37
4.3	Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung	37
4.4	Steuerungsprojekt eID-Strategie	38
4.5	Datensicherheit im Verbindungsnetz	39
5	Technik und Organisation	41
5.1	Neue Technologien	41
5.1.1	Smart Meter auf dem richtigen Weg	41
5.1.2	Datenschutzgerechte Fernmesswasserzähler	43
5.1.3	iPad/iCloud-Nutzung im Landtag	43
5.1.4	Cloud-Computing	45
5.1.5	Orientierungshilfe zum neuen Internetprotokoll IPv6	48
5.1.6	Elektronische Zeiterfassung in der Landesregierung (ZEUS)	50
5.1.7	Dokumentenmanagement in der Landesverwaltung (BEATA)	51
5.1.8	Bring Your Own Device (BYOD)	53
5.1.9	Datentrennung trotz Zentralisierung	54

Seite

5.2	Videoüberwachung	56
5.2.1	Schummeln in der Prüfung - keine Chance!	56
5.2.2	Unzulässige Videoüberwachung auf einer Großbaustelle	57
5.2.3	Am Biertresen gefilmt	58
5.2.4	Videoüberwachung auf dem Friedhof	59
5.2.5	Durchfahrtskontrolle per Blitzsäule	60
5.2.6	Videoüberwachung an der Wiecker Klappbrücke	61
5.2.7	Arztpraxis mit Ausblick - Webcam in Schwerin	63
5.2.8	Videoüberwachung von Bäckereifilialen	63
5.2.9	Luftbildaufnahmen mit Hintergrund	64
6	Datenschutz in verschiedenen Rechtsgebieten	66
6.1	Rechtswesen	66
6.1.1	Auskunftsverfahren bei der Staatsanwaltschaft	66
6.1.2	Anspruch auf Informationen zur Durchsetzung von Rehabilitierungsansprüchen	67
6.1.3	Anonymisierung von Gerichtsentscheidungen	68
6.2	Polizei - Straßenbahnkontrolleure als „Fahnder“	69
6.3	Verfassungsschutz	70
6.3.1	Umsetzung des Urteils des Bundesverfassungsgerichtes zum Antiterrordateigesetz	70
6.3.2	Gesetz zur Änderung des Landesverfassungsschutzgesetzes und des Sicherheits- und Ordnungsgesetzes	71
6.3.3	PRISM, TEMPORA, XKeyscore und Co.	73
6.4	Kommunales/Meldewesen	75
6.4.1	Zugang zu Geodaten	75
6.4.2	Übermittlung von Daten eines Grundstückseigentümers	76
6.4.3	Zweckwidrige Nutzung von besonderen Meldescheinen	77
6.4.4	Übermittlung von Meldedaten an Religionsgemeinschaften und an die GEZ	78
6.4.5	Der neue Personalausweis	79
6.4.6	E-Government-Verfahren - sind Kommunen überfordert?	84
6.5	Soziales	85
6.5.1	Schweigepflichtentbindungserklärung im Sozialbereich	85
6.5.2	Fragen zum SGB II - Arbeitslosengeld II	86
6.5.3	Unzulässige Übermittlung von Sozialdaten	89
6.5.4	Projekt „Kita-Verwaltung-Online“	90
6.6	Gesundheitswesen	91
6.6.1	Datenschutz in der Arztpraxis	91
6.6.2	Zentrales klinisches Krebsregister in Mecklenburg-Vorpommern	93
6.6.3	Clearingstelle der Apothekerverbände	94
6.6.4	Pseudonymisierung im gemeinsamen Krebsregister	95
6.6.5	Datenschutz in der medizinischen Forschung	97
6.6.6	Forschungsvorhaben HARMONIC	98
6.6.7	Krankenhausinformationssysteme (KIS)	99
6.7	Zensus 2011	103

Seite

6.8	Finanzwesen	105
6.8.1	Kartenzahlung per Funk	105
6.8.2	Datenschutz beim Abruf elektronischer Lohnsteuerabzugsmerkmale (ELSTAM)	107
6.8.3	Einführung der „Bettensteuer“ in Schwerin?	108
6.8.4	Kontendatenabrufe nehmen weiterhin zu	109
6.8.5	IT-Dienstleister - ein datenschutzrechtliches Risiko für Kommunen?	110
6.9	Bildung	111
6.9.1	Online-Befragung der Lehrkräfte an öffentlichen Schulen	111
6.9.2	E-Mail mit unverschlüsselten Personaldaten	112
6.9.3	Schulinformations- und Planungssystem (SIP)	114
6.9.4	Erhebung von personenbezogenen Stellenplandaten von Hochschulen	116
6.9.5	Hochschule übermittelt Personalausweisnummern von Studierenden an Praktikumsbetriebe	117
6.9.6	Nutzen von sozialen Netzwerken im Internet für schulische Zwecke	118
6.10	Weitere Fälle	120
6.10.1	Zweckbindungsprinzip beim Bodenordnungsverfahren	120
6.10.2	Fingierte Aktenfunde	121
7	Arbeitskreis „Technische und organisatorische Datenschutzfragen“	122
7.1	Turnusmäßige Sitzungen des AK Technik	122
7.2	Workshop des AK Technik	124
7.3	Technology Subgroup - Zusammenarbeit auf europäischer Ebene	125
8	Datenschutz-Fachtagungen	125
8.1	2012: Datenschutz - Fortschrittsbremse oder Bildungschance?	125
8.2	2013: Intelligente Gebäude - Datenschutz eingebaut?	127
9	Informationsfreiheitsgesetz Mecklenburg-Vorpommern - IFG M-V	129
9.1	Rechtliche Entwicklungen	129
9.2	Open Data/Open Government	130
9.3	Einsicht in Verkehrswertgutachten	130
9.4	Auskünfte zu Fördermittelanträgen	131
9.5	Auskunftsrechte der Kommunalverfassung vs. IFG M-V	133
9.6	Anspruch auf Herausgabe von Kopien	134
9.7	Informationen zu Hinweisgebern	134
9.8	Herausgabe von Informationen zu Öko-Eiern?	135
10	Organigramm	137
11	Abkürzungsverzeichnis	138
12	Stichwortverzeichnis	142

0 Einleitung

Das Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983, mit dem das Grundrecht auf informationelle Selbstbestimmung als Ausfluss des allgemeinen Persönlichkeitsrechts und der Menschenwürde etabliert wurde, gilt als Meilenstein des Datenschutzes. Über dieses Grundrecht ist noch nie so viel gesprochen worden wie im Zeitraum, den dieser Tätigkeitsbericht umfasst.

Und wenn sogar Bundespräsident Joachim Gauck in seiner Rede zum Festakt am Tag der Deutschen Einheit am 3. Oktober 2013 in Stuttgart das Thema aufgreift und eindrücklich darauf hinweist, dass der Datenschutz für den Erhalt der Privatsphäre so wichtig werden sollte wie Umweltschutz für den Erhalt der Lebensgrundlagen, muss schon etwas Bedeutsames passiert sein. Und es war tatsächlich etwas passiert, das den Datenschutz in den Blickpunkt der Öffentlichkeit rückte.

Im Juni 2013 wurden erste Hinweise bekannt, dass amerikanische Geheimdienste in bisher ungeahntem Umfang die weltweite elektronische Kommunikation abhören. Edward Snowden, ehemaliger Mitarbeiter des größten Auslandsgeheimdienstes der Vereinigten Staaten, der National Security Agency (NSA), hatte unzählige Dokumente, die die Spionageaktivitäten der NSA im Rahmen des Geheimprogramms PRISM dokumentieren, sichergestellt und an die Presse weitergegeben. Die Vorwürfe beschränkten sich jedoch nicht nur auf die NSA, sondern betrafen auch das britische Gegenstück zum US-Geheimdienst NSA, das Government Communications Headquarter (GCHQ) und dessen Spionageprogramm TEMPORA. Im Laufe des Jahres 2013 wurden die dramatischen Ausmaße der Abhöraktionen immer deutlicher. Unter Berufung auf Dokumente des Whistleblowers Edward Snowden berichtete die Washington Post über das so genannte „schwarze Budget“, nach dem die USA im Jahr 2013 52,6 Milliarden US-Dollar (rund 40 Milliarden Euro) für ihre insgesamt 16 Geheimdienste ausgegeben hätten. Der Ruf nach Aufklärung der Affäre wurde immer lauter. Obwohl die Gespräche des damaligen Bundesinnenministers Hans-Peter Friedrich mit Vertretern der NSA im Juli 2013 wenig Licht ins Dunkel brachten, zeigten die nach und nach von Snowden veröffentlichten Dokumente das Ausmaß der Spionage (detailliert dokumentiert unter http://www.heise.de/ extras/timeline).

Aber anstatt den Vorfall weiter mit höchster Priorität zu untersuchen, erklärte der damalige Geheimdienstkoordinator der Bundesregierung im August 2013 die Affäre für beendet, da die Geheimdienste NSA, GCHQ und BND versichert hätten, sich in Deutschland an die Gesetze zu halten. Doch damit nicht genug. Der damalige Bundesinnenminister postulierte im Juli 2013 das „Supergrundrecht auf Sicherheit“ und verabschiedete gemeinsam mit seinem Parteikollegen Hans-Peter Uhl das informationelle Selbstbestimmungsrecht quasi in den Ruhestand. Dabei handle es sich um eine „Idylle aus vergangenen Zeiten“, wurde der Innenexperte der CDU/CSU-Bundestagsfraktion zitiert. Die USA könnten dieses Grundrecht daher eigentlich gar nicht verletzt haben. Im gleichen Atemzug forderte Friedrich eine Diskussion über mehr Selbstdatenschutz. Die Bürgerinnen und Bürger müssten ihre Aufmerksamkeit mehr auf Verschlüsselungstechnik und Virenschutz richten.

Offenbar hatte Herr Friedrich das Urteil des Bundesverfassungsgerichts vom 27. Februar 2008 völlig vergessen, das dem Staat die Pflicht auferlegt, die Integrität und Vertraulichkeit informationstechnischer Systeme zu gewährleisten. Schon die Bezeichnung des Grundrechts beschreibt mit „Recht auf Gewährleistung“ eine staatliche Schutzpflicht. Es definiert einen objektiven Auftrag an den Staat, Maßnahmen zu ergreifen, um die Vertraulichkeit und Integrität informationstechnischer Systeme zu gewährleisten. Aus diesem Auftrag erwächst neben der grundrechtlichen Absicherung auch eine staatliche Infrastrukturverantwortung. Der Staat wird angehalten, den Bürgerinnen und Bürgern durch Rechtsetzung, Rechtsprechung oder Exekutivmaßnahmen einen sicheren Rahmen zu setzen, in dem sie - soweit möglich - trotz mangelnder Selbstschutzmaßnahmen auf die Unangetastetheit der von ihnen vielfältig genutzten komplexen Systeme vertrauen können. Der Staat kann sich auch angesichts der Spionageaffäre nicht aus seiner Verantwortung stehlen und seinen Bürgerinnen und Bürgern auferlegen, doch gefälligst selbst für die Sicherheit ihrer Smartphones und ihrer Personalcomputer zu sorgen.

Angesichts dieser Entwicklung müssen wir uns besorgt fragen, ob es schon wieder soweit ist, dass wir uns überlegen müssen, was wir am Telefon sagen, was wir einer E-Mail anvertrauen und welche Seiten wir im Internet besuchen. Können wir sicher sein, dass Geheimdienste nur das tun, was sie dürfen oder dürfen Geheimdienste inzwischen all das, was sie tun? Ist die Bundesregierung noch in der Lage, die Grundrechte zu gewährleisten? Sind unsere Grundrechte in Gefahr?

Prof. Dr. Heribert Prantl (Chefredaktion Süddeutsche Zeitung) hat das Dilemma in seiner Rede anlässlich der Festveranstaltung zum 8. Europäischen Datenschutztag in Berlin auf den Punkt gebracht, indem er unter dem Vortragstitel „Bettelnde Grundrechte“ beschrieb, wie sich Geheimdienste über die Verfassung und die Fundamente des Rechts erheben. „Digitale Inquisition“ nannte Heribert Prantl diese umfassende Überwachung des Internet. Sie tue zwar nicht körperlich weh, aber mache Kommunikation unfrei. Das Fernmeldegeheimnis gelte nur noch dem Namen nach. Bürgerinnen und Bürger könnten nicht mehr wissen, wer was wann über sie wisse, so Prantl.

Was hatte das Bundesverfassungsgericht in seinem wegweisenden Urteil im Dezember 1983 gesagt?: „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen.“

Angesichts dieser Bedrohungen muss vor allem die Bundesregierung handeln. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat jedoch in ihrer Entschließung vom 5. September 2013 festgestellt, dass noch immer nicht alles getan wurde, um das Ausmaß der nachrichtendienstlichen Ermittlungen mithilfe von Programmen wie PRISM und TEMPORA für die Bundesrepublik Deutschland aufzuklären (siehe Punkt 6.3.3). Nicht nur eine bessere Kontrolle der Geheimdienste und völkerrechtlichen Abkommen sind gefordert. Nötig sind auch Gesetzesinitiativen, die die informationelle Selbstbestimmung und das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme sicherstellen. Da ist sicher die Frage angebracht, ob die entsprechenden Aktivitäten der Bundesregierung diesen Anforderungen genügen.

Die Bilanz fällt eher bescheiden aus, wie die folgenden Beispiele zeigen.

Mit dem neuen Personalausweis wurde zwar eine hervorragende technische Infrastruktur geschaffen, die endlich eine sichere gegenseitige Identifizierung zwischen Bürgern und Dienstleistern im staatlichen und kommerziellen Bereich erlaubt. Doch die Bundesregierung konterkariert diese wunderbare Technik, indem sie einen eher fragwürdigen Umgang mit Berechtigungen zum Auslesen der Daten aus dem Ausweis zulässt und zudem nach wie vor und wider besseren Wissens den Bürgerinnen und Bürgern die Nutzung unsicherer Kartenlesegeräte empfiehlt und somit das Vertrauen in die neue Technik untergräbt (siehe Punkt 6.4.5).

Mit De-Mail unternimmt die Bundesregierung den Versuch, eine vertrauenswürdige und sichere Kommunikationsinfrastruktur zu entwickeln. Aber anstatt eine dem Stand der Technik genügende Struktur mit sicherer Ende-zu-Ende-Verschlüsselung bereitzustellen, werden Sollbruchstellen eingebaut, die prinzipiell das unbefugte Mitlesen und Verändern von De-Mails ermöglichen (siehe Punkt 3.2).

Das Artikelgesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften ist am 1. August 2013 in wesentlichen Teilen in Kraft getreten. Ziel des Gesetzes ist es, die elektronische Kommunikation mit der Verwaltung zu erleichtern. Es drängt sich der Eindruck auf, dass Erleichterung in diesem Zusammenhang vor allem ein Absenken der Sicherheitsanforderungen an die elektronische Kommunikation bedeutet. Denn offenbar hat es die Bundesregierung nun endgültig aufgegeben, das hervorragende Konzept der qualifizierten elektronischen Signatur in die Fläche zu bringen. Stattdessen werden andere Verfahren bereitgestellt, mit denen die handschriftliche Unterschrift durch die elektronische Form ersetzt werden kann. Jedoch ist festzustellen, dass die mit dem Artikelgesetz neu zugelassenen Möglichkeiten zum Ersatz einer durch Rechtsvorschrift angeordneten Schriftform durch die elektronische Form hinsichtlich Vertrauenswürdigkeit und Sicherheit mit der qualifizierten elektronischen Signatur nicht zu vergleichen sind. Der Gesetzgeber spricht nämlich lediglich von „anderen Verfahren“ und vermeidet offenbar bewusst den Begriff „vergleichbare Verfahren“ (siehe Punkt 3.2).

Auf die Kommunen unseres Landes kommen mit den neuen E-Government-Vorhaben erhebliche technische und organisatorische Anforderungen zu. Die Kommunen sind erster Anlaufpunkt für Bürgerinnen und Bürger, wenn sie staatliche Dienstleistungen in Anspruch nehmen wollen. Dies erfordert auch dort eine funktionierende, vertrauenswürdige und vor allem sichere IT-Infrastruktur. Da verwundert es schon, dass der IT-Planungsrat mit der „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ zwar für Bundes- und Landesbehörden verbindliche Sicherheitsziele für die Informationstechnik vorgibt, die Anwendung der Leitlinie den Kommunen jedoch lediglich empfiehlt (siehe Punkt 4.3). Die Mehrzahl der Mitglieder des IT-Planungsrates befürchtet offenbar, dass die Kommunen mit der Durchsetzung der Leitlinie und der Anwendung der IT-Grundschutzmethodik fachlich, personell und finanziell überfordert wären.

Und leider sind diese Befürchtungen offenbar berechtigt. Im Sommer 2013 haben wir eine Sicherheitslücke im Verfahren für das Personenstandswesen festgestellt (siehe Punkt 6.4.6). Uns überrascht das nicht sonderlich, denn bereits im Neunten Tätigkeitsbericht hatten wir im Ergebnis einer umfangreichen Untersuchung auf zahlreiche Datenschutzprobleme in den Kommunalverwaltungen hingewiesen (siehe Neunter Tätigkeitsbericht, Punkt 6). Es ist schon bedenklich, dass offenbar nach wie vor keine angemessenen Konsequenzen gezogen wurden und die Kommunen mangels ausreichender Personal- und Finanzausstattung erhebliche Schwierigkeiten bei der Umsetzung der sicherheitstechnischen und datenschutzrechtlichen Anforderungen etwa der neuen E-Government-Verfahren haben.

Es stellen sich zwangsläufig einige Fragen: Wäre es zielführend, die Kommunen besser finanziell und personell auszustatten? Sollte der Landesdienstleister, die DVZ M-V GmbH, mehr Aufgaben im kommunalen Bereich übernehmen? Sollte das Beispiel der interkommunalen Zusammenarbeit zwischen der Landeshauptstadt Schwerin und dem Landkreis Ludwigslust-Parchim Schule machen? Brauchen wir künftig kommunale Rechenzentren als Dienstleister für Städte und Gemeinden? Es ist schnellstmöglich zu klären, wie mit Blick auf die ständig zunehmenden Anforderungen an Datenschutz und IT-Sicherheit im kommunalen Bereich reagiert werden muss.

Im Jahr 2014 wird das amerikanische Unternehmen Facebook zehn Jahre alt. Die weltweiten Nutzerzahlen haben inzwischen die Milliardengrenze überschritten. Da wir die Dienste dieses Unternehmens nicht mit deutschem Datenschutzrecht vereinbar halten, haben wir insbesondere den öffentlichen Stellen in Mecklenburg-Vorpommern bereits im Oktober 2011 empfohlen, keine Facebook-Fanpages einzurichten. Inzwischen hat aber das Schleswig-Holsteinische Verwaltungsgericht auf drei Klagen von Unternehmen in Schleswig-Holstein geurteilt, dass deutsche Betreiber von Facebook-Fanpages für die bei Facebook erfolgende Datenverarbeitung datenschutzrechtlich in keiner Weise verantwortlich gemacht werden können. Für den Datenschutz im Internet sind die Entscheidungen eine weitgehende Kapitulation. Mit aufsichtsrechtlichen Maßnahmen können deutsche Datenschutzbehörden dem Treiben von Facebook und Co. nun kaum noch Einhalt gebieten. Umso wichtiger ist es, Nutzerinnen und Nutzer über die Risiken der Nutzung zu informieren und sie für einen datenschutzgerechten Umgang mit personenbezogenen Daten zu sensibilisieren.

Wir haben daher ein umfangreiches Bildungspaket initiiert, das insbesondere auf die Zielgruppe der jungen Menschen in Mecklenburg-Vorpommern ausgerichtet ist (siehe Punkt 2). Verschiedene Projekte sollen sowohl die Chancen aufzeigen, die die mediale Welt bietet, als auch die Risiken, die mit der Nutzung der modernen Technik verbunden sind. Ein Schwerpunkt ist das Projekt „Medienscouts MV“ (siehe Punkt 2.2). Es unterstützt insbesondere Jugendliche im Alter von 14 - 16 Jahren, aber auch Lehrerinnen und Lehrer und Schulsozialarbeiterinnen und Schulsozialarbeiter dabei, das Wissen zum Umgang mit diesen Medien zu erwerben und zu erweitern. Die Umsetzung des Ziels „Datenschutz durch Bildung“ fängt im Kindesalter an und hört bei der Ausbildung, im Studium und bei der Fortbildung nicht auf. Wir sind in diesen Projekten intensiv tätig und auch zu weiterem Engagement bereit. Künftig wird jedoch noch mehr die Unterstützung der staatlichen Bildungsinstitutionen und die des Parlaments erforderlich sein, damit jeder junge Mensch in Mecklenburg-Vorpommern mehrmals qualifizierte Bildungsangebote zu den Themen Medienkompetenz, Datenschutz und Urheberrecht wahrnehmen kann.

Die NSA-Affäre hat sicher dazu beigetragen, dass auch Unternehmen in zunehmendem Maße den Datenschutz berücksichtigen. Sie haben erkannt, dass ihre Angebote, Produkte und Dienstleistungen nur dann für Kundinnen und Kunden vertrauenswürdig und somit wettbewerbsfähig sind, wenn sie den Datenschutz in angemessener Weise berücksichtigen. Unternehmen erkennen immer öfter, dass Datenschutz ein Wettbewerbsvorteil sein kann und tatsächlich ist. Manchmal ist dafür zwar auch intensive Beratung durch uns nötig (siehe Punkt 5.1.2), aber wenn im Ergebnis datenschutzfreundliche Lösungen gefunden werden, ist die Beratungszeit gut investiert.

Im Bereich der Videoüberwachung (siehe Punkt 5.2) hat sich die Idee vom Kundenvertrauen durch Datenschutz noch nicht überall durchgesetzt. Oft lassen sich Unternehmen von kostengünstigen Produkten verleiten, die inzwischen immer öfter um moderne Internettechnologien ergänzt werden. Dass durch preiswerte Technik, die zudem einfach bedienbar ist, sehr schnell neue Begehrlichkeiten entstehen, liegt auf der Hand. Und wenn dann die klassische Videoüberwachung durch Technologien zur Gesichts- und sogar Verhaltenserkennung ergänzt wird, sind Eingriffe in die Privatsphäre sowohl von Kundinnen und Kunden als auch von Beschäftigten vorprogrammiert. Mit dieser Technik werden in zunehmendem Maße Daten unter dem Vorwand erhoben, den Service zu verbessern. Zur lückenlosen Überwachung von Beschäftigten ist es dann nur noch ein kleiner Schritt, der von manchen Arbeitgebern leider allzu bedenkenlos gegangen wird. Offenbar wird in vielen Fällen ein Rechtsbruch bewusst einkalkuliert. Sanktionen sind zunächst ja auch nicht zu erwarten, ein diesbezügliches Ordnungswidrigkeitsverfahren dauert inzwischen 3 Jahre.

Unsere Beratungspraxis zeigt jedoch, dass betriebliche Interessen durchaus mit Persönlichkeitsrechten in Übereinstimmung gebracht werden können, wenn die Prinzipien des Datenschutzes von vornherein berücksichtigt werden.

Die Aufgaben, die uns der Gesetzgeber mit dem Informationsfreiheitsgesetz zugewiesen hat, nehmen immer mehr Zeit in Anspruch. Der Abschnitt 9 dieses Berichts gibt nur einen kleinen Einblick in die Vielfalt der Fragen, mit denen wir konfrontiert werden. Obwohl es kein Grundrecht auf Informationsfreiheit gibt, haben neben dem Bund inzwischen elf Bundesländer ein Informationsfreiheits- bzw. Transparenzgesetz verabschiedet. Es wird inzwischen in zunehmendem Maße deutlich, dass Informationen notwendig sind, damit Bürgerinnen und Bürger Entscheidungen aller Ebenen von Legislative und Exekutive verstehen und möglichst daran mitwirken - Vertrauen durch Transparenz! Mit den vielfältigen Projekten in den Bereichen Open Data und Open Government ist ein erfolgversprechender Prozess in Gang gekommen, noch verhalten, aber in die richtige Richtung.

Die Gewährleistung von Datenschutz und Informationsfreiheit ist neben rechtlichen Vorschriften natürlich auch an bestimmte technische Voraussetzungen gebunden. Vorrangig ist es aber eine Einstellungsfrage. Es geht um die Gewährleistung von Bürgerrechten. Es geht um Grundrechte.

1 Empfehlungen

1.1 Zusammenfassung aller Empfehlungen

Wir empfehlen der Landesregierung, kurzfristig dafür Sorge zu tragen, dass jeder junge Mensch in Mecklenburg-Vorpommern mehrmals qualifizierte Bildungsangebote zu den Themen Medienkompetenz (Mediennutzung), Datenschutz und Urheberrecht wahrnimmt (siehe Punkt 2.10).

Wir empfehlen den Kommunen, unabhängig von der Position des IT-Planungsrates die Vorgaben der „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ umzusetzen und erwarten, dass sie für Verfahren zur automatisierten Verarbeitung personenbezogener Daten insbesondere bei modernen E-Goverment-Verfahren die Grundschutzmethodik des BSI in vollem Umfang anwenden (siehe Punkt 4.3).

Wir empfehlen der Landesregierung, Datenschutzaspekte bei der Entwicklung und beim Einsatz elektronischer Identifizierungs- und Signaturverfahren im E-Government in angemessener Weise zu berücksichtigen und insbesondere den Datenschutzanforderungen im Hinblick auf Transparenz, Betroffenenrechte und Zweckbindung den erforderlichen Stellenwert zukommen zu lassen (siehe Punkt 4.4).

Wir empfehlen der Landesregierung, bei der elektronischen Übermittlung personenbezogener Daten, insbesondere bei modernen E-Goverment-Verfahren, regelmäßig Verschlüsselungsverfahren nach dem Stand der Technik einzusetzen und nur in begründeten Ausnahmefällen auf eine Ende-zu-Ende-Verschlüsselung zu verzichten (siehe Punkt 4.5).

Wir empfehlen der Landesregierung, sich frühzeitig mit den künftigen Datenschutzanforderungen an Cloud-Computing zu befassen, damit vorhandene Strukturen nach dem Inkrafttreten der EU-Datenschutz-Grundverordnung schnell angepasst und laufende Planungen schon jetzt entsprechend beeinflusst werden können (siehe Punkt 5.1.4).

Wir empfehlen der Landesregierung, bei der Planung und Entwicklung von IT-Verfahren, die die gemeinsame Nutzung von Systemen und Programmen zur automatisierten Verarbeitung personenbezogener Daten vorsehen, die gegebenenfalls erforderliche Mandantenfähigkeit durch die Anwendung der Orientierungshilfe sorgfältig zu prüfen. Zudem sollten bereits im Betrieb befindliche Verfahren auf ihre Mandantenfähigkeit überprüft und gegebenenfalls nachgebessert werden (siehe Punkt 5.1.9).

Wir empfehlen der Landesregierung, sich dafür einzusetzen, dass bei der Übermittlung der Meldedaten von den Meldebehörden an die Kirchen und an die GEZ ein dem Stand der Technik entsprechendes Verfahren eingesetzt wird. Hierbei bietet sich das OSCI-Protokoll an, welches schon für die regelmäßige Datenübermittlung zwischen den Meldebehörden verschiedener Länder genutzt wird. Aufgrund seiner Möglichkeit zur kryptographischen Verschlüsselung und Signatur wird das OSCI-Protokoll hier in § 2 Abs. 3 Satz 1 der 1. Verordnung zur Durchführung von regelmäßigen Datenübermittlungen der Meldebehörden (BMeldDÜV) gefordert (siehe Punkt 6.4.4).

Angesichts der zunehmenden Bedeutung des neuen Personalausweises (siehe bspw. Punkt 3.2) empfehlen wir den Bürgerinnen und Bürgern nach wie vor, nur Ausweislesegeräte mit eigenem Tastaturfeld zu nutzen. Der Landesregierung wird empfohlen, vorhandene Risiken nicht zu verharmlosen, sondern den Einsatz von Lesern und mit eigener Tastatur ausdrücklich zu empfehlen und im Rahmen von E-Government-Initiativen finanziell zu fördern (siehe Punkt 6.4.5).

Wir empfehlen allen Stellen, die die eID-Funktion des neuen Personalausweises über den einheitlichen nPA-Identifikationsdienst im Bürgerportal nutzen möchten, sehr sorgfältig zu prüfen, ob das vom eGo-MV beschaffte Berechtigungszertifikat mit genutzt werden kann oder ob nicht ein separates Berechtigungszertifikat erforderlich ist (siehe Punkt 6.4.5).

Wir empfehlen der Landesregierung, die Leitlinie zur Informationssicherheit auch für die Kommunalverwaltungen verbindlich vorzuschreiben und die Kommunen dabei zu unterstützen, eine angemessene Informationssicherheit und den erforderlichen Datenschutz zu gewährleisten. Dies gilt insbesondere für die Verarbeitung personenbezogener Daten in modernen E-Government-Verfahren (siehe Punkt 6.4.6).

Es ist wünschenswert, dass die Landesregierung die vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit angesprochenen Überlegungen in der weiteren Diskussion über den bundesrechtlichen Rahmen für den Zensus 2021 unterstützt und auch die im Rahmen der Durchführung des Zensus 2011 gesammelten Erfahrungen bei der Ausgestaltung der landesrechtlichen Vorschriften für den Zensus 2021 berücksichtigt (siehe Punkt 6.7).

Wir bitten die Landesregierung, die im Bericht dargelegten datenschutzrechtlichen Bedenken im weiteren Verfahren hinsichtlich der Einführung der „Bettensteuer“ zu berücksichtigen und sich für eine satzungsrechtliche Regelung einzusetzen, die den datenschutzrechtlichen Belangen in der beschriebenen Weise entspricht (siehe Punkt 6.8.3).

Wir empfehlen der Landesregierung, für eine einheitliche Ausstattung der Arbeitsplätze in den Landesbehörden mit Verschlüsselungstechnik zu sorgen, damit ein gesicherter Versand von vertraulichen Nachrichten möglich ist (siehe Punkt 6.9.2).

Wir empfehlen, die Erfahrungen zum Beispiel Hamburgs berücksichtigend, eine Novellierung des Informationsfreiheitsgesetzes zu prüfen. Wichtig sind dabei insbesondere eine proaktive Veröffentlichungspflicht aller öffentlichen Stellen, die Veröffentlichung von Verträgen, die mit der öffentlichen Hand geschlossen werden, und die Einrichtung eines Open-Data-Portals (siehe Punkt 9.1).

Wir empfehlen dem Landtag, den Gesetzeswortlaut von § 1 Abs. 3 IFG M-V nicht zu ändern (siehe Punkt 9.5).

1.2 Umsetzung der Empfehlungen des Zehnten Tätigkeitsberichtes

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt im 10. TB
1	Ich empfehle der Landesregierung, sich hinsichtlich der Umsetzung der Koalitionsziffern 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).	Seit längerer Zeit arbeitet auf Landesebene die LAG Rahmenvereinbarung unter dem Vorsitz der Staatskanzlei, die sich seit etwa zwei Jahren auch explizit mit dem Thema Datenschutz befasst. Auch ist hierbei eine Vernetzung mit dem Landesnetzwerk „Medienkompetenz“ geplant. Darüber hinaus sind uns keine Maßnahmen der Landesregierung auf diesem Gebiet bekannt.	2.1
2	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.	Bislang haben wir hierzu keine Rückmeldung von der Landesregierung erhalten. Stichprobenartig durchgeführte Kontrollen ergaben aber, dass die Empfehlung zum großen Teil nicht berücksichtigt wurde.	2.2.1
3	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.	Wir konnten diesbezüglich keine Aktivitäten der Landesregierung beobachten.	3.1
4	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.	Es sind keine Unternehmungen der Landesregierung auf diesem Gebiet bekannt, die eine aktive Begleitung des Prozesses der Schaffung eines einheitlichen europäischen Datenschutzstandards zeigen.	3.1.1

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt im 10. TB
5	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.	Uns ist nicht bekannt, dass die Landesregierung diese Empfehlung aufgegriffen hat. Durch das neue E-Government-Gesetz wurden die Anwendungsmöglichkeiten von De-Mail sogar ausgeweitet. Die Landesregierung hat diese Entwicklung nicht nur widerspruchslos hingenommen, sondern sich im IT-Planungsrat ausdrücklich für das E-Government-Gesetz eingesetzt. Dem Entwurf eines Zweiten Gesetzes zur Änderung des Landesverwaltungsverfahrensgesetzes zufolge sollen die Regelungen des entsprechenden Bundesgesetzes im Rahmen der Simultangesetzgebung vollständig übernommen werden. Ausdrücklich zu begrüßen ist allerdings der Hinweis in der Begründung zu § 99 des Entwurfs, der auf die Besonderheiten des Versandes besonders schutzwürdiger Daten über De-Mail-Dienste verweist. Hier wird ausdrücklich darauf hingewiesen, dass von zusätzlichen Schutzvorkehrungen wie der Ende-zu-Ende-Verschlüsselung Gebrauch gemacht werden soll.	3.2.6
6	Ich empfehle der Landesregierung, sich für die personelle und finanzielle Unabhängigkeit der geplanten Stiftung Datenschutz einzusetzen und darauf hinzuwirken.	Das Ministerium für Inneres und Sport ist unserer Aufforderung gefolgt und hat das BMI im Juni 2012 gebeten darzulegen, ob und ggf. wie unsere Empfehlungen umgesetzt werden.	3.2.8
7	Ich empfehle dem Landesgesetzgeber, bestehende Unklarheiten im jetzigen § 18 DSG 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.	Unseres Wissens plant die Landesregierung eine Novellierung der entsprechenden Regelungen mit dem Ergebnis einer klaren Zuständigkeit der Medienanstalt Mecklenburg-Vorpommern. Wir begrüßen diese Absicht.	3.3.1
8	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.	Neben der Inanspruchnahme von Cloud-ähnlichen Dienstsleistungen der DVZ M-V GmbH sind uns keine Bestrebungen der Landesregierung zur Förderung landeseigener Cloud-Dienste bekannt.	4.1.1

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt im 10. TB
9	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.	Die Landesregierung erarbeitet gemeinsam mit der DVZ M-V GmbH eine Mobile-Device-Management-Lösung, mit der die Rahmenbedingungen für den Einsatz mobiler Geräte festgelegt werden soll.	4.1.4
10	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.	Uns sind keine Verfahren bekannt bzw. vorgestellt worden, bei denen die Hinweise der Broschüre relevant sind.	4.1.6
11	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.	Über die in der Stellungnahme der Landesregierung beschriebenen Maßnahmen im Zusammenhang mit der IP-Telefonie hinaus ist uns nicht bekannt, dass solche Prüfungen aufgenommen wurden.	4.3.1
12	Ich empfehle der Landesregierung, das IT-Managementsystem auf die gesamte Landesver-waltung 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.	Die Landesregierung weist in ihrer Stellungnahme darauf hin, dass alle Ressorts, die das sogenannte IT-Grundsystem einführen, automatisch Nutzer des IT-Managementsystems sind. In die Entwicklung des IT-Grundsystems wurde der Landesdatenschutz-beauftragte nicht einbezogen, sodass eine datenschutzrechtliche Bewertung nicht möglich ist.	4.3.6
13	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.	Nach Darstellung der Landesregierung werden zum Signieren von Urkunden Zertifikate benutzt, die aussagekräftige Angaben zur Identität der ausstellenden Amtsperson und ihrer Behörde enthalten. Die genannten Rechtsvorschriften wurden jedoch nicht klargestellt; die Landesregierung hat auch nicht darauf hingewirkt, soweit es dem Landesdatenschutzbeauftragten bekannt ist.	4.4.4

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt im 10. TB
14	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.	Die Landesregierung weist darauf hin, dass bei Einzelanfragen zu Meldedaten eine Datenübermittlung mittels verschlüsselter E-Mail oder E-Mail mit verschlüsseltem Anhang (neben einer schriftlichen Übermittlung) möglich ist, da hierdurch der Datenschutz ausreichend gewährleistet wird. Alle landesrechtlichen Regelungen zur gesicherten automatisierten Datenübermittlung aus dem ZIR wird im Rahmen der Einführung des Bundesmeldegesetzes auf eine neue Grundlage gestellt und dabei erneut überprüft.	5.4.6
15	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.	Die Landesregierung ist dieser Empfehlung nicht gefolgt und hat unsere diesbezüglichen Bemühungen im IT-Planungsrat nicht unterstützt. Die Kommunen sollen finanziell entlastet werden, indem akzeptiert wird, dass ein Berechtigungszertifikat für mehrere Anwendungen genutzt werden darf.	5.4.7
16	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.	In die Satzung des Norddeutschen Rundfunks über das Verfahren zur Leistung der Rundfunkbeiträge sind die datenschutzrechtlichen Belange zum größten Teil berücksichtigt worden. Kritikwürdig ist jedoch nach wie vor, dass der Beitragsservice ab dem 31.12.2014 Adressen von privaten Händlern ankaufen kann.	5.7.3

2 Bildungsprojekte

2.1 Ausgangspunkt

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

So wird im Beschluss der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder 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.“

Weiterhin wurde in einem Beschluss der Kultusministerkonferenz (KMK) zur „Medienbildung in der Schule“ vom 8. März 2012 erklärt: „Die Entwicklung von umfassender Medienkompetenz durch Medienbildung ist eine gesamtgesellschaftliche Aufgabe, die nur im Zusammenwirken von Schule und Elternhaus sowie mit den Verantwortlichen in Politik, Wirtschaft und Kultur bewältigt werden kann. Die neue KMK-Erklärung „Medienbildung in der Schule“ soll dazu beitragen, Medienbildung als Pflichtaufgabe schulischer Bildung nachhaltig zu verankern. Medienbildung befähigt zur Datensparsamkeit und zur Vermeidung von Datenspuren und fördert die digitale Sicherheit der persönlichen Kommunikation. Insoweit trägt Medienbildung auch zur eigenverantwortlichen informationellen Selbstbestimmung und zum persönlichen Datenschutz bei. Wünschenswert wären die Aktualisierung und Akzentuierung der Medienbildung in den einzelnen Fächern und die Formulierung eigener fächerübergreifender Kriterien der Medienbildung. In diesem Sinne ist Medienbildung sowohl in den Bildungswissenschaften als auch in der fachbezogenen Lehrerausbildung der ersten und zweiten Phase in den Prüfungsordnungen ausreichend und verbindlich zu verankern.

Diese grundlegende Ausbildung der Lehrkräfte muss fortgeführt und ergänzt werden durch entsprechende bedarfsgerechte Qualifizierungs- und Fortbildungsangebote, in denen Medienkompetenz und medienpädagogische Kompetenzen für bestimmte Anwendungssituationen und Aufgabenstellungen im Zusammenhang von Schule und Unterricht vermittelt und erworben werden können.“ (dritte Phase der Lehrerbildung).

Im KMK-Beschluss zur „Verbraucherbildung an Schulen“ vom 12. September 2013 wird noch einmal darauf hingewiesen, dass „Informationsbeschaffung und -bewertung, Datenschutz und Urheberrechte sowie Mediennutzung“ wichtige Themen und Handlungsfelder im Bereich Medien und Information sind. Nur wer die Verflechtungen des Marktes unter der Berücksichtigung verschiedener Perspektiven und die Einflussmöglichkeiten kennt, kann diese auch reflektieren und ein selbstbestimmtes Konsumverhalten entwickeln.

Es besteht eine weite Einigkeit in Bund und Ländern, dass es wichtig ist, Kinder und Jugendliche in unserer mediatisierten Welt zu begleiten, ihnen Chancen, aber auch Risiken aufzuzeigen. Hiermit halten wir die folgenden Maßnahmen für unverzichtbar:

- dauerhafte Implementierung der Themen wie Datenschutz, Datenspur, Umgang in sozialen Netzwerken, web 2.0, Umgang mit Schülerdaten in die Lehrerbildung (erste und zweite Phase) mit Einstufung als prüfungsrelevant, um die Qualitätsstandards zu sichern,
- kontinuierliche Fortbildung der Lehrerinnen und Lehrer (dritte Phase),
- Aktualisierung der Rahmenpläne in Bezug auf die mediale Bildung,
- qualifizierte Angebote für Schülerinnen und Schüler aller Altersgruppen.

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

2.2 Projekt „Medienscouts MV“

Die Nutzung der neuen Medien wird immer komplexer. Insbesondere bei der Nutzung des Internet geht es um Netzwerke, Chats, Communities, um den Schutz der persönlichen Daten, um das urheberrechtlich geschützte Hochladen von Fotos und Videos bei Youtube, Facebook & Co. oder um das illegale Film- und Musikdownload - und dabei gibt es viel zu beachten. Jedoch sind die digitalen Medien aus unserem Alltag nicht mehr wegzudenken und sie machen auch eine weltweite Kommunikation möglich - mit allen Chancen und Risiken.

Das Projekt „Medienscouts MV“ des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (www.medienscouts-mv.de) möchte sowohl die Chancen aufzeigen, die die mediale Welt bietet, als auch die Risiken. Es unterstützt insbesondere Jugendliche im Alter von 14 - 16 Jahren, aber auch Lehrerinnen und Lehrer und Schulsozialarbeiterinnen und Schulsozialarbeiter dabei, das Wissen zum Umgang mit diesen Medien zu erwerben und zu erweitern.

Was ist an dem Projekt „Medienscouts MV“ so besonders? Die Konzeptidee beruht auf dem peer-to-peer-Ansatz: Die Teilnehmerinnen und Teilnehmer erlernen Neues und erweitern ihr Wissen im Umgang mit den digitalen Medien und geben das Wissen dann an Freundinnen/Freunde, Mitschülerinnen/Mitschüler und andere Gleichaltrige weiter - das nennt man ,,Peer-Education". Mit diesem Ansatz gehen wir in ein Pilotprojekt, das es so in Mecklenburg-Vorpommern bisher noch nicht gab. Projektstart war im Juni 2012. Im ersten Schritt wurden mögliche Partner für dieses Gemeinschaftsprojekt angefragt. Das „Medienscouts MV“-Projekt wird seither unterstützt von der Landeskoordinierungsstelle für Suchtvorbeugung Mecklenburg-Vorpommern (LAKOST), dem Landesjugendring Mecklenburg-Vorpommern (LJR M-V), dem Landeskriminalamt Mecklenburg-Vorpommern (LKA M-V), der Medienanstalt Mecklenburg-Vorpommern (MMV) und deren Online-Selbsthilfeplattform juuuport sowie der ComputerSpielschule Greifswald (CSG).

Jugendliche können ihr Wissen viel besser untereinander weitergeben. So werden die Jugendlichen im Rahmen eines „Medienscouts MV“-Wochenendes von Freitag bis Sonntag fit gemacht im Umgang mit digitalen Medien. Nach einem Datenschutz-Plenum am Freitagnachmittag haben die Jugendlichen am Samstag unterschiedliche Workshops zur Auswahl: Cybercrime (LKA M-V), Datenspur & Urheberrecht (LfDI M-V), Cybermobbing (LAKOST) und Computerspiele (CSG). Weiterhin erhalten die Jugendlichen ein Methodentraining, um sich den Aufbau von Vorträgen und Workshops zu erarbeiten. Samstagabend unterstützen dann die „Medientrecker“ der Medienanstalt Mecklenburg-Vorpommern das Team der Organisatoren. Die „Medientrecker“ sind in der Medienkompetenzvermittlung ein wichtiger Baustein, denn hier können die Jugendlichen visuelle oder Audiobeiträge produzieren. Diese aktive Medienarbeit hat sich sehr bewährt, denn die Jugendlichen nehmen das Angebot gut an, sodass zahlreiche kreative Hörfunk- und Videobeiträge entstanden sind. Gleichzeitig erfahren sie dabei, wie manipulierbar mediale Produkte sein können.

Dieser ganzheitliche medienpädagogische Ansatz in Verbindung mit dem Kontakt zu den Jugendlichen sowie der Bereitstellung von Arbeitsmaterialien hat sich während der ersten drei Durchgänge (November 2012, Juni 2013 und Oktober 2013) bewährt. Die Medienscouts MV spezialisieren sich auf ein Thema. Gleichzeitig ist durch den Kontakt zum Expertenteam gesichert, dass sie fortwährend Ansprechpartner für die Durchführung von Vorträgen und Workshops an ihren Schulen finden. Somit ist auch die Nachbetreuung gesichert. Zusätzlich führen wir einmal jährlich ein landesweites Treffen aller Medienscouts MV durch, um neueste Entwicklungen aufzuzeigen, aber auch den Austausch mit den bereits ausgebildeten Medienscouts MV zu vertiefen.

Neben den Jugendlichen kann pro vertretener Schule auch eine Lehrkraft und/oder eine Schulsozialarbeiterin bzw. ein Schulsozialarbeiter an dem Wochenende teilnehmen. Dadurch erreichen wir eine enge Bindung an die Schule und an die Arbeit der Medienscouts MV direkt vor Ort. So haben die Medienscouts MV des ersten und des zweiten Durchgangs (ca. 40) allein im Jahr 2013 rund 1.800 Mitschülerinnen und Mitschüler, teilweise in der gleichen Klassenstufe bis hin zu Grundschulklassen, geschult. Damit erreichen wir eine Multiplikation des Wissens zum selbstbestimmten und sicheren Umgang im Netz, die mit alleiniger Kapazität des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern nicht möglich wäre. Mittlerweile gibt es an einigen Schulen in Mecklenburg-Vorpommern bereits die „2. Generation“ der Medienscouts MV. Das Projekt wird weitergeführt.

2.3 Schulungen für Lehrerinnen und Lehrer, Schulsozialarbeiterinnen und Schulsozialarbeiter sowie Fachkräfte der Jugendhilfe

Im Berichtszeitraum haben wir sechs Ganztagsschulungen für Lehrerinnen und Lehrer, Schulsozialarbeiterinnen und Schulsozialarbeiter sowie Fachkräfte der Jugendhilfe in Güstrow Schabernack durchgeführt und haben damit über 150 Multiplikatoren aus dem ganzen Land geschult. In den Schulungen ging es um Themen wie Datenschutz als Menschenrecht, Urheberrecht, meine Datenspur im Netz sowie der Umgang mit Schülerdaten und Sozialdatenschutz. Zu den Schulungen wurde jeweils ein Partner aus dem Medienaktiv-Netzwerk mit einbezogen, sodass auch Themen wie Mobbing, Cybercrime oder aktive Medienarbeit mit angeboten werden konnten. Diese Schulungen sind vom Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern als Fortbildungsveranstaltung anerkannt.

Darüber hinaus fanden auf Einladung beispielsweise Schulungen während der Kinderschutztagung 2012, der Schulleitertagung, der Familienbotschaften Mecklenburg-Vorpommern, der Fachtagung der Schulsozialarbeiter Mecklenburg-Vorpommern sowie für Fachkräfte der Suchthilfe statt. Durch die Kooperation mit dem Institut für Qualitätsmanagement (IQMV) halten wir unsere Angebote an Weiterbildungen für Schulen über den Bildungsserver Mecklenburg-Vorpommern stets aktuell, die jede Schule einzeln als „SchiLF-Tag“ (Schulinterne Lehrerfortbildung) belegen kann. So wurde beispielsweise am Albert-Einstein-Gymnasium Neubrandenburg eine komplette Fortbildungsreihe zum Thema Datenschutz durchgeführt. Auch fanden Ganztagsschulungen für Teilnehmerinnen und Teilnehmer am „Freiwilligen Sozialen Jahr“ statt. Diese sind zwischen 16 und 25 Jahre alt gewesen und arbeiteten beispielsweise in integrativen Werkstätten oder Kindergärten. Weiterhin wurden auf Anfrage Mitarbeiterinnen und Mitarbeiter der Ministerien, die medienpädagogischen Beraterinnen und Berater der Staatlichen Schulämter sowie von freien Trägern der Jugendhilfe geschult, zum Beispiel vom Paritätischen Wohlfahrtsverband, VSP gemeinnützige GmbH Verbund für Soziale Projekte Schwerin und andere.

2.4 Landesweite Netzwerke für Medienkompetenz

Auf dem Netzwerktreffen der Medienkompetenz-Partner in Mecklenburg-Vorpommern sind im September 2013 in Güstrow die bisher nebeneinander bestehenden Netzwerke „Medienaktiv M-V“ und das anlässlich des Safer Internet Day 2012 in Güstrow ins Leben gerufene „Medienkompetenz-Netzwerk M-V“ endgültig unter dem Namen „Medienaktiv M-V“ zusammengeführt worden. Zu den Initiatorinnen und Initiatoren gehören das Kompetenzzentrum und die Beratungsstelle für exzessive Mediennutzung und Medienabhängigkeit Schwerin der Evangelischen Suchtkrankenhilfe Mecklenburg-Vorpommern gGmbH, die Landeskoordinierungsstelle für Suchtvorbeugung Mecklenburg-Vorpommern, das Landeskriminalamt Mecklenburg-Vorpommern, die Medienanstalt Mecklenburg-Vorpommern, der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern und der Landesjugendring Mecklenburg-Vorpommern.

Das landesweite Netzwerk „Medienaktiv M-V“ (www.medienaktiv-mv.de) sieht seine Aufgabe darin, den konstruktiven Umgang mit Medien zu fördern. Etwa 50 Mitglieder - darunter Schulen, Vereine und Landesbehörden ebenso wie Suchtberater, Ärzte und Medienpädagogen - unterstützen die Vermittlung von Medienkompetenz. Sie ist eine Schlüsselkompetenz des 21. Jahrhunderts. „Medienaktiv M-V“ hat regionale Knotenpunkte, es macht Vorhandenes bekannter und verknüpft die medialen Partner. Gerade im Bereich der Medien ist es wichtig, dass beispielsweise Medienpädagogen, Jugendhilfe, Schule und Suchthilfe zusammenarbeiten, damit Kinder und Jugendliche lernen, ihr Leben inmitten der digitalen Medienwelt zu gestalten.

Durch die enge Kooperation aller Institutionen wurde ein weitumspannendes Netzwerk geschaffen, das es in diesem Umfang nur in Mecklenburg-Vorpommern gibt. Aus anderen Bundesländern wird daher sehr interessiert auf dieses Netzwerk geschaut. Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern nimmt durch die derzeitige Projektarbeit eine zentrale Rolle in den Mediennetzwerken und Kooperationen des Landes ein. Dies ist Ergebnis des stetigen und engagierten Auftretens und Unterstützens von Medienkompetenzprojekten.

Weiterhin nimmt unsere Behörde eine unterstützende Rolle bei der Umsetzung der Rahmenvereinbarung zur Medienkompetenzförderung in Mecklenburg-Vorpommern ein. Im Zuge der jetzigen Rahmenvereinbarung wurde bereits das Medienkompetenzportal durch die Medienanstalt Mecklenburg-Vorpommern umgesetzt. Auf dieser Internetseite (www.medienkompetenz-in-mv.de) sind alle Institutionen, Vereine und Verbände aufgeführt, die Medienbildung in Mecklenburg-Vorpommern anbieten. Dazu gehört ebenfalls der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern. Weiterhin haben wir zur Erstellung des Medienkompass MV ebenfalls mögliche Bausteine an Unterrichtseinheiten für alle Klassenstufen bereitgestellt. Der Medienkompass MV soll als Handreichung und Arbeitsmaterial den Lehrkräften hilfreiche Arbeitshinweise geben, wie Medienbildung aktiv in der Schule umgesetzt werden kann. Die Rahmenvereinbarung ist momentan unterzeichnet durch die Staatskanzlei sowie das Ministerium für Arbeit, Gleichstellung und Soziales Mecklenburg-Vorpommern, das Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern sowie die Medienanstalt Mecklenburg-Vorpommern. Im Zuge der Evaluation und Neuschreibung der Rahmenvereinbarung wird auch der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, auf Anregung der Staatskanzlei, Mitunterzeichner der neuen Vereinbarung.

2.5 „TEO - Tage ethischer Orientierung“

„Mein Klick - meine Verantwortung!?“ ist der Untertitel des neuen TEO-Moduls „protect privacy“, das in einer neuen Kooperation mit dem Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern durchgeführt wurde. „Tage ethischer Orientierung“ (TEO) ist ein schulkooperatives Modell der Evangelisch-Lutherischen Kirche in Norddeutschland und des Erzbistums Hamburg. Weiterhin unterstützen Referenten der Landeskoordinierungsstelle für Suchtvorbeugung Mecklenburg-Vorpommern, des Kompetenzzentrums und der Beratungsstelle für exzessive Mediennutzung und Medienabhängigkeit Schwerin der Evangelischen Suchtkrankenhilfe Mecklenburg-Vorpommern gGmbH, der ComputerSpielschule Greifswald und der „Medientrecker“ der Medienanstalt Mecklenburg-Vorpommern das Projekt. Innerhalb eines Jahres wurde dieses viertägige Modul gemeinsam konzipiert und im November 2013 dann erstmalig durchgeführt.

Dieses Modul ist speziell für die 5. und 6. Klassen konzipiert. Es geht dabei um Themen wie Datenspuren im Netz, soziale Netzwerke im Internet, Cybermobbing, Apps, Smartphones, Handys und Computerspiele und um den Blick auf die Menschenwürde angesichts der Nutzung digitaler Medien. Während der vier Tage haben die Schülerinnen und Schüler jeden Workshop besucht und gleichzeitig die Möglichkeit gehabt, in den Gruppenarbeitsphasen das Erlernte zu reflektieren. So haben sie sich nicht nur mit dem technischen Umgang mit den digitalen Medien vertraut gemacht, sondern sie haben sich auch eine Haltung und Einstellung zur Kommunikation im Internet erarbeitet. An dieser Veranstaltung haben über 100 Schülerinnen und Schüler aus Wesenberg und Bad Doberan teilgenommen.

Dieses Projekt wird weitergeführt, da es den Bedarf an den Schulen gibt.

2.6 Veranstaltungen an Schulen

Im Berichtszeitraum haben Mitarbeiterinnen und Mitarbeiter des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern im Rahmen der Projekte zum Datenschutz verschiedene Veranstaltungen an Schulen in Mecklenburg-Vorpommern durchgeführt. Die Zahl der Schulungen vor Ort ist insbesondere durch die zusätzliche personelle Verstärkung (Projekt) umsetzbar geworden. Die Vorträge, Workshops, Schulungen, Projekttage oder Unterrichtseinheiten von 1,5 Stunden und darüber hinaus auch thematische Elternabende waren kostenfrei und wurden sehr gern angenommen, da ein spezielles Budget für derartige Schulungen nur selten in ausreichender Höhe an den Schulen vorhanden ist. Gab es an den Schulen bereits ausgebildete Medienscouts MV, wurden diese bei der Durchführung der Veranstaltungen mit einbezogen.

Die Nachfrage nach diesen Veranstaltungen hat stetig zugenommen, sodass die Termine meist ein halbes Jahr im Voraus geplant und gebucht waren. Allein im Jahr 2013 wurden rund 2.000 Schülerinnen und Schüler zu Themen wie Datenschutz, Datenspur und Urheberrecht geschult. Dazu kommen noch Multiplikatoren wie Lehrerinnen und Lehrer, Schulsozialarbeiterinnen und Schulsozialarbeiter sowie Fachkräfte der Jugendhilfe.

Die Einschätzung dieser Veranstaltungen durch die Schülerinnen und Schüler war durchweg positiv - sie nahmen Tipps und Hinweise sehr gern auf. Denn es war meist das erste Mal, dass sie überhaupt auf die Gefahren im Netz sowie die technischen und rechtlichen Gegebenheiten (Persönlichkeitsrecht, Urheberrecht, Recht am eigenen Bild) aufmerksam gemacht wurden. Dabei verfolgen wir nicht den Ansatz der Reglementierung, sondern den des gemeinsamen Erarbeitens von Chancen und Risiken im Internet. Die Schülerinnen und Schüler werden zu einem selbstbestimmten Umgang mit den digitalen Medien motiviert. Denn nur wer die Gefahren kennt, kann ihnen auch begegnen. Die Einschätzung der Multiplikatoren war ebenfalls durchweg positiv. Sie schätzen diese Möglichkeiten, da sie oft nicht selbst über dieses Wissen zum Thema digitale Medien und Datenschutz verfügen.

2.7 Projekt „Medientango“

„Medientango - die emotionale Seite einer digitalen Welt“ ist ein gemeinsames Projekt folgender Partner: Evangelische Suchtkrankenhilfe Mecklenburg-Vorpommern gGmbH (dort: Kompetenzzentrum und Beratungsstelle für exzessive Mediennutzung und Medienabhängigkeit Schwerin), Landeskriminalamt Mecklenburg-Vorpommern, Landesbeauftragter für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, Landeskoordinierungsstelle für Suchtvorbeugung Mecklenburg-Vorpommern, Medienanstalt Mecklenburg-Vorpommern, Staatliche Schulämter des Landes (dort: medienpädagogische Beraterinnen/Berater) und ComputerSpielSchule Greifswald.

Im Jahr 2013 wurden diese Multiplikatoren-Schulungen zu digitalen Medien in Rostock und in Schwerin durchgeführt. Sie sind gedacht für Pädagoginnen und Pädagogen, für (Schul-)Sozialarbeiterinnen und (Schul-)Sozialarbeiter und auch für Eltern. Die dreistündigen Workshops befassen sich unter anderem mit folgenden Themen: Potenziale und Risiken von Computerspielen; Chancen und Risiken in sozialen Netzwerken im Internet; digitale Kommunikation - Dialog, Aufklärung und Regeln sind notwendig; Datenschutz und Privatsphäre; wie bewege ich mich sicher im Netz – die Gefahren sind vielfältig - Überblick und Aufklärung; Beispiele eines mediengestützten Unterrichts. Dabei wird nicht nur theoretisches Wissen vermittelt, sondern die Teilnehmerinnen und Teilnehmer können ihre Kenntnisse auch praktisch umsetzen.

Das Projekt wird weitergeführt.

2.8 Projekt „Netzwerkstar II“

Um auf spielerische Art und Weise Informationen und Wissen rund um das Thema soziale Netzwerke im Internet zu vermitteln, hatte der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern zusammen mit Frau Prof. Dr.-Ing. Antje Düsterhöft von der Hochschule Wismar, Bereich Elektrotechnik und Informatik, Multimediasysteme/Datenbanken, und einigen Studenten der Hochschule Wismar sowie der Designerin Caterina Muth aus Neubrandenburg bereits 2010/2011 das Online-Lernspiel „Netzwerkstar I“ (www.netzwerkstar.de) entwickelt. Das Spiel ist konzipiert für Kinder im Alter von sieben bis zehn Jahren, die sich erstmalig in sozialen Netzwerken im Internet anmelden. Da dieses Spiel gut angenommen und 2011 mit dem Landespräventionspreis ausgezeichnet wurde, gab es den Wunsch nach einem Online-Lernspiel für Kinder und Jugendliche der Altersgruppe zehn bis vierzehn - „Netzwerkstar II“.

„Netzwerkstar II“ setzt sich mit dem verantwortungsvollen und selbstbestimmten Umgang in der digitalen Welt auseinander. Die Mediennutzung wird immer komplexer: Datenschutz, Urheberrecht, Leistungsschutzrecht etc. - es sind viele Punkte zu beachten; doch sind die digitalen Medien aus unserem Alltag nicht mehr wegzudenken und sie machen auch eine weltweite Kommunikation möglich.

„Netzwerkstar II“ gehört zu dem Genre der Point-&-Click-Adventures. Das Spiel beinhaltet Wissen zu den Themen Urheberrecht, Umgang in sozialen Netzwerken, Passwörter, Privatsphäreeinstellungen etc., das von den Kindern und Jugendlichen eher unbewusst und spielerisch aufgenommen werden soll. Wir haben diese Form des impliziten Lernens gewählt, da sie es ermöglicht, den Spielerinnen und Spielern Wissen zu aktuellen und wichtigen Themen zu vermitteln. Es ist ein Browserspiel, das in „html 5“ programmiert wird. Es sollte auf jedem üblichen Browser spielbar sein, unabhängig vom Ausgabemedium und Betriebssystem. Das Spiel eignet sich auch dazu, im Unterricht eingesetzt zu werden, da es auf eine Schulstunde angelegt ist.

Für dieses Projekt konnten wir wieder Frau Prof. Dr.-Ing. Antje Düsterhöft von der Hochschule Wismar gewinnen sowie die Grafik- und Designschule Schwerin. Das Landeskriminalamt Mecklenburg-Vorpommern kooperiert ebenfalls bei der Entwicklung des Spiels. Derzeit haben wir eine Beta-Version, die im laufenden Semester von Studenten der Hochschule Wismar modifiziert wird im Hinblick auf Animationen und Bewegungsabläufe. Danach ist „Netzwerkstar II“ ebenfalls zu finden unter www.netzwerkstar.de.

2.9 Projekt „PeerCon“

Vor allem Kinder und Jugendliche bewegen sich ganz selbstverständlich in sozialen Netzwerken im Internet wie Facebook und geben dabei zahlreiche persönliche Daten preis, präsentieren ihre Lebensumstände offen und detailliert im Netz. In zunehmendem Maße werden solche Netze auch im schulischen Bereich eingesetzt, zum Beispiel für die Bereitstellung von Unterrichtsmaterialien oder zur Koordinierung schulischer Termine (siehe auch Punkt 6.9.6).

Der Umgang mit personenbezogenen Daten im Internet beschäftigt die Datenschutzbeauftragten von Bund und Ländern schon geraume Zeit. Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) hat die sogenannte Reichweitenanalyse bei Facebook (siehe Neunter Tätigkeitsbericht, Punkt 2.2.1) datenschutzrechtlich bewertet. Die technische und rechtliche Untersuchung hat gezeigt, dass nicht nur diese Analysen nach Einschätzung der Datenschutzbehörden gegen das Telemediengesetz (TMG) und das Bundesdatenschutzgesetz (BDSG) bzw. die jeweiligen Landesdatenschutzgesetze verstoßen und eine rechtskonforme Nutzung von den meisten großen sozialen Netzwerken zurzeit nicht möglich ist. Es ist allerdings wenig erfolgversprechend, Kindern und Jugendlichen die Nutzung zentraler Netzwerke wie Facebook zu verbieten.

Vor diesem Hintergrund haben wir uns überlegt, dass es neben der Aufklärung von Kindern und Jugendlichen hinsichtlich des bewussten Umgangs mit personenbezogenen Daten im Internet sinnvoll ist, eine soziale Plattform zu bieten, die dem deutschen Datenschutzrecht entspricht und keine Datensammelstelle ist. Dieses Vorhaben erfährt nun ganz aktuellen Nachdruck durch das Bekanntwerden der digitalen Überwachung und Auswertung von persönlichen Daten bei großen Internetkonzernen durch US-amerikanische Geheimdienste im Zuge des Programms „PRISM“ (siehe Punkt 6.3.3).

Sollen soziale Netzwerke im Internet auch für schulische Zwecke genutzt werden, müssen diese Netze auch den Anforderungen des deutschen Datenschutzrechts genügen. Insbesondere muss erreicht werden, dass die Daten der Nutzerinnen und Nutzer weitgehend unter eigener Kontrolle bleiben. Eine Übermittlung der Daten an Plattformbetreiber in den USA wie Facebook muss ausgeschlossen werden. Mit zentral organisierten sozialen Netzen lässt sich dies praktisch nicht realisieren. Als Alternative kommen Netze in Frage, die dezentral organisiert sind. Besonders hervorgetan hat sich diesbezüglich das Netz Friendica.

Friendica ist ein dezentrales soziales Netzwerk auf Basis von Open Source Software und ähnelt im Seitenaufbau und in der intuitiven Bedienung stark denen anderer sozialer Netzwerke. Auch das Trennen sozialer Sphären durch Erstellen von verschiedenen Profilen wird angeboten. So ist es möglich, ein öffentliches, für jeden einsehbares Profil zu generieren und darüber hinaus weitere Profile anzulegen, die ganz gezielt nur von ausgewählten Kontakten eingesehen werden können. Dies ist gerade im Umfeld eines Schulnetzes sinnvoll, weil dort ein besonderes Interesse zu erwarten ist, mit verschiedenen Identitäten zu agieren, etwa mit dem Klarnamen gegenüber den Lehrkräften, mit Pseudonym A im Kreise der Familie und mit Pseudonym B im Freundeskreis. Außerdem bietet Friendica die Möglichkeit, bereits bestehende Kontakte aus Facebook, Twitter und anderen Diensten einzubinden, sodass keine Abkapselung vom bestehenden Freundeskreis befürchtet werden muss.

Unser Projekt „PeerCon“ (Peer Connection) soll Kinder und Jugendliche animieren, für die private Kommunikation in zunehmendem Maße die datenschutzkonforme Alternative Friendica zu nutzen. Zudem soll die Möglichkeit eröffnet werden, die schulbezogene Kommunikation mit und zwischen Lehrerinnen und Lehrern, Eltern, Schulsozialarbeiterinnen und Schulsozialarbeitern über Friendica abzuwickeln, außerschulische Projekte, Wettbewerbe und Aktionen zu bewerben und Informationen zu Ausbildung und Studium bereitzustellen und somit in allen Bereichen des Alltags von Kindern und Jugendlichen, ob diese nun schulischen oder außerschulischen Inhalts sind, unterstützend zur Verfügung zu stehen.

Prinzipiell könnten sofort bereits bestehende öffentliche Friendica-Server genutzt werden. Sinn des Projektes soll jedoch vor allem sein, dass jede Nutzerin bzw. jeder Nutzer selbst kontrolliert, was mit ihren/seinen Daten geschieht und auch lernt, sorgsam und verantwortungsbewusst mit den eigenen Daten und den Daten Dritter umzugehen. Nur, wer einen eigenen Server betreibt, kann uneingeschränkt bestimmen, welche Optionen genutzt werden und was mit den auf dem Server gespeicherten Daten geschieht.

Im Rahmen des Projektes soll zum Aufbau der erforderlichen Infrastruktur zunächst ein Server aufgesetzt werden, um Friendica an etwa fünf Schulen anzubieten. An diesen Schulen wird erprobt, wie die Interaktion der entsprechenden Interessengruppen (Schülerinnen und Schüler, Eltern, Lehrkräfte, Schulsozialarbeiterinnen und Schulsozialarbeiter, Jugendarbeiterinnen und Jugendarbeiter, Verwaltung u. a.) und die Verknüpfung der einzelnen Schulen gelingen. Im nächsten Schritt soll angestrebt werden, dass möglichst viele Schulen einen eigenen Server erhalten, auf dem jede Schülerin und jeder Schüler ihr bzw. sein Friendica-Profil nach eigenen Wünschen einrichten kann. Im letzten Schritt sollten dann möglichst viele Schülerinnen und Schüler mit Hilfe ihres Heim-PC einen eigenen Friendica-Server aufsetzen.

Es ist unrealistisch anzunehmen, dass jede Schülerin und jeder Schüler ihren bzw. seinen eigenen Friendica-Server betreibt. Ziel des Projektes ist es jedoch, das Netz stark zu dezentralisieren, indem möglichst viele Schülerinnen und Schüler eigene Server aufsetzen und somit „Herr ihrer Daten“ werden. Auch sollen die Schülerinnen und Schüler erkennen, dass der überwiegende Teil der jetzt über Facebook stattfindenden Kommunikation in praktisch gleicher Qualität über das Friendica-Projekt „PeerCon“ abgewickelt werden kann, mit dem Vorteil der weitgehenden Selbstbestimmung über die personenbezogenen Daten und der Möglichkeit der Gestaltung und der Reichweite der Kommunikation.

Zur Koordinierung und datenschutzrechtlichen Begleitung des Projektes stellen wir eine Projektstelle zur Verfügung. Durch Verzahnung mit unserem bereits laufenden Projekt „Medienscouts MV“ (siehe Punkt 2.2) können Kenntnisse zum Projekt „PeerCon“ vermittelt werden. Zur Realisierung des Projektes ist auch die Zusammenarbeit mit dem Ministerium für Arbeit, Gleichstellung und Soziales Mecklenburg-Vorpommern als Unterstützung im Rahmen des Landesjugendplanes, mit dem Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern als Werbeplattform bei Schulleiterinnen und Schulleitern sowie Lehrerinnen und Lehrern und mit einem technischen Dienstleister für das Aufsetzen und den Betrieb der Friendica-Server geplant.

An dieser Stelle soll auf die aktuelle Diskussion zum Verbot des dienstlichen Lehrer-Schüler-Kontakts über Facebook wie in Baden-Württemberg, Rheinland-Pfalz, Bayern und Schleswig-Holstein eingegangen werden. Unsere Erfahrungen in zahlreichen Schulungs- und Informationsveranstaltungen vor Ort sowie in regelmäßigen Fortbildungen für Lehrkräfte und Schulsozialarbeiterinnen und Sozialarbeiter zeigen, dass auch hier in Mecklenburg-Vorpommern Facebook längst in den Schulalltag eingezogen ist. Dies ist vielleicht naheliegend, da die Kommunikation über soziale Netzwerke für Lehrkräfte, beispielsweise die Nachricht über kurzfristige Stundenplanänderungen, schnell erfolgen kann. Teilweise fordern einzelne Lehrkräfte Schülerinnen und Schüler offiziell auf, alle schulischen Informationen über Facebook auszutauschen (weitere Informationen siehe Punkt 6.9.6).

2.10 Ausblick

In seiner bis heute uneingeschränkt gültigen Rechtsprechung zum Grundrecht auf informationelle Selbstbestimmung machte das Bundesverfassungsgericht unmissverständlich deutlich, dass dann nicht mehr von einem modernen Rechtsstaat im Sinne unseres Grundgesetzes gesprochen werden kann, wenn die Menschen in diesem Staat nicht mehr wissen können, wer was wann bei welcher Gelegenheit über sie weiß.

Auch unter Berücksichtigung dieser eindeutigen Vorgabe lautete die Ziffer 392 im Koalitionsvertrag zwischen der SPD und der CDU: „Datenschutz ist ganz wesentlich eine Bildungsaufgabe. Impulse und Regelungen zur Vermittlung von Datenschutzbewusstsein als Sensibilität gegenüber Grundrechten eines jeden Menschen sollen daher nicht nur in den Datenschutzgesetzen, sondern auch in den Lehrplänen von Bildungseinrichtungen in den Bereichen Schule und Hochschule sowie Aus-, Fort- und Weiterbildung verankert werden."

Mit der Initiierung und unverzichtbaren Verstetigung der Projekte „Medienscouts MV", „Bildungsarbeit mit Schülerinnen und Schülern und Multiplikatoren", „TEO protects Privacy", „Netzwerkstar" oder „PeerCon" und der Beteiligung an Projekten wie „Medientango", dem „Netzwerk Medien-Aktiv" oder der „LAG Rahmenvereinbarung" sowie der Durchführung bzw. Mitveranstaltung von Fachveranstaltungen zum Thema Datenschutz versuchen wir, unser Ziel, dass sich jeder junge Mensch im Laufe seiner Kindergartenzeit, Schulzeit oder Ausbildung mehrmals mit Angeboten zum Datenschutz qualifiziert auseinandersetzt, nach und nach zu erreichen.

Dabei stoßen wir als relativ kleine Behörde bei allem persönlichen Engagement zunehmend an quantitative Grenzen, die sich nur in Kooperation mit staatlichen Institutionen überwinden lassen. Mit der jüngsten Änderung des Lehrerbildungsgesetzes und der darin explizit festgelegten Berücksichtigung des Datenschutzes als festem Bestandteil der regulären Ausbildung der Lehrkräfte wurde ein weiterer wichtiger Schritt zur Sensibilisierung wichtiger Multiplikatoren getan. Will man die informationelle Selbstbestimmung im Zeitalter der allgegenwärtigen Informationsverarbeitung ermöglichen, so ist dies nicht ohne diesbezüglich qualifizierte Lehrkräfte möglich, die erst in die Lage versetzt werden müssen, Kinder und Jugendliche entsprechend substantiiert zu informieren. Gleiches gilt für die Elterngeneration, die Jugendhilfe als wichtigstem außerschulischem Partner und der beruflichen Ausbildung, die zwar spät, aber bisweilen noch nicht zu spät entsprechende Defizite mildern bzw. beseitigen können. So wie Lesen und Schreiben bzw. die grundlegende Mathematik unbestritten als „Basiskompetenzen" anerkannt und staatlich gewährleistet vermittelt werden, so muss auch die informationelle Selbstbestimmung als faktische Basiskompetenz breit anerkannt und entsprechend gefördert werden. Diese Förderung und Ermöglichung von gesellschaftlicher Partizipation kann und darf nicht alleine Aufgabe einer kleinen Behörde wie dem Landesbeauftragten für Datenschutz und Informationsfreiheit bleiben, sondern muss - um letztendlich erfolgreich sein zu können - mit Kooperationsbereitschaft und entsprechender Aktivität der für Bildung zuständigen staatlichen Institutionen einhergehen.

Medienkompetenz ist eine Schlüsselqualifikation des 21. Jahrhunderts, die ebenso wie die Basiskompetenzen prüfungsrelevant mit konkreten Inhalten zur informationellen Selbstbestimmung angereichert und gelehrt werden muss. Aus diesem Grund ist eine weitere Aufgabe, die Rahmenpläne zu evaluieren und zu aktualisieren, so wie es der KMK-Beschluss vorsieht. Die vorhandenen Rahmenpläne zur Medienbildung in Mecklenburg-Vorpommern, aber auch Fächer wie Sozialkunde, Deutsch, Geschichte und Informatik etc. sehen bereits solche Themen vor. Jedoch ist die Behandlung des Themas „Das Internet“ in der 7. Klasse bereits viel zu spät. Hierbei ist es möglich, auf das vorhandene Wissen in den Netzwerken zurückzugreifen sowie auch die Unterstützung des Landesbeauftragten für Datenschutz und Informationsfreiheit zu erhalten, so wie es bereits in der Lehrerausbildung nun geschieht.

Dementsprechend ist es kurzfristig unverzichtbar, dass die Rahmenpläne fächerübergreifend aktualisiert werden, dass die Lehrkräfte und deren Leitungskräfte laufend entsprechend fortgebildet und die kommenden Lehrkräfte entsprechend ausgebildet werden. Zudem ist es erforderlich, dass die Multiplikatoren bzw. die Fachkräfte der Jugendhilfe, also auch die Erzieherinnen und Erzieher in Kitas und Krippen und die Fachkräfte in der Tagespflege entsprechende Fortbildungsangebote wahrnehmen und innerhalb der Ausbildung dieser Fachkräfte - vergleichbar zum Lehrerbildungsgesetz - die erforderlichen Angebote rasch installiert werden.

Wir sind - wie schon ausgeführt - in diesen Arbeitsfeldern intensiv tätig und auch zu weiterem Engagement bereit - benötigen jedoch auch in diesen Bereichen die verstärkte Unterstützung der staatlichen Bildungsinstitutionen und die des Parlaments.

Wir empfehlen der Landesregierung, kurzfristig dafür Sorge zu tragen, dass jeder junge Mensch in Mecklenburg-Vorpommern mehrmals qualifizierte Bildungsangebote zu den Themen Medienkompetenz (Mediennutzung), Datenschutz und Urheberrecht wahrnimmt.

Eine weitere Gruppe für Schulungen im Bereich der informationellen Selbstbestimmung ist die Gruppe der Seniorinnen und Senioren. Die Zahl der im Netz Aktiven und damit auch der im Netz Gefährdeten verschiebt sich - unter anderem alterspyramidenbedingt - stetig in Richtung der über 55-Jährigen. Da diese Altersgruppe im Unterschied zu den jungen Generationen noch nicht mit dem Internet als „natürlichem“ Kommunikations- und Informationsmittel aufgewachsen ist, trifft die Gewährleistung der informationellen Selbstbestimmung in dieser (wachsenden) Gruppe auf besondere Herausforderungen. Bisher konnten wir aufgrund fehlender personeller Mittel, bei gleichzeitig in allen Bereichen des Datenschutzes stetig wachsenden Anforderungen, noch keine Schulungstätigkeit in der Gruppe der Seniorinnen und Senioren beginnen. Klar ist jedoch, dass wir uns dem zunehmenden Bedarf in diesem Handlungsfeld nicht auf Dauer werden verschließen können. Eine erfolgversprechende (verstetigte) Sensibilisierung dieser gesellschaftlich zunehmend relevant werdenden Gruppe wird jedoch seitens unserer Behörde nur möglich sein, wenn auch der hierfür notwendige Personalkörper gesichert werden kann. Hierzu bedarf es einer entsprechenden mittelfristigen und verbindlichen Planung.

3 Entwicklung des Datenschutzrechts

3.1 Die EU-Datenschutz-Grundverordnung

Im Zehnten Tätigkeitsbericht, Punkt 3.1.1, haben wir bereits darauf hingewiesen, dass die EU-Kommission beabsichtigt, das Datenschutzrecht durch die Einführung der EU-Datenschutz-Grundverordnung für alle 28 Mitgliedsstaaten einheitlich zu regeln. Nachfolgend sollen die wichtigsten Punkte der bisher angestrebten Regelungen kurz vorgestellt werden:

- Vor dem Hintergrund der Skandale um das Abhören von Nachrichten insbesondere durch US-amerikanische und britische Geheimdienste soll eine Norm eingeführt werden, welche die Übermittlung von personenbezogenen Daten aus der EU an Drittländer nur erlaubt, wenn europäisches Recht oder ein vergleichbares Abkommen dies ausdrücklich vorsieht.
- Zur Nutzung von personenbezogenen Daten soll es prinzipiell einer expliziten, frei abgegebenen und informierten Einwilligung des Betroffenen bedürfen. Schweigen oder Inaktivität reichen nicht. Bei unter 13-Jährigen muss die entsprechende Einwilligung der Eltern eingeholt werden.
- Ein „Recht auf Löschen“ soll derart umgesetzt werden, dass der für die illegale Veröffentlichung von personenbezogenen Daten Verantwortliche dafür Sorge zu tragen hat, dass jede Kopie dieser Daten - auch bei Dritten - wieder gelöscht wird.
- Unternehmen, die pro Jahr personenbezogene Daten von 5.000 Betroffenen verarbeiten, haben demnach einen eigenen Datenschutzbeauftragten zu bestellen, eine Risikoanalyse und eine Folgenabschätzung durchzuführen und die Einhaltung der entsprechenden Auflagen alle zwei Jahre von externen Experten überprüfen zu lassen.
- Die Unternehmen sollen verpflichtet werden, dem Nutzer auf Anfrage in verständlicher Sprache alle Informationen zu geben, die über ihn gespeichert sind.
- Schriftliche Datenschutzerklärungen sollen durch Piktogramme veranschaulicht und zudem mit Links zu ausführlichen juristischen Bestimmungen versehen werden.
- Etwaige Datenschutzpannen sollen gegebenenfalls in der Regel binnen 72 Stunden den Betroffenen mitgeteilt werden.
- Um auch große globale Unternehmen präventiv erreichen zu können, sollen mögliche Strafzahlungen auf bis zu 5 % des jährlichen Weltumsatzes eines Unternehmens oder 100 Millionen Euro bei der Verletzung bestimmter Pflichten aus der Grundverordnung angehoben werden.
- Nutzungsprofile dürfen demnach nur erstellt werden, wenn die Betroffenen etwa durch Privatsphäre-Einstellungen ihres Browsers signalisieren, dass sie hiergegen keine Einwände haben. Entsprechende technische Standards sollen auf EU-Ebene zertifiziert werden.
- Des Weiteren ist auch die Einführung eines Europäischen Datenschutz-Gütesiegels beabsichtigt, um das Vertrauen in entsprechend zertifizierte Dienste zu stärken und die Rechtssicherheit der Anbieter zu erhöhen.
- Ein sogenannter „one stop“-Ansatz soll bewirken, dass Betroffene sich innerhalb der EU nur noch an eine (zentrale) Datenschutzbehörde als Ansprechpartner wenden müssen, deren Unternehmen dementsprechend nur noch an die Datenschutzbehörde des Landes, in dem ihr Hauptsitz ist. Bei Streitfragen soll dann nicht die europäische Kommission entscheiden, sondern ein neu zu gründender europäischer Datenschutzausschuss.

Sicherlich sind die Vereinheitlichung des Datenschutzniveaus in der EU, die weitgehende Reduzierung des Verwaltungsaufwandes für die Beteiligten, die Verbesserung der Durchsetzung von Rechten Betroffener sowie eine wirksame länderübergreifende Überwachung erstrebenswerte Ziele. Zu kritisieren ist jedoch die Tatsache, dass grundlegende Voraussetzungen für eine datenschutzrechtlich geschützte, aber dennoch freie Kommunikation im Internet nicht in das Regelwerk aufgenommen worden sind.

Vernünftigerweise hätte die oft befürwortete Neutralität des Internet, also die neutrale Datenverarbeitung durch Netzanbieter unabhängig vom Inhalt, Ursprung oder Ziel des Datenpakets, in der Grundverordnung verankert werden müssen. Eine Beschränkung der Datenverarbeitung - sei sie zunächst auch nur technischer Art - führt zur Beschränkung der Verfügbarkeit des Internets und eröffnet die Möglichkeit, Inhalte zu bewerten und damit auch Inhalte zu zensieren. Wenn man die Stärkung des Datenschutzrechts als gesellschaftliche Aufgabe definiert, dann kommt man nicht umhin, einer derartigen Einschränkung der freien Kommunikation entgegenzuwirken. Dies ist in den Regularien bisher aber nicht verwirklicht worden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihren „Eckpunkten eines modernen Datenschutzrechts“ vom 18. März 2010 verlangt, dass das Recht normiert werden müsse, Dienstleistungen im Internet anonym oder zumindest pseudonym nutzen zu können. Dies insbesondere im Hinblick darauf, dass der digitale Raum dem realen Raum, in welchem sich eine Person frei und unbeobachtet - quasi ohne Namensschild - bewegen kann, gleichgestellt werden muss. Im Zeitalter von großen Datensammlungen ist es elementar zu ermöglichen, dass solche Datensammlungen nicht selbstverständlich identifizierbar, das heißt, einer Person zuzuordnen, sind. Jede betroffene Bürgerin und jeder betroffene Bürger soll möglichst weitgehend selbst kontrollieren können, ob und wie ihre/seine Identifikationsdaten im Netz verwendet werden. Auch dieser Aufforderung wurde im vorliegenden Entwurf der Verordnung nicht nachgekommen.

Ausdrücklich zu begrüßen ist hingegen, dass zumindest ein Teil der Forderungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die auf Anraten des Arbeitskreises Technik (siehe Punkt 7) in die Stellungnahme zur EU-Datenschutz-Grundverordnung vom 11. Juni 2012 aufgenommen wurden, Einzug in den Gesetzestext gefunden hat. Es geht dabei um weitgehend technikneutrale Formulierungen zur Begründung für Maßnahmen des technischen und organisatorischen Datenschutzes. Der Arbeitskreis Technik hatte empfohlen, in die Verordnung grundlegende Regelungsziele aufzunehmen, wie sie seit geraumer Zeit in mehreren Landesdatenschutzgesetzen verankert sind. Von den sechs vorgeschlagenen Schutzzielen sind nun die drei bekannten Schutzziele der IT-Sicherheit, Vertraulichkeit, Integrität und Verfügbarkeit im Artikel 30 der Grundverordnung manifestiert. Die drei weiteren datenschutzrechtlich motivierten Schutzziele Transparenz, Intervenierbarkeit und Nichtverkettbarkeit wurden bisher nicht mit aufgenommen.

Insgesamt ist festzustellen, dass die geplante Schaffung eines europäischen Datenschutzrahmens leider noch immer hinter den Erwartungen der deutschen Datenschützer zurückbleibt. Dabei ist zu bedenken, dass die Verordnung - anders als die bisherige Datenschutzrichtlinie - unmittelbar gelten wird und von den betroffenen Stellen wie Behörden und Gerichten direkt angewendet und nicht erst vom Mitgliedsstaat umgesetzt werden muss. Dadurch wird die EU-Datenschutz-Grundverordnung zu einer abschließenden Regelung mit der Folge, dass nationales Recht ohne ausdrückliches Zulassen in der Verordnung nicht mehr anwendbar ist und somit obsolet wird.

Aufgrund des sehr unterschiedlichen Datenschutzniveaus der einzelnen Mitgliedsstaaten fällt es daher schwer, eine gemeinsame Grundlage zu finden. Obwohl der Innenausschuss des EU-Parlaments einen Kompromissentwurf der EU-Datenschutz-Grundverordnung im Oktober 2013 angenommen hat, bleibt dennoch fraglich, ob es möglich ist, bis zu den Neuwahlen des EU-Parlaments im Mai 2014 einen Konsens der 28 Staaten zu finden und die Verordnung in Kraft treten zu lassen.

3.2 Förderung der elektronischen Verwaltung

Am 1. August 2013 ist das Artikelgesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften in wesentlichen Teilen in Kraft getreten. Ziel des Gesetzes ist es, die elektronische Kommunikation mit der Verwaltung zu erleichtern. Dazu soll unter anderem die Schriftform neben der qualifizierten elektronischen Signatur (QES) auch durch andere sichere Verfahren ersetzt werden. Schon im Jahr 2003 sollte eine Änderung des Verwaltungsverfahrensgesetzes (VwVfG) der bereits 1997 im Signaturgesetz eingeführten QES zum Durchbruch verhelfen. Dieser Versuch ist jedoch kläglich gescheitert, da die Bundesregierung die für die QES erforderlichen Signaturkarten und Zertifikate nicht als notwendige Infrastruktur gefördert, sondern deren Verbreitung dem Markt überlassen hat.

Nun soll die Schriftform neben der QES durch weitere Verfahren ersetzt werden können. Mit dem Artikelgesetz wird somit ein weiterer Versuch unternommen, die elektronische Kommunikation mit der Verwaltung zu erleichtern. Zu diesem Zweck führt das aus 31 Artikeln bestehende Gesetz mit Artikel 1 das neue E-Government-Gesetz ein und ändert weitere 24 Gesetze und vier Verordnungen. Für datenschutzrechtlich besonders diskussionswürdig halten wir die Änderungen im De-Mail-Gesetz, im VwVfG, im Sozialgesetzbuch Erstes Buch (SGB I) und in der Abgabenordnung (AO).

<u>Änderung des Verwaltungsverfahrensgesetzes und des De-Mail-Gesetzes</u>
Artikel 3 des Gesetzes ändert § 3a Abs. 2 VwVfG. Eine durch Rechtsvorschrift angeordnete Schriftform kann nun auch durch Versendung von Dokumenten per De-Mail ersetzt werden. Mit den Änderungen des De-Mail-Gesetzes (Artikel 2) sollen die Voraussetzungen dafür geschaffen werden. Um die Schriftform bei einer zu übermittelnden Nachricht ersetzen zu können, muss sich der Absender der Nachricht zunächst auf eine sichere Weise an seinem De-Mail-Konto anmelden. Der De-Mail-Diensteanbieter des Absenders soll dem Empfänger der Nachricht die sichere Anmeldung des Absenders bestätigen, indem er dessen Nachricht mit seiner eigenen QES versieht.

Dieses Verfahren, das für den Absender der Nachricht die gleichen Rechtsfolgen wie die einer handschriftlichen Unterschrift hat, wirft zumindest folgende zwei Fragen auf:

a) Kann der sichere Nachweis der Identität des Absenders (Authentisierung) die Integrität der übermittelten Nachricht bei der Übermittlung garantieren?
b) Hat die Signatur des De-Mail-Diensteanbieters die gleiche Rechtswirkung wie die eigenhändige Unterschrift des Absenders?

Zu a)

Für die Beantwortung dieser Frage ist es wichtig, die technischen Vorgänge und Zielstellungen von Verfahren zur Gewährleistung der Integrität (einer Nachricht) von denen zum Nachweis der Identität einer Person (Authentisierung) zu unterscheiden. Elektronische Signaturen liefern Aussagen über elektronische Dokumente, insbesondere über deren Integrität *(siehe Kasten)*. Authentisierungsverfahren liefern hingegen lediglich eine Aussage über die Identität einer Person oder einer Systemkomponente *(siehe Kasten)*. Die mit § 3a Abs. 2 Satz 2 als Schriftformersatz zugelassene QES ist zweifellos in der Lage, die Integrität des betreffenden Dokuments nachprüfbar zu machen. Jede Veränderung des Dokuments während der elektronischen Übermittlung würde bei der Signaturprüfung durch den Empfänger bemerkt werden. Bei dem nunmehr zugelassenen Verfahren bleibt unklar, auf welche Weise die Integrität des übermittelten Dokuments geprüft werden kann. Der Nachweis der Identität des Absenders ist hierfür jedenfalls nicht geeignet. Der Nachweis der Unversehrtheit einer per De-Mail übermittelten Nachricht ist aber besonders wichtig, weil diese gerade nicht während der gesamten Übermittlung vor Veränderungen geschützt ist. Die datenschutzrechtlichen Defizite des De-Mail-Gesetzes haben wir bereits im Zehnten Tätigkeitsbericht (Punkt 3.2.6) erläutert.

Das gesamte Verfahren lässt erhebliche Zweifel zu, ob die Sicherheit und die Vertrauenswürdigkeit dieser neuen Form des Schriftformersatzes tatsächlich garantiert werden können.

Zu b)

Das Verfahren sieht vor, dass nicht der Absender der Nachricht, sondern der De-Mail-Diensteanbieter die Nachricht (im Auftrag des Absenders) signiert. Die eigenhändige Unterschrift unter einem Text wahrt nach deutschem Zivilrecht sowohl die gesetzlich vorgeschriebene als auch die freiwillige Schriftform sowie den Urkundencharakter von privaten Urkunden gemäß § 440 ZPO. Sinn der Unterschrift ist, die Echtheit des unterschriebenen Dokumentes zu garantieren. Ein solcher Namenszug gilt der Rechtsprechung zufolge als einmalig und als Bekundung des Willens, in der Rechtspraxis vor allem bei Willenserklärungen. Es bestehen erhebliche Zweifel, ob die QES eines Dritten (hier die des De-Mail-Diensteanbie-ters) geeignet ist, den Willen des Absenders im oben benannten Sinne zu bekunden.

Die Änderung von § 3a Abs. 2 VwVfG lässt neben QES und De-Mail noch ein weiteres Verfahren zu. Eine durch Rechtsvorschrift angeordnete Schriftform kann nun auch durch Abgabe einer Erklärung in elektronischen Formularen im Zusammenhang mit der Identifizierungsfunktion des neuen Personalausweises ersetzt werden. Auch hier soll offenbar die sichere Identifizierung des Absenders dazu beitragen, die Unversehrtheit der Nachricht zu garantieren. Dass ein Verfahren zum Nachweis der Identität des Absenders jedoch nicht geeignet ist, die Integrität des übermittelten Dokumentes zu gewährleisten, wurde oben bereits begründet.

Fraglich ist bei diesem Verfahren zudem, wie eine (unberechtigte) Veränderung von Formulardaten verhindert werden soll. Dass der Gesetzgeber die Gefahr der Manipulation von ausgefüllten Dokumenten erkannt hat, zeigt die Gesetzesbegründung. Hier wird darauf hingewiesen, dass „… die Behörde durch die technische Ausgestaltung der zur Verfügung gestellten Anwendung … Manipulationen ausschließen kann“. Die Manipulationssicherheit des Formularverfahrens muss aber genauso hoch wie bei der QES sein, da auch dieses Verfahren die Schriftform ersetzen soll. Ein Blick in das Signaturgesetz und die Signaturverordnung macht deutlich, welcher erhebliche technische Aufwand jedoch erforderlich ist, um die technischen Anforderungen an Verfahren zur qualifizierten elektronischen Signatur umzusetzen. Ausweislich der Zulassungsliste der Bundesnetzagentur (http://www.nrca-ds.de/ZDAliste.htm) sind in Deutschland dazu zurzeit nur neun Unternehmen durch den Betrieb von Hochsicherheits-Rechenzentren in der Lage. Dass Behörden insbesondere im kommunalen Bereich in der Lage sind, diese Anforderungen zu erfüllen, ist zu bezweifeln. Beleg für diese Zweifel sind nicht nur unsere Prüfergebnisse im kommunalen Bereich (vgl. bspw. Neunter Tätigkeitsbericht, Punkt 6), sondern auch die Tatsache, dass die Anwendung der „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ (siehe Punkt 4.3) den Kommunen lediglich empfohlen wird, da im IT-Planungsrat erhebliche Zweifel bestanden, dass die Kommunen zurzeit fachlich, personell und finanziell in der Lage sind, die Anforderungen der Leitlinie umzusetzen.

Änderung des SGB I und der Abgabenordnung

Artikel 4 des Artikelgesetzes ändert auch im SGB I die Anforderungen an den Schriftformersatz. Hier sind künftig dieselben, oben bereits beschriebenen, Verfahren zugelassen, die § 3a VwVfG im Bereich der allgemeinen Verwaltung zulässt. Somit stellen sich auch im Bereich des SGB I die oben aufgeworfenen Fragen.

Aber anders als im Bereich der allgemeinen Verwaltung wird hier für die Kommunikation zwischen den Versicherten und ihrer Krankenkasse als sicherer Identitätsnachweis neben dem neuen Personalausweis auch die elektronische Gesundheitskarte zugelassen. Bei der Ausgabe der Gesundheitskarte werden jedoch wesentlich geringere Anforderungen an die Prüfung der Identität der Antragsteller gestellt als bei der Beantragung und Aushändigung eines Personalausweises. Deshalb ist zu bezweifeln, ob die Gesundheitskarte tatsächlich zum sicheren Nachweis der Identität bei Verfahren zum Schriftformersatz geeignet ist.

Auch im Bereich der Steuerverwaltung sieht die Abgabenordnung (AO) seit langem die Möglichkeit vor, die Schriftform durch eine QES zu ersetzen (§ 87a Abs. 3 AO). Artikel 7 des Artikelgesetzes ändert diese Vorschrift und lässt künftig auch im Bereich der Steuerverwaltung De-Mail in der oben beschriebenen Form als Schriftformersatz zu. Neben den bereits beschriebenen Problemen ist mit Blick auf die nicht vorhandene Ende-zu-Ende-Verschlüsselung von De-Mail das Steuergeheimnis von besonderer Bedeutung. Mit gutem Grund wird in der AO gefordert, dass an die Finanzbehörden übermittelte Steuerdaten mit einem geeigneten Verfahren zu verschlüsseln sind. De-Mail verstößt systembedingt gegen das Verschlüsselungsgebot. Das Problem wird nun nicht etwa dadurch gelöst, dass für die Übermittlung von Steuerdaten per De-Mail eine Ende-zu-Ende-Verschlüsselung gefordert wird. Vielmehr hat der Gesetzgeber einen zusätzlichen Satz in die AO aufgenommen, nach dem die technisch bedingte Entschlüsselung beim Versenden einer De-Mail-Nachricht nicht gegen das Verschlüsselungsgebot verstößt. Ob eine solche „gesetzliche definierte Sicherheit“ einer möglichen rechtlichen Überprüfung etwa vor Verwaltungsgerichten standhält, ist mehr als fraglich.

Im Ergebnis lässt sich feststellen, dass die mit dem Artikelgesetz neu zugelassenen Möglichkeiten zum Ersatz einer durch Rechtsvorschrift angeordneten Schriftform durch die elektronische Form hinsichtlich Vertrauenswürdigkeit und Sicherheit mit der QES nicht zu vergleichen sind. Der Gesetzgeber spricht lediglich von *anderen Verfahren* und vermeidet offenbar bewusst den Begriff *vergleichbare Verfahren*. Gleichwohl werden beide Möglichkeiten vom Gesetzgeber explizit als Ersatz für die Schriftform zugelassen.

Ende Oktober 2012 legte das BSI den Entwurf der Technischen Richtlinie TR-03107 „Elektronische Identitäten im eGovernment“ des BSI vor. Auch dieses Dokument räumt unsere Bedenken hinsichtlich des niedrigeren Sicherheitsniveaus der neuen Verfahren nicht aus. In einer ersten Stellungnahme zum Richtlinienentwurf haben wir daher gefordert, dass unter dem Blickwinkel der Transparenz die Technische Richtlinie dieses offen legen und deutlich machen sollte, dass die Bewertung des Sicherheitsniveaus sich nicht primär auf zusätzliche technische und organisatorische Sicherheitsmaßnahmen abstützt, sondern auf die gesetzlichen Rahmenbedingungen.

Für die praktische Anwendung der neuen Vorschriften in der Verwaltung empfehlen wir daher dringend, in jedem Einzelfall zu prüfen, welchen Schutzbedarf die zu übermittelnden Daten haben und ob die Schriftform bei Bedarf nicht besser mit der sicheren und bewährten QES realisiert wird. Wir verweisen auf eine Handreichung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum datenschutzgerechten Umgang mit besonders schützenswerten Daten beim Versand mittels De-Mail (http://www.bfdi.bund.de/SharedDocs/Publikationen/Sachthemen/DEMail/DeMailHandreichung.html).

Begriffsdefinition des BSI: „Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind.“ (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz Kataloge/Inhalt/Glossar/glossar_node.html)
Begriffsdefinition des BSI: „Authentisierung bezeichnet den Nachweis eines Kommunikationspartners, dass er tatsächlich derjenige ist, der er vorgibt zu sein.“ (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html)

3.3 Datenschutz-Beirat

Mit der Novellierung des Landesdatenschutzgesetzes (DSG M-V) im Jahr 2011 wurde in § 33b auch die Bildung eines Beirates beim Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (Datenschutz-Beirat) beschlossen. Mitglied im Datenschutz-Beirat sind der Landtag Mecklenburg-Vorpommern, die Landesregierung Mecklenburg-Vorpommern, der Städte- und Gemeindetag Mecklenburg-Vorpommern, der Landkreistag Mecklenburg-Vorpommern, der Deutsche Gewerkschaftsbund Bezirk Nord, der Deutsche Beamtenbund Landesbund Mecklenburg-Vorpommern, die Vereinigung der Unternehmensverbände für Mecklenburg-Vorpommern und der Landesverband der Freien Berufe Mecklenburg-Vorpommern (siehe auch unter www.datenschutz-mv.de).

Der Datenschutz-Beirat soll sich neben datenschutzrechtlichen Fragen auch mit dem Thema der Informationsfreiheit befassen, da der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern für beide Themenbereiche zuständig ist. Da insbesondere der Datenschutz zunehmend gesamtgesellschaftliche Relevanz besitzt und somit generationsunabhängig in allen Lebensbereichen an Bedeutung gewinnt, lag die Bildung eines Gremiums nahe, das – ergänzend zur Tätigkeit des Landesbeauftragten für Datenschutz und Informationsfreiheit – sich aus unterschiedlichen Perspektiven mit diesem ständig präsenten und schnell verändernden Thema befassen soll. Der Beirat wird sich jährlich und nach Bedarf zusammenfinden, um anstehende Sachfragen zu diskutieren. Die Sitzungen des Datenschutz-Beirates sind – außer in begründeten Einzelfällen - öffentlich.

Am 22. Januar 2013 trafen sich die Mitglieder des Datenschutz-Beirates zur konstituierenden Sitzung. Gemäß § 33b DSG M-V waren die Vorsitzende und ihr Stellvertreter aus den Mitgliedern des Landtages Mecklenburg-Vorpommern zu wählen. Darüber hinaus beschlossen die Mitglieder die Geschäftsordnung des Beirates und besprachen erste gemeinsame Ziele und Aufgaben.

In der Sitzung am 29. April 2013 standen die Arbeitsweise und die Tätigkeitsschwerpunkte der Behörde des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern im Mittelpunkt. Die einzelnen Referate stellten ihre Aufgaben sowie die Mitarbeiterinnen und Mitarbeiter vor. Die Mitglieder des Beirates regten an, dass in den künftigen Sitzungen jeweils bestimmte Themen ausführlicher erläutert und diskutiert werden und dass der Datenschutz-Beirat als beratendes und unterstützendes Gremium zu einzelnen diskutierten Themenkomplexen eine Empfehlung an den Landesbeauftragten für Datenschutz und Informationsfreiheit formuliert.

Die Sitzung am 9. September 2013 befasste sich schwerpunktmäßig mit den Themen GovData - Das Datenportal für Deutschland, IT-Sicherheit in der Landesverwaltung sowie eGovernment und IT-Sicherheit - Handlungsfeld für Land und Kommunen. Die Referentin/die Referenten erläuterte/n den aktuellen Stand und stand/en den Mitgliedern des Beirates anschließend für Fragen zur Verfügung. Darüber hinaus wurden allgemeine Angelegenheiten des Beirates besprochen.

4 IT-Planungsrat

4.1 Beratung des IT-Planungsrates durch die Datenschutzbeauftragten von Bund und Ländern

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Konferenz) hat im Jahr 2010 beschlossen, uns in der Eigenschaft als Vorsitzendem des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ (AK Technik, siehe Punkt 7) in den IT-Planungsrat zu entsenden, um dort zusätzlich zum gesetzlich verankerten Beratungsauftrag des Bundesdatenschutzbeauftragten die Datenschutzinteressen der Bundesländer mit beratender Stimme zu vertreten. Dieses Mandat nehmen wir seit September 2010 wahr (siehe Zehnter Tätigkeitsbericht, Punkt 3.2.7).

Im Berichtszeitraum nahmen wir an sechs Sitzungen des IT-Planungsrates und weiteren Beratungen auf Arbeitsebene teil. Der IT-Planungsrat hat inzwischen zahlreiche Arbeits-, Projekt- und Kooperationsgruppen eingesetzt, die Steuerungs- und Koordinierungsprojekte federführend begleiten und umsetzen sollen. Unsere zeitlichen und personellen Ressourcen lassen es natürlich nicht zu, in allen Arbeitsgremien vertreten zu sein. Daher hat die Konferenz unserer Bitte zugestimmt, weitere Vertreter des AK Technik in die Gremien des IT-Planungsrates zu entsenden. Auf diese Weise war es möglich, Datenschutzvertreter unter anderem in den Beirat der Koordinierungsstelle für IT-Standards (KoSIT), in die Kooperationsgruppe Informationssicherheit, in die Projektgruppe eID-Strategie und in die Arbeitsgruppe Netzsicherheit zu entsenden.

Alle Beratungen und Arbeitsergebnisse des IT-Planungsrates hier zu erörtern, würde den Rahmen des Berichts sprengen. Wir verweisen daher insbesondere auf die Veröffentlichungen des IT-Planungsrates im Internet (http://www.it-planungsrat.de/DE/Home/home_node.html). In diesem Bericht soll jedoch auf einige Beratungsschwerpunkte des IT-Planungsrates mit besonderem Datenschutzbezug eingegangen werden.

4.2 Soziale Netze in der Verwaltung

In der 7. Sitzung im März 2012 befasste sich der IT-Planungsrat auf unsere Anregung hin mit Datenschutzfragen bei der Nutzung sozialer Netze durch öffentliche Stellen. In ihrer Jahreskonferenz am 22./23. September 2011 hatten sich auch die Chefinnen und Chefs der Staats- und Senatskanzleien mit dem Thema befasst und ein abgestimmtes Handeln zwischen Bund und Ländern gefordert. Mit Blick auf diese Forderung und unter Verweis auf die Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28./29. September 2011 (siehe Zehnter Tätigkeitsbericht, Punkt 2.2.1) haben wir dem IT-Planungsrat empfohlen, die öffentlichen Stellen des Bundes und der Länder aufzufordern, bei der Verwendung sozialer Netzwerke die Belange des Datenschutzes zu berücksichtigen und von der direkten Einbindung von Social-Plugins und der Einrichtung von Fan-Pages bei Facebook bis zur Klärung der offenen rechtlichen und technischen Fragen abzusehen.

Dieser Empfehlung schloss sich der IT-Planungsrat jedoch nicht an. Nach ausführlicher und zum Teil kontroverser Diskussion nahm der IT-Planungsrat zwar unseren Bericht zum Datenschutz in sozialen Netzwerken zur Kenntnis, begrüßte dann aber lediglich die Initiative des Bundes, eine entsprechende Selbstregulierung herbeizuführen. Immerhin empfahl er den öffentlichen Stellen des Bundes und der Länder, insbesondere vor der direkten Einbindung von Social-Plugins und bei der Nutzung von Fan-Pages eine sorgfältige Prüfung unter Einbeziehung der Datenschutzbeauftragten vorzunehmen.

4.3 Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung

Ein weiterer Schwerpunkt unserer Beratungstätigkeit im IT-Planungsrat betraf Fragen der Informationssicherheit für die zahlreichen neuen E-Government-Verfahren in den Behörden des Bundes, der Länder und der Kommunen. Der IT-Planungsrat hatte bereits im September 2010 das Thema IT- und Datensicherheit als Schwerpunkt für seine weitere Arbeit vereinbart. Die Mitglieder des IT-Planungsrates beschlossen daraufhin, verbindliche Sicherheitsziele für die Informationstechnik zu vereinbaren. Die zu diesem Zweck eingerichtete Kooperationsgruppe „Leitlinie Informationssicherheit“ wurde damit beauftragt, das Ziel, den Geltungsbereich und die Inhalte einer Leitlinie für Informationssicherheit bei der Gestaltung von IT-Verfahren der öffentlichen Verwaltung festzulegen. Ein wesentliches Ziel unserer Mitwirkung in dieser Kooperationsgruppe war die Verankerung von grundsätzlichen Datenschutzprinzipien in der Leitlinie. Gemeinsam mit unseren Kollegen aus Schleswig-Holstein konnten wir den IT-Planungsrat davon überzeugen, dass in der Leitlinie den Datenschutzaspekten der gleiche Stellenwert einzuräumen ist wie den IT-Sicherheitsaspekten. Im Ergebnis unserer Beratungen schreibt die Leitlinie nun auch die folgende Rahmenbedingung fest:

„Die gemeinsame Leitlinie für Informationssicherheit bezieht sich auf die Schutzziele der Informationssicherheit Verfügbarkeit, Vertraulichkeit und Integrität der Daten sowie die technisch-organisatorische Umsetzung der Datenschutzanforderungen im Hinblick auf Transparenz, Betroffenenrechte und Zweckbindung.“

Kontrovers diskutiert wurde im IT-Planungsrat dann jedoch die Methodik, mit der die oben genannten Schutzziele zu erreichen sind. Unstrittig war von Beginn an, dass die Grundschutzmethodik des Bundesamtes für Sicherheit in der Informationstechnik (BSI) als Orientierung für das angestrebte Sicherheitsniveau dienen soll. Wir haben diesen Ansatz ausdrücklich befürwortet, da wir seit langem den Nutzen und die Effektivität dieser Methode für den Datenschutz erkannt haben (siehe bspw. Achter Tätigkeitsbericht, Punkt 2.15.5). Einige Mitglieder des IT-Planungsrates waren jedoch der Auffassung, dass die Grundschutzmethodik allenfalls empfohlen werden sollte, während die Mehrzahl für eine verbindliche Regelung votierte. Im Ergebnis konnte sich der IT-Planungsrat lediglich zu folgender Formulierung durchringen: „Die Festlegung des Mindestsicherheitsniveaus erfolgt einheitlich orientiert am IT-Grundschutz des BSI“.

Schließlich war noch die Frage zu klären, für welche Bereiche der öffentlichen Verwaltung die Leitlinie gelten soll. Die Mehrzahl der Mitglieder befürchtete, dass die Kommunen mit der Durchsetzung der Leitlinie und der Anwendung der IT-Grundschutzmethodik fachlich, personell und finanziell überfordert wären. Mit Blick auf die hohen Sicherheitsanforderungen von E-Government-Verfahren in den Kommunen etwa im Meldewesen oder im Personenstandswesen (siehe Punkte 6.4.5 und 6.4.6) forderten wir gemeinsam mit den im IT-Planungsrat vertretenen kommunalen Spitzenverbänden die uneingeschränkte Geltung der Leitlinie auch im kommunalen Bereich. Der IT-Planungsrat ignorierte diese Forderungen jedoch und beschloss, den Kommunen die Anwendung der Leitlinie für die Informationssicherheit lediglich zu empfehlen.

Wir empfehlen den Kommunen, unabhängig von der Position des IT-Planungsrates die Vorgaben der „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ umzusetzen und erwarten, dass sie für Verfahren zur automatisierten Verarbeitung personenbezogener Daten insbesondere bei modernen E-Goverment-Verfahren die Grundschutzmethodik des BSI in vollem Umfang anwenden.

4.4 Steuerungsprojekt eID-Strategie

Die vom IT-Planungsrat im September 2010 verabschiedete Nationale E-Government- Strategie (NEGS) beschreibt zahlreiche Handlungsfelder, aus denen konkrete Projekte abgeleitet wurden. Mit dem Steuerungsprojekt „eID-Strategie“ soll eine Gesamtstrategie für den Einsatz elektronischer Identifizierungs- und Signaturverfahren im E-Government entwickelt und umgesetzt werden. Die datenschutzrechtliche Begleitung dieses Projektes insbesondere durch unsere hessischen Kollegen hat sich leider als sehr schwierig herausgestellt.

Die Eckpunkte der eID-Strategie werden geprägt durch die Begriffe Akzeptanz, Sicherheit und Wirtschaftlichkeit. Obwohl die Leitlinie für die Informationssicherheit (siehe oben) neben den Schutzzielen der IT-Sicherheit ausdrücklich auch die Umsetzung von darüber hinausgehenden Datenschutzanforderungen im Hinblick auf Transparenz, Betroffenenrechte und Zweckbindung fordert, finden sich in der eID-Strategie und in den dazugehörigen Eckpunkten diese Datenschutzziele nicht.

Zudem haben wir mehrfach darauf hingewiesen, dass die Ziele Identität, Authentizität, Integrität und Vertraulichkeit noch durchgängig durch die (Rechts-)Verbindlichkeit ergänzt werden müssten. Während der Beratungen in der Projektgruppe des IT-Planungsrates wurden Datenschutzaspekte zu keiner Zeit in ausreichendem Maße erörtert. Unser hessischer Kollege sah sich deshalb veranlasst, die Geschäftsstelle des IT-Planungsrates auf diesen Missstand hinzuweisen und zu fordern, dem Datenschutz in einer neuen Fassung des Papiers den ihm gebührenden Stellenwert einzuräumen und die wesentlichen Kritikpunkte zu berücksichtigen.

Nach kontroverser Diskussion beschloss der IT-Planungsrat in seiner 12. Sitzung im Oktober 2013 die eID-Strategie jedoch in unveränderter Form. Der vom hessischen Vertreter eingebrachte und von uns nachdrücklich unterstützte Vorschlag, die eID-Strategie noch nicht zu verabschieden, sondern zunächst in datenschutzrechtlicher Hinsicht nachzubessern, wurde abgelehnt. Somit ist festzustellen, dass eines der für künftige E-Government-Vorhaben wichtigsten Strategiepapiere Datenschutzfragen unzureichend berücksichtigt. Der IT-Planungsrat hat in seinem Beschluss zur eID-Strategie zwar darauf hingewiesen, dass bei der Umsetzung der Maßnahmen der Strategie die Erfordernisse des Datenschutzes besonders zu berücksichtigen sind. Ob dieses Statement tatsächlich zu angemessener Berücksichtigung der Datenschutzaspekte bei der Entwicklung und beim Einsatz elektronischer Identifizierungs- und Signaturverfahren im E-Government führt, bleibt abzuwarten.

Ende Oktober 2012 legte das BSI den Entwurf der Technischen Richtlinie TR-03107 „Elektronische Identitäten im eGovernment“ des BSI vor. Auch dieses Dokument räumt die datenschutzrechtlichen Bedenken nicht aus. In einer ersten Stellungnahme zum Entwurf (siehe Punkt 3.2) haben wir zahlreiche Änderungen und Ergänzungen empfohlen, damit die Richtlinie ein geeignetes Hilfsmittel zur sicheren und datenschutzgerechten Ausgestaltung von E-Government- Anwendungen wird und eine angemessene Bewertung von Identitätsmechanismen für verschiedene Prozesse des eGovernment sowie eine zweckmäßige Zuordnung von Vertrauensniveaus ermöglicht.

Wir empfehlen der Landesregierung, Datenschutzaspekte bei der Entwicklung und beim Einsatz elektronischer Identifizierungs- und Signaturverfahren im E-Government in angemessener Weise zu berücksichtigen und insbesondere den Datenschutzanforderungen im Hinblick auf Transparenz, Betroffenenrechte und Zweckbindung den erforderlichen Stellenwert zukommen zu lassen.

4.5 Datensicherheit im Verbindungsnetz

Im Gesetz über die Verbindung der informationstechnischen Netze des Bundes und der Länder (IT-NetzG) ist vorgeschrieben, dass der Bund zu diesem Zweck ein sogenanntes Verbindungsnetz errichtet. Dieses Netz muss zum Datenaustausch zwischen Bund und Ländern ab dem 1. Januar 2015 genutzt werden. Es löst das Netz des Vereins Deutschland Online Infrastruktur e. V. (DOI) ab. Der IT-Planungsrat definiert die Anforderungen an das Verbindungsnetz, auch im Hinblick auf die Informationssicherheit.

Zur Planung dieses Netzes hat der IT-Planungsrat verschiedene Arbeitsgremien eingesetzt, die wir aus datenschutzrechtlicher Sicht unter anderem gemeinsam mit der KoSIT begleiten und beraten. In diesem Rahmen wurde auch erörtert, ob das neu zu schaffende Verbindungsnetz allein alle erforderlichen sicherheits- und datenschutzrelevanten Mechanismen beinhaltet oder ob andere etablierte Standards wie OSCI-Transport weiter erforderlich sind.

Ein Weg zum Schutz von Daten gegen unbefugtes Abhören und Verändern ist die Anwendung kryptographischer Methoden - bei der Übertragung über offene Kommunikationsverbindungen wie über das Internet ist dies der einzige erfolgversprechende Weg. Deshalb haben sich die Datenschutzbeauftragten von Bund und Ländern immer wieder für den Einsatz kryptographischer Methoden eingesetzt, beispielsweise in den Entschließungen „Forderungen zur sicheren Übertragung elektronisch gespeicherter personenbezogener Daten“ (1996), „Eckpunkte der deutschen Kryptopolitik - ein Schritt in die richtige Richtung“ (1999) und andere.

Wenn nur Absender und Empfänger eine verschlüsselte Nachricht entschlüsseln können, spricht man von Ende-zu-Ende-Verschlüsselung. Bekannte Protokolle für diese Form der Verschlüsselung ist beispielsweise das von der Internet-Standardisierungsorganisation IETF genormte OpenPGP.

Zahlreiche andere Verfahren bieten keine Ende-zu-Ende-Verschlüsselung. Dazu gehören beispielsweise De-Mail (siehe Punkt 3.2 und Zehnter Tätigkeitsbericht, Punkt 3.2.6). In diesem Fall findet eine Verschlüsselung immer nur abschnittsweise statt. Am Ende eines jeden Abschnitts steht eine Institution, die Zugriff auf den Klartext der übertragenen Nachricht hat. So werden De-Mails von den De-Mail-Diensteanbietern des Absenders und des Empfängers jeweils entschlüsselt und für die Zwischenspeicherung und den weiteren Transport neu verschlüsselt. Nach der Entschlüsselung ist es grundsätzlich möglich, die Nachrichteninhalte zur Kenntnis zu nehmen oder zu verändern.

Das DOI-Netz und dessen Nachfolger, das Verbindungsnetz, bieten ebenfalls nur eine Verbindungsverschlüsselung, die lediglich die Vertraulichkeit der übermittelten Daten zwischen den Routern gewährleistet. An den Routern liegen die Daten wieder im Klartext vor. Im landeseigenen Netz LAVINE gibt es selbst so eine Verbindungsverschlüsselung zwischen Routern nur auf Anfrage und gegen Aufpreis. Ob in den hinter dem DOI-Netz oder hinter LAVINE liegenden Behördennetzen verschlüsselt wird, ist Sache der jeweiligen Behörde. Auch die Nutzung von Zusatzangeboten, die eine Ende-zu-Ende-Sicherheit gewährleisten können, obliegt den jeweiligen Behörden.

Lösungen mit einer Verbindungsverschlüsselung eignen sich nur bedingt zur Übertragung personenbezogener Daten. Bei sensiblen, beispielsweise medizinischen, Daten ist eine zusätzliche Ende-zu-Ende-Verschlüsselung erforderlich. Dieser Umstand wird von vielen Verantwortlichen jedoch immer wieder ignoriert, meist aus Kostengründen. Sie gehen fälschlicher Weise davon aus, dass Netze wie DOI oder LAVINE als „sichere Netze“ zu betrachten sind und die dort getroffenen Maßnahmen ausreichend wären.

Mit OSCI-Transport steht seit langem eine bewährte Protokollfamilie für die sichere Kommunikation von Bürgerinnen und Bürgern und Unternehmen mit der öffentlichen Verwaltung und von Behörden untereinander zur Verfügung. OSCI-Transport beruht ebenfalls auf offenen Standards wie die vom World Wide Web Consortium definierte XML Encryption. OSCI-Transport gewährleistet ebenfalls Ende-zu-Ende-Sicherheit. Deshalb haben die Datenschutzbeauftragten aus Bund und Ländern bereits in der Entschließung „Sicherheit bei E-Government durch Nutzung des Standards OSCI“ aus dem Jahr 2005 für dieses Verfahren geworben (siehe Siebter Tätigkeitsbericht, Anlage 23).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im Oktober 2013 eine Entschließung unter dem Titel „Sichere elektronische Kommunikation gewährleisten - Ende-zu-Ende-Verschlüsselung einsetzen und weiterentwickeln“ gefasst. Darin bringen die Datenschutzbeauftragten zum Ausdruck, dass sie den Einsatz von Standards zur Ende-zu- Ende-Verschlüsselung wie OSCI-Transport für geboten halten. Sie fordern den IT-Planungsrat auf, diese kontinuierlich weiterzuentwickeln und verbindlich festzulegen. Sie fordern daneben Bund, Länder und Kommunen auf, die vorhandenen Standards bereits jetzt einzusetzen.

Wir empfehlen der Landesregierung, bei der elektronischen Übermittlung personenbezogener Daten, insbesondere bei modernen E-Goverment-Verfahren, regelmäßig Verschlüsselungsverfahren nach dem Stand der Technik einzusetzen und nur in begründeten Ausnahmefällen auf eine Ende-zu-Ende-Verschlüsselung zu verzichten.

5 Technik und Organisation

5.1 Neue Technologien

5.1.1 Smart Meter auf dem richtigen Weg

Bereits im Jahr 2009 hat die EU-Kommission mit dem Richtlinienentwurf 2009/28/EG den Grundstein für eine nachhaltige Energieversorgung gelegt. Mit Hilfe von intelligenten Energienetzen (Smart Grids) und dazugehörigen intelligenten Zählern (Smart Meter) soll die Energie möglichst umweltfreundlich, ressourcenschonend und effizient produziert und verteilt werden. So soll bis zum Jahr 2020 eine Reduktion des CO^2-Ausstoßes um 20 % und eine Anhebung des Anteils der erneuerbaren Energien auf 20 % erreicht werden.

Gerade mit Hilfe der Smart Meter soll es den Bürgerinnen und Bürgern gelingen, den eigenen Stromverbrauch zu kontrollieren und zu regulieren. Damit diese intelligenten Messzähler ihrer Aufgabe gerecht werden, zeichnen sie langfristig und detailliert den Verbrauch auf und ermöglichen dabei prinzipiell auch eine sekundengenaue Übermittlung dieser Verbrauchsdaten an externe Marktteilnehmer. Zu den externen Marktteilnehmern gehören dabei potenzielle Kommunikationspartner eines Smart Meter, etwa die Verteilnetzbetreiber (betreiben das Stromnetz zum Kunden), die von den Bürgerinnen und Bürgern frei wählbaren Messstellenbetreiber (betreiben die Messgeräte und übernehmen deren Ablesung) und die Stromlieferanten. Da sich mit den gesammelten Daten ohne Weiteres detaillierte Verbrauchsprofile erstellen lassen, die mit beliebigen weiteren Daten verknüpft werden können, kann sich hieraus sehr schnell eine massive Verletzung der Privatsphäre ergeben.

Um einem Missbrauch vorzubeugen, hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Orientierungshilfe zum datenschutzgerechten Smart Metering (https://www.datenschutz-mv.de/datenschutz/publikationen/informat/smart_meter/OH_Smart Meter.pdf) erarbeitet, welche Empfehlungen und Forderungen an eine datenschutzgerechte Konzeption der technischen Systeme enthält. Mit der zugehörigen Entschließung (https://www.datenschutz-mv.de/datenschutz/themen/beschlue/Ent_OH_SmartMeter.pdf) wurde sie am 27. Juni 2012 von der Konferenz verabschiedet. Im Rahmen unseres Vorsitzes im Arbeitskreis „Technische und organisatorische Datenschutzfragen“ (siehe AK Technik, Punkt 7) haben wir aktiv an der Erstellung mitgewirkt.

In der Orientierungshilfe werden verschiedene Einsatzszenarien von Smart Metern beschrieben (sogenannte Use Cases) und die jeweiligen Datenverarbeitungsprozesse erläutert und datenschutzrechtlich bewertet. Diese Use Cases reichen von der Messung an sich über die Verarbeitung im Zähler bis hin zur Abrechnung beim Stromanbieter. Im Mittelpunkt der Betrachtungen stehen dabei stets Empfehlungen und Umsetzungsvorschläge, mit denen die im Datenschutzrecht fest verankerten Datenschutzforderungen umgesetzt werden können. Eine wesentliche Rolle spielt hierbei die Gewährleistung der im Datenschutzrecht verankerten Zweckbindung, nach der Daten nur erhoben, gespeichert und verarbeitet werden dürfen, wenn diese für den gesetzlich vorgesehenen Zweck erforderlich sind oder die Betroffenen ausdrücklich eingewilligt haben. Um dem Grundsatz der Datenvermeidung und Datensparsamkeit Rechnung zu tragen, müssen die Speicher- und Ableseintervalle so groß sein, dass aus dem Verbrauch keine Rückschlüsse auf das Verhalten der Nutzerinnen und Nutzer gezogen werden können. Die Daten sollten dabei möglichst nur anonymisiert, pseudonymisiert oder aggregiert an so wenig Stellen wie nötig übermittelt werden.

Ein weiterer zentraler Kernpunkt ist die im Datenschutzrecht verankerte Forderung nach Transparenz, nach der den Nutzerinnen und Nutzern klar sein muss, zu welchem Zweck Daten über sie erhoben werden und wie lange diese gespeichert bleiben. Um diese Transparenz beim Einsatz von Smart Meter zu erhöhen, sollten die vorhandenen Kommunikations- und Verarbeitungsschritte zu jeder Zeit sichtbar und nachweisbar sein. Die Nutzerinnen und Nutzer müssen folglich die Zugriffe auf das Smart Meter erkennen und diese im Zweifel unterbinden können. Klar ist hierbei auch, dass es eindeutige Profile für den berechtigten Zugang zu den Smart Metern und den zugehörigen Daten geben muss. Erfahrungsgemäß lässt sich der Datenschutz stets dann am einfachsten gewährleisten, wenn er schon bei der Konzeption und Gestaltung der technischen Systeme berücksichtigt wird (Privacy by Design).

5.1.2 Datenschutzgerechte Fernmesswasserzähler

Ein Petent hat sich Ende 2012 an uns gewandt, weil er Bedenken beim eichrechtlich bedingten Austausch seines alten analogen Wasserzählers gegen ein neues digitales Modell hatte, welches einen deutlich größeren Funktionsumfang mit sich brachte. Das neue Modell konnte die Verbrauchsdaten sehr detailliert in einem internen Speicher ablegen. Darüber hinaus war ein Kommunikationsmodul integriert, das die Übertragung der Verbrauchsdaten in kleinen Zeitintervallen per Funk ermöglichte. Die Sorge des Petenten, dass durch detaillierte Verbrauchsprofile seine Privatsphäre verletzt werden könnte, war offensichtlich berechtigt: Unsere Anfrage bei der zuständigen Wohnungsgesellschaft zu dem Verfahren ergab, dass man sich dort tatsächlich noch keine ausreichenden Gedanken zum Thema Datenschutz gemacht hatte.

So fehlte als Grundlage für die Verarbeitung der Daten durch den technischen Dienstleister, der neben dem Betrieb der Geräte auch für die Erstellung der Betriebskostenabrechnung verantwortlich ist, bereits ein Vertrag für eine datenschutzgerechte „Datenverarbeitung im Auftrag“. Weiterhin waren der Wohnungsgesellschaft die technischen Details der installierten Zähler zum Zeitpunkt unserer Nachfrage nicht bekannt, obwohl sie als Auftraggeber gemäß § 11 Abs. 1 Bundesdatenschutzgesetz (BDSG) weiterhin für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich bleibt. Entsprechend war auch die gesamte Transparenz des Verfahrens gegenüber den Betroffenen nicht gegeben.

Die Bearbeitung der Petition gestaltete sich in der Folge äußerst schwierig: Erst nach einem halben Jahr informierte uns der Dienstleister über technische und organisatorische Details zum Verfahren des Fernmessens. Diese Details warfen neue Fragen auf. Es zeigte sich, dass eine Profilbildung über die Kundinnen und Kunden mit der uns dargestellten Verfahrensweise ohne Weiteres möglich war. Erst nach mehreren Gesprächen lenkte die Wohnungsgesellschaft ein und versicherte schließlich, dass das Verfahren datenschutzgerecht ausgestaltet würde. Nach über einem Jahr Verhandlungen wurde der Datenabruf kurzfristig neu konfiguriert. Jetzt wird nur noch einmal im Monat ein konsolidierter und verschlüsselter Verbrauchswert als Monatsendwert an das Rechenzentrum des Dienstleisters übertragen. Eine Profilbildung durch eine tages- oder gar minutengenaue Auswertung der Verbrauchswerte ist somit nicht mehr möglich. Letzten Endes bleibt jedoch die Frage, ob man dieses datenschutzgerechte Ergebnis nicht auch schneller hätte erzielen können.

5.1.3 iPad/iCloud-Nutzung im Landtag

Ende 2011 meldete die Schweriner Volkszeitung, dass der Landtag Mecklenburg-Vorpommern dem Beispiel des Deutschen Bundestages folgen will und seine 71 Abgeordneten mit sogenannten „lüfterlosen Lesegeräten“, besser bekannt unter der Bezeichnung Tablet-Computer, ausstatten möchte. Die Landtagsverwaltung hatte sich für das Modell iPad der amerikanischen Firma Apple entschieden. Bereits im Vorfeld zu der Pressemeldung hatte sich die Landtagsverwaltung mit der Bitte um eine datenschutzrechtliche Bewertung des Einsatzes dieser mobilen Endgeräte an uns gewandt.

Schon im ersten Gespräch mit der Landtagsverwaltung zeigte sich, dass von einigen Landtagsabgeordneten nicht nur Zugang zu öffentlich zugänglichen Dokumenten gewünscht wurde. Vielmehr bestand auch die Forderung, eigene PIM-Daten (engl. Personal Information Manager; persönliche Daten wie Kontakte, Termine, Aufgaben und Notizen) mit den entsprechenden Daten des iPad zu synchronisieren und dazu auch den Apple-eigenen Cloud-Dienst iCloud (siehe auch Punkt 5.1.4) zu nutzen.

Dass jedoch derartige Dienste mit dem Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) unvereinbar sind, zeigte sich sehr deutlich, als wir Apples Allgemeine Geschäftsbedingungen (AGB) für die Nutzung der iCloud genauer untersuchten. Jede iCloud-Nutzerin/jeder iCloud-Nutzer willigt mit der Zustimmung zu den AGB nämlich ein, dass die „Daten in die USA oder in andere Länder übermittelt werden können, um von Apple, seinen verbundenen Unternehmen und/oder deren Dienstleistern gespeichert, verarbeitet und genutzt zu werden“. Weiterhin behält sich Apple das Recht vor, „jederzeit die Bedingungen und Richtlinien des Programms ändern zu können, mit oder ohne vorherige Mitteilung“. Beachtenswert ist auch die Regelung, Inhalte „ohne vorherige Ankündigung und in seinem alleinigen Ermessen […] jederzeit vorab sichten, verschieben, ablehnen, modifizieren und/oder entfernen, […]“ zu können. Damit werden die im Datenschutzrecht verankerten Datenschutzforderungen wie Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz (vgl. § 21 Abs. 2 Nr. 1 - 6 DSG M-V) praktisch komplett missachtet. Und diese Beispiele verdeutlichen lediglich einen Teil der Datenschutzverstöße, die bei der Nutzung von Apples iCloud-Dienst unvermeidbar sind.

Folgerichtig haben wir der Landtagsverwaltung empfohlen, auf die iCloud-Nutzung zu verzichten. Da die Geräte den Abgeordneten jedoch mit Ausnahme der Installation von Zertifikaten, die den Zugang zu einer geschlossenen WLAN-Infrastruktur des Landtages ermöglichen, komplett ohne einschränkende Konfiguration oder beschränkte Rechte ausgeliefert werden, ist eine Kontrolle der Einhaltung dieser Maßnahme nicht möglich. Der Landtagsverwaltung blieb somit nur übrig, den Abgeordneten zu empfehlen, die iCloud nicht zu nutzen. Diese Empfehlung wird regelmäßig während der Einweisung der Abgeordneten in die Nutzung ihrer iPads ausgesprochen.

Dass angemessene Sicherungsmechanismen für iPads zwingend erforderlich sind, zeigte sich bereits kurz nach der Ausgabe der Geräte an die Abgeordneten. Schon im Februar 2012 hatte ein Abgeordneter sein iPad verloren. Jedoch wurde das Gerät gefunden und der Abgeordnete erhielt es nach kurzer Zeit zurück. Nach wie vor gibt es jedoch keine verbindlichen Regelungen dafür, was bei einem endgültigen Verlust derartiger Geräte zu tun ist.

Inzwischen gibt es aber praxistaugliche Möglichkeiten, mit mobilen Geräten wie iPad & Co. datenschutzkonform umzugehen. Unsere Empfehlungen zu diesem Thema sind unter Punkt 5.1.8 nachzulesen.

5.1.4 Cloud-Computing

TrustedCloud-Projekt des Bundeswirtschaftsministeriums
Das Bundesministerium für Wirtschaft (BMWi) hat Ende 2011 das Technologieprogramm „Sichere Internet-Dienste - Sicheres Cloud-Computing für Mittelstand und öffentlichen Sektor (Trusted Cloud)“ gestartet, um deutsche Unternehmen zu unterstützen, die Potenziale von Cloud-Computing zu erschließen. Zu diesem Zweck wurde das Kompetenzzentrum Trusted Cloud gegründet. Eine der vier Arbeitsgruppen des Kompetenzzentrums befasst sich mit rechtlichen Fragestellungen des Cloud-Computing und bearbeitet schwerpunktmäßig datenschutzrechtliche Themen. Mit Blick auf die vom AK Technik (siehe Punkt 7) verabschiedete Orientierungshilfe zum Thema Cloud-Computing (siehe Zehnter Tätigkeitsbericht, Punkt 4.1.1) sind wir gebeten worden, gemeinsam mit Vertretern des Bundesdatenschutzbeauftragten (BfDI), des Landesdatenschutzbeauftragten Nordrhein-Westfalen und des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) in der AG Rechtsrahmen des Projektes mitzuarbeiten. Neben Rechtsfragen zur Vertragsgestaltung, zur Lizenzierung und zur Haftung standen zunächst die Datenschutzfragen im Mittelpunkt der Arbeitsgruppentätigkeit.

Das erste Arbeitsergebnis der Gruppe war folgerichtig das Arbeitspapier „Datenschutzrechtliche Lösungen für Cloud-Computing“ (http://trusted-cloud.de/documents/Datenschutzrechtliche-Loesungen-fuer-Cloud-Computing.pdf). Im Mittelpunkt des Papiers stehen Fragen der Datenverarbeitung im Auftrag, die für die datenschutzrechtskonforme Ausgestaltung des Cloud-Computing eine zentrale Rolle spielen. Das Papier zeigt in zehn Thesen den Reformbedarf der Auftragsdatenverarbeitung auf und entwirft einen konkreten Reformvorschlag. Ziel ist es, in der künftigen EU-Datenschutz-Grundverordnung (siehe Punkt 3.1) Möglichkeiten der Datenschutz-Zertifizierung von Cloud-Diensten zu verankern.

Die Arbeitsgruppe geht davon aus, dass die Auftragsdatenverarbeitung auch bei neuen Formen der Datenverarbeitung eine wichtige Rolle spielen wird (These 1), die bisherigen Regeln zur modernen Technik jedoch nicht mehr passen (These 2). An der datenschutzrechtlichen Verantwortung des Auftraggebers wird jedoch festgehalten (These 3). Allerdings müssen die Anforderungen an die Vertragsgestaltung angepasst werden (These 4). Als wesentliche Neuerung wird vorgeschlagen, dass das Kontrollerfordernis des Auftraggebers vor Ort künftig auch durch das Testat eines unabhängigen Dritten ersetzt werden kann (These 5), wobei dieses Testat einem standardisierten Anforderungskatalog genügen muss (These 6). Als Voraussetzung für ein solches Verfahren wird gefordert, dass die Prüfkriterien auf gesetzlicher Grundlage für den europäischen Binnenmarkt einheitlich festgesetzt werden (These 7) und dass das Testat durch qualifizierte private Stellen vergeben wird, die sich zuvor einer Akkreditierung unterziehen müssen (These 8). Die Akkreditierungsvoraussetzungen sind gemeinsam von Datenschutzaufsichtsbehörden und potenziellen Auftraggebern und Auftragnehmern festzulegen (These 9). Die Akkreditierung soll durch besonders qualifizierte unabhängige Stellen erfolgen (These 10).

Auf der Basis des Thesenpapiers wollte die Arbeitsgruppe dann relativ kurzfristig einen Formulierungsvorschlag für die EU-Datenschutz-Grundverordnung zu Fragen der Auftrags-Datenverarbeitung und des vorgeschlagenen Zertifizierungsverfahren erarbeiten. Es wurde empfohlen, den Verordnungsentwurf um zwei neue Textpassagen (Art. 26 Abs. 3a und Art. 39a) zu ergänzen. Leider wurden die Hinweise aus den Datenschutzbehörden, insbesondere des BfDI und des ULD, für den Vorschlag der Arbeitsgruppe nicht angemessen berücksichtigt. Der Formulierungsvorschlag, der dann kurzfristig dem Europäischen Parlament und dem Bundesinnenministerium zugeleitet wurde, deckt sich somit leider nicht vollständig mit den Auffassungen der Datenschutzbeauftragten von Bund und Ländern. Die Bundesregierung hat dennoch wesentliche Aspekte aus dem Konzept aufgegriffen und einen Gesetzgebungsvorschlag in die europäischen Verhandlungen eingebracht. Der aktuelle Kompromissvorschlag wurde von der irischen Ratspräsidentschaft sowie von der Ratsarbeitsgruppe in seinen wesentlichen Grundgedanken positiv aufgenommen.

Trotz der vorübergehend unterschiedlichen Auffassungen setzen wir unsere Zusammenarbeit mit dem Kompetenzzentrum Trusted Cloud fort, da wir das Projekt nach wie vor unterstützen möchten. Das Thesenpapier, das wir in vollem Umfang mittragen, muss nun in praktische Handlungsanweisungen und Verfahrensvorschläge umgesetzt werden, damit entsprechende Regelungen der EU-Datenschutz-Grundverordnung nach deren Inkrafttreten möglichst schnell in die Praxis umgesetzt werden sollen. Wir haben uns daher gerne bereit erklärt, das Kompetenzzentrum bei der Ausgestaltung des künftigen Zertifizierungsverfahrens zu beraten und insbesondere bei der Erarbeitung der erforderlichen Kriterienkataloge zu unterstützen.

Wir empfehlen der Landesregierung, sich frühzeitig mit den künftigen Datenschutzanforderungen an Cloud-Computing zu befassen, damit vorhandene Strukturen nach dem Inkrafttreten der EU-Datenschutz-Grundverordnung schnell angepasst und laufende Planungen schon jetzt entsprechend beeinflusst werden können.

Der Landtag in der Cloud?

Die Landtagsverwaltung hat uns Anfang des Jahres 2013 um die datenschutzrechtliche Bewertung eines sogenannten Datenraumes gebeten. Als Datenraum wurde ein digitales Schließfach bezeichnet, in dem verschiedene Gremien des Landtags verschiedenste Informationen wie Dateien, Bilder, Anlagen von Notizen oder Internetlinks ablegen können. Der Datenraum sollte die Kommunikation etwa zwischen den Abgeordneten und der Landtagsverwaltung oder zwischen der Landesregierung und dem Landesrechnungshof unterstützen. Er sollte zudem Funktionen bereitstellen, die das Versenden und Empfangen von Nachrichten sowie eine Nutzung von Terminkalendern, Wiedervorlagen und Adressbüchern unterstützen. Die vom Landtag ausgewählte technische Lösung sollte von einem externen Dienstleister realisiert und betrieben werden. Das gesamte Verfahren kann gemäß den allgemein anerkannten Begriffsbestimmungen als ein Cloud-Dienst eingestuft werden. Als Grundlage für die datenschutzrechtliche Bewertung wurden uns die bereits unterzeichneten Verträge mit dazugehörigen Anlagen zur Verfügung gestellt.

Den Unterlagen war zu entnehmen, dass auch solche Dokumente bereitgestellt werden sollten, die in nichtöffentlichen Sitzungen, wie beispielsweise in Ausschüssen des Landtages, behandelt werden. Somit wären auch sensible, personenbezogene Daten betroffen, im Fall des Petitionsausschusses sogar besonders schutzbedürftige Daten von Petentinnen und Petenten und im Fall von Untersuchungsausschüssen oftmals auch Daten mit besonders schutzbedürftigen Betriebs- und Geschäftsgeheimnissen. Nach der bundesweit anerkannten und für die Landesverwaltung verbindlich vorgeschriebenen BSI-Grundschutzmethodik werden solche Daten als „hoch schutzbedürftig“ eingestuft und erfordern somit erhebliche technische und organisatorische Maßnahmen, um den Anforderungen an Datenschutz und Datensicherheit gerecht werden zu können.

Da der Datenraum von einem externen Dienstleister bereitgestellt werden sollte und jedenfalls personenbezogene Daten betroffen sind, kommt nur eine Datenverarbeitung im Auftrag in Frage. Gemäß § 4 Abs. 1 Satz 3 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) hat der Auftraggeber den Auftragnehmer unter besonderer Berücksichtigung seiner Eignung für die Gewährleistung der nach §§ 21 und 22 notwendigen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Ein Auftraggeber ist in der Regel nur dann in der Lage, die Eignung der technischen und organisatorischen Maßnahmen zu beurteilen, wenn ihm ein Sicherheitskonzept vorliegt, dass gemäß § 22 Abs. 5 DSG M-V für jedes automatisierte Verfahren zu erstellen ist. Deshalb müssen die Auftragnehmer ein solches Sicherheitskonzept vorlegen, um ihre Eignung nachzuweisen.

Bei der Durchsicht der uns zum Zeitpunkt der Beurteilung zur Verfügung stehenden Unterlagen mussten wir feststellen, dass ein solches Sicherheitskonzept nicht vorhanden war und dementsprechend auch nicht zur Eignungsprüfung des ausgewählten Auftragnehmers herangezogen werden konnte. Auch bei weiteren vom ausgewählten Anbieter bereitgestellten Unterlagen fanden sich nur sporadische Angaben, die auf eine Gewährleistung einer sicheren Datenverarbeitung schließen ließen. Eine abschließende datenschutzrechtliche Bewertung konnte von uns daher nicht abgegeben werden. Vielmehr offenbarten sich uns viele Fragen und Hinweise, die auf eine datenschutzrechtlich unzulässige Verarbeitung personenbezogener Daten hindeuteten.

So räumte sich der Auftragnehmer unter Hinweis auf die Sicherstellung der Verfügbarkeit der Daten die Möglichkeit ein, die Daten selbst entschlüsseln zu können. Diese Zugriffsmöglichkeiten des Auftragnehmers sind angesichts der Sensibilität der verarbeiteten und mit Blick auf die zu gewährleistende Vertraulichkeit der Daten (§ 21 Abs. 2 Nr. 1 DSG M-V) nicht hinnehmbar. Weiterhin sollte der Zugang zu den abgelegten Daten mithilfe der Eingabe von Kennung und Passwort ermöglicht werden. Angesichts der besonderen Sensibilität der Daten ist allerdings fraglich, ob der Zugang zu diesen Daten ausschließlich über einen solch einfachen Mechanismus ermöglicht werden darf. Stand der Technik sind heute sogenannte Zwei-Faktor-Authentisierungen, deren höheres Sicherheitsniveau auf Besitz (bspw. Chipkarte) und Wissen (bspw. PIN) beruht. Mangels einer aussagekräftigen Schutzbedarfsfeststellung und einer darauf aufbauenden Risikoanalyse (gemäß den Vorgaben der BSI-Grundschutzmethodik) konnte aber auch hier keine abschließende Bewertung vorgenommen werden. Ein weiterer Punkt, der uns an einer datenschutzrechtlich zulässigen Verarbeitung zweifeln ließ, betraf die Gewährleistung der Verfügbarkeit der Daten, die sich aus § 21 Abs. 2 Nr. 3 DSG M-V ableiten lässt.

So behielt sich der Auftragnehmer vor, „… den Service auch ganz einzustellen…“ und wies diesbezüglich jegliche Erfüllungs- und Schadensersatzansprüche von sich. Weiterhin räumte sich der Auftragnehmer das Recht ein, „… rechtswidrige Inhalte ohne Vorankündigung [...] zu entfernen“. Diese Rechte stehen klar im Widerspruch zu den rechtlichen Rahmenbedingungen einer Auftragsdatenverarbeitung in § 4 Abs. 2 DSG M-V, nach der Auftragnehmer personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten dürfen. Das Löschen von Daten ohne ausdrückliche Anweisung des Auftraggebers wäre im Rahmen der Datenverarbeitung im Auftrag nicht zulässig und würde zudem die Verfügbarkeit der Daten in unzulässiger Weise beeinträchtigen. Auch die vom Auftragnehmer zum Auftraggeber abgewälzte Pflicht, die Verfügbarkeit der Daten selbst zu gewährleisten, indem „… eingestellte Inhalte in maschinenlesbarer Form vorzuhalten und gesondert zu sichern sind“, ist aus Sicht des Datenschutzrechts in diesem Fall schlicht nicht zulässig.

Im Ergebnis unserer Prüfung mussten wir feststellen, dass die Verarbeitung personenbezogener Daten durch den ausgewählten Auftragnehmer unter den uns vorliegenden Bedingungen aus datenschutzrechtlicher Sicht nicht zulässig ist. Wir haben der Landtagsverwaltung daraufhin empfohlen zu prüfen, ob nicht auf ein vergleichbares Angebot des IT-Landesdienstleisters, der DVZ M-V GmbH, zurückgegriffen werden kann.

5.1.5 Orientierungshilfe zum neuen Internetprotokoll IPv6

Jeder Rechner mit Internet-Zugang benötigt eine Adresse, unter der er angesprochen werden kann - den Internet-Providern gehen jedoch die Adressen aus, weil die meisten Anbieter von Internet-Zugängen und anderen Internet-Diensten noch die Version 4 des Internet-Protokolls benutzen. Dieses schon 1981 definierte Protokoll sieht 32 Bit lange Adressen vor. Daraus resultiert eine maximale Zahl von etwa 4,3 Milliarden Adressen. Die zur Verfügung stehenden Adressen sind weitgehend an die Internet-Provider verteilt.

Der Mangel an IP-Adressen hat sich lange angekündigt, wissen doch das Internet-Normungsgremium IETF, die verschiedenen Stellen, die Adresskontingente verwalten, und die Provider schon seit geraumer Zeit, dass der Adressvorrat nicht ausreicht (siehe auch Zehnter Tätigkeitsbericht, Punkt 4.1.2). Der Nachfolgerstandard (Version 6 des Internet-Protokolls - IPv6), der dieses Problem behebt, wurde bereits 1998 von der IETF in seiner noch heute geltenden Fassung vorgestellt. Doch die verschiedenen Akteure im Netzwerkmarkt, darunter die Provider, zögerten lange, diesen Standard einzuführen. Internet-Zugänge mit IPv6 sind noch immer selten. Inzwischen arbeiten die Provider jedoch mit Hochdruck an der Umstellung ihrer Netze. Der Adressmangel wird sich zuerst bei denjenigen Betreibern bemerkbar machen, die Endkunden direkt versorgen. Aufgrund des Wachstums in diesem Marktsegment ist eine Umstellung auf IPv6 hier unvermeidbar, da insbesondere neueren mobilen Endgeräten und Routern mit ständig erreichbaren Diensten wie Internet-Telefonie global eindeutige Adressen zugewiesen werden müssen.

Mit der Einführung von IPv6 wird die Knappheit an Adressen durch einen Überfluss abgelöst, denn es sind nun $2^{128} \approx 3{,}4 \cdot 10^{38}$ Adressen verfügbar. Die Menge ist so groß, dass theoretisch jedem Sandkorn auf der Erde mehrere Internet-Adressen zugewiesen werden könnten. Auch wenn einige dieser Adressen besonderen Zwecken dienen oder für künftige Anwendungen reserviert sind, reicht dieser riesige Adressraum nach derzeitigem Kenntnisstand aus, um jedem heutigen oder künftigen elektronischen Gerät mehrere eigene Adressen zuzuweisen.

Datenschutzrechtlich problematisch ist folgender Aspekt: Würde jedes Gerät eine feste Adresse erhalten (statische Adressvergabe), wäre jedes dieser Geräte an seiner Adresse wieder erkennbar. Damit können leicht Nutzungsprofile zu einem Gerät und damit zu dessen Nutzern gebildet und zusammengeführt werden. Um eine Adresse nicht nur einem Gerät, sondern auch einer Person zuordnen zu können, muss häufig nicht einmal der Zugangsanbieter mitwirken. Insbesondere Betreibern von Internetdiensten, die eine Identifikation erfordern (etwa online-shops oder soziale Netzwerke), stehen dazu bereits genügend Informationen zur Verfügung.

Die Umstellung von IPv4 auf IPv6 wirkt sich also direkt auf Datenschutz und Datensicherheit aus. Allerdings bietet IPv6 diesbezüglich zahlreiche Gestaltungsmöglichkeiten. Die Datenschutzbeauftragten des Bundes und der Länder möchten alle Beteiligten bei der datenschutzgerechten und sicheren Nutzung von IPv6 unterstützen. Sie haben daher erste Empfehlungen in der Orientierungshilfe „Datenschutz bei IPv6 – Hinweise für Hersteller und Provider im Privatkundengeschäft“ zusammengefasst (siehe http://www.datenschutz-mv.de/datenschutz/publikationen/informat/ipv6/oh_ipv6_privat.pdf).

Dazu gehören Folgende:

- IPv6-Adressen bestehen aus einem Adresspräfix (vordere Hälfte) und einem Interface Identifier (hintere Hälfte). Um das Tracking von Nutzern zu vermeiden, sollen Adresspräfixe grundsätzlich dynamisch an Endkunden vergeben werden. Sollte sich ein Provider für die Vergabe eines (einzelnen) statischen Präfixes an einen Endkunden entscheiden, dann muss dieser Präfix auf Wunsch des Kunden gewechselt werden können. Hierzu muss dem Kunden eine einfache Bedienmöglichkeit am Router oder Endgerät zur Verfügung gestellt werden. Verlangt ein Kunde ausdrücklich einen statischen Präfix, so kann auf die Wechselmöglichkeit verzichtet werden.

- Um den Ortsbezug von Adressen zu verringern, sollten Provider die Adressen für Einwahl-Knoten und sonstige Infrastrukturkomponenten zufällig aus dem ganzen ihnen zur Verfügung stehenden Pool auswählen und regelmäßig innerhalb des Pools wechseln.

- Die sogenannten Privacy Extensions sorgen für eine zufällige Vergabe des Interface Identifiers. Privacy Extensions müssen auf Endgeräten implementiert und sollten standardmäßig eingeschaltet sein. Ist dies nicht möglich, muss eine benutzerfreundliche manuelle Wechselmöglichkeit für den Interface Identifier bestehen. Zusätzlich sollten die Betriebssystem-Hersteller benutzerfreundliche Konfigurationsmöglichkeiten einbauen, mit denen Kunden die Wechselfrequenz des Interface Identifiers auf kurze Werte festlegen können (z. B. alle 10 Minuten) bzw. einen Wechsel zu bestimmten Ereignissen anstoßen lassen können (z. B. beim Start des Browsers oder beim Start oder Aufwachen des Rechners).

- Interface Identifier und Präfix sollten synchron gewechselt werden.

- Die Endgeräte-Hersteller sollten ihre Produkte mit korrekt und sinnvoll vorkonfigurierten IPv6-fähigen Paketfiltern ausstatten und diese über eine leicht zu bedienende Oberfläche zugänglich machen. Bei der Aktivierung der IPv6-Unterstützung im Router sollte die Aktivierung des Paketfilters automatisch stattfinden, dem Nutzer aber zumindest empfohlen werden.

- An die Betreiber von Internetdiensten auf der Basis von IPv6 richtet sich die Empfehlung, zur wirkungsvollen Anonymisierung von IPv6-Adressen die unteren 88 bis 96 Bit jeder Adresse zu löschen.

5.1.6 Elektronische Zeiterfassung in der Landesregierung (ZEUS)

Bereits im Neunten (siehe Punkt 2.11.7) und im Zehnten Tätigkeitsbericht (siehe Punkt 4.3.4) haben wir uns mit dem Projekt der elektronischen Zeiterfassung „ZEUS“ auseinandergesetzt. Unser Optimismus im Zehnten Bericht, dass seitens des Innenministeriums eine Streichung der seinerzeit vorgesehenen Vorlagepflicht des Monatsjournals erwogen würde, hat sich jedoch leider als unbegründet herausgestellt. Anstatt vor dem Hintergrund der allumfassenden Datenskandale nun ein „Weniger“ an personenbezogenen Daten zu erheben bzw. zu nutzen, ist offenbar aufgrund verbesserter technischer Möglichkeiten ein „Mehr“ an Datensammlungen geplant. Die allgemein zu beobachtende Tendenz, das eventuell Nützliche mit dem Erforderlichen gleichzusetzen und grundsätzlich Vertrauen durch umfassende und auf mehr oder weniger geeignete Messdaten basierende Kontrolle zu ersetzen, scheint sich auch in diesem Feld durchzusetzen.

So wird im diesbezüglich unter anderem pilotierenden Innenministerium seitens der Leitungsebenen über die ursprünglich geplante (und von uns schon datenschutzrechtlich monierte) Vorlage des Monatsjournals hinaus eine arbeitstägige Saldenliste praktiziert und darüber hinaus auch detaillierte und jederzeit niederschwellig elektronisch verfügbare Informationen über die Kernzeit- und Pausenregelungen, über das Urlaubsguthaben, Krankheit, Dienstreisen und Sollarbeitszeiten für erforderlich gehalten. Zur Begründung führt das Ressort auch hier vor allem die Fürsorgeverpflichtung der Dienstherren und die damit ermöglichte Steuerungsoptimierung an.

An unserer zu einer deutlich milderen Datenerfassung schon im Zehnten Tätigkeitsbericht geäußerten Kritik (siehe oben) hat sich nichts geändert. Angesichts der nun offenbar noch weitergehenden Planungen halten wir in Ergänzung dieser Ausführungen die folgenden datenschutzrechtlichen Hinweise für erforderlich:

Zur Wahrnehmung der Personalverantwortung reicht es regelmäßig aus, wenn den jeweiligen Vorgesetzten im Bedarfsfalle, das heißt, aus gegebenem Anlass, Kenntnis von den gespeicherten relevanten Arbeitszeiten gegeben wird. Dieser Bedarfsfall kann selbstverständlich automatisiert gekennzeichnet werden.

Solange sich die Mitarbeiterinnen und Mitarbeiter jedoch innerhalb des vorgegebenen Rahmens der gleitenden Arbeitszeit bewegen, was schon durch eine automatisierte Kontrolle festgestellt werden kann, und solange kein begründeter Verdacht einer Manipulation des Zeiterfassungssystems vorliegt, besteht keine Erforderlichkeit im obigen Sinne auch nur die Monatsjournale der Mitarbeiterinnen und Mitarbeiter anlassfrei den Vorgesetzten vorzulegen. Die bestehenden Gleitzeitregelungen gehen im Allgemeinen von einer Eigenverantwortlichkeit der Beschäftigten aus, die eigenständig auf die Einhaltung der gesetzlich oder tariflich festgelegten Arbeitszeit (einschließlich der festgelegten Minderzeiten oder Guthaben) zu achten haben. Auch bei evtl. nachgewiesenen Einzelfällen des Missbrauchs dieses notwendigen arbeitgeberseitigen Vertrauens kann somit nicht von dem Erfordernis einer lückenlosen, das heißt, auch den bisher unauffälligen Beschäftigten betreffenden, Kontrolle ausgegangen werden. Ein ständiger (niederschwellig auf Mausklick möglicher) Online-Zugriff durch Vorgesetzte oder auch nur die anlassfreie, flächendeckende und regelmäßige Auswertung aller Zeiterfassungsdaten wäre datenschutzrechtlich unzulässig. Eine derartige Praxis führte über die schon genannten Gründe hinaus zu einer Datenvorratsspeicherung seitens der Leitungsebenen zu nicht festgelegten bzw. zulässigen Zwecken und stellte auch insoweit einen Verstoß gegen den Verhältnismäßigkeitsgrundsatz dar.

Was nun für die bisher kritisch zu bewertende Praxis der anlassfreien Vorlage der Tagessaldi schon festzustellen ist, gilt noch stärker für die offenbar darüber hinaus erwogenen verbundenen Datenbestände hinsichtlich der diversifizierten Stundenangaben (Kommen und Gehen), der Krankheitszeiten, der Urlaubskonten und Dienstreisen etc. Durch die damit einfach mögliche Verbindung der Daten lägen Profilbildungen des Mitarbeiterverhaltens quasi auf der Hand, die aus gutem Grund datenschutzrechtlich unzulässig und zudem wohl kaum noch mit dem gegenseitigen Vertrauensgrundsatz der Tarifparteien bzw. einem vertrauensvollen und kooperativen Miteinander in der Behörde zu vereinbaren wären. Die wahrscheinliche subjektive Wirkung dieses Verhaltens auf die Mitarbeiterinnen und Mitarbeiter würde unseres Erachtens in diesem Falle mit dem objektiven Befund einer schlichten (fast lückenlosen) Arbeitsplatzkontrolle übereinstimmen.

5.1.7 Dokumentenmanagement in der Landesverwaltung (BEATA)

Bereits seit 2008 beraten wir die Landesregierung bei der Einführung des einheitlichen Dokumentenmanagement- und Vorgangsbearbeitungssystems DOMEA® in den Ministerien und in der Staatskanzlei (siehe dazu auch Zehnter Tätigkeitsbericht, Punkt 4.3.2). Nun plant das Landesbesoldungsamt (LBesA) mit dem Projekt BEATA (**B**ezügedaten **e**lektronisch **a**nweisen, **t**ransportieren und **a**rchivieren) die Nutzung einer speziellen Variante von DOMEA®. Das elektronische Aktenablage- und Verwaltungssystem für Bezügeakten soll als behördenübergreifendes System den elektronischen Austausch von bezügerelevanten Daten unterstützen und den Landesbediensteten die Möglichkeit geben, elektronisch mit dem LBesA zu kommunizieren.

Der modulare Aufbau von BEATA ermöglicht die Nutzung verschiedener technischer Basiskomponenten, die in Umsetzung des E-Government-Masterplans der Landesregierung bereitgestellt wurden. Dazu gehören neben DOMEA® auch Formularserver und Portale. Von besonderer Bedeutung ist die Einbindung einer weiteren Komponente, mit der Daten und Dokumente rechtswirksam bis zum Ende der jeweiligen Aufbewahrungsfristen beweiswerterhaltend, vertrauenswürdig und nachweislich gespeichert werden können. Zum Einsatz kommt hier ein von der BOS Bremen entwickeltes Modul, mit dem die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) vorgegebene „Technische Richtlinie zur Beweiserhaltung kryptographisch signierter Dokumente“(TR-ESOR 03125) vollständig umgesetzt wird. BEATA setzt damit die im E-Government-Masterplan formulierte Zielstellung nach einer durchgehenden, elektronischen Abwicklung von Verwaltungsvorgängen zwischen den einzelnen Behörden des Landes und einer bürgernahen Verwaltung durch spätere Anbindung von Online-Dienstleistungen um.

Dass das LBesA dem Thema Datenschutz den angemessenen Stellenwert zukommen lässt, zeigt sich schon darin, dass wir seit Beginn der Planungen im Jahr 2011 in das Projekt einbezogen wurden. So konnte frühzeitig damit begonnen werden, BEATA am Konzept „Privacy by Design“ auszurichten. Datenschutzrechtliche Vorgaben wurden also schon bei der Projektplanung und -entwicklung berücksichtigt und nicht erst nach einer erfolgten Umsetzung. Somit wurde vermieden, dass ggf. erst später auftretende Datenschutzprobleme mit zeitaufwändigen und kostenintensiven Korrekturprogrammen oder umständlichen Dienstvereinbarungen gelöst werden müssen.

Besonders positiv ist anzumerken, dass das LBesA unserer Forderung nach einer Transport- und Dokumentenverschlüsselung gefolgt ist. Wesentlichen Anforderungen des Landesdatenschutzgesetzes Mecklenburg-Vorpommern (DSG M-V) nach Gewährleistung der Vertraulichkeit der übermittelten und gespeicherten Daten *(siehe Kasten)* konnten somit umgesetzt werden.

Aktuell begleiten wir sowohl die Umsetzung des Dienststellenportals, mit dessen Hilfe Formulare zwischen den einzelnen Dienststellen und dem LBesA ausgetauscht werden, als auch die Planung eines Mitarbeiterportals, welches den Angestellten die Möglichkeit eröffnet, von zu Hause aus Dokumente mit dem LBesA auszutauschen. Von zentraler Bedeutung ist hierbei neben den Anforderungen an Vertraulichkeit auch die Sicherstellung der Integrität und Authentizität der Daten gemäß § 21 Abs. 2 Nr. 2 und 4 DSG M-V *(siehe Kasten)*. Demnach muss die Integrität der verarbeiteten Daten jederzeit überprüfbar sein und zudem nachvollziehbar sein, wer der Urheber der Daten ist. Hierfür sind elektronische Signaturen nach dem Signaturgesetz das geeignete Mittel. Zu prüfen ist aber auch, ob gegebenenfalls die neuen schriftformwahrenden Verfahren in Betracht kommen, die mit dem Artikelgesetz zur Förderung der elektronischen Verwaltung (siehe Punkt 3.2) geschaffen wurden.

§ 21 Allgemeine Maßnahmen zur Datensicherheit
(1) Die Ausführung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz ist durch technische und organisatorische Maßnahmen sicherzustellen, die nach dem Stand der Technik und nach der Schutzbedürftigkeit der zu verarbeitenden Daten erforderlich und angemessen sind.
(2) Dabei ist insbesondere zu gewährleisten, dass
1. nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit).
2. personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität),
3. …
4. personenbezogene Daten jederzeit ihrem Ursprung zugeordnet werden können (Authentizität der Daten).

5.1.8 Bring Your Own Device (BYOD)

Bereits im Zehnten Tätigkeitsbericht, Punkt 4.1.4, wurde auf die steigende Anzahl von Anfragen aus der öffentlichen Verwaltung zum datenschutzgerechten Einsatz von mobilen Endgeräten wie Smartphones (z. B. BlackBerry und iPhone) oder Tablet PC (z. B. iPad oder Galaxy Pad) und die mit der Nutzung dieser Geräte verbundenen Risiken hingewiesen. Die dort formulierten Empfehlungen sind nach wie vor aktuell. Inzwischen sind jedoch weitere Bedrohungen und Risiken bekannt geworden.

Sollen dennoch mobile Endgeräte in der öffentlichen Verwaltung zum Einsatz kommen, ist zunächst zu klären, ob der Dienstherr Endgeräte zur Verfügung stellt oder ob vorhandene private Endgeräte eingebunden werden sollen. Wir empfehlen nachdrücklich den Einsatz von behördeneigenen Geräten. Nur so lassen sich rechtliche Vorgaben mit angemessenem Administrationsaufwand umsetzen. Die Administratoren müssen sich beispielsweise nicht mit den Betriebssystemen und Anwendungen (so genannte Apps) unterschiedlicher Hersteller und den damit verbundenen, teils sehr unterschiedlichen Sicherheitsniveaus auseinandersetzen. Stattdessen kann gezielt das für den angestrebten Einsatzzweck geeignetste Endgerät und Betriebssystem sowie das dazu passende MDM-Verwaltungssystem (Mobile Device Management) ausgewählt werden, um so eine einheitliche und weitgehend administrierbare Systemumgebung für die mobilen Endgeräte zu schaffen.

Aber auch mit dem Einsatz von behördeneigenen mobilen Endgeräten bleiben noch viele Risiken, die zusätzliche Sicherheitsmaßnahmen erfordern. Auf jeden Fall muss sichergestellt werden, dass dienstliche und private Daten strikt voneinander getrennt werden. Zudem müssen der Empfang und der Versand von dienstlichen E-Mails, die Bereitstellung eines Terminkalenders inklusive Adressbuch oder der Zugriff auf Dokumente aus dem internen Behördennetz ohne eine Verringerung des notwendigen Sicherheitsniveaus möglich sein. Die zahlreichen Gefährdungen, die sich durch einen mobilen Zugriff zusätzlich ergeben, müssen in einer Risikoanalyse bewertet werden. Bekannte Risiken sind beispielsweise der unbefugte Zugriff auf Daten durch einen Geräteverlust oder durch unbemerkt installierte Schadsoftware sowie eine unberechtigte Modifikation des Betriebssystems (Jailbreak oder Rooting) oder der Einsatz veralteter Firm- oder Software.

Die aus der Risikoanalyse resultierenden Maßnahmen sind in einem Sicherheitskonzept - möglichst gemäß den entsprechenden Standards des Bundesamtes für Sicherheit in der Informationstechnik - festzuschreiben. Aktuell zeichnet sich der Trend ab, dass sich so genannte App-Container als eine geeignete technische Lösung im mobilen Umfeld etablieren. Die App-Container stellen sicher, dass eine Verarbeitung der Daten zwar zwischen den darin enthaltenen Apps möglich ist, diese den Container jedoch nicht verlassen können. Zudem bieten sie weitere Sicherheitsmaßnahmen wie notwendige Verschlüsselungsmechanismen sowie verschlüsselte Datenübertragungen. Dennoch sind technische Sicherheitsvorkehrungen allein in der Regel jedoch nicht ausreichend. Zusätzlich sind immer organisatorische Maßnahmen wie Dienstvereinbarungen, transparente Dokumentationen der Administrationsaktivitäten und Sensibilisierungen der Mitarbeiterinnen und Mitarbeiter im Umgang mit den Endgeräten umzusetzen.

Die Empfehlung lautet, zunächst stets zu prüfen, ob der Einsatz mobiler Endgeräte wirklich erforderlich ist. Wird die Nutzung tatsächlich als notwendig erachtet, sollte der Zugriff von mobilen Geräten in die Behördeninfrastruktur sorgfältig geplant und so restriktiv wie möglich ausgestaltet werden. Als Planungshilfsmittel wird in absehbarer Zeit ein Konzept zum Aufbau und Betrieb eines Systems zur Verwaltung mobiler Endgeräte zur Verfügung stehen, das von der DVZ M-V GmbH im Auftrag des Innenministeriums und in Abstimmung mit dem Landesbeauftragten für Datenschutz und Informationsfreiheit erarbeitet wird.

5.1.9 Datentrennung trotz Zentralisierung

Zur Zentralisierung und Konsolidierung verteilter Datenverarbeitung sowie aus Kostengründen greifen datenverarbeitende Stellen zunehmend auf kooperative Betriebsmodelle zurück, die die gemeinsame Nutzung von Systemen und Programmen zur automatisierten Verarbeitung personenbezogener Daten vorsehen. Die gemeinsame Nutzung einer solchen Infrastruktur unterliegt erhöhten Anforderungen an die Trennung der personenbezogenen Daten, um die aus der gemeinsamen Nutzung entstehenden Risiken für die informationelle Gewaltenteilung, die Zweckbindung und Vertraulichkeit hinreichend zu reduzieren.

In diesem Zusammenhang werden die Begriffe „Mandant“ und „Mandantenfähigkeit“ relevant. Mandantenfähigkeit ist gegeben, wenn Unternehmen, Behörden oder Organisationen in der Lage sind, Daten in einer Datenbank logisch zu trennen und zu verwalten. Mit Hilfe der Mandantenfähigkeit können zum Beispiel Daten verschiedener Abteilungen einer Organisation bzw. eines Unternehmens oder Daten verschiedener Kunden eines IT-Services bzw. eines Rechenzentrums getrennt vorgehalten werden.

Die Kontroll- und Beratungstätigkeit der Datenschutzaufsichtsbehörden hat gezeigt, dass einerseits erheblicher Bedarf an mandantenfähigen Verfahren vorhanden ist, andererseits aber immer wieder Schwierigkeiten bestehen, die Mandantenfähigkeit solcher Lösungen zu prüfen oder nachzuweisen. Das betrifft sowohl länderübergreifende Verfahren wie das gemeinsame Telekommunikationsüberwachungszentrum der norddeutschen Bundesländer als auch landeseigene Verfahren wie das zentrale Informationsregister im Meldewesen (ZIR), das gemeinsame Dokumentenmanagementsystem DOMEA oder die Personalverwaltungssoftware EPOS.

Vor diesem Hintergrund hat der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ (AK Technik, siehe Punkt 7) die Orientierungshilfe „Mandantenfähigkeit“ erarbeitet. Diese Orientierungshilfe soll die verantwortlichen Stellen in die Lage versetzen, ihre Verfahren in einem mehrstufigen Prüfverfahren auf Mandantenfähigkeit zu prüfen.

Im ersten Schritt ist zu prüfen, ob eine ausreichende Trennung bei der gemeinsamen Nutzung einer IT-Infrastruktur gewährleistet wird und ob die Datenschutz- und Datensicherheitsanforderungen angemessen und wirksam umgesetzt werden. Im zweiten Schritt muss die Ausgestaltung von Übermittlungen zwischen Mandanten untersucht werden. Bei einer getrennten Verarbeitung auf gemeinsamer IT-Infrastruktur ist nämlich die Verarbeitung von Daten eines Mandanten in einem anderen Mandanten als Datenübermittlung auszugestalten. Die rechtlichen Grundlagen und Anforderungen an die Zulässigkeit der Übermittlung und die Form ihrer Durchführung sind daher vorab zu prüfen. Zur Prüfung auf eine ausreichende Trennung der einzelnen Mandanten auf einer gemeinsamen Infrastruktur gehört im dritten Schritt die Prüfung der Abgeschlossenheit der Transaktionen innerhalb eines Mandanten. Die Prüfung auf Abgeschlossenheit muss transaktionsbasiert erfolgen und nachweisen, dass die Datentrennung erhalten bleibt. Der vierte Prüfschritt soll dann nachweisen, dass die Zugriffsberechtigungen, die Verarbeitungsfunktionen und die Konfigurationseinstellungen je Mandant eigenständig festgelegt werden können. Da es bei der gemeinsamen Nutzung von Systemen und Programmen oft sinnvoll ist, mandantenübergreifende Funktionen zur Verwaltung der Mandanten und der gemeinsam genutzten Infrastruktur bereitzustellen, muss der fünfte Schritt nachweisen, dass mit Hilfe solcher Verwaltungsfunktionen grundsätzlich keine Verarbeitung personenbezogener Daten eines Mandanten möglich ist. Im Ergebnis dieser Prüfschritte fordert die Orientierungshilfe, das Datenschutz- und Sicherheitsmanagement auf diese besondere Form der Datenverarbeitung anzupassen.

Wir empfehlen der Landesregierung, bei der Planung und Entwicklung von IT-Verfahren, die die gemeinsame Nutzung von Systemen und Programmen zur automatisierten Verarbeitung personenbezogener Daten vorsehen, die gegebenenfalls erforderliche Mandantenfähigkeit durch die Anwendung der Orientierungshilfe sorgfältig zu prüfen. Zudem sollten bereits im Betrieb befindliche Verfahren auf ihre Mandantenfähigkeit überprüft und gegebenenfalls nachgebessert werden.

5.2 Videoüberwachung

5.2.1 Schummeln in der Prüfung - keine Chance!

Eine Journalistin, die davon erfuhr, dass ein Professor in einer Universität während einer Klausur ohne Wissen der Studierenden Videokameras zu Kontrollzwecken eingesetzt hatte, wandte sich an uns, um die Rechtmäßigkeit dieses Vorgehens prüfen zu lassen.

Auf unsere Veranlassung hin prüfte der Datenschutzbeauftragte der Universität den Sachverhalt. Es handelte sich in diesem Fall um einen Hörsaal, der mit einer Kameraanlage ausgestattet ist. Diese Anlage ist jedoch grundsätzlich dafür bestimmt, entsprechende Demonstrationen für alle Teilnehmerinnen und Teilnehmer der Lehrveranstaltungen sichtbar über einen Beamer auf einer großen Leinwand im Hörsaal darzustellen. Außerdem werden die Bilder auf den Monitoren im Rednerpult zur Kontrolle wiedergegeben. Die beiden Kameras sind technisch jedoch nicht geeignet gewesen, die erfassten Bilder aufzuzeichnen. Während der Klausur wurde die Kameraanlage durch die Klausuraufsicht insofern „zweckentfremdet“, als die Kameras auf die Studierenden gerichtet wurden, die auf den schlechter einsehbaren hinteren Plätzen des Hörsaales Platz genommen hatten. Der Professor konnte dann auf einem Bildschirm an seinem Rednerpult das Verhalten der Studierenden beobachten.

Rechtsgrundlage für die Verarbeitung personenbezogener Daten an Hochschulen ist § 7 Landeshochschulgesetz (LHG M-V). Danach darf die Hochschule auf der Grundlage des Landesdatenschutzgesetzes (DSG M-V) die Verarbeitung von Daten für Prüfungen regeln. Eine entsprechende Regelung bestand jedoch nicht, sodass in diesem Fall die Bestimmungen des § 37 DSG M-V zu beachten waren. Danach ist eine Videoüberwachung nur zur Wahrnehmung des Hausrechtes zulässig und muss durch geeignete Maßnahmen erkennbar gemacht werden. Außerdem muss eine Abwägung der Interessen an einer Überwachung mit den schutzwürdigen Belangen der Betroffenen stattfinden. Nur wenn die gesetzlichen Voraussetzungen des § 37 DSG M-V erfüllt sind, wäre eine Videoüberwachung rechtmäßig. Eine Videoüberwachung zur Vermeidung/Aufdeckung von Betrugshandlungen bei Prüfungen fällt nicht unter das Hausrecht und ist somit unzulässig.

Da wir bereits ein Jahr zuvor einen ähnlichen Fall bearbeitet hatten und - wie die Erfahrung gezeigt hat - die Informationen zum datenschutzgerechten Umgang bei Prüfungen nicht immer alle Betroffenen erreichen, haben wir der Universität empfohlen, nicht nur die Mitarbeiterinnen und Mitarbeiter im Prüfungsbereich, sondern alle Hochschullehrerinnen und Hochschullehrer sowie Mitarbeiterinnen und Mitarbeiter der Universität darauf hinzuweisen, dass eine Videoüberwachung bei Prüfungen unzulässig ist und Betrugsversuche durch organisatorische Vorkehrungen sowie eine entsprechende Aufsicht unterbunden werden sollten.

Die Universität ist unserer Empfehlung gefolgt.

5.2.2 Unzulässige Videoüberwachung auf einer Großbaustelle

Aufgrund einer Petition haben wir einen Informations- und Kontrollbesuch auf einer Großbaustelle durchgeführt. Es stellte sich heraus, dass die verantwortliche Stelle - ein großes Bauunternehmen - die Bauarbeiter auf dem jeweils oberen Stockwerk des Rohbaus eines Hochhauses während der gesamten Arbeitszeit durch Videokameras überwacht. Dazu waren die beiden Baukräne der Baustelle jeweils mit einer Kamera bestückt worden.

In seiner Stellungnahme hat das Unternehmen mitgeteilt, die Videoüberwachung diene unter anderem dazu, den reibungslosen Bauablauf zu kontrollieren und den Einsatz von größeren Geräten zu überwachen. Ziel sei ferner der Eigentumsschutz des Arbeitgebers, die Vermeidung von Havarien und die Erhöhung der Arbeitssicherheit.

Wir haben das Unternehmen darauf hingewiesen, dass eine lückenlose Videoüberwachung von Arbeitnehmern während der gesamten Arbeitszeit nach der Rechtsprechung des Bundesarbeitsgerichtes unzulässig ist. Wenn die Videoüberwachung allein den genannten Zwecken dienen soll, so hätten zur Erreichung dieser Zwecke Alternativlösungen bestanden, die weniger schwer in das informationelle Selbstbestimmungsrecht der betroffenen Arbeitnehmer eingreifen.

So bestand etwa die Möglichkeit, vor und nach den Arbeitszeiten sowie in den Pausen Aufnahmen anzufertigen, um die Einhaltung von Bauabläufen und den erfolgten Großgeräteeinsatz zu überwachen. Auch wäre es möglich gewesen, anlassbezogene einzelne Fotosequenzen anzufertigen - beschränkt auf besonders risikobehaftete Einsatzphasen bei Großgeräten. Auf diese Weise wären die Videoaufnahmen auf die relevanten Arbeitsabläufe eingeschränkt worden und eine zeitlich unbeschränkte und insofern undifferenzierte Überwachung und Kontrolle der Arbeiter während der gesamten Arbeitszeit würde vermieden. Zudem sind aufgezeichnete Bilder generell zur Vermeidung von Havarien ungeeignet. Havarien erfordern ein sofortiges Eingreifen. Durch gespeicherte Bilder der Videokamera besteht keine sofortige Interventionsmöglichkeit im Havariefall. Insgesamt war somit die Videoüberwachung weder durch § 6b Bundesdatenschutzgesetz (BDSG) noch durch § 32 BDSG legitimiert.

Nach § 32 BDSG dürfen personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses nur verarbeitet werden, wenn dies für die Durchführung des Beschäftigungsverhältnisses erforderlich ist oder falls tatsächliche Anhaltspunkte den Verdacht begründen, dass ein Beschäftigter eine Straftat begangen hat. Auch in letzterem Fall muss die Datenverarbeitung zu diesem Zweck erforderlich und darf nicht unverhältnismäßig sein und das schutzwürdige Interesse des Arbeitnehmers darf nicht überwiegen. Dies war hier allerdings der Fall. Zudem hatten die betroffenen Arbeiter keinen Anlass für die Videoüberwachung gegeben (etwa durch Rechtsverletzungen Diebstähle etc.) und es hätten für das Unternehmen geeignete Alternativlösungen bestanden, um die genannten Zwecke auch ohne die umfassende Videoüberwachung der Arbeitnehmer zu erreichen.

Wir haben die genannten Alternativlösungen mit dem Unternehmen erörtert und das Unternehmen auf die Rechtswidrigkeit der Überwachung hingewiesen. Das Unternehmen hat trotz Kenntnis der Rechtswidrigkeit die Videoüberwachung bis zum Abschluss der Großbaustelle fortgesetzt und überwacht seine Arbeiter auf anderen Baustellen in gleicher Weise.

Im Hinblick auf den langen Überwachungszeitraum (im vorliegenden Fall ca. zehn Monate) und wegen der großen Anzahl der ganztägig überwachten Arbeiter, die keinen Anlass für die Überwachung gegeben hatten, haben wir ein Bußgeld in fünfstelliger Höhe festgesetzt. Gegen den Bußgeldbescheid hat das Unternehmen Rechtsmittel eingelegt, sodass das zuständige Amtsgericht mit der Angelegenheit befasst ist.

5.2.3 Am Biertresen gefilmt

In einer Rostocker Kneipe mit einem rundum begehbaren Tresen, aus dessen Mitte heraus bedient wird, waren vier Videokameras installiert worden. Neben den Tischen und Sitzgelegenheiten war auch der runde Tresen im Kamerafokus. Aus dieser Videoüberwachung ergaben sich zwei gravierende datenschutzrechtliche Probleme: Zum einen die Überwachung der Besucher/innen und der Gäste und zum anderen die Überwachung des Personals der gastronomischen Einrichtung.

Die Tische und Sitzgelegenheiten im Kundenbereich, die in aller Regel zum längeren Verweilen, Entspannen und Kommunizieren einladen, dürfen grundsätzlich nicht videoüberwacht werden. Beim Besuch einer Kneipe ist das Verhalten des Gastes seinem Freizeitbereich zuzuordnen. Sein Persönlichkeitsrecht genießt deshalb einen besonders hohen Schutzbedarf. Die Intensität des Eingriffes wird dadurch deutlich, dass der Gast nicht unbeobachtet und somit unbeeinträchtigt kommunizieren kann. Die Unzulässigkeit der Videoüberwachung von Tischen und Sitzgelegenheiten in gastronomischen Einrichtungen wurde gerichtlich im sogenannten Balzac-Urteil festgestellt. Das schutzwürdige Interesse des Gastes, nicht überwacht zu werden, überwiegt in diesen Fällen in der Regel gegenüber dem berechtigten Interesse des Gastronomieinhabers an einer Überwachung.

Auch die Videoüberwachung des Personals, der Mitarbeiter/innen oder Angestellten ist nach der Rechtsprechung des Bundesarbeitsgerichtes grundsätzlich unzulässig, wenn diese ununterbrochen und nicht anlassbezogen ist. § 32 Bundesdatenschutzgesetz (BDSG), der die Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten regelt, ist streng auszulegen. Nur, wenn tatsächliche Anhaltspunkte für eine im Beschäftigungsverhältnis begangene Straftat bestehen und diese Anhaltspunkte dokumentiert wurden, darf ausnahmsweise videoüberwacht werden, wenn zusätzlich die folgenden drei Voraussetzungen vorliegen:

Als erstes muss die Videoüberwachung erforderlich sein, das heißt, falls die Straftat auf andere Weise mit milderen Mitteln nachgewiesen werden kann, ist die Videoüberwachung nicht erforderlich. Kommt man jedoch zum Ergebnis, dass die Überwachung erforderlich ist, so ist zweitens zu prüfen, ob das schutzwürdige Interesse der Beschäftigten nicht überwiegt. Insbesondere ist darauf zu achten, dass das schutzwürdige Interesse, nicht überwacht zu werden, vor allem bei denjenigen Betroffenen, die sich nichts zu Schulden kommen lassen haben, grundsätzlich überwiegt. Drittens müssen die Art und das Ausmaß der Überwachung verhältnismäßig sein. Wenn beispielsweise Anhaltspunkte für eine Straftat im Kassenbereich bestehen, wäre es unverhältnismäßig, das gesamte Geschäft zu überwachen. Unverhältnismäßig wäre es auch, die Kamera zeitlich unbegrenzt installiert und filmen zu lassen. Ist beispielsweise der Nachweis für die Straftat erbracht, ist die Kamera nicht mehr erforderlich. Das spiegelt die einschlägige Rechtsprechung der Arbeitsgerichte wider.
Auf unsere datenschutzrechtliche Bewertung hin wurde die Videoüberwachung in der Kneipe durch die Geschäftsführung eingestellt.

5.2.4 Videoüberwachung auf dem Friedhof

Der Landesverband eines bundesweiten eingetragenen Vereins hatte sich an uns gewandt, weil er als verantwortliche Stelle für eine große Friedhofs-/Gedenkanlage beabsichtigte, dort eine Videoüberwachungsanlage zu installieren. Auf dem Gelände des Friedhofes sei es in den vergangenen Jahren mehrfach zu Diebstählen von Buntmetall in erheblichem Umfang gekommen.

Auf dem Gelände befanden sich zwölf Gedenk-Bronzetafeln mit einem Gewicht von jeweils ca. 100 Kilogramm mit den Namen der bei einem Luftangriff gegen Ende des Krieges umgekommenen Personen. Drei dieser Bronzetafeln seien entwendet worden. Es habe sich um eine Schadenshöhe von mehreren zehntausend Euro gehandelt. Auf unsere Nachfrage zu einer möglichen Wiederholungsgefahr im Hinblick auf den Zweck der beabsichtigten Videoüberwachung erklärte die verantwortliche Stelle allerdings, man habe inzwischen die restlichen neun Bronzeplatten abgebaut und gesichert. Es sei geplant, diese durch Kunststoff- oder Aluplatten in Bronzeoptik zu ersetzen.

Im Rahmen der Erforderlichkeitsprüfung nach § 6b Abs. 1 BDSG war zu berücksichtigen, dass die verbleibenden neun Bronzetafeln bereits vorsorglich gesichert worden waren, sodass sie kein Zielobjekt für weitere Diebstähle bildeten. Hinsichtlich der Kunststoff- oder Aluminiumduplikate kam zudem gegenüber der Videoüberwachung als milderes Mittel eine Sicherung durch Bewegungsmelder gegebenenfalls in Verbindung mit Scheinwerfern sowie die Aufschaltung an einen Sicherheitsdienst oder die Polizei zur Prüfung in Betracht.

Auch wenn in Fällen dieser Art eine Erforderlichkeit bejaht werden kann, überwiegen jedoch speziell bei Friedhofsanlagen in der Regel die schutzwürdigen Interessen der betroffenen Besucherinnen und Besucher gemäß § 6b BDSG. Betroffene sind insbesondere die Angehörigen der auf dem Friedhof beerdigten Personen, die deren Grabstätten besuchen, um ihrer verstorbenen Verwandten und Freunde zu gedenken und dort Blumen niederzulegen. Insofern kommt hier den schutzwürdigen Interessen der betroffenen Angehörigen gerade unter Pietätsgesichtspunkten ein besonders hoher Stellenwert zu, der eine Videobeobachtung bzw. -aufzeichnung an Gräbern und Gedenkstätten - innerhalb der Öffnungszeiten - in der Regel nicht rechtfertigt. Zudem war zu berücksichtigen, dass die erwähnten Diebstähle sich nicht tagsüber, sondern zur Nachtzeit ereigneten, also in einem Zeitraum, in dem sich keine Besucher/innen auf dem Friedhof befinden.

Da sich außerhalb der Öffnungszeiten keine (legalen) Besucherinnen und Besucher auf dem Friedhof aufhalten, deren schutzwürdige Interessen von der Videoüberwachung berührt sein könnten, bestehen insofern grundsätzlich keine datenschutzrechtlichen Bedenken gegen eine auf diesen Zeitraum beschränkte Videoüberwachung.

Die verantwortliche Stelle hat auf unsere Beratung hin von der (auch während der Öffnungszeiten geplanten) Videoüberwachungsmaßnahme zunächst Abstand genommen und prüft derzeit Sicherungsmaßnahmen in Verbindung mit polizeilichen Stellen.

5.2.5 Durchfahrtskontrolle per Blitzsäule

Im Innenstadtbereich der Stadt Schwerin war seitens der Stadt die Installation einer stationären Verkehrs-Überwachungsanlage beabsichtigt. Es handelte sich dabei weder um eine Rotlicht- noch um eine Geschwindigkeitsüberwachungseinrichtung, sondern um ein Durchfahrtskontrollsystem kombiniert mit einem Kennzeichenlesegerät. Überwacht werden sollte die unberechtigte Durchfahrt von Kraftfahrzeugen Bereich eines zentralen Platzes in der Fußgängerzone, der insbesondere von Straßenbahnen und Nahverkehrsbussen stark frequentiert wird.

Das System sollte in Verbindung mit einem Kennzeichenlesesystem arbeiten. Hierbei wird zunächst das Kennzeichen gelesen, um es dann mit einer Liste („whitelist“) der durchfahrtberechtigten Fahrzeuge (Nahverkehr, Krankenwagen, Einsatzfahrzeuge der Feuerwehr/der Polizei etc.) abzugleichen. Nur dann, wenn das betreffende Kennzeichen nicht in der Liste steht, wird die Kamera mit Blitz ausgelöst. Insofern sollte sichergestellt werden, dass nur bei einem Anfangsverdacht „geblitzt“ wird.

Wir haben das Projekt mit Vertretern der Stadt Schwerin erörtert. Aus der Besprechung ergab sich, dass die Straßen, die den Platz queren, von Einsatzfahrzeugen sowohl der Polizei als auch der Feuerwehr häufig im Notfalleinsatz benutzt werden. Zudem fahren in diesem Bereich Straßenbahnen und Busse des öffentlichen Nahverkehrs im Minutentakt. Obwohl der zu überwachende Bereich als Fußgängerzone gewidmet ist, hatten Zählungen der Stadt Schwerin zudem eine hohe Anzahl von unberechtigten Fahrten durch diese Zone ergeben, die auch zu zahlreichen Unfällen führten. Man habe alternative Maßnahmen (Schranken, versenkbare Poller, Stichprobenkontrollen durch die Polizei etc.) geprüft und auch mit der Polizei erörtert. Diese Alternativlösungen seien jedoch nach Erörterung mit der Polizei - insbesondere wegen der regelmäßig notwendigen Durchfahrten von Fahrzeugen der Feuerwehr und der Polizei sowie Krankenwagen im Notfalleinsatz - in der Praxis nicht realisierbar gewesen. Beabsichtigt war daher die Installation von zwei Geräten zur stationären Überwachung der durchfahrenden Kraftfahrzeuge in Verbindung mit dem Kennzeichenlesesystem. Dabei löst das System eine Aufnahme aus, falls es sich (nach Abgleich mit der „whitelist“) um eine unberechtigte Durchfahrt handelt. Die Aufnahmen sollten durch das Ordnungsamt an die Bußgeldstelle weiterleitet werden, die dann ein Ordnungswidrigkeitsverfahren einleitet. Das System sollte auf der Rechtsgrundlage gemäß § 100h Abs. 1 Nr. 1 Satz 1 StPO i. V. m. § 46 Abs. 1 OWiG betrieben werden.

Wir haben hierzu auf den Beschluss des OLG Stuttgart vom 29. Januar 2010 (AZ: IV Ss 1525/09) zur Videoüberwachung im fließenden Straßenverkehr hingewiesen. Danach ist eine Videoaufnahme des fließenden Verkehrs zur Feststellung und Beweissicherung bei Verkehrsverstößen nicht zu beanstanden, sofern personenbezogene Aufnahmen nur im Verdachtsfall ausgelöst werden (verdachtsabhängige Überwachung). Gleiches gilt für fotografische Einzelaufnahmen. Eine verdachtsabhängige Überwachung liegt vor, wenn die Feststellung des Verkehrsverstoßes und dessen Beweissicherung, zum Beispiel durch Fotoaufnahme, nach Begehen der Ordnungswidrigkeit - im vorliegenden Falle nach dem Passieren eines Verbotszeichen - erfolgt. Dadurch, dass die Aufnahme erst nach Abgleich mit der„whitelist“ erfolgt, konnte unseres Erachtens in Analogie zu der genannten Entscheidung des OLG Stuttgart davon ausgegangen werden, dass die Erfassung der Kennzeichen nur in konkreten Verdachtsfällen erfolgt - wobei diese Verdachtsfälle dann identisch sind mit allen nicht in der „whitelist“ gespeicherten Kennzeichen.

Ferner war erforderlich, dass keine Daten von Nichtbetroffenen (Besitzer einer Ausnahmegenehmigung) erfasst werden (§ 100h Abs. 2, 3 StPO) oder - falls sie zum Zwecke des Kennzeichenabgleichs technisch notwendigerweise erfasst werden müssen - nicht gespeichert bzw. unverzüglich nach dem Kennzeichenabgleich unwiederbringlich zu löschen sind. Eine Datenspeicherung darf somit ausschließlich die personenbezogenen Daten von Betroffenen (Nicht-Durchfahrtsberechtigten) umfassen.

Wir haben deshalb darauf hingewiesen, dass es zwingend erforderlich ist, die vorgesehene „whitelist“ laufend so aktuell zu halten, dass es nicht (oder nur ausnahmsweise) zu einer Fehlerfassung von durchfahrtsberechtigten Betroffenen kommt. Dies wurde uns seitens der Stadt Schwerin zugesichert. Zusätzlich sollen die Kennzeichenbilder aus den Geräten durch Mitarbeiter/innen des Ordnungsamtes vor Weitergabe an die Bußgeldstelle nochmals mit der „whitelist“ abgeglichen werden.

Zu berücksichtigen war auch, dass es sich rein technisch um ein System handelt, dessen Funktionsweise den Kennzeichenlesesystemen ähnelt, die die Polizei zu Fahndungszwecken (aufgrund des Sicherheits- und Ordnungsgesetzes - SOG M-V) benutzt. Im vorliegenden Fall handelte es sich allerdings nicht um eine „blacklist“ (Fahndungsdatei), sondern um eine „whitelist“ (der Personen mit Durchfahrtserlaubnis). Wegen der technisch vergleichbaren Funktionsweise haben wir darauf hingewiesen, dass ein solches System ausschließlich zu den genannten Zwecken eingesetzt werden darf. Eine Verknüpfung mit anderen (z. B. Fahndungs-) Zwecken ist rechtlich und technisch auszuschließen.

Unter Einhaltung der genannten Voraussetzungen haben wir das System auf der Rechtsgrundlage des § 100h Abs. 1 Satz 1 Nr. 1 StPO i. V. m. § 46 OWiG als datenschutzrechtlich vertretbar bewertet.

5.2.6 Videoüberwachung an der Wiecker Klappbrücke

Der Oberbürgermeister der Universitäts- und Hansestadt Greifswald hat uns die „Anordnung über die Installation einer Bildaufzeichnungsanlage an der Klappbrücke in Greifswald-Wieck“ mit der Bitte um Kenntnisnahme nach § 32 Abs. 3 Sicherheits- und Ordnungsgesetz (SOG M-V) übersandt. Begründet wurde die Anordnung damit, dass Straftatbestände gegeben seien, und zwar Verkehrsgefährdung, Sachbeschädigung öffentlichen Eigentums und Gewässerverschmutzung.

Zum Hintergrund: Die Klappbrücke in Greifswald-Wieck ist nach ihrer Teileinziehung im Jahre 1998 als Fuß- und Radweg gewidmet. Ausnahmen zur Befahrung mit Kraftfahrzeugen regelt die jeweils gültige Satzung über die Sondernutzung an öffentlichen Straßen, Wegen und Plätzen der Universitäts- und Hansestadt Greifswald. Im Zusammenhang mit der Neuerrichtung des Zugangskontrollsystems an der Klappbrücke im August 2011 wurde versucht, die missbräuchliche Benutzung der Brücke durch „Hinterherfahren“ einzuschränken. Aufgrund der technischen Ausgestaltung des Pollers kam es hierbei zu zahlreichen Beschädigungen sowohl des Pollers als auch diverser Kraftfahrzeuge.

Wir haben dem Oberbürgermeister mitgeteilt, dass wir die Rechtslage wie folgt beurteilen: Aus datenschutzrechtlicher Sicht ist nicht überzeugend dargelegt, dass an der Wiecker Klappbrücke wiederholt Straftaten begangen wurden, die eine Bildaufzeichnung im Sinne des § 32 SOG M-V rechtfertigen und die von der Gewichtung her einen Kriminalitätsbrennpunkt darstellen würden. Diese sogenannten Kriminalitätsbrennpunkte sind aufgrund von objektiv nachvollziehbaren ortsbezogenen Lageerkenntnissen zu ermitteln, vgl. hierzu Gesetzesbegründung zur Drucksache 4/2116 vom 22. Februar 2006, Seite 21. Solche Lageerkenntnisse, die von der Polizei festzustellen sind, sind uns nicht bekannt. Bei der von der Universitäts- und Hansestadt Greifswald angeführten Leistungserschleichung (§ 265a StGB) handelt es sich um ein Bagatelldelikt. Auch ist nicht dargelegt, dass bei unberechtigten Durchfahrten ein gefährlicher Eingriff in den Straßenverkehr vorliegt (§ 315b StGB). Ebenso wenig ist zu erkennen, dass der Tatbestand der Sachbeschädigung vorliegt, denn dieser setzt Vorsatz voraus. Tatsächlich verhält es sich ja so, dass jeder, der mit seinem Fahrzeug die Brücke überquert, darauf vertraut, dass weder der Poller noch das eigene Fahrzeug beschädigt wird. Niemand würde derart kostspielige Schäden sowohl am eigenen Eigentum als auch an öffentlichem Eigentum in Kauf nehmen, nur um kostenlos die Brücke zu passieren. Insofern liegt kein Vorsatz vor, der jedoch zwingende Voraussetzung für den Tatbestand der Sachbeschädigung ist.

Inzwischen wurde die Videoüberwachungsfunktion deaktiviert. Testweise wurde dann ein Verfahren eingeführt, wonach Kfz-Kennzeichen und Personen verpixelt werden sollten und erst dann, wenn es zu einem Schadenfall kommt, der betreffende Fall entpixelt werden soll. Die entsprechenden Unterlagen wurden uns übersandt. Die entscheidende Frage ist, ob der betreffende Vorgang datenschutzrechtlich als Videoaufzeichnung zu bewerten ist. Es stellte sich heraus, dass die personenbezogenen Daten zwar zunächst verpixelt werden, aber letztendlich doch gespeichert werden. Eine Speicherung ist jedoch gemäß § 32 Abs. 3 SOG M-V nicht erlaubt. Da für die Bürgerinnen und Bürger nicht erkennbar ist, ob aufgezeichnet wird oder nicht, hatten wir von der Stadt Greifswald gefordert, die Videoüberwachungsanlage abzubauen.

Daraufhin hat uns der Oberbürgermeister nochmals ausführlich dargelegt, dass seiner Meinung nach doch ein Kriminalitätsbrennpunkt vorliegt und hat eine umfangreiche Liste der Unfälle mit Pollerschäden beigefügt. Das Innenministerium, welches als oberste Fachaufsichtsbehörde eingeschaltet wurde, vertrat im Wesentlichen die gleiche Auffassung. Es führte im Einzelnen aus, dass die Stadt Greifswald hinreichend Umstände vorgetragen habe, die „die Annahme der Verwirklichung von Straftaten belegen und die, wegen der Serie, auch künftig das Begehen von Straftaten erwarten lassen. Die Einlegung von Strafanträgen ist keine Voraussetzung für die Anwendung von § 32 Abs. 3 Satz 2 SOG“.

Diese Auffassung ist jedoch, wie bereits eingangs dargestellt, nicht richtig. Es sind keine polizeilichen Lageerkenntnisse, Statistiken oder sonstige Unterlagen seitens der Polizei beigebracht worden, wie dies bei anderen Anordnungen nach § 32 Abs. 3 SOG M-V regelmäßig der Fall war. Lediglich eine Beurteilung der Stadt, dass eine Häufung von Straftaten vorliege, reicht nicht aus. Zurzeit ist die Videoüberwachungsanlage abgeschaltet, wie uns die Stadt Greifswald versicherte.

Wir werden der Auffassung des Innenministers in einem gesonderten Schreiben nochmals entgegentreten.

5.2.7 Arztpraxis mit Ausblick – Webcam in Schwerin

Webcams erfreuen sich immer größerer Beliebtheit. Sie dienen in den meisten Fällen den Nutzerinnen und Nutzern dazu, sich einen Überblick über die Landschaft und das Wetter zu verschaffen. So auch bei einer Arztpraxis in Schwerin, die ihren Patientinnen und Patienten, aber auch anderen Interessierten, mit ihrer Webcam einen Überblick über das ehemalige Bundesgartenschau-Gelände geben wollte. Neben dem Schweriner Schloss, dem Schlossgarten und dem Burgsee waren allerdings auch Personen zu erkennen. Dass das äußerst problematisch ist, war dem Arzt nicht bewusst.

Wir informierten den Arzt darüber, dass es durch die Abbildung von erkennbaren Personen zu erheblichen Persönlichkeitsverletzungen kommen kann, da die Übertragung der Bilder ins Internet in aller Regel nicht mehr rückgängig gemacht werden kann. Die einfachen technischen Möglichkeiten der Vervielfältigung und Bearbeitung der Aufnahmen verstärkt dieses Problem noch. Darüber hinaus kann eine solche Veröffentlichung von Bildnissen von Personen nach dem Kunsturheberrechtsgesetz (KunstUrhG) strafrechtliche Konsequenzen haben. Das kommt insbesondere dann in Betracht, wenn die abgebildete Person in diese Veröffentlichung nicht eingewilligt hat und eine Verletzung des Rechts am eigenen Bild vorliegt. Sind demgegenüber auf den aufgenommenen Bildern, etwa aufgrund Kamerapositionierung, fehlender Zoom-Möglichkeiten oder niedriger Auflösung, Personen oder Kfz-Kennzeichen nicht zu erkennen, kann der Einsatz der Webcam aus datenschutzrechtlicher Sicht als grundsätzlich unbedenklich eingestuft werden.

Der Arzt veranlasste kurzfristig die Umstellung seiner Kamera, sodass Personen nicht mehr erkennbar waren und die Webcam als datenschutzrechtlich unbedenklich bewertet werden konnte. Sie zeigt nun die Wetterlage über dem Schweriner Schloss, dem Schlossgarten und dem Burgsee, ohne dass Personen zu identifizieren sind.

5.2.8 Videoüberwachung von Bäckereifilialen

Von einem großen Bäckereiunternehmen wurde ein komplexes Videoüberwachungssystem betrieben, durch das von der Zentrale aus eine Überwachung von über 90 Bäckereifilialen des Unternehmens stattfand. Dabei wurden sowohl Tische und Sitzbereiche und damit die Kundinnen und Kunden der Filialen überwacht als auch die Angestellten während ihrer gesamten Arbeitszeit.

Wir haben das Unternehmen mehrfach, sowohl schriftlich als auch in Gesprächen und bei einem Kontrollbesuch, auf die datenschutzrechtliche Unzulässigkeit hingewiesen und gleichzeitig Empfehlungen für ein datenschutzgerechtes Betreiben der Videoanlage gegeben. Trotz mehrfacher Aufforderungen hat das Unternehmen eine Änderung des Videosystems entsprechend unseren Empfehlungen mit den verschiedensten Gründen abgelehnt. So wurde etwa über eine beauftragte Rechtsanwaltskanzlei wiederholt die Besorgnis mitgeteilt, Opfer von Überfällen zu werden, wenn die Videoüberwachungsanlage in ihren Funktionen eingeschränkt werde. Der Leiter des Unternehmens informierte ferner während unseres Kontrollbesuchs unter anderem darüber, dass es bis zum Zeitpunkt des Kontrollbesuches ca. 40 Einbrüche in Bäckereifilialen des Unternehmens gegeben habe.

Auf Nachfrage räumte er jedoch ein, dass diese Einbrüche bisher nicht tagsüber, sondern nachts stattfanden. Demgegenüber war es tagsüber trotz der Vielzahl der Filialen lediglich zu zwei Vorfällen gekommen. Nachts wiederum bestehen aus datenschutzrechtlichen Gründen keine Bedenken gegen eine Videoüberwachung, da die Gefahr einer Überwachung der Kundinnen und Kunden sowie der Angestellten naturgemäß lediglich während der Öffnungszeiten besteht.

Obwohl sich das weitere Verfahren und der Schriftwechsel mit der von dem Unternehmen beauftragten Rechtsanwaltskanzlei sehr langwierig gestalteten, konnten wir im Ergebnis erreichen, dass das Unternehmen die Videoüberwachung seiner Filialen nunmehr datenschutzgerecht betreibt.

Die ursprünglich mitüberwachten Ruhebereiche der Gäste der Bäckereifilialen sind ausgeblendet - ebenso größere Teile des Arbeitsbereiches des Personals, sodass die Angestellten nicht mehr während ihrer gesamten Arbeitszeit überwacht werden. Insbesondere findet nunmehr keine „Live“-Beobachtung mehr statt, sondern lediglich eine Aufzeichnung im Black-Box-Verfahren, wobei der Zugriff auf die Bilder nur bei konkreten Vorfällen und nur unter Wahrung des Vier-Augen-Prinzips und unter Einbeziehung des betrieblichen Datenschutzbeauftragten erfolgt.

5.2.9 Luftbildaufnahmen mit Hintergrund

Ein Unternehmen hatte sich wegen der datenschutzrechtlichen Beurteilung eines Luftbildprojektes an uns gewandt. Ziel des Projektes sei es, auf der Basis einer aktuellen hochauflösenden Luftbildkarte von Mecklenburg-Vorpommern behinderten Mitbürgerinnen und Mitbürgern in elektronischer Form (ggf. mit Ortungsfunktion) Hilfestellung zu geben. Geplant sei in diesem Zusammenhang eine komplette Neubefliegung für das Land Mecklenburg-Vorpommern.

Der Vertreter des Unternehmens, der auch für eine große Entwicklungs- und Beteiligungsgesellschaft firmiert, informierte darüber, dass es sich bei dieser Gesellschaft um eine Holding einer Unternehmensgruppe handele. Von dieser Unternehmensgruppe seien ca. 90 % aller Geodaten geliefert worden, die von Google für Deutschland verwendet werden. Demgegenüber sei sein Unternehmen unter dem Aspekt Gemeinnützigkeit separat gegründet worden. Man plane eine integrierte Datenbank mit entsprechenden Informationen für behinderte Mitbürgerinnen und Mitbürger. In die integrierte Datenbank könnten unter Umständen später auch medizinische Daten aufgenommen werden. Ferner gebe es Überlegungen für ein sogenanntes „passives Tracking“ (Ortung von behinderten Menschen über GPS).

Wir haben in diesem Zusammenhang insbesondere darauf hingewiesen, dass eine passive Ortung nur mit schriftlicher Einwilligung der Betroffenen zulässig ist (bei geistig-seelischer Behinderung ggf. durch die Betreuerin/den Betreuer). Für den Fall der zusätzlichen Aufnahme medizinischer Daten gelten widerum besondere Voraussetzungen (u. a. hinsichtlich der Verschlüsselung der Daten). Ferner muss insbesondere die Gefahr einer Profilbildung ausgeschlossen werden können.

Das Unternehmen informierte ferner darüber, dass Kameraaufnahmen im Format 10cm-Auflösung pro Pixel beabsichtigt seien. Wir haben darauf hingewiesen, dass bei einer derart hohen Auflösung die Gefahr sehr wahrscheinlich ist, dass personenbezogene Einzeldaten von Betroffenen erfasst und deren schutzwürdige Interessen nach dem Landesdatenschutzgesetz Mecklenburg-Vorpommern bzw. dem Geoinformations- und Vermessungsgesetz Mecklenburg-Vorpommern oder dem Bundesdatenschutzgesetz verletzt werden, was zur Unzulässigkeit nach den jeweiligen Gesetzen führen würde.

Zudem ergab sich aus dem zur Prüfung übersandten Material, dass eine Nutzung der hochauflösenden Luftbildaufnahmen nicht nur zum Zweck der Unterstützung von behinderten Menschen, sondern auch zu anderen Zwecken geplant war (u. a. für Einsatzentscheidungen von Behörden und Organisationen mit Sicherheitsaufgaben, für die Aktualisierung von Katasterplänen, Verkehrsplanungen und für Tourismusanwendungen). Wir haben hierbei darauf hingewiesen, dass insbesondere die Datenerhebungs- und Verarbeitungszwecke sauber zu trennen sind und die Zulässigkeit jeweils nach den oben genannten Rechtsgrundlagen zu prüfen ist.

Der Vertreter des Unternehmens wies darauf hin, dass die datenverantwortliche Stelle nicht sein Unternehmen sei, sondern dieses vielmehr vom Wirtschaftsministerium Mecklenburg-Vorpommern beauftragt worden sei. Auch der geplante Befliegungsauftrag werde ggf. seitens des Ministeriums erteilt werden. Ferner gebe es eine sogenannte „Private Public Partnership“ mit dem oben genannten Unternehmen, das Geodaten für Deutschland an Google geliefert hatte. Dieses Unternehmen plane, die entstandenen hochauflösenden Luftaufnahmen für „andere wirtschaftliche Verwendungen“ (z. B. Deutsche Bahn etc.) zu verarbeiten und zu nutzen.

Wir haben darauf hingewiesen, dass es sich in diesem Falle um eine Datenverarbeitung im Auftrag nach § 4 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) handelt und sowohl die Zulässigkeit der Erhebung solcher Luftbildaufnahmen als auch die Frage der Weitergabe an private Unternehmer und andere öffentliche Stellen nach dem Geoinformations- und Vermessungsgesetz Mecklenburg-Vorpommern zu beurteilen ist.

Insbesondere haben wir im Rahmen der Nutzung zum Zweck der Unterstützung von behinderten Menschen auf gleich (oder besser) geeignete datenschutzgerechte Alternativen zu hochauflösenden Luftbildaufnahmen hingewiesen. Denkbar ist beispielsweise eine digitale Karte mit eingeblendeten näheren Informationen zu den jeweiligen „points of Interest“ - analog den Punkt-Informationen bei Google Maps. Für behinderte Menschen wichtig wäre zum Beispiel die Information, dass in einem bestimmten Hotel eine Rollstuhlrampe vorhanden ist oder dass das gewählte Restaurant über eine behindertengerechte (barrierefreie) Ausstattung verfügt. Auch die Ergänzung entsprechender Fotos ist in Absprache mit dem Betreiber denkbar.

Wir haben das Wirtschaftsministerium Mecklenburg-Vorpommern sowohl über die noch erforderliche Klärung der genannten datenschutzrechtlichen Voraussetzungen informiert als auch die Frage aufgeworfen, ob derartige hochauflösende Luftbilder überhaupt geeignet sind, um die mit dem Projekt erwünschten Hilfestellungen leisten zu können (beispielsweise Kenntlichmachung von Rampen oder behindertengerechten Ampeln). Von der Eignung der Daten für den beabsichtigten Zweck hängen die Erforderlichkeit und schließlich auch die Zulässigkeit der Übermittlung der Daten ab. Das Projekt ist nach unserer Kenntnis nicht weiter verfolgt worden.

6 Datenschutz in verschiedenen Rechtsgebieten

6.1 Rechtswesen

6.1.1 Auskunftsverfahren bei der Staatsanwaltschaft

Das Verfahren zur Auskunftserteilung bei Staatsanwaltschaften in den einzelnen Bundesländern ist häufig unterschiedlich. Nach § 491 Strafprozessordnung (StPO) ist dem Betroffenen auf Antrag Auskunft über die in Dateien gespeicherten Daten nach Maßgabe des § 19 Bundesdatenschutzgesetz (BDSG) zu erteilen. Nach § 19 BDSG ist Auskunft zu erteilen über die zur Person des Betroffenen gespeicherten Daten. Damit sind grundsätzlich alle zur Person gespeicherten Daten gemeint.

In der Praxis ist es so, dass der Betroffene häufig nur eine sehr knapp gehaltene Auskunft erhält (hauptsächlich bestehend aus den Verfahrensdaten, das heißt Aktenzeichen, Deliktsbezeichnung, Tatzeit, Entscheidung). Diese genügt den gesetzlichen Anforderungen nicht. Häufig wird für die Erteilung von Auskünften an die Betroffenen die sogenannte Mehrländer-Staatsanwaltschafts-Automation-Vorgangsliste (MESTA-Vorgangsliste) genutzt. Diese dient eigentlich dazu, den zuständigen Dezernenten über weitere in MESTA erfasste Verfahren mit Beteiligung eines Beschuldigten zu informieren.

Ob hingegen eine Vollauskunft aus staatsanwaltschaftlichen Dateien für die Betroffenen zielführend ist, darf bezweifelt werden. Solche Dateien enthalten in der Regel mehrere hundert Datenfelder, von denen zahlreiche Datenfelder lediglich interne Informationen zum Verfahrensablauf enthalten.

Der Generalstaatsanwalt des Landes Schleswig-Holstein hatte die Initiative ergriffen und dem dortigen Datenschutzbeauftragten einen Vorschlag unterbreitet, der - mit einigen Ergänzungen - den für den Betroffenen wesentlichen Datenbestand abbildet. Aus Sicht der Datenschutzbeauftragten wären zu ergänzen zumindest Angaben zur Staatsangehörigkeit, zum Aufenthalt in einer Justizvollzugsanstalt (JVA), zum Vollstreckungsverfahren, zur Aberkennung der Bürgerrechte, zu den Weisungen bei Strafaussetzung zur Bewährung (falls nicht bereits im Tenor der Entscheidung enthalten), zu Zahlungsdaten bei Geldstrafe, zu Gnadenverfahren, zu Ordnungsgeld und -haft sowie zur Erzwingungshaft.

Wir hatten unseren Generalstaatsanwalt angeschrieben und angefragt, ob er - zwecks Vereinheitlichung auf Bundesebene - mit dem Vorschlag des Generalstaatsanwalts von Schleswig-Holstein übereinstimmt. Der Generalstaatsanwalt hat erklärt, dass er unsere Anfrage zum Anlass nehmen wird, innerhalb des MESTA-Verbundes auf der Grundlage des Vorschlags eine einheitliche Regelung über den Auskunftsumfang zu erzielen, die sodann für die Staatsanwaltschaften in Mecklenburg-Vorpommern für verbindlich erklärt werden könne.
Der Generalstaatsanwalt des Landes Schleswig-Holstein hatte daraufhin erneut einen konkreten Entwurf einer MESTA-Auskunft und einer internen Handlungsanweisung erstellt; beide Entwürfe wurden akzeptiert. Aus datenschutzrechtlicher Sicht ist dies ein gutes Beispiel für eine koordinierte Zusammenarbeit auf Länderebene.

6.1.2 Anspruch auf Informationen zur Durchsetzung von Rehabilitierungsansprüchen

Die Landesbeauftragte für Mecklenburg-Vorpommern für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR bat uns um Unterstützung bei einer Frage, die sich mit der Übermittlung personenbezogener Daten zur Durchsetzung von Rehabilitierungsansprüchen ehemaliger DDR-Heimkinder beschäftigte. Dabei ging es insbesondere darum, dass die Betroffenen den Staatsanwaltschaften, an die diese Anträge zu richten sind, die für die Entscheidung erforderlichen Unterlagen vorlegen müssen.

Um im Einzelfall zu einem gerechten Urteil zu gelangen, ist eine genaue Betrachtung der Unterlagen erforderlich. Um dieses gewährleisten zu können, sind die Betroffenen insbesondere auf Informationen aus Akten der DDR-Jugendhilfe angewiesen. Die Behörden, die über diese Unterlagen verfügen (vor allem Jugendämter), sollen aber manchmal die Anträge auf Akteneinsicht unter Hinweis auf hierin enthaltene personenbezogene Daten von Mitarbeitern oder Beteiligten an DDR-Verfahren und deren Schutzwürdigkeit abgelehnt haben.

Die Auskunftsrechte für die Betroffenen ergeben sich aus den §§ 24 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) und 83 Sozialgesetzbuch Zehntes Buch (SGB X). Diese Auskunftsrechte gewähren neben den Daten zur eigenen Person auch einen Zugang zu Informationen über ehemalige Erzieherinnen und Erzieher oder Angestellte von Kinderheimen und Jugendwerkhöfen (Funktionsträgerdaten), da bei einer datenschutzrechtlichen Abwägung das Interesse eines Funktionsträgers an der Geheimhaltung hinter das Informationsinteresse der Betroffenen zurücktritt. Etwas anderes gilt hinsichtlich des Zugangs zu personenbezogenen Daten ehemaliger anderer Heimkinder, die geheimhaltungswürdig und in den betreffenden Unterlagen unkenntlich zu machen sind.

Des Weiteren war bei der Bewertung des Sachverhaltes aber auch noch folgender besonderer Umstand zu beachten:

Die Entscheidung, ob ein Kind/Jugendlicher in ein Spezialheim eingewiesen wird, wurde durch einen sogenannten Jugendhilfeausschuss getroffen. Dieses Gremium setzte sich sowohl aus hauptamtlich Tätigen (Funktionsträger) als auch aus weiteren Beteiligten zusammen. Als weitere Beteiligte traten beispielsweise Vertreter des elterlichen Betriebes, Lehrer und Mitarbeiter der Staatssicherheit in Erscheinung.

Auch bei diesem Personenkreis handelt es sich um Funktionsträger, da die weiteren Beteiligten freiwillig (ehrenamtlich) in diesen Jugendhilfeausschüssen mitgewirkt haben. Hinzu kommt noch, dass diese Personen erforderliche Verfahrensbeteiligte waren, ohne die die Beratung über die weitere Entscheidung der Heimunterbringung nicht hätte getroffen werden können.

Im Ergebnis sind wir auch hier zu der Einschätzung gekommen, dass das Informationsinteresse der betreffenden Heimkinder gegenüber dem Geheimhaltungsinteresse dieser weiteren Beteiligten überwiegt, sodass auch diese personenbezogenen Daten offenbart werden dürfen. Eine parallel mit den Landesdatenschutzbeauftragten aus Berlin und Thüringen durchgeführte Abstimmung hat die hiesige datenschutzrechtliche Bewertung bestätigt.

6.1.3 Anonymisierung von Gerichtsentscheidungen

Ein Rechtsanwalt hat sich darüber beschwert, dass bei Beck-online ein Urteil des Oberverwaltungsgerichts Mecklenburg-Vorpommern (OVG M-V) abgedruckt ist, welches eine Hilfeempfängerin mit vollem Namen nennt. Der Anwalt vermutete, dass möglicherweise seitens der Justizbehörden nicht - wie es sonst üblich ist - korrekt anonymisiert worden ist und eine nicht korrekte Fassung an Beck-online weitergegeben worden ist.

Wir haben daraufhin das OVG M-V um Stellungnahme gebeten und ergänzend darauf hingewiesen, dass zu überprüfen wäre, ob die Betroffene gemäß § 23 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) zu benachrichtigen ist.

Das OVG M-V hat mitgeteilt, dass eine nicht anonymisierte Ausfertigung des Urteils elektronisch an Beck-online übermittelt wurde, obwohl eine anonymisierte elektronische Fassung des Urteils hergestellt und autorisiert worden war. Warum im Verlauf der Erledigung der Veröffentlichungsverfügung diese anonymisierte elektronische Fassung durch eine nicht anonymisierte Fassung ersetzt wurde, lässt sich nicht mehr nachvollziehen. Im konkreten Einzelfall ist Beck-online gebeten worden, die nicht anonymisierte Fassung durch die anonymisierte Fassung zu ersetzen. Damit derartiges in Zukunft nicht wieder passiert, wurde seitens des OVG M-V die Anweisung erteilt, ab sofort vor Versendung der Dateien zwecks Veröffentlichung diese daraufhin zu überprüfen, dass es sich um die tatsächlich anonymisierte Fassung der Entscheidung handelt.

Des Weiteren war eine Benachrichtigung der betroffenen Hilfeempfängerin gemäß § 23 DSG M-V zu prüfen. Danach hat die datenverarbeitende Stelle einen Betroffenen unverzüglich zu benachrichtigen, wenn sie Grund zu der Annahme oder Kenntnis hat, dass unrichtige, unzulässig erhobene oder unzulässig gespeicherte Daten in der Weise genutzt wurden, dass dem Betroffenen durch den dortigen Umgang mit seinen Daten ein Nachteil zu entstehen droht oder bereits entstanden ist. Die Hilfeempfängerin stand ungefähr ein Jahr mit vollem Namen und Adresse unter Angabe diverser psychischer Erkrankungen, mithin äußerst sensibler personenbezogener Daten, im Internet und war dadurch durch einen unbegrenzt großen Empfängerkreis abrufbar. Aus datenschutzrechtlicher Sicht stellt dies einen Nachteil dar, und zwar einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung, der auch bereits eingetreten ist.

Es liegt daher auch im Interesse der datenverarbeitenden Stelle, die Betroffene zu benachrichtigen, um eine mögliche, die öffentliche Stelle selbst treffende Schadensersatzpflicht nach § 27 DSG M-V zu begrenzen oder von vornherein zu vermeiden. Das OVG M-V hat die Sach- und Rechtslage geprüft und hat die Betroffene schriftlich von der Angelegenheit unterrichtet.

6.2 Polizei - Straßenbahnkontrolleure als „Fahnder“

Aus den Medien haben wir erfahren, dass Polizeibeamte der Polizeiinspektion Rostock Tabellen mit Daten von 20 Männern und Frauen aus dem Raum Rostock an Kontrolleure der Rostocker Straßenbahn AG (RSAG) weitergegeben haben sollen, verbunden mit der Bitte um Benachrichtigung, falls die mit Haftbefehl Gesuchten angetroffen werden.

Daraufhin haben wir das Polizeipräsidium Rostock um Stellungnahme gebeten und insbesondere nachgefragt, auf welcher Rechtsgrundlage die Übermittlung personenbezogener Daten erfolgte, aus welchen polizeilichen Dateien die Daten stammten und um welche personenbezogenen Daten es sich im Einzelnen handelte. Des Weiteren war aus datenschutzrechtlicher Sicht von Interesse, ob auch Lichtbilder der betroffenen Personen übermittelt wurden und ob eine mögliche Korrelation zwischen mit Haftbefehl Gesuchten und Schwarzfahrern gesehen wurde.

Die Polizei teilte mit, dass die handelnden Polizeibeamten in Verkennung der Rechtslage von der Zulässigkeit der Übermittlung personenbezogener Daten an die RSAG ausgingen. Nach dem Bekanntwerden dieses Vorgangs sei diese Verfahrensweise von den Vorgesetzten der Polizeibeamten dauerhaft unterbunden worden. Die personenbezogenen Daten seien sowohl aus den bestehenden Einträgen im Elektronischen Vorgangsassistenten der Landespolizei (EVA) und dem Informationssystem der Polizei (INPOL) als auch aus den vorliegenden Haftbefehlen entnommen worden. Die übermittelten Datensätze bestanden jeweils aus Nachnamen, Vornamen, Geburtsdatum und Geburtsort. Lichtbilder wurden nicht übermittelt. Es wurde eine Verbindung zwischen den mit Haftbefehl gesuchten Personen und den Fahrgästen, welche ohne gültigen Fahrschein fuhren, gesehen, weil bereits gegen einen nicht unerheblichen Teil der gesuchten Personen strafrechtliche Ermittlungsverfahren unter anderem wegen des Erschleichens von Leistungen geführt worden seien. Insofern sei es nicht unwahrscheinlich gewesen anzunehmen, dass diese Personen wiederholt auffällig werden könnten. Die Maßnahme stellte keinen Einzelfall dar, sondern wurde mehrfach lediglich in der Polizeiinspektion Rostock durchgeführt. Es wurden zu unterschiedlichen Zeiten jeweils neue Datensätze übermittelt und nicht mehr aktuelle für erledigt erklärt.

Die Rostocker Straßenbahn AG hat abschließend mitgeteilt, dass die gespeicherten personenbezogenen Daten unmittelbar mit Beginn der polizeilichen Untersuchung nach Bekanntwerden des Sachverhaltes gelöscht wurden.

Da die Polizei sehr schnell eingesehen hat, dass es keine Rechtsgrundlage für eine derartige Datenübermittlung gab, und die personenbezogenen Daten bei der RSAG sofort gelöscht wurden, haben wir von einer förmlichen Beanstandung abgesehen.

6.3 Verfassungsschutz

6.3.1 Umsetzung des Urteils des Bundesverfassungsgerichtes zum Antiterrordateigesetz

Mit dem Urteil vom 24. April 2013 hat das Bundesverfassungsgericht (BVerfG) entschieden, dass verschiedene Vorschriften des Antiterrordateigesetzes mit dem Grundgesetz unvereinbar sind. Gleichzeitig hat das Gericht dem Gesetzgeber eine Übergangsfrist zur Neuregelung gesetzt und festgelegt, dass die Vorschriften bis dahin nur mit folgender Maßgabe angewendet werden dürfen:

„Als Voraussetzung für eine vorübergehende weitere Anwendbarkeit ist allerdings zuvor die Zugriffsmöglichkeit auf Daten von Kontaktpersonen gemäß § 2 Satz 1 Nr. 3 Antiterrordateigesetz (ATDG) auszuschließen sowie sicherzustellen, dass bei Recherchen in den erweiterten Grunddaten und in Daten, die aus Eingriffen in das Telekommunikationsgeheimnis und das Grundrecht auf Unverletzlichkeit der Wohnung herrühren, im Trefferfall allein ein Zugang zu Informationen gemäß § 3 Absatz 1 Nr. 3 ATDG, nicht aber zu Informationen gemäß § 3 Abs. 1 Nr. 1a ATDG <Grunddaten zur Person> gewährt wird.“

Dies gilt ab Urteilsverkündung. Ausnahmen hiervon hat das Bundesverfassungsgericht für Eilfälle zugestanden, solange die genannten Voraussetzungen noch nicht sichergestellt sind.

Nach unserer Auffassung ist aus diesen Fortgeltungsbedingungen für die an der Antiterrordatei (ATD) beteiligten Landeskriminalämter und Verfassungsschutzbehörden abzuleiten, dass sie Daten zu Kontaktpersonen i. S. d. § 2 Satz 1 Nr. 3 ATDG ab sofort nicht mehr in der ATD speichern dürfen. Denn wenn der Zugriff auf sie insgesamt auszuschließen ist, ist ihre Speicherung nicht erforderlich und damit nicht zulässig.

Für Daten, die durch Eingriffe der beteiligten Sicherheitsbehörden in Artikel 10 oder Artikel 13 Grundgesetz (GG) erhoben wurden, schließt das BVerfG den Zugang zwar nicht generell aus. Für die Einbeziehung dieser Daten in die ATD fordert es aber normenklare, einschränkende Regelungen. Soweit aufgrund dieser Daten recherchiert wird, sollen im Trefferfall - als Übergangslösung - nur die Fundstelle und nicht direkt Grunddaten der Person verfügbar werden. Für das Landeskriminalamt und die Verfassungsschutzbehörde bedeutet dies, dass sie schon jetzt bei der Speicherung dieser Daten in der ATD strengere Maßstäbe an die Erforderlichkeit und Verhältnismäßigkeit anlegen müssen als bisher.

Darüber hinaus hat das BVerfG die Speicherung von Daten zu solchen Personen für verfassungswidrig erklärt, die eine Gruppierung, welche eine terroristische Vereinigung unterstützt, nur „unterstützen“, § 2 Satz 1 Nr. 1 b, und die Gewaltanwendung im Sinne des § 2 Satz 1 Nr. 2 nur „befürworten“. Hier gilt die übergangsweise Weitergeltung bis zur Neuregelung. Dies hindert das Landeskriminalamt und die Verfassungsschutzbehörde nicht, bereits jetzt Konsequenzen aus dem Urteil zu ziehen und eine Speicherung zu diesen Personen in der ATD zu unterlassen. Die Pflicht der beteiligten Behörden nach § 2 Satz 1 ATDG kann sich nicht auf eine Datenverarbeitung beziehen, deren Verfassungswidrigkeit das BVerfG festgestellt hat.

Etwas Entsprechendes gilt für merkmalsbezogene Recherchen (Inverssuche) in erweiterten Grunddaten, soweit dies im Trefferfall direkt den Zugriff auf die Personengrunddaten und nicht nur auf die Fundstelle ermöglicht. Dies ist verfassungswidrig und muss umgehend ausgeschlossen werden. Bis dahin hat das BVerfG allerdings in Eilfällen einen entsprechenden Zugriff vorübergehend zugelassen. Auch hier sind das Landeskriminalamt und die Verfassungsschutzbehörde nicht gehindert, dem Urteil des BVerfG bereits heute dadurch zu entsprechen, dass sie auch im Eilfall auf derartige Recherchen verzichten bzw. sich – soweit technisch möglich - auf die Fundstellen beschränken.

Eine besondere Bedeutung hat das BVerfG der Kontrolle durch die Datenschutzaufsichtsbehörden - „sowohl auf Bundes- wie auf Landesebene“ - eingeräumt. Das BVerfG fordert zudem Kontrollen in angemessenen Abständen - deren Dauer ein gewisses Höchstmaß, etwa zwei Jahre, nicht unterschreiten darf“. Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern wird diesen Auftrag des Gerichts zur Kontrolle der Protokolldaten möglichst zeitnah und in Kooperation mit dem Bundesbeauftragten und gegebenenfalls anderen Landesbeauftragten nachkommen.

Das Landeskriminalamt und auch die Verfassungsschutzbehörde wurden gebeten mitzuteilen, welche Konsequenzen sie aus dem Urteil für die Praxis ihrer Speicherung in der ATD ziehen.

Der Minister für Inneres und Sport Mecklenburg-Vorpommern hat uns mitgeteilt, dass Polizei und Verfassungsschutz in Mecklenburg-Vorpommern unmittelbare Konsequenzen aus dem Urteil gezogen haben, indem ein Zugriff auf Daten von Kontaktpersonen sowie auf Daten aus Eingriffsmaßnahmen in Artikel 10/13 GG ausgeschlossen wurde. Ebenso erfolgt keine Speicherung von Daten zu Personen, die eine Gruppierung nur unterstützen, die wiederum eine terroristische Vereinigung unterstützt, oder zu Personen, die Gewaltanwendung lediglich befürworten. Des Weiteren wurde uns mitgeteilt, dass es einen Bericht geben wird, der im Rahmen der IMK erarbeitet und abschließend auf der Herbstsitzung im Dezember 2013 beschlossen werden soll. Der Minister hat uns zugesagt, dass er uns diesen Bericht zur Verfügung stellen wird.

6.3.2 Gesetz zur Änderung des Landesverfassungsschutzgesetzes und des Sicherheits- und Ordnungsgesetzes

Das Gesetz zur Änderung des Landesverfassungsschutzgesetzes und des Sicherheits- und Ordnungsgesetzes zur Regelung der Bestandsdatenauskunft ist am 1. Juli 2013 in Kraft getreten. In der schriftlichen Stellungnahme und während der mündlichen Anhörung zum Entwurf des Gesetzes - Drucksache 6/1603 - hat sich unsere Behörde im Wesentlichen wie folgt geäußert:

<u>Änderungen im Landesverfassungsschutzgesetz</u>
Aufgrund der verabschiedeten Neuregelung zur Bestandsdatenauskunft auf Bundesebene ergibt sich auch auf Landesebene ein entsprechender Änderungsbedarf. Es sollte in § 24b des vorliegenden Gesetzentwurfs sichergestellt werden, dass, wenn sich das Auskunftsersuchen der Verfassungsschutzbehörde auf Zugangssicherungscodes bezieht oder unter Nutzung von dynamischen Internetprotokoll-Adressen (IP-Adressen) erfolgt, auch der entsprechende Behördenleitervorbehalt gilt und die G-10-Kommission unseres Landtages über entsprechende Anordnungen unterrichtet wird.

Darüber hinaus sollte auch die Parlamentarische Kontrollkommission unterrichtet werden. Auskunftsersuchen über Zugangssicherungscodes stellen regelmäßig eine Vorstufe zu Maßnahmen dar, die ihrerseits den Schutzbereich des Artikel 10 Grundgesetz berühren können. Daher ist zusätzlich eine Unterrichtung dieses parlamentarischen Kontrollgremiums anzuraten.

Änderungen im Sicherheits- und Ordnungsgesetz

Im novellierten Telekommunikationsgesetz (des Bundes) ist festgeschrieben worden, dass Auskunftsersuchen über Zugangssicherungscodes sowie über den Inhaber einer dynamischen IP-Adresse einem Richtervorbehalt unterliegen. Auch ist eine Benachrichtigung des Betroffenen bei beiden Maßnahmen vorgesehen. Dies muss in unserem Landesgesetz ebenfalls mit folgender Begründung umgesetzt werden:

Sowohl der Richtervorbehalt als auch die Benachrichtigung des Betroffenen tragen dem Umstand Rechnung, dass es sich bei den zugrunde liegenden Maßnahmen um gewichtige Grundrechtseingriffe handelt, die wesentlich schwerer wiegen als die bloße Bestandsdatenabfrage. Die Zuordnung dynamischer IP-Adressen zu deren Nutzern setzt eine Analyse der Verkehrsdaten voraus und greift daher in Artikel 10 Grundgesetz ein, wie es das Bundesverfassungsgericht in seiner Entscheidung vom 24. Januar 2012 - 1 BvR 1299/05 - ausdrücklich klargestellt hat.

Ähnlich ist die Auskunft über Zugangssicherungscodes wie PIN und PUK zu bewerten. Diese Daten mögen zwar Bestandsdaten sein. Sie dienen der Polizei aber dazu, sich Kenntnis von weiteren Daten zu verschaffen. Diese weiteren Daten sind üblicherweise Verkehrs- und Inhaltsdaten über bereits abgeschlossene Telekommunikationsvorgänge. Sie sind vom Schutzbereich des Rechts auf informationelle Selbstbestimmung umfasst. Die Erhebung dieser Daten stellt regelmäßig einen tiefgreifenden Eingriff in dieses Grundrecht dar. Denn hierdurch können zum einen der Umfang der Kommunikationsbeziehungen sowie die näheren Umstände der Kommunikation, oftmals für einen weitreichenden Zeitraum erschlossen werden. Zum anderen können Inhalte abgeschlossener Kommunikation erfasst werden, die mit dem Kommunikationspartner in der Annahme der Vertraulichkeit der Kommunikation ausgetauscht wurden und die höchstpersönliche Bereiche betreffen können.

Daher sind aus datenschutzrechtlicher Sicht sowohl der Richtervorbehalt als auch die Benachrichtigung geeignete Mittel, um den Schutz der Betroffenen zu erhöhen.

Im vorliegenden Gesetzentwurf ist bislang nur die Benachrichtigung des Betroffenen anhand einer zu einem bestimmten Zeitpunkt zugewiesenen IP-Adresse vorgesehen, nicht jedoch bei Auskünften über Zugangssicherungscodes wie PIN und PUK. Die Eingriffsintensität auch bei letztgenannter Maßnahme ist vorstehend dargelegt worden.

Ein Richtervorbehalt - wie im geänderten Telekommunikationsgesetz (des Bundes) - ist im vorliegenden Gesetzentwurf bisher gar nicht vorgesehen. In unserer schriftlichen Stellungnahme sind konkrete Formulierungsvorschläge zu § 28a unterbreitet worden.

Leider wurden unsere Bedenken im laufenden Gesetzgebungsverfahren im Wesentlichen nicht berücksichtigt. So konnte in Mecklenburg-Vorpommern ein Gesetz in Kraft treten, das in entscheidenden Punkten hinter den auf Bundesebene und in einigen Bundesländern verabschiedeten Regelungen zurückbleibt. Einige Landespolitiker von BÜNDNIS 90/ DIE GRÜNEN haben daher eine Sammelbeschwerde vor dem Landesverfassungsgericht in Greifswald gestartet und wollen damit gegen die entsprechenden Neuregelungen vorgehen.

6.3.3 PRISM, TEMPORA, XKeyscore und Co.

Der amerikanische Whistleblower Edward Snowden hat im Sommer 2013 die Medien darüber informiert, dass US-amerikanische und britische Geheimdienste anlasslos massenhaft den Telekommunikationsverkehr weltweit überwachen, speichern und analysieren - in einem Umfang, der bisher nicht bekannt war.

PRISM ist ein streng geheimes Überwachungsprogramm des US-Geheimdienstes NSA, welches der Auswertung von elektronisch gespeicherten Daten dient.

TEMPORA ist das Spionageprogramm des britischen Geheimdienstes GCHQ, der sich damit rühmt, Zugang zu transatlantischen Glasfaserkabeln zu haben. Dadurch sei er ebenfalls in der Lage, Unmengen von Daten - auch von Deutschen - abzuschöpfen, die auch mit dem amerikanischen Geheimdienst geteilt würden.

Des Weiteren wurde in den Medien berichtet, dass die NSA das Bundesamt für Verfassungsschutz mit XKeyscore ausgestattet haben soll. Das Programm soll über einen Zwischenspeicher verfügen, der für mehrere Tage einen „full take“ aller ungefilterten Daten aufnehmen könne. XKeyscore soll in der Lage sein, nicht nur Verbindungsdaten, sondern auch zumindest teilweise Kommunikationsinhalte zu erfassen. Zudem lasse sich mit dem System rückwirkend sichtbar machen, welche Stichwörter Zielpersonen in Internetsuchmaschinen eingaben und welche Orte sie über Google Maps suchten.

Auf Nachfragen hin teilte uns die Verfassungsschutzbehörde unseres Landes mit, dass sie diese Software nicht nutze. Das Bundesamt für Verfassungsschutz erklärte, dass es eine Variante der Software XKeyscore zwar teste, diese aber derzeit nicht für seine Arbeit einsetze.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist sich einig, dass sowohl auf nationaler als auch auf europäischer und internationaler Ebene alles dafür getan werden muss, damit unbescholtene Bürgerinnen und Bürger nicht anlasslos und umfassend durch Nachrichtendienste überwacht werden.

Die Konferenz hat dazu am 5. September 2013 (siehe unter www.lfd.m-v.de/datenschutz/themen/beschlue/Geheimdienste.pdf) eine Entschließung verabschiedet und gefordert:

- Nationales, europäisches und internationales Recht ist so weiterzuentwickeln und umzusetzen, dass es einen umfassenden Schutz der Privatsphäre, der informationellen Selbstbestimmung, des Fernmeldegeheimnisses und des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme garantiert.
- Sofern verfassungswidrige nachrichtendienstliche Kooperationen erfolgen, müssen diese abgestellt und unterbunden werden.
- Die Kontrolle der Nachrichtendienste muss durch eine Erweiterung der Befugnisse sowie eine gesetzlich festgelegte verbesserte Ausstattung der parlamentarischen Kontrollgremien intensiviert werden. Bestehende Kontrolllücken müssen unverzüglich geschlossen werden. In diesem Zusammenhang ist zu prüfen, ob die Datenschutzbeauftragten verstärkt in die Kontrolle der Nachrichtendienste eingebunden werden können.
- Es sind Initiativen zu ergreifen, die die informationelle Selbstbestimmung und das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme sicherstellen.
- Völkerrechtliche Abkommen wie das Datenschutz-Rahmenabkommen und das Freihandelsabkommen zwischen der EU und den USA dürfen nur abgeschlossen werden, wenn die europäischen Grundrechte ausreichend geschützt werden. Das bedeutet auch, dass jeder Mensch das Recht hat, bei vermutetem Datenmissbrauch den Rechtsweg zu beschreiten. Das Fluggastdatenabkommen und das Überwachungsprogramm des Zahlungsverkehrs müssen auf den Prüfstand gestellt werden.
- Auch innerhalb der Europäischen Union ist sicherzustellen, dass die nachrichtendienstliche Überwachung durch einzelne Mitgliedsstaaten nur unter Beachtung grundrechtlicher Mindeststandards erfolgt, die dem Schutzniveau des Artikels 8 der Charta der Grundrechte der Europäischen Union entsprechen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert alle Verantwortlichen auf, die umfassende Aufklärung mit Nachdruck voranzutreiben und die notwendigen Konsequenzen zügig zu treffen. Es geht um nichts weniger als das Grundvertrauen der Bürgerinnen und Bürger in den Rechtsstaat.

In den USA hatten zwei Bürger Klage eingereicht gegen die Sammlung ihrer Verbindungsdaten durch die US-Regierung. Ein US-amerikanischer Bezirksrichter hat am 16. Dezember 2013 entschieden, dass die NSA höchstwahrscheinlich gegen die Verfassung verstößt, indem sie Daten aller US-Telefonate speichert. Der Richter hat verfügt, dass die US-Regierung die Sammlung von Verbindungsdaten der zwei Beschwerdeführer stoppen müsse und alle gespeicherten Daten über sie löschen muss. Gleichzeitig erlaubte er der US-Regierung eine Einspruchsfrist von sechs Monaten, weil Belange der nationalen Sicherheit betroffen seien. Diese Entscheidung wird als erster juristischer Erfolg gegen die Überwachung, die Edward Snowden enthüllt hat, gewertet.

Es bleibt abzuwarten, ob und inwieweit die Forderungen der Datenschutzbeauftragten des Bundes und der Länder umgesetzt werden.

6.4 Kommunales/Meldewesen

6.4.1 Zugang zu Geodaten

Immer wieder taucht die Frage auf, inwieweit unterschiedlichen Organisationseinheiten einer Verwaltung personenbezogene Daten zur Verfügung gestellt werden können. Das Ministerium für Landwirtschaft, Umwelt und Verbraucherschutz Mecklenburg-Vorpommern hat beispielsweise um eine datenschutzrechtliche Bewertung eines Sachverhaltes gebeten, wonach in einer hiesigen Kommunalverwaltung auf Seiten des Stadtplanungsamtes und des Liegenschaftsamtes der Wunsch bestand, dass in dem bei der betreffenden Stadtverwaltung geführten, frei zugänglichen Geo-Portal generell alle Flächen gekennzeichnet werden, die Altlastverdachtsflächen oder Altlastflächen darstellen.

Im vorliegenden Fall war hinsichtlich der Beurteilung der Zulässigkeit der Datenverarbeitung § 8 Landesbodenschutzgesetz (LBodSchG M-V) einschlägig, wobei Absatz 5 der vorgenannten Vorschrift auf die Vorschriften des Landesdatenschutzgesetzes Mecklenburg-Vorpommern (DSG M-V) verweist.

Voraussetzung für einen datenschutzrechtlichen Bezug und damit die Beurteilung nach dem DSG M-V war aber auch, dass es sich bei den Angaben über Altlasten und altlastverdächtige Flächen überhaupt um personenbezogene Daten handelt. Dieses ist in der Darstellung im Geo-Portal nicht automatisch der Fall. Die vorgenannten Daten können aber mit weiteren Informationen zu den Grundstückseigentümern (bspw. über Katasterangaben oder andere Datenquellen) verknüpft werden, sodass sich schnell ein Personenbezug herstellen ließe. Ein datenschutzrechtlicher Bezug wäre allerdings dann nicht gegeben, wenn es sich bei den betreffenden Bereichen nicht um private, sondern bzw. um öffentliche Flächen handeln würde.

Auch das häufig von Verwaltungen angeführte Argument, dass eine Datenübermittlung innerhalb derselben Behörde ja wohl möglich sein müsse, spielt keine Rolle, da im Datenschutzrecht der funktionale Behördenbegriff gilt. Danach sind nicht nur die Behörden, sondern auch ihre funktionalen Einheiten im Verhältnis zueinander als Dritte im Sinne des § 3 Abs. 6 DSG M-V zu behandeln.

Somit war nach § 14 Abs. 1 DSG M-V insbesondere der Erforderlichkeitsaspekt zu prüfen. Der Begriff der Erforderlichkeit ist dabei eng auszulegen. Erforderlich ist die Verarbeitung personenbezogener Daten nur dann, wenn die Aufgabe sonst nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllt werden kann. Außerdem ist für jede einzelne Information zu prüfen, ob sie zur rechtmäßigen Aufgabenwahrnehmung der datenverarbeitenden Stelle übermittelt werden muss. Auf eine bloße Nützlichkeit der Daten kommt es hierbei nicht an. Außerdem dürfen die Daten nicht nur für eine leichtere oder wirtschaftlichere Erfüllung der Aufgabe dienlich sein, sondern sie müssen tatsächlich für die Aufgabenerfüllung benötigt werden.

Eine pauschale Übermittlung der Daten würde dem Grundsatz der Erforderlichkeit widersprechen. Vielmehr ist eine Datenübermittlung nur dann möglich, wenn es für die Aufgabenerfüllung (beispielsweise für die Planung bestimmter Gebiete) erforderlich ist.

Aus vorgenannten Gründen haben wir empfohlen, die Altlastverdachtsflächen und Altlastflächen für die betreffenden Ämter nur im Einzelfall unter Berücksichtigung der Maßgabe der Erforderlichkeit zur Verfügung zu stellen.

6.4.2 Übermittlung von Daten eines Grundstückseigentümers

Einige Male wurden wir mit der Frage konfrontiert, unter welchen Bedingungen personenbezogene Daten von Grundstückseigentümern an Kaufinteressenten herausgegeben werden dürfen.

Nach § 33 Abs. 2 Nr. 2 Geoinformations- und Vermessungsgesetz (GeoVermG M-V) dürfen Stellen oder Personen außerhalb des öffentlichen Bereiches personenbezogene Daten zur Verfügung gestellt werden, soweit diese ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft darlegen und der Betroffene kein schutzwürdiges Interesse am Ausschluss der Bereitstellung hat.

Gemäß dieser Regelung muss eine Abwägung zwischen einem berechtigten Offenbarungsinteresse auf der einen und dem Geheimhaltungsinteresse (schutzwürdige Interessen) des Betroffenen auf der anderen Seite durchgeführt werden. Das Offenbarungsinteresse kann dabei bereits obsiegen, wenn wirtschaftliche Interessen vorliegen. Dies wäre beispielsweise dann der Fall, wenn dem Grundstückseigentümer ein Kredit gewährt werden soll oder Ansprüche auf Rückübertragung an dem Grundstück angemeldet wurden. Kaufmännischen Auskunfteien oder Immobilienmaklern wird unseres Erachtens ein allgemeines Recht auf Nutzung personenbezogener Geodaten zu versagen sein, es sei denn, die Daten werden im Zusammenhang beispielsweise mit der Geltendmachung von Ansprüchen aus einem Maklervertrag benötigt.

Ein mögliches Kaufinteresse, bei dem durch die Einsicht beziehungsweise Offenbarung der personenbezogenen Daten erst der Name des Grundstückseigentümers in Erfahrung gebracht werden soll, dürfte keinen Vorrang vor dem Geheimhaltungsinteresse der Eigentümer besitzen. Zu berücksichtigen ist dabei insbesondere der Umstand, dass nicht jede Eigentümerin bzw. nicht jeder Eigentümer eine Kontaktaufnahme durch Kaufinteressenten wünscht und sich von einer solchen belästigt fühlen dürfte.

Um aber in einem solchen Fall dem Offenbarungsinteresse trotzdem Rechnung tragen zu können, käme als mögliche (und aus unserer Sicht datenschutzfreundliche) Alternative das sogenannte Adressmittlungsverfahren in Frage.

Das Adressmittlungsverfahren ist grundsätzlich nicht geregelt. Es kann unseres Erachtens in Einzelfällen zur Anwendung kommen, wenn zwar eine Übermittlung der Anschrift an den Auskunftsersuchenden mangels Vorliegen der gesetzlichen Voraussetzungen nicht zulässig ist, das verfolgte Anliegen aber grundsätzlich unterstützenswert erscheint und hierdurch keine Beeinträchtigung schutzwürdiger Belange der Betroffenen zu erwarten ist. Ein Rechtsanspruch hierauf besteht jedoch nicht.

Beim Adressmittlungsverfahren werden der Verwaltung die Anschreiben (z. B. Bekunden des Kaufinteresses) übergeben, die diese dann adressiert und versendet. Die Anschreiben müssen der Verwaltung unverschlossen übergeben werden, da die Verwaltung bei einem Adressmittlungsverfahren gegenüber den Einzelnen hinsichtlich der Datennutzung für diesen Zweck in der Verantwortung steht, zum Beispiel, warum sie ein bestimmtes Vorhaben in dieser Weise unterstützt und wie sie dabei sicherstellt, dass das Verfahren transparent gestaltet und die Betroffenen in geeigneter Weise aufgeklärt werden.

In dem Anschreiben sind die Betroffenen über das Adressmittlungsverfahren sowie über die Freiwilligkeit der Teilnahme an den jeweiligen Vorhaben zu informieren. Für die Empfänger muss erkennbar sein, auf welchem Weg dieses Schreiben an sie gelangt ist, also auch, dass ihre Adresse nicht weitergegeben wurde und dass es ausschließlich ihnen vorbehalten bleibt, ob sie in der Angelegenheit aktiv werden. Diese beiden Aspekte, Transparenz des Verfahrens und Aufklärung, sind bei der Formulierung des Anschreibens zu berücksichtigen.

6.4.3 Zweckwidrige Nutzung von besonderen Meldescheinen

Durch eine Landkreisverwaltung wurden baurechtswidrige Zustände kontrolliert und geahndet. Konkret ging es dabei um ungenehmigte Nutzungen von Wohngebäuden als Ferienhäuser. Im Rahmen einer Petition wurden wir darüber in Kenntnis gesetzt, dass die Landkreisverwaltung dabei auf die Idee gekommen war, sich von den betreffenden Eigentümerinnen und Eigentümern die besonderen Meldescheine vorlegen zu lassen. Hierüber sollte ermittelt werden, ob die Häuser unerlaubterweise als Ferienhäuser an Urlauber vermietet werden.

Urlauber müssen nach § 26 Abs. 2 Landesmeldegesetz (LMG) am Tag ihrer Ankunft handschriftlich einen besonderen Meldeschein ausfüllen und unterschreiben. Der Vermieter der jeweiligen Unterkunft wiederum ist nach § 27 Abs. 4 LMG verpflichtet, diese Meldescheine bis zum Ablauf des auf den Tag der Ankunft folgenden Kalenderjahres aufzubewahren, für die Polizei sowie für die örtlich zuständige Meldebehörde zur Einsichtnahme bereitzuhalten und der Polizei auf Verlangen auszuhändigen. Die Meldescheine sind dabei vor unbefugter Einsichtnahme zu sichern und nach Ablauf der Aufbewahrungsdauer zu vernichten.

Die mit dem besonderen Meldeschein erhobenen Daten unterliegen einer strengen Zweckbindung, die in § 29 LMG normiert ist. Nach § 29 Abs. 1 LMG dürfen diese Daten nur von der Meldebehörde und den in § 31 Abs. 3 LMG genannten Behörden (Sicherheitsbehörden) für Zwecke der Gefahrenabwehr oder Strafverfolgung sowie zur Aufklärung der Schicksale von Vermissten und Unfallopfern ausgewertet und verarbeitet werden. Darüber hinaus dürfen die Daten von den Gemeinden zur Kurbeitragserhebung sowie für Zwecke der Fremdenverkehrsstatistik ausgewertet und verarbeitet werden.

Eine Übermittlung zu einem anderen Zweck hat der Gesetzgeber nicht vorgesehen. Aus diesem Grund hätte die Landkreisverwaltung die besonderen Meldescheine nicht abfordern dürfen.

Der Empfehlung, diese Vorgehensweise einzustellen, ist die Verwaltung im Ergebnis gefolgt.

6.4.4 Übermittlung von Meldedaten an Religionsgemeinschaften und an die GEZ

Im Rahmen von Datenschutzkontrollen in mehreren Bundesländern wurde geprüft, auf welchem Weg und mit welchen Sicherheitsvorkehrungen Meldedaten an die öffentlich-rechtlichen Religionsgemeinschaften und an die GEZ übermittelt werden. Die Ergebnisse dieser Kontrollen wurden auch im Arbeitskreis „Technische und organisatorische Datenschutzfragen“ (siehe auch Punkt 7) beraten. Für die Bewertung der Sicherheitsvorkehrungen war zu berücksichtigen, dass die zu übermittelnden Daten besonders schutzbedürftige Angaben über die Religionszugehörigkeit enthalten. Zudem ist zu beachten, dass auch solche Meldedaten übermittelt werden, für die eine Auskunfts- und Übermittlungssperre (beispielsweise wegen Gefahr für Leib und Leben) im Meldedatensatz eingetragen ist. Angesichts der hohen Sensibilität solcher Daten sind technische und organisatorische Maßnahmen erforderlich, die den Datenschutz und die Datensicherheit in angemessener Weise sicherstellen. Hierzu müssen insbesondere die Vertraulichkeit und Unversehrtheit der im Melderegister gespeicherten und übermittelten Daten gemäß § 8 Abs. 2 Satz 2 Melderechtsrahmengesetz (MRRG) gewährleistet werden. Zudem dürfen die Daten nur übermittelt werden, wenn gemäß § 18 Abs. 1a MRRG über die Identität der anfragenden Stelle kein Zweifel besteht.

Für die Meldebehörden in Mecklenburg-Vorpommern hat das Ministerium für Inneres und Sport Mecklenburg-Vorpommern die Fachaufsicht. Deshalb haben wir das Ministerium gebeten zu evaluieren, wie die Übermittlung der Daten im Einzelnen umgesetzt ist und welche Sicherheitsvorkehrungen die Meldebehörden des Landes nutzen. Im Ergebnis stellte sich heraus, dass kein einheitliches Vorgehen bei der Datenübermittlung existiert. Einige Behörden übermittelten die fraglichen Daten mit dem sicheren Standard OSCI-Transport (siehe auch Punkt 4.5). Andere nutzen für eine Übermittlung lediglich unverschlüsselte CDs oder DVDs. Teilweise wurden Daten online übertragen und deren Vertraulichkeit mittels einer SSL/TLS-Verschlüsselung *(siehe Kasten)* gesichert. Wir haben darauf hingewiesen, dass nur der Einsatz von OSCI-Transport den Anforderungen an die Übermittlung der hoch schutzbedürftigen Daten genügt und somit offensichtlich dringender Handlungsbedarf bestand.

Da ein ähnliches Ergebnis auch von den Kolleginnen und Kollegen der anderen Bundesländer ermittelt wurde, sah sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder veranlasst, mit der Entschließung „Übermittlung von Meldedaten an die Kirchen und die GEZ sicher, vertraulich und rechtskonform gestalten“ (siehe http://www.datenschutz- mv.de/datenschutz/themen/beschlue/84_DSK/ent_Melde.html) auf die Missstände hinzuweisen und bundesweit entsprechende Änderungen einzufordern.

Wir empfehlen der Landesregierung, sich dafür einzusetzen, dass bei der Übermittlung der Meldedaten von den Meldebehörden an die Kirchen und an die GEZ ein dem Stand der Technik entsprechendes Verfahren eingesetzt wird. Hierbei bietet sich das OSCI-Protokoll an, welches schon für die regelmäßige Datenübermittlung zwischen den Meldebehörden verschiedener Länder genutzt wird. Aufgrund seiner Möglichkeit zur kryptographischen Verschlüsselung und Signatur wird das OSCI-Protokoll hier in § 2 Abs. 3 Satz 1 der 1. Verordnung zur Durchführung von regelmäßigen Datenübermittlungen der Meldebehörden (BMeldDÜV) gefordert.

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.

Auf Schwachstellen von SSL und TLS haben wir bereits im Zehnten Tätigkeitsbericht hingewiesen (siehe Punkt 4.2.6). Die dort formulierten Empfehlungen sollten unbedingt berücksichtigt werden.

6.4.5 Der neue Personalausweis

Der neue Personalausweis (nPA) war schon mehrfach Gegenstand unserer Berichterstattung. Im Neunten Tätigkeitsbericht haben wir unter Punkt 2.4.9 die Datenschutzaspekte der neuen Funktionen des Ausweises erläutert und auf die Risiken der Kartenleser ohne eigenes Tastaturfeld hingewiesen. Schwerpunkt der Erläuterungen im Zehnten Tätigkeitsbericht, Punkt 5.4.7, waren künftige Anwendungen des Ausweises im öffentlichen Bereich und die hohen Kosten der sogenannten Berechtigungszertifikate. Unsere Empfehlungen zur datenschutzgerechten Ausgestaltung der Verfahren zur Nutzung des neuen Personalausweises wurden insbesondere aus Kostengründen bisher jedoch nicht angemessen berücksichtigt.

Sicherheit bei der Nutzung des neuen Personalausweises
Am 18. Oktober 2013 titelte die Schweriner Volkszeitung: „Wie sicher ist der ePerso?“. Wenige Tage zuvor hatte der Chaos Computer Club erneut öffentlich demonstriert, wie mit Hilfe eines sogenannten Keyloggers die Geheimzahl abgefangen werden kann, die für die Nutzung der eID-Funktion des Ausweises erforderlich ist. Dieser Angriff war erfolgreich, weil ein - auch von uns mehrfach kritisierter - Basisleser ohne eigenes Tastaturfeld an den Bürger-PC angeschlossen und genutzt wurde.

Diese Angriffsmöglichkeit ist nicht neu. Bereits in der vom Bundesinnenministerium (BMI) beauftragten Studie vom Oktober 2010 zu den Restrisiken der Ausweis-App auf dem Bürger-PC weisen die Forscher auf das „Restrisiko Basisleser“ hin und empfehlen ausdrücklich, einen Leser ohne eigenes Tastaturfeld nicht zu nutzen, da die Vertrauenswürdigkeit des Bürger-PC von einem Großteil der Nutzerinnen und Nutzer nicht gewährleistet werden kann.

Aber auch nach den wiederholt durchgeführten erfolgreichen Angriffen sieht die Bundesregierung keine Veranlassung, Konsequenzen zu ziehen. Mit Beantwortung einer schriftlichen Anfrage des Bundestagsabgeordneten Jan Korte vom 30. August 2013 weist das BMI erneut lediglich darauf hin, dass derartige Angriffe verhindert werden können, indem die Nutzerin/der Nutzer des Ausweises das Betriebssystems ihres/seines PC regelmäßig aktualisiert sowie eine Firewall und ein Virenschutzprogramm installiert. Die von den Forschern beschriebenen Risiken werden schlichtweg ignoriert und mit dem Hinweis zur Seite geschoben, dass es in den drei Jahren seit Einführung des elektronischen Ausweises keinerlei Vorfälle gab, die Zweifel an der Sicherheit des Chips und der darin gespeicherten Daten hervorrufen.

Angesichts der zunehmenden Bedeutung des neuen Personalausweises (siehe bspw. Punkt 3.2) empfehlen wir den Bürgerinnen und Bürgern nach wie vor, nur Ausweislesegeräte mit eigenem Tastaturfeld zu nutzen. Der Landesregierung wird empfohlen, vorhandene Risiken nicht zu verharmlosen, sondern den Einsatz von Lesern und mit eigener Tastatur ausdrücklich zu empfehlen und im Rahmen von E-Government-Initiativen finanziell zu fördern.

Berechtigungen zum Auslesen von ID-Daten aus dem Personalausweis

Nach wie vor kostet es ein Unternehmen oder eine öffentliche Stelle viel Geld, wenn der Personalausweis in automatisierte E-Commerce- oder E-Government-Verfahren etwa zur Feststellung der Identität eines Antragstellers eingebunden werden soll. Im Personalausweisgesetz (PAuswG) ist festgelegt, dass für jede Anwendung jeweils ein so genanntes Berechtigungszertifikat erworben werden muss, mit dem das Bundesverwaltungsamt (BVA) festlegt, welche Daten ausgelesen werden dürfen. Leider haben sich unsere im Zehnten Tätigkeitsbericht, Punkt 5.4.7, geäußerten Befürchtungen bestätigt, dass das BVA unter dem vorherrschenden Kostendruck insbesondere im kommunalen Bereich in zunehmendem Maße für mehrere unterschiedliche Fachverfahren gemeinsame Berechtigungszertifikate erteilt.

Eine besondere Rolle für E-Government-Anwendungen spielen in diesem Zusammenhang Bürgerportale. Die Nutzung von E-Government-Anwendungen (im PAuswG als Dienst bezeichnet) setzt in der Regel die Identifizierung der Nutzerin/des Nutzers voraus. Aus Kostengründen wird in zunehmendem Maße diese Identifizierung von der eigentlichen Fachaufgabe getrennt und in Bürgerportale verlagert, über die viele verschiedene Verwaltungsaufgaben angesteuert werden können. Diese Bürgerportale werden nicht mehr von der Verwaltung als eigentlicher Anbieterin eines Dienstes, sondern von Dritten wie kommunalen Rechenzentren oder Zweckverbänden betrieben. Das Bundesverwaltungsamt erteilt nun nicht mehr unterschiedliche, auf Fachaufgaben bezogene Berechtigungszertifikate, sondern nur noch ein Zertifikat für den Identifizierungsdienst im Bürgerportal. Obwohl das BVA vor der Erteilung dieses einen Zertifikates die dahinter liegenden Dienste analysiert, hat diese Praxis erhebliche rechtliche und technische Auswirkungen.

Aus rechtlicher Sicht ist festzustellen, dass die Erteilung eines Zertifikates die datenschutzrechtliche Verantwortung für die entsprechende Fachaufgabe voraussetzt. Die datenschutzrechtliche Verantwortung trägt die Stelle, der die Fachaufgabe per Gesetz zugewiesen ist. Die Identifizierung ist jedoch zunächst keine eigenständige Fachaufgabe im Sinne des PAuswG. Betreibt nun etwa ein Zweckverband wie in unserem Bundesland das Bürgerportal, muss ihm die datenschutzrechtliche Verantwortung für den der eigentlichen Fachaufgabe vorgelagerten Identifizierungsdienst übertragen werden, damit er beim BVA ein Berechtigungszertifikat beantragen kann. In Absprache mit unseren Kolleginnen und Kollegen von Bund und Ländern akzeptieren wir unterschiedliche Varianten der Aufgabenübertragung. In Mecklenburg-Vorpommern wird beispielsweise die Möglichkeit der Einrichtung von gemeinsamen Verfahren nach § 2 Abs. 10 DSG M-V genutzt (zu Details des Verfahrens siehe weiter unten). In anderen Bundesländern waren spezielle gesetzliche Regelungen erforderlich. Auch der Weg der Beauftragung eines Dienstleisters auf dem Wege der Beleihung ist denkbar.

Aus technischer Sicht sind die Auswirkungen gravierender, da das aus datenschutzrechtlicher Sicht lobenswerte Konzept durch derartige Bürgerportale teilweise unterlaufen wird. Das Ursprungskonzept der eID-Funktion des neuen Personalausweises haben wir immer ausdrücklich befürwortet, weil die kryptographisch hervorragenden und zertifikatsbasierten Mechanismen des Ausweises auf sehr sichere Weise eine dienstespezifische Preisgabe von ID-Daten des Ausweises garantieren und somit kaum missbräuchlich genutzt werden können. Diese dienstespezifische Datenfreigabe verhindert zudem die Zusammenführung unterschiedlicher Aktivitäten der Ausweisinhaberin/des Ausweisinhabers, sodass die Erstellung von Nutzungsprofilen praktisch nicht möglich ist.

Wenn nun im Bürgerportal für verschiedene Anwendungen ID-Daten aus dem Ausweis mit nur einem einzigen Berechtigungszertifikat ausgelesen werden, besteht prinzipiell die Möglichkeit, die Aktivitäten der Ausweisinhaberin/des Ausweisinhabers zu verknüpfen und somit Nutzungsprofile zu bilden. Zudem bestimmt nun nicht mehr die sichere Hardware des Ausweises die Preisgabe einzelner Daten. Nun steuert lediglich die wesentlich leichter manipulierbare Software des Bürgerportals, welche der dort (temporär oder dauerhaft) gespeicherten ID-Daten der Nutzerin/des Nutzers an welche Verfahren weitergegeben werden. Rechtlich zulässig ist ein solches Verfahren ohnehin nur unter der Voraussetzung, dass alle Fachanwendungen, die dieses eine Berechtigungszertifikat bedienen, genau alle Daten erfordern, die vom Zertifikat umfasst sind (Prinzip des kleinsten gemeinsamen Nenners). Würde ein Fachverfahren weniger Daten benötigen, müsste ein anderes Zertifikat genutzt werden, das den reduzierten Datenumfang beschreibt. Das BVA teilt diese Auffassung und hat wiederholt bestätigt, dass die beschriebenen Mehrfachzertifikate nur unter diesen Bedingungen erteilt werden.

Für das Bürgerportal unseres Landes, das vom Zweckverband „Elektronische Verwaltung in Mecklenburg-Vorpommern“ (eGo-MV) betrieben wird, haben wir deshalb konkrete Vorgaben formuliert, die im Folgenden erläutert werden:

Nutzung des neuen Personalausweises in Mecklenburg-Vorpommern
Im Zweckverband „Elektronische Verwaltung in Mecklenburg-Vorpommern“ (eGo-MV) haben sich Städte und Gemeinden des Landes zusammengeschlossen, um IT-Sicherheits- und Datenschutzfragen bei komplexen Projekten mit vereinten Kräften zu klären. Der Zweckverband betreibt gemeinsam mit seinen Mitgliedern verschiedene Fachverfahren. Anwendungen des neuen Personalausweises sind im Berichtszeitraum neu dazugekommen. Der eGo-MV möchte seine Mitglieder bei der Realisierung der oben genannten komplexen technischen Anforderungen unterstützen. Insbesondere sollen die Mitgliedskommunen organisatorisch und finanziell entlastet werden, indem sie sich nicht selbst in größerem Umfang mit Berechtigungszertifikaten des Bundesverwaltungsamtes eindecken müssen. Auch die Infrastrukturkomponenten sollen möglichst gebündelt angeschafft und betrieben werden. Insbesondere vor dem Hintergrund der oben beschriebenen rechtlichen und technischen Hürden haben wir den Zweckverband in Bezug auf erforderliche Datenschutz- und IT-Sicherheitsmaßnahmen beraten.

Berechtigungszertifikate werden vom Bundesverwaltungsamt an einen Diensteanbieter zur Erfüllung eigener Aufgaben oder Geschäftszwecke ausgestellt (siehe oben). Der Zweckverband baut nun aber einen einheitlichen nPA-Identifikationsdienst im Sinne der oben beschriebenen Strukturen auf (temporäres Bürgerportal). Anwender dieses Dienstes sind mehrere verschiedene Behörden aus unterschiedlichen Kommunen mit verschiedenen Fachaufgaben. Der Identifikationsdienst ist mit einem einzigen Berechtigungszertifikat des Bundesverwaltungsamtes ausgestattet. Der Identifikationsdienst leitet die verschlüsselten Identitätsdaten aus dem nPA direkt an das Fachverfahren der Gemeinde weiter. Es handelt sich hier um ein temporäres Bürgerkonto, da die aus dem Personalausweis ausgelesenen ID-Daten im Portal nicht dauerhaft gespeichert werden.

Wir halten den Einsatz des Verfahrens unter folgenden Bedingungen für rechtlich tolerabel:

a) Sofortige Löschung
Die Identitätsdaten müssen sofort nach der Übertragung an das Fachverfahren gelöscht werden. Andernfalls bestünde die Möglichkeit, die Nutzungsvorgänge der Bürgerinnen und Bürger behörden- und verfahrensübergreifend zu überwachen.

b) Keine personenbezogene Protokollierung
Das temporäre Bürgerkonto darf die Portalnutzung nicht personenbezogen, also auch nicht pseudonym protokollieren. Sinn und Zweck des im Personalausweisgesetz festgelegten Verfahrens zur Pseudonymisierung ist es, dass der Verwender eines Berechtigungszertifikates nichts über anderweitige Nutzungen eines Ausweises erfährt. Die Nutzungsdaten von verschiedenen Anwendungen desselben Betreibers und von Anwendungen unterschiedlicher Betreiber sollen nicht miteinander verkettet werden können. Dieses Konzept könnte durch das temporäre Bürgerkonto gebrochen werden, wenn es personenbezogene Protokolldaten erzeugt und speichert.

c) Gleiches Datenprofil für alle Anwendungen
Alle Verfahren, die das temporäre Bürgerkonto nutzen, benötigen den gleichen Satz an Identitätsdaten aus dem nPA (also dieselben Attribute). Benötigt eine Anwendung weniger Daten, darf sie die Lösung nicht nutzen, weil damit mehr als die zur Aufgabenerfüllung erforderlichen Daten erhoben würden. Sollen Anwendungen mit abweichendem Datenprofil bedient werden, ist ein anderes Berechtigungszertifikat erforderlich.

d) Transparenz hinsichtlich der beteiligten Stellen
Noch vor Anforderung der Identitätsdaten müssen die Nutzerinnen und Nutzer unmissverständlich darüber informiert werden, welche Behörde welche Daten zu welchem Zweck benötigt. Außerdem ist darzulegen, welche Rolle der Zweckverband bezüglich der Identitätsprüfung für die jeweilige Behörde einnimmt.

e) Zertifizierung
Es sollte geprüft werden, ob die eingesetzte Lösung hinsichtlich der Einhaltung des Datenschutzes zertifiziert werden kann. Wir begrüßen, dass die Lösung in einem ISO 27001-zertifizierten Rechenzentrum betrieben werden soll. Wir regen an, die Nutzerinnen und Nutzer über die vorhandenen Zertifizierungen in angemessener Weise zu informieren, beispielsweise in den Datenschutzerklärungen der Websites.

Wie fehleranfällig eine solche Lösung sein kann, mussten wir bei der ersten vom eGo-MV freigeschalteten Anwendung feststellen. Über das sogenannte Urkundenportal soll es künftig möglich sein, Personenstandsurkunden auf elektronischem Wege direkt bei den jeweiligen Standesämtern abzurufen. Der Abruf erfordert die eindeutige Identifizierung des Antragstellers. Dafür soll im Bürgerportal des Zweckverbandes die eID-Funktion des neuen Personalausweises verwendet werden. Mit Verwunderung stellten wir bei der ersten Präsentation des Verfahrens fest, dass das verwendete Berechtigungszertifikat gerade nicht zum Verfahren des Urkundenportals passte. Eine der wesentlichen von uns formulierten Bedingungen (siehe oben: Anforderung c) war nicht eingehalten worden.

Der Zweckverband bestätigte dann tatsächlich, „… dass das Urkundenportal nicht den Anforderungen des Berechtigungszertifikats genügt.“ Die Kompatibilität zwischen Anwendung und Zertifikat war offensichtlich nicht ausreichend geprüft worden. In diesem Fall wurde allerdings kein neues Zertifikat beantragt, sondern das Urkundenportal den rechtlichen Anforderungen angepasst und - im Übrigen bundesweit - neu ausgerollt, sodass dann auch das bereits vorhandene Zertifikat passte.

Wir empfehlen allen Stellen, die die eID-Funktion des neuen Personalausweises über den einheitlichen nPA-Identifikationsdienst im Bürgerportal nutzen möchten, sehr sorgfältig zu prüfen, ob das vom eGo-MV beschaffte Berechtigungszertifikat mit genutzt werden kann oder ob nicht ein separates Berechtigungszertifikat erforderlich ist.

6.4.6 E-Government-Verfahren – sind Kommunen überfordert?

Ein neues E-Government-Verfahren ermöglicht es berechtigten Personen, elektronisch gespeicherte Personenstandsurkunden über das Internet abzurufen. Im dazu eingerichteten Urkundenportal unseres Landes (siehe Punkt 6.4.5) müssen diese Personen ihre Berechtigung zum Abruf nachweisen, indem sie sich mit dem neuen Personalausweis (nPA) ausweisen. Bei Beratungen mit dem Betreiber dieses Portals, dem Zweckverband „Elektronische Verwaltung in Mecklenburg-Vorpommern“ (eGo-MV), haben wir im Sommer 2013 eine schwerwiegende Sicherheitslücke im Verfahren für das Personenstandswesen festgestellt, wodurch nicht sicher auszuschließen war, dass es bei unbefugter Nutzung des Verfahrens zu besonders schweren Auswirkungen kommen könnte.

Wir haben daraufhin den Zweckverband aufgefordert, die Missstände schnellstmöglich zu beseitigen und einen entsprechenden Zeitplan vorzulegen. Angesichts des großen Schadenspotenzials und weil ein datenschutzgerechter Zustand nicht in angemessener Zeit hergestellt werden konnte, haben wir das Verfahren wegen unzureichender technischer und organisatorischer Maßnahmen (§ 21 DSG M-V) gegenüber dem Zweckverband formell beanstandet.

Beim Personenstandswesen arbeiten die Kommunen mit dem Zweckverband „Elektronische Verwaltung in Mecklenburg-Vorpommern“ und der DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH (DVZ) in einem gemeinsamen Verfahren nach § 3 Abs. 10 DSG M-V zusammen (siehe Zehnter Tätigkeitsbericht, Punkt 4.4.4). Bei der Beratung von Lösungsalternativen für das beanstandete Verfahren haben wir erfahren, dass es in vielen Kommunen unseres Landes nach wie vor an elementaren Voraussetzungen für die Gewährleistung der Informationssicherheit und des technischen Datenschutzes mangelt. So sind zahlreiche Kommunen nicht in der Lage, kryptographische Zertifikate, die ein Grundelement für die Sicherstellung der Vertraulichkeit, Integrität und Authentizität der Daten in vielen Verfahren sind, ordnungsgemäß zu verwalten. Solche Zertifikate werden nach einer vorher festgelegten Zeit ungültig und müssen dann ersetzt werden. Oft werden die dazu nötigen Anträge nicht richtig oder nicht rechtzeitig gestellt. Sollten aber einmal Zertifikate auf Chipkarten oder Rechnern etwa durch einen Diebstahl in die Hände Unbefugter gelangen, müssen sie schnellstmöglich für ungültig erklärt und ersetzt werden. Wir haben hier Bedenken, dass ein solcher Prozess unter dem dann entstehenden hohen zeitlichen und finanziellen Druck nicht korrekt abgewickelt wird und somit personenbezogene Daten nicht mehr ausreichend geschützt sind.

Der hier beschriebene Einzelfall zeigt beispielhaft, dass elementare Anforderungen an die Informationssicherheit und den technischen Datenschutz im kommunalen Bereich unseres Landes vielfach immer noch nicht erfüllt werden. Bereits im Neunten Tätigkeitsbericht hatten wir im Ergebnis einer umfangreichen Untersuchung auf zahlreiche Datenschutzprobleme in den Kommunalverwaltungen hingewiesen (siehe Neunter Tätigkeitsbericht, Punkt 6). Es ist schon sehr bedenklich, dass offenbar nach wie vor keine angemessenen Konsequenzen gezogen wurden und die Kommunen mangels ausreichender Personal- und Finanzausstattung erhebliche Schwierigkeiten bei der Umsetzung der sicherheitstechnischen und datenschutzrechtlichen Anforderungen der neuen E-Government-Verfahren haben.

Auch von außen erhalten die Kommunen nur wenige Impulse, die zu einer Verbesserung der Lage führen könnten. So hat es der IT-Planungsrat abgelehnt, die „Leitlinie zur Informationssicherheit in der öffentlichen Verwaltung“ auch für die Kommunalverwaltungen verbindlich vorzuschreiben. Damit vergibt der IT-Planungsrat die Chance, die Kommunalverwaltungen zur Anwendung der Grundschutz-Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu verpflichten (siehe Punkt 4.3). Im eigenen Bundesland scheitern die dringend notwenigen Investitionen und Personalverstärkungen oftmals mit Verweis auf das Konnexitätsprinzip.

Wir empfehlen der Landesregierung, die Leitlinie zur Informationssicherheit auch für die Kommunalverwaltungen verbindlich vorzuschreiben und die Kommunen dabei zu unterstützen, eine angemessene Informationssicherheit und den erforderlichen Datenschutz zu gewährleisten. Dies gilt insbesondere für die Verarbeitung personenbezogener Daten in modernen E-Government-Verfahren.

6.5 Soziales

6.5.1 Schweigepflichtentbindungserklärung im Sozialbereich

Regelmäßig erreichen uns Anfragen zu Schweigepflichtentbindungserklärungen im Sozialbereich.

In einem Fall hat sich eine Mutter an uns gewandt, weil ihre Kinder aus dem Hort ein Formular mitgebracht hatten, auf dem die Eltern einer Schweigepflichtentbindungserklärung in allen Angelegenheiten auch Dritten gegenüber zustimmen sollten. Begründet wurde dies damit, dass die Einrichtung ein Intensivhort ist und man sich so mit der Grundschule schneller und unkompliziert über die Entwicklung der Kinder austauschen könnte. Da die Mutter Zweifel an der Rechtmäßigkeit der Schweigepflichtentbindungserklärung hatte, hat sie uns gebeten, diese datenschutzrechtlich zu prüfen.

Nach der Rechtsprechung muss eine Schweigepflichtentbindungserklärung hinreichend bestimmt sein, wenn damit ein Privatgeheimnis befugt offenbart werden soll. Diese Voraussetzung erfüllte diese Erklärung in mehrfacher Hinsicht nicht, da aus ihr nicht hervorging, wer gegenüber wem in welchem Umfang (kann zeitlich oder sachlich definiert werden) von der Verpflichtung befreit ist, das Privatgeheimnis zu wahren. Das Recht auf informationelle Selbstbestimmung fordert jedoch eine deutliche Transparenz für die Betroffenen bei der Verarbeitung ihrer Daten. Wenn, wie in der Formulierung des Hortes vorgesehen, unbestimmte Sachverhalte an unbestimmte Dritte weitergegeben werden sollen, liegt die Entscheidung, welche Daten für welchen Zweck in welcher Form an die Schule übermittelt werden, allein bei den Mitarbeiterinnen und Mitarbeitern der Einrichtung. Eine solche Einwilligungserklärung ist aus datenschutzrechtlicher Sicht nicht zulässig. Außerdem war fraglich, ob der Hort eine solche Schweigepflichtentbindung überhaupt benötigte.

Wenn der Hortbetreuung künftig ein besonderes pädagogisches Konzept zugrunde liegen soll, kommt es vielmehr darauf an, dass dieses den Eltern vermittelt wird und sie in Kenntnis des Konzeptes der Hortbetreuung durch den zu schließenden Vertrag zustimmen. Wenn die Eltern dieses besondere pädagogische Konzept akzeptiert haben, könnte der gebotene Unterrichtsstoff beispielsweise während der Hortbetreuung durch individuelle Übungen vertieft werden, über die sich die Lehrerinnen und Lehrer und die Erzieherinnen und Erzieher des Hortes austauschen könnten.

Wir haben der Petentin empfohlen, unsere datenschutzrechtlichen Hinweise mit dem Hort zu besprechen. Sollte sie keinen Erfolg haben, haben wir ihr unsere Unterstützung angeboten. Da sie sich nicht erneut an uns gewandt hat, gehen wir davon aus, dass das Gespräch erfolgreich war.

In einem anderen Fall hatte ein Jugendamt eine Schweigepflichtentbindungserklärung erarbeitet, um die Zusammenarbeit mit den Tagesmüttern zu verbessern. Wir wurden gebeten, diese Erklärung datenschutzrechtlich zu prüfen.

Auch hier sollten mit einer Einwilligungserklärung sehr unterschiedliche Zwecke abgedeckt werden. Dies bedeutete unter anderem, dass die für den jeweiligen Einzelfall erforderlichen personenbezogenen Daten der Tagespflegepersonen sehr unterschiedlich sein können. Das Recht auf informationelle Selbstbestimmung fordert jedoch eine deutliche Transparenz für die Betroffenen bei der Verarbeitung ihrer Daten. Nur wenn die betroffenen Personen Kenntnis darüber haben, wer was über sie weiß, können sie ihr Recht auf informationelle Selbstbestimmung wahrnehmen. Eine Schweigepflichtentbindungserklärung ist jedoch unwirksam, wenn die bzw. der Einwilligende Zweck, Art und Umfang der geplanten Datenverarbeitung nicht abschätzen kann. In dem Entwurf wurden die Betroffenen zwar auch darüber aufgeklärt, dass sie ihre Einwilligung jederzeit widerrufen können, aber es fehlten Hinweise dazu, welche Stelle den Widerruf entgegennimmt, welche Folgen eintreten, wenn die Einwilligung verweigert wird, und wie der Widerruf umgesetzt wird, zum Beispiel durch Löschung der Daten.

Daher haben wir dem Jugendamt empfohlen, die Schweigepflichtentbindungserklärung entsprechend zu präzisieren.

6.5.2 Fragen zum SGB II - Arbeitslosengeld II

Nach wie vor fragen uns viele Antragstellerinnen und Antragsteller oder Bezieherinnen und Bezieher von Leistungen nach dem Sozialgesetzbuch Zweites Buch (SGB II - Arbeitslosengeld II), zu welchen Angaben sie gegenüber dem Jobcenter verpflichtet sind. Häufig können diese Anfragen und Beschwerden von unserer Behörde nicht bearbeitet werden, weil der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) zuständig ist. Für Bürgerinnen und Bürger ist die Zuständigkeit oft schwer erkennbar, weil die Bezeichnung „Jobcenter“ sowohl für Stellen verwendet wird, die der Aufsicht des BfDI unterliegen, als auch für Stellen, die unserer Aufsicht unterliegen (vgl. § 6d SGB II).

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern ist für die sogenannten Optionskommunen in Mecklenburg-Vorpommern zuständig. Dies sind das Jobcenter des Landkreises Vorpommern-Rügen sowie das Jobcenter des Landkreises Mecklenburgische Seenplatte für das Gebiet des ehemaligen Landkreises Mecklenburg-Strelitz.

Im Folgenden möchten wir einige Beispiele der bei uns eingegangenen Petitionen schildern:

1. Technisch-organisatorische Maßnahmen

In einem Fall informierte uns ein Petent darüber, dass er bei einer Mitarbeiterin des Jobcenters Unterlagen abgeben wollte. Von der Mitarbeiterin wurde er dann gebeten, diese in den Briefkasten des Jobcenters zu werfen. Bei dem Briefkasten handelte es sich um einen schlichten Pappkarton, der mit einer großen Einwurföffnung versehen war. Da sich der Briefkasten in der für die Öffentlichkeit zugänglichen Wartezone befand und keiner erkennbaren Aufsicht oder Kontrolle des Personals des Jobcenters unterlag, bat der Petent uns um Unterstützung.

Die Sozialleistungsträger haben gemäß § 78a Sozialgesetzbuch Zehntes Buch (SGB X) die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um unter anderem die Daten vor dem Zugriff Dritter zu schützen. Wir haben das Jobcenter gebeten, sich dieses Problems anzunehmen.

Aufgrund unseres Hinweises hat die Datenschutzbeauftragte des Jobcenters diese unbefriedigende Situation umgehend behoben. Für die Kundinnen und Kunden steht nun ein verschlossener handelsüblicher Postbriefkasten zur Verfügung, in den sie ihre Unterlagen einwerfen können. Außerdem haben sie die Möglichkeit, diese persönlich im Jobcenter abzugeben.

2. Umgang mit eingehender Post

Aber auch behördliche Datenschutzbeauftragte wenden sich an uns, wenn sie Fragen zum Umgang mit Sozialdaten haben. So sollte in einem Landkreis der Umgang mit der eingehenden Post in einer Dienstvereinbarung geregelt werden. Dabei ist die Frage aufgetreten, ob das in § 35 Sozialgesetzbuch Erstes Buch (SGB I) normierte Sozialgeheimnis auch innerhalb des Leistungsträgers zu wahren ist.

Das Sozialgeheimnis verpflichtet die Sozialleistungsträger sowohl gegenüber Dritten als auch gegenüber den bei den Stellen Beschäftigten, Sozialdaten durch positive Vorkehrungen vor der Kenntnisnahme Dritter zu schützen (§ 35 Abs. 1 Satz 2 und 3 SGB I). Hilfesuchende vertrauen darauf, dass ihre Sozialdaten, wozu auch schon der Name in Verbindung mit einer Sozialleistung gehört, geheimgehalten werden. § 35 SGB I begründet insoweit eine besondere Fürsorgepflicht, der vor allem durch personelle sowie organisatorische und technische Maßnahmen Rechnung zu tragen ist. Das bedeutet auch, dass Maßnahmen zu ergreifen sind, die geeignet und erforderlich sind, um zu verhindern, dass Sozialdaten von Unbefugten zur Kenntnis genommen werden können. Der erforderliche Aufwand richtet sich nach dem Grundsatz der Verhältnismäßigkeit und muss in einem angemessenen Verhältnis zum Grad der Schutzbedürftigkeit und der Gefährdung der Sozialdaten stehen.

Es ist anzunehmen, dass der Absender bei der Adressierung regelmäßig davon ausgeht, dass sein an eine Stelle gerichteter Brief nach den dortigen Postgepflogenheiten behandelt wird, um dann intern an den Erstadressaten weitergeleitet zu werden. Zu den üblichen Gepflogenheiten von Behörden oder Stellen gehört es aber, dass die dort eingehende Post auf der zuständigen Poststelle geöffnet und mit einem Eingangsstempel versehen wird. Es darf vorausgesetzt werden, dass dies dem Absender bekannt ist. Die Bestimmung, ob ein Brief „vertraulich“ oder „persönlich“ ist, trifft somit der Absender.

Wir haben daher empfohlen, dass, sofern die Eingangspost als Sozialangelegenheit gekennzeichnet ist, diese ungeöffnet an den Adressaten weiterzuleiten ist. Fehlen solche Angaben, darf die Post geöffnet werden. Durch organisatorische Regelungen sollte dann aber bestimmt werden, dass sie dann direkt an das zuständige Amt weitergeleitet wird.

3. Umgang mit Kontoauszügen durch die Jobcenter bei der Beantragung von Sozialleistungen

Im Berichtszeitraum wurden wir von Antragstellerinnen und Antragstellern auch zur Zulässigkeit der Vorlage von Kontoauszügen bei der Beantragung von Sozialleistungen befragt sowie dazu, welche Angaben für die Aufgabenerfüllung der Jobcenter erforderlich sind.

In der Regel verlangen die Jobcenter von den Antragstellerinnen und Antragstellern Kontoauszüge, um sich ein Bild über deren finanzielle Verhältnisse zu verschaffen. Lange Zeit war umstritten, ob und unter welchen Voraussetzungen dies zulässig ist, insbesondere ob ein konkreter Verdacht auf Leistungsmissbrauch vorliegen muss, bevor die Kontoauszüge verlangt werden. Mittlerweile hat das Bundessozialgericht in zwei Entscheidungen (Urteil vom 19. September 2008, Az. B 14 AS 45/07 R, und Urteil vom 19. Februar 2009, Az. B 4 AS 10/08 R) für mehr Klarheit gesorgt: Danach ist die Anforderung der Kontoauszüge jedenfalls der letzten drei Monate bei der Beantragung von Leistungen nach dem Sozialgesetzbuch Zweites Buch (SGB II) auch ohne konkreten Verdacht des Leistungsmissbrauchs zulässig. Die Pflicht, Kontoauszüge vorzulegen, gilt allerdings nicht in vollem Umfang für die Ausgabenseite, das heißt für die Frage, wofür Antragsteller/innen ihre Mittel verwenden. Eine Einschränkung ergibt sich hier vor allem für besondere Arten personenbezogener Daten. Dies sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Geschützt ist die Geheimhaltung des Verwendungszwecks bzw. des Empfängers der Überweisung. Dementsprechend dürfen etwa Angaben über Gewerkschaftsbeiträge, Spenden an Kirchen oder an politische Parteien hinsichtlich des Empfängers, nicht aber der Höhe, ohne weiteres geschwärzt werden. Lediglich für den Fall, dass sich aus den insoweit geschwärzten Kontoauszügen ergibt, dass in auffälliger Häufung oder hohe Beträge überwiesen werden, ist nach Auffassung des Bundessozialgerichts im Einzelfall zu entscheiden, inwieweit ausnahmsweise doch eine Offenlegung auch des bislang geschwärzten Adressaten gefordert werden kann. Die Jobcenter müssen die Antragstellerinnen und Antragsteller darauf hinweisen, dass sie die Adressaten auf der Ausgabenseite der Kontoauszüge schwärzen können.

Wir möchten daher auch noch einmal auf die von den Landesbeauftragten für den Datenschutz der Länder Berlin, Brandenburg, Hamburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und Schleswig Holstein herausgegebenen Hinweise zur datenschutzgerechten Ausgestaltung der Anforderungen von Kontoauszügen bei der Beantragung von Sozialleistungen aufmerksam machen, die in unserem Internetangebot unter www.datenschutz-mv.de unter Datenschutz/Publikationen zu finden sind.

6.5.3 Unzulässige Übermittlung von Sozialdaten

Ein Petent teilte uns mit, dass er durch das Gericht zum Betreuer bestellt sei. In dieser Tätigkeit hatte er sich an das Veterinär- und Lebensmittelüberwachungsamt des Landkreises gewandt, weil die Wohnung der durch ihn zu betreuenden Person, die darin allein mit Haustieren lebt, in einem sehr unhygienischen Zustand war. Es sollte daher geprüft werden, ob die Haustiere in der Wohnung artgerecht gehalten werden. Der Petent war dann allerdings überrascht, dass das Amt zwischenzeitlich ohne seine Kenntnis und Einwilligung Daten aus der Betreuungsangelegenheit an das Jugendamt sowie Fotos der Wohnung an das Gesundheitsamt übermittelt hatte. Er bat uns, den Sachverhalt datenschutzrechtlich zu prüfen.

Wir haben den Landkreis um die Angabe der Rechtsgrundlagen für diese Datenübermittlungen gebeten. Der Landkreis nannte in seiner Stellungnahme keine Rechtsgrundlagen, führte aber aus, dass die Gesundheit der betroffenen Person gegenüber dem Datenschutz als höheres Rechtsgut anzusehen sei. Auch, wenn man hier beste Absichten des Veterinär- und Lebensmittelüberwachungsamtes annimmt, kann auf eine solche pauschale Aussage alleine keine rechtmäßige Datenübermittlung gestützt werden. Eine Übermittlung personenbezogener Daten ist nur zulässig, wenn eine Rechtsvorschrift dies zulässt oder zwingend vorschreibt oder wenn die Betroffene/der Betroffene eingewilligt hat.

Für die betroffene Person war durch ein Gericht ein Betreuer mit einem umfassenden Sorgeauftrag bestellt. In einem solchen Fall tritt der Betreuer an die Stelle der zu betreuenden Person, das heißt, alle Maßnahmen, zu denen sonst die Einwilligung oder Zustimmung der betroffenen Person erforderlich wäre, müssen mit dem Betreuer abgestimmt werden. Der Betreuer kann folglich auch, sofern keine gesetzliche Norm für die Datenübermittlung besteht, eine entsprechende Einwilligung erteilen, die den Bestimmungen des § 8 Landesdatenschutzgesetz (DSG M-V) entsprechen muss. Wenn der Betreuer nicht erreichbar und sofortiges Handeln angezeigt ist, muss geprüft werden, aufgrund welcher Rechtsvorschrift personenbezogene Daten an andere öffentliche Stellen übermittelt werden können. Nach den allgemeinen datenschutzrechtlichen Bestimmungen in § 14 DSG M-V ist eine Übermittlung an Stellen innerhalb des öffentlichen Bereiches unter anderem zulässig, wenn die Nutzung der Daten zu einer in der Zuständigkeit des Empfängers liegenden Aufgabe erforderlich und nach § 10 DSG M-V zulässig ist.

Für die Übermittlung der Daten und Fotos an das Gesundheitsamt hätte daher geprüft werden müssen, ob die Übermittlung zur Aufgabenerfüllung des Gesundheitsamtes erforderlich ist. Die Aufgaben des Gesundheitsamtes sind im Gesetz über den Öffentlichen Gesundheitsdienst (ÖGDG M-V) festgeschrieben. Sofern die gesetzlichen Voraussetzungen nicht erfüllt sind, ist auch eine Datenübermittlung nach § 14 DSG M-V nicht erforderlich und damit unzulässig.

Es ist allerdings auch nachvollziehbar, dass nicht jede öffentliche Stelle/Behörde die Handlungsmöglichkeiten des Gesundheitsamtes kennt; deswegen sollte vor einer Übermittlung personenbezogener Daten der Fall dem Amt anonym geschildert und nach den Handlungsmöglichkeiten gefragt werden. Sofern das Gesundheitsamt eine Handlungsmöglichkeit sieht, könnte die Übermittlung auf § 14 DSG M-V gestützt werden.

In Bezug auf die Datenübermittlung an das Jugendamt haben wir dem Landkreis mitgeteilt, dass eine solche Datenübermittlung zulässig sein kann, wenn Kenntnisse oder tatsächliche Anhaltspunkte dafür vorliegen, dass sich in der Wohnung der zu betreuenden Person regelmäßig ein Kind aufhält. Ist das nicht der Fall, ist eine Datenübermittlung nicht erforderlich und damit unzulässig. Im Übrigen besteht auch hier die Möglichkeit, dass vor einer Datenübermittlung der Fall dem Jugendamt anonym geschildert und um dessen fachliche Beratung gebeten wird. Das Jugendamt könnte dann gegebenenfalls auf der Grundlage von § 8a Sozialgesetzbuch Achtes Buch (SGB VIII) tätig werden.

Im Ergebnis wurde mit dem Landkreis hinsichtlich der Rechtseinschätzung Einvernehmen hergestellt. Um künftig eine unrechtmäßige Weitergabe von Sozialdaten auszuschließen, wurden alle Mitarbeiterinnen und Mitarbeiter des entsprechenden Fachbereiches zum Datenschutz geschult.

6.5.4 Projekt „Kita-Verwaltung-Online“

Im Berichtszeitraum wurde uns das Projekt „Kita-Verwaltung-Online“ vorgestellt verbunden mit der Bitte, zu den wesentlichen datenschutzrechtlichen Voraussetzungen für die Realisierung dieses Projektes Stellung zu nehmen.

Da in den künftigen Verfahren auch personenbezogene Daten verarbeitet werden sollen, haben wir im Rahmen einer ersten Beratung auf folgende datenschutzrechtliche Schwerpunkte hingewiesen:

Bei der Umsetzung des Projektes haben die Jugendämter bei der Verarbeitung von Sozialdaten insbesondere die Vorschriften des § 35 Sozialgesetzbuch Erstes Buch (SGB I) sowie die Bestimmungen der §§ 61 bis 68 Sozialgesetzbuch Achtes Buch (SGB VIII) sowie der §§ 67 bis 85a Sozialgesetzbuch Zehntes Buch (SGB X) zu beachten. Darüber hinaus haben die Jugendämter bei der Inanspruchnahme von Einrichtungen und Diensten der Träger der freien Jugendhilfe den Schutz der personenbezogenen Daten bei der Erhebung und Verwendung in einer den Bestimmungen des Sozialgesetzbuches entsprechenden Weise zu gewährleisten, § 61 Abs. 3 SGB VIII. Da die Förderung von Kindern in Kindertageseinrichtungen und in der Kindertagespflege eine Aufgabe der öffentlichen Jugendhilfe ist, haben die öffentlichen Träger der Jugendhilfe die Einhaltung der Bestimmungen des Sozialdatenschutzes bei den freien Trägern zu gewährleisten. Nach unserer Auffassung sollten deswegen zwischen den öffentlichen Trägern und den freien Trägern Vereinbarungen geschlossen werden, die eine den Bestimmungen des Sozialgesetzbuches entsprechende Datenverarbeitung gewährleisten.

Außerdem enthält das Sozialgesetzbuch keine gesetzlichen Bestimmungen zur gemeinsamen Datenverarbeitung durch öffentliche und freie Träger. Dies ist aber ein wesentlicher Bestandteil des künftig in Kommunen des Landes einzusetzenden Verfahrens. Die personenbezogenen Daten können somit nur auf der Basis einer Einwilligung gemeinsam durch öffentliche und freie Träger verarbeitet werden.

Die Einwilligung muss die Voraussetzungen des § 67b Abs. 2 SGB X erfüllen. Insbesondere unterliegt sie der freien Entscheidung der Betroffenen, hier also der Eltern bzw. des oder der Personensorgeberechtigten, was auch zur Folge hat, dass sie jederzeit von den Betroffenen widerrufen werden kann. Eine Einwilligung setzt darüber hinaus voraus, dass die Betroffenen auf den Zweck der vorgesehenen Verarbeitung und Nutzung der Daten sowie auf die Folgen der Verweigerung der Einwilligung hingewiesen werden. Wir haben empfohlen, die Betroffenen darüber aufzuklären, welche Daten für welchen Zweck erhoben und wie sie verarbeitet werden. Darüber hinaus sollte die Einwilligung auch vom Jugendamt für die Dauer der Teilnahme der Eltern bzw. des oder der Personensorgeberechtigten an dem Verfahren aufbewahrt werden.

Außerdem sind bei dem Projekt auch die Vorgaben des § 36a SGB I hinsichtlich der elektronischen Kommunikation zu erfüllen. Deswegen sollte im Verfahren festgelegt werden, wie die Freischaltung des Benutzerkontos erfolgen soll. Des Weiteren sollten die zu treffenden Maßnahmen beschrieben werden, die bei einem Widerruf der Einwilligung zu treffen sind. Ab dem Widerruf darf nach unserer Auffassung jede Stelle die Daten nur für ihre Zwecke verarbeiten. Sofern Daten an die jeweils andere Stelle zu übermitteln sind, ist dafür eine Rechtsgrundlage oder die Einwilligung der Betroffenen erforderlich. In diesem Zusammenhang haben wir auch vorgeschlagen, für das gesamte automatisierte Verfahren ein Sicherheitskonzept zu erstellen, das die gesamte Datenverarbeitung zwischen den Clients der externen und internen Nutzer, der entsprechenden Netzinfrastrukturen, des Onlineportals, des Applikationsservers und des Datenservers umfasst. Für die Erstellung eines solch umfassenden Konzeptes haben wir die Grundschutzmethodik des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) empfohlen.

Im Rahmen der Beratung haben wir darum gebeten, uns über das Projekt auf dem Laufenden zu halten, und unsere weitere Unterstützung für die Entwicklung des Projektes angeboten.

6.6 Gesundheitswesen

6.6.1 Datenschutz in der Arztpraxis

Mein Arzt macht ein Foto von mir - ist das datenschutzrechtlich zulässig?
Im Berichtszeitraum haben uns auch verschiedene Anfragen zum Umgang mit Patientendaten bei niedergelassenen Ärztinnen und Ärzten erreicht. So hat uns ein Versicherter mitgeteilt, dass er beim Besuch einer HNO-Arztpraxis fotografiert worden ist und dieses Foto in der ärztlichen Dokumentation gespeichert wurde. Er wollte nun wissen, was er unternehmen kann, damit dieses Foto wieder gelöscht wird.

Den Versicherten haben wir darüber informiert, dass der Arzt ein Porträtfoto nur speichern darf, wenn dies für ein Vertragsverhältnis erforderlich ist und keine anderen, weniger in die Persönlichkeitsrechte eingreifenden, Maßnahmen den Zweck erfüllen.

Da der Versicherte jedoch mit der Chipkarte auch seinen Personalausweis vorlegen musste, konnte sich das ärztliche Personal anhand dieser Dokumente von seiner Identität überzeugen. Es war somit auch nicht erforderlich, das Foto ohne seine Einwilligung in der Dokumentation zu speichern. Weil das Vertragsverhältnis erfüllt werden konnte, ohne das Foto zu speichern, und außerdem keine Rechtsgrundlage, die eine Speicherung des Fotos erlaubt hätte, ersichtlich war, hätte das Foto nur mit der Einwilligung des Versicherten gespeichert werden dürfen. Da diese Einwilligung jedoch nicht vorlag, war die Speicherung des Fotos unzulässig.

Gemäß § 35 Abs. 2 Bundesdatenschutzgesetz (BDSG) sind unzulässig gespeicherte personenbezogene Daten zu löschen, sodass wir dem Versicherten empfohlen haben, sich mit unserer Begründung an den Arzt zu wenden und eine Löschung seines Fotos zu verlangen. Sofern der Arzt seiner Bitte nicht entsprechen sollte, haben wir ihm unsere Unterstützung angeboten. Da er sich nicht wieder bei uns gemeldet hat, gehen wir davon aus, dass der Arzt seinem Anliegen nachgekommen ist.

Darf ich Patientenunterlagen per Telefax übersenden?

Auch Arztpraxen haben sich mit Fragen an uns gewandt. So informierte uns beispielsweise ein Facharzt, dass er von Hausärztinnen/Hausärzten immer wieder aufgefordert wird, OP-Berichte/Befunde oder andere Patientenunterlagen per Telefax zu übersenden. Dies hat er, nach Rücksprache mit uns, bisher immer aus datenschutzrechtlichen Gründen abgelehnt. Inzwischen hat sich eine Hausärztin hierzu an die Kassenärztliche Vereinigung (KV MV) gewandt und die Auskunft erhalten, dass das Faxen von Patientenunterlagen unproblematisch sei und es ähnlich wie eine Kopie anzusehen ist. Der Facharzt wollte nun von uns wissen, wie die aktuelle Rechtslage ist.

Eine Rechtsvorschrift, die die Übermittlung von Patientenunterlagen per Telefax ausdrücklich untersagt, gibt es nicht. Nach den Bestimmungen des § 73 Abs. 1b Sozialgesetzbuch Fünftes Buch (SGB V) dürfen Patientenbefunde an eine Hausärztin/einen Hausarzt nur mit schriftlicher Einwilligung der Versicherten, die widerrufen werden kann, übermittelt werden. Wenn die Übermittlung nicht zeitkritisch ist, also keine Gefahr für Leib und Leben der Patienten besteht, sollten Befunde aus datenschutzrechtlicher Sicht bevorzugt per Briefpost übermittelt werden. Eine Übermittlung per Telefax enthält Risiken hinsichtlich der Vertraulichkeit der zu übermittelnden Daten. Dies haben wir in einer Orientierungshilfe „Datenschutz und Telefax“ dargestellt, die in unserem Internetangebot unter www.datenschutz-mv.de zu finden ist. Darin ist auch beschrieben, dass medizinische Daten nur ausnahmsweise und wenn, dann unter Einhaltung zusätzlicher Sicherheitsvorkehrungen, übermittelt werden sollten. Außerdem besteht nach unserer Kenntnis die Möglichkeit, vertrauliche medizinische Daten sicher über das KV-Safenet[1] an andere Ärztinnen und Ärzte zu übermitteln.

Wir haben auch die Kassenärztliche Vereinigung Mecklenburg-Vorpommern über diese Anfrage und unsere rechtliche Bewertung informiert. Die KV MV teilt unsere Rechtsauffassung und hat unsere Schreiben zum Anlass genommen, die Mitarbeiterinnen und Mitarbeiter auf die mit der Übermittlung von Patientendaten per Telefax verbundenen Risiken hinzuweisen.

1 Sicheres, vom Internet getrenntes Netz für eine datenschutzgerechte und sichere Übertragung von Patientendaten; nutzt moderne kryptographische Verfahren für die Verschlüsselung.

Dass die Gefahren der Verletzung der Vertraulichkeit bei einer Übermittlung von Patientendaten per Telefax nicht nur theoretisch bestehen, sondern eine reale Gefahr sind, zeigt ein Beispiel aus unserer Praxis. So ist im Oktober 1995 in unserer Dienststelle ein Telefax eingegangen, mit dem ein umfangreicher Diagnose- und Befundbericht übermittelt wurde. Beim Versenden ist eine falsche Telefaxnummer eingegeben worden, sodass das Telefax beim Anschluss unserer Dienststelle aufgelaufen ist (siehe Zweiter Tätigkeitsbericht, Punkt 2.12.10).

6.6.2 Zentrales klinisches Krebsregister in Mecklenburg-Vorpommern

Im Zehnten Tätigkeitsbericht (siehe Punkt 3.3.4 sowie Punkt 5.9.2) haben wir darüber informiert, dass die Landesregierung das Ziel verfolgt, die in den vier regionalen Klinischen Krebsregistern (KKR - Greifswald, Neubrandenburg, Rostock und Schwerin) gespeicherten Daten zu einem Zentralen Klinischen Krebsregister (ZKKR) zusammenzuführen. Mit dem Gesetz über das Zentrale Klinische Krebsregister (Klinisches Krebsregistergesetz - KlinKrebsRG M-V) vom 6. Juli 2011 wurde in Mecklenburg-Vorpommern die rechtliche Voraussetzung für den Aufbau eines Zentralen Klinischen Krebsregisters geschaffen.

Mit der Verordnung zur Bestimmung der Errichtung nach dem Klinischen Krebsregistergesetz Mecklenburg-Vorpommern vom 15. Februar 2013 wurde das Institut für Community Medicine der Universitätsmedizin Greifswald als Einrichtung bestimmt, die sowohl das ZKKR als auch die Treuhandstelle führt. Zu den Hauptaufgaben des Zentralen Klinischen Krebsregisters gehören die registerübergreifende Qualitäts- und Vollständigkeitssicherung der Daten der regionalen Klinischen Krebsregister sowie die registerübergreifende Datenauswertung zu onkologisch relevanten Fragestellungen. Ziel der Auswertung ist es, den Erfolg von Tumortherapien einzuschätzen und zu verbessern, um damit auch die Entscheidung für oder gegen bestimmte Behandlungen zu erleichtern.

Die regionalen KKR sind nach den Bestimmungen des KlinKrebsRG M-V verpflichtet, die bei ihnen erfassten Behandlungsdaten (Identitätsdaten der Patientinnen und Patienten sowie die klinischen Daten) sowohl an die Treuhandstelle als auch an das ZKKR zu übermitteln. Um den Schutz der Patientendaten zu gewährleisten, übermitteln die regionalen KKR zunächst die Identitätsdaten der Patientinnen und Patienten (wie Name, Vorname, Anschrift, Geburtsdatum) an die Treuhandstelle, die aus diesen Angaben ein Pseudonym[2] bildet. Dieses Pseudonym wird von der Treuhandstelle an die KKR übermittelt und dort mit den klinischen Daten der Patientinnen und Patienten verknüpft. Dieser zusammengefasste pseudonyme Datensatz wird dann an das ZKKR übermittelt. Damit ist es dem ZKKR nicht möglich, anhand der dort vorliegenden Daten einen Bezug zu einer bestimmten Patientin bzw. einem bestimmten Patienten herzustellen.

Um die in diesem Zusammenhang anstehenden datenschutzrechtlichen Fragen zu klären, haben wir uns im August 2013 mit den Mitarbeiterinnen und Mitarbeitern des ZKKR beraten.

[2] Bei einer Pseudonymisierung werden die genannten Identifikationsmerkmale durch ein Kennzeichen ersetzt, welches es Dritten unmöglich macht oder wesentlich erschwert, diese Daten einer Patientin/einem Patienten zuzuordnen.

Diese sahen ein Hauptproblem darin, dass der Datenbestand im ZKKR nicht aktuell ist. Außerdem gaben sie zu bedenken, dass Patientinnen und Patienten in den Registern doppelt erscheinen könnten, da die Tumorerkrankung zum Beispiel in Rostock festgestellt wurde, die weitere Behandlung dann aber in Wismar erfolgt. Somit besteht die Möglichkeit, dass dieser Fall sowohl in der Meldung des KKR Rostock als auch in der des KKR Schwerin erscheint. Darüber hinaus sieht das Klinische Krebsregistergesetz Mecklenburg-Vorpommern vor, dass nur einmal im Jahr ein Abgleich mit den Daten der Melderegister erfolgt. Dieser Zeitraum erscheint den Mitarbeiterinnen und Mitarbeitern des ZKKR zu lang, da Patientinnen oder Patienten inzwischen verstorben oder umgezogen sein könnten.

Um Doppelerfassung zu vermeiden, haben wir vorgeschlagen, die Daten aus den verschiedenen Registern mit Hilfe eines (eindeutigen) Pseudonyms zusammenzuführen. Entscheidend ist aus datenschutzrechtlicher Sicht, dass keine Zwischenwerte gebildet werden, aus denen Rückschlüsse auf Identitätsdaten möglich sind. Auf der 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 13. und 14. März 2013 in Bremerhaven wurde hierzu die Entschließung „Pseudonymisierung von Krebsregisterdaten verbessern“ verabschiedet, die in unserem Internetangebot zu finden ist.

Da es eine gesetzliche Meldepflicht gibt, haben wir empfohlen, das Verfahren aus datenschutzrechtlicher Sicht für die Patientinnen und Patienten transparent zu gestalten. Den Patientinnen und Patienten sollte ein Informationsblatt ausgehändigt werden, in dem sie über Inhalt, Umfang und Zweck der Meldung sowie auch darüber aufgeklärt werden, dass sie das Recht haben, der Übermittlung ihrer Daten zu widersprechen. Der Widerspruch sollte dann in der Patientenakte bei der behandelnden Ärztin bzw. bei dem behandelnden Arzt bzw. dem Krankenhaus aufbewahrt werden. Die Mitarbeiterinnen und Mitarbeiter des ZKKR haben stattdessen vorgeschlagen, den Widerspruch bei der Treuhandstelle zu speichern. Patientinnen und Patienten brauchen dann nur gegenüber einer Stelle widersprechen. Der Widerspruch würde dann bei allen folgenden Meldungen automatisch berücksichtigt werden können.

Die Errichtung des Zentralen Klinischen Krebsregisters in Mecklenburg-Vorpommern werden wir auch weiterhin datenschutzrechtlich begleiten.

6.6.3 Clearingstelle der Apothekerverbände

Im Rahmen des länderübergreifenden Fachaustausches erfuhren wir von der Planung der Apotheken, eine externe Clearingstelle mit der Prüfung von Rezepten für Hilfsmittel, Medizinprodukte, Diätetika etc. zu beauftragen. Da die Clearingstelle bei den Apothekerverbänden eingerichtet werden sollte, haben wir uns mit dem Apothekerverband Mecklenburg-Vorpommern beraten.

Die Vertreter des Verbandes schilderten, dass gesetzlich Versicherten oftmals vorgegeben werde, von welchem Hersteller sie ein benötigtes Medikament oder Hilfsmittel erhalten sollen. Dies sei damit begründet, dass Krankenkassen Rabattvereinbarungen mit einzelnen Pharmaunternehmen treffen, um auf diese Weise die Kosten zu senken. Derzeit gibt es ca. 200 Krankenkassen mit jeweils eigenen Vertragsinhalten, sodass für ein Medikament oder Hilfsmittel zum Teil sehr unterschiedliche Preise bestehen.

Die Apotheken übernehmen für ihre Kundinnen und Kunden die Prüfung, welche Krankenkasse welches Medikament/welches Hilfsmittel von welchem Hersteller bezahlt. Aufgrund der Vielzahl der Krankenkassen und da die Apotheken auch nicht mit jeder Krankenkasse eine Vertragsbeziehung haben, war diese Prüfung für viele Apotheken offenbar nicht mehr handhabbar. Aus diesem Grund übernahm die Clearingstelle der Apothekerverbände diese Aufgabe. Zu diesem Zweck übersenden die Apotheken der Clearingstelle das Rezept/die Verordnung mit den Versicherten- und Arztdaten per Telefax. Die Clearingstelle prüft dann, ob das Medikament/das Hilfsmittel genehmigungspflichtig ist, und wenn ja, nimmt sie Kontakt zu der zuständigen Krankenkasse hinsichtlich der Kostenübernahme auf.

Es war zu klären, auf welche Rechtsgrundlage die nicht anonymisierte Übermittlung der Rezeptdaten von den Apotheken an die Clearingstelle gestützt werden kann. Dabei war zu berücksichtigen, dass die Apotheken neben dem allgemeinen Datenschutzrecht auch ihre besondere berufliche Schweigepflicht (§ 203 Strafgesetzbuch) zu beachten haben. Die Frage nach der Rechtsgrundlage konnte nicht zufriedenstellend geklärt werden, sodass für die Übermittlung der personenbezogenen Daten an die Clearingstelle die informierte und freiwillige Einwilligung der betroffenen Versicherten (Kundinnen/Kunden) einzuholen war. Sofern keine Einwilligung vorliegt, dürfen die Rezeptdaten nur übermittelt werden, wenn sie zuvor ausreichend pseudonymisiert werden. Eine Pseudonymisierung der Versichertendaten kam jedoch nicht in Betracht, da die Krankenkassen anhand der personenbezogenen Daten auch prüfen, ob das Medikament/das Hilfsmittel nicht bereits durch eine andere Ärztin oder einen anderen Arzt verordnet wurde.

Wir haben den Apothekerverband daher aufgefordert, die Arbeit der Clearingstelle auf ein datenschutzgerechtes Verfahren umzustellen und für die Übermittlung der Rezepte/Hilfsmittelverordnungen die Einwilligung der Versicherten einzuholen. Des Weiteren haben wir darauf hingewiesen, dass die Übermittlung von Versicherten- und Arztdaten auf Rezepten und Hilfsmittelverordnungen mittels Telefax aus datenschutzrechtlicher Sicht bedenklich ist, da die Kenntnisnahme der Daten durch unbefugte Dritte nicht ausgeschlossen werden kann. Wir haben daher die Prüfung des Anschlusses der Apotheken an das KV-Safenet vorgeschlagen.

Aufgrund unserer Empfehlungen entwarf der Apothekerverband eine Einwilligungserklärung, die von den Versicherten zu unterzeichnen ist und in der über das Verfahren aufgeklärt wird. Allerdings stellt sich zwischenzeitlich erneut die Frage der Erforderlichkeit der Clearingstelle, da offenbar beabsichtigt ist, jede Apothekensoftware um Informationen zu den für die einzelne Apotheke geltenden Verträgen zu ergänzen.

6.6.4 Pseudonymisierung im gemeinsamen Krebsregister

Das Gesetz über Krebsregister (KRG) in Verbindung mit dem Staatsvertrag ist seit dem Jahr 1995 die gesetzliche Basis für ein gemeinsames Krebsregister der neuen Bundesländer und Berlin (GKR). Im gemeinsamen Krebsregister werden bevölkerungsbezogen (epidemiologisch) Daten über das Auftreten und die Häufigkeit von Krebserkrankungen in definierten Erfassungsgebieten erhoben, gespeichert, verarbeitet, analysiert und interpretiert. Es bietet somit eine wertvolle Grundlage, um noch mehr über Ursachen und Entwicklung von Krebskrankheiten herauszufinden.

Da es sich bei den erhobenen Daten um sehr sensible Gesundheitsdaten handelt, hat der Gesetzgeber entsprechende Regelungen vorgesehen, um die Betroffenen vor einer Verletzung ihres Rechts auf informationelle Selbstbestimmung zu schützen. Besonders wichtig ist dabei, dass Identitätsdaten getrennt von den medizinischen Daten gespeichert werden. Für diesen Zweck werden sogenannte Pseudonymisierungsverfahren genutzt. Unsere Berliner Kollegen stellten bei einer Kontrolle des gemeinsamen Krebsregisters jedoch fest, dass die Sicherheitsvorkehrungen zum Schutz der Privatsphäre der Patientinnen und Patienten nicht ausreichend waren. So entsprachen die Verfahren zur Pseudonymisierung und zur Verschlüsselung der Identitätsdaten der Patientinnen und Patienten vor ihrer Speicherung in der Registerstelle nicht mehr dem Stand der Technik.

Die klinischen und epidemiologischen Krebsregister der Länder und das Zentrum für Krebsregisterdaten unterliegen der Kontrolle der jeweils regional zuständigen Landesbeauftragten für den Datenschutz. Durch Abstimmung in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) sollen bundesweit einheitliche datenschutzrechtliche Anforderungen an den Betrieb der Krebsregister formuliert werden. Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ (AK Technik, siehe auch Punkt 7) hat die DSK auch in diesem Fall zu datenschutztechnischen Fragen beraten. Dazu war es erforderlich, die technischen Details mit den zuständigen Gremien detailliert zu erörtern. Gesprächspartner waren insbesondere das Bundesministerium für Gesundheit und die Gesellschaft der epidemiologischen Krebsregister e. V. (GEKID), welche hierbei als Ansprechpartner der Krebsregister bei länderübergreifenden Fragestellungen dient. Entgegen der Auffassung der Datenschutzbeauftragten und entgegen der Bewertung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) schätzte die GEKID die Sicherheitslage jedoch grundsätzlich als ausreichend ein. Offenbar befürchtete die GEKID, dass im Falle einer Einführung von neuen Verfahren erhebliche Kosten entstehen würden und es zu bundesweit unterschiedlichen Umsetzungen kommen würde. In der Folge befürchtete man somit einen erschwerten oder gar unmöglichen Datenabgleich zwischen den beteiligten Bundesländern. Dieser Auffassung konnte sich die DSK hingegen nicht anschließen.

Um auf die Sachlage hinzuweisen und Verbesserungen durchsetzen zu können, verabschiedete die DSK im März 2013 die Entschließung „Pseudonymisierung von Krebsregisterdaten verbessern“ (http://www.datenschutz-mv.de/datenschutz/themen/beschlue/85_DSK/Ent_Pseudo.html). Dabei verwies die Konferenz auf einen vom AK Technik erarbeiteten Anforderungskatalog, in dem die Rahmenbedingungen für die zukünftige Gestaltung und für den Einsatz des Algorithmus zur Bildung von Kontrollnummern zur Pseudonymisierung von Daten über individuelle Fälle von Krebserkrankungen formuliert wurden (http://www.datenschutz- mv.de/datenschutz/themen/beschlue/85_DSK/Anlage_Pseudo.html). Die Entschließung richtet sich in erster Linie an die zuständigen Fachaufsichtsbehörden der Länder. Diese werden aufgefordert, für eine koordinierte Umstellung des Verfahrens bei den ihrer Aufsicht unterstehenden Stellen zu sorgen.

Aktuell befinden wir uns unter der Federführung unserer Kollegen des Berliner Datenschutzbeauftragten in Gesprächen mit den zuständigen Verantwortlichen, um das weitere Vorgehen bezüglich einer zukünftig verbesserten Gestaltung des Pseudonymisierungsverfahrens zu konkretisieren.

6.6.5 Datenschutz in der medizinischen Forschung

In der medizinischen Forschung stellen sich immer wieder bestimmte Fragen zum datenschutzgerechten Umgang mit Probanden- und Patientendaten sowie mit Proben von biologischem Material, wie Blut und Gewebeteilen. Deshalb hat der Verein TMF - Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V. bereits 2003 einen „Leitfaden zum Datenschutz in medizinischen Forschungsprojekten“ verfasst. Im Rahmen der Überarbeitung des Leitfadens hat der TMF im Sommer 2013 das Gespräch mit den Datenschutzaufsichtsbehörden des Bundes und der Länder gesucht. Deren Arbeitskreise „Wissenschaft“ und „Technische und organisatorische Datenschutzfragen“ (siehe Punkt 7) haben den TMF bei der Überarbeitung des Leitfadens beraten.

Der nun vorliegende Text beschreibt einen modularen und skalierbaren Ansatz, nach dem medizinische Forschungsverbünde datenschutzgerecht aufgebaut und betrieben werden können. Er erläutert, wie die Datenschutzanforderungen mit Anonymisierungs-, Pseudonymisierungs- oder Verschlüsselungstechniken umgesetzt werden können. Vier verschiedene Module fassen Anforderungen und Maßnahmeempfehlungen an verschiedene Arten von Forschungsverbünden zusammen:

1. Das Klinische Modul beschreibt, was zu tun ist, wenn Forschungsdaten aus dem direkten Behandlungszusammenhang gewonnen werden und wenn sich behandelnde Ärztinnen/Ärzte mit führenden Experten im direkten Interesse der Patientin/des Patienten austauschen. Die Anwendung dieses Moduls ermöglicht den datenschutzgerechten Umgang mit Patientendaten bei der umfassenden Betreuung chronischer, seltener oder besonders schwerer Erkrankungen. Während der Behandlung stehen die Patienten-Daten im Online-Zugriff, wobei die behandelnden Ärztinnen und Ärzte Zugriff auf personenbezogene medizinische Daten haben. Anderen Teilnehmern des Verbundes können pseudonymisierte Daten zur Verfügung gestellt werden. Die Daten sollen eher langfristig gespeichert bleiben.

2. Das Studienmodul stellt die Datenschutzanforderungen an klinische Studien dar, die auch den besonderen Regularien des Arzneimittelgesetzes (AMG) oder Medizinproduktegesetzes (MPG) unterliegen können. Da solche Studien der Klärung spezieller, im Voraus feststehender Fragen dienen, ist die Speicherdauer eher kurz und der Zweck einfach zu beschreiben. Je nach Rechtsgrundlage und Anwendungsfall haben Forscher Zugriff auf anonymisierte oder aber pseudonymisierte Daten.

3. Im Forschungsmodul geht es um Kriterien für die datenschutzgerechte Zusammenführung und Verarbeitung besonders qualitätsgesicherter Daten für langfristige Forschungsprojekte, die für die Behandlung der einzelnen Patientin/des einzelnen Patienten keine direkte Relevanz haben und daher aus dem Behandlungskontext nicht zugänglich sein müssen. Beispiele hierfür sind epidemiologische Register. Als Datenquellen für Forschungsmodule sind Klinische Module oder Studienmodule vorgesehen. Um die speziellen Anforderungen des Forschungsmoduls zu erfüllen, ist ein besonderes Pseudonymisierungsverfahren vorgesehen.

4. Das Biobankenmodul beschäftigt sich mit Datenschutzfragen bei der Sammlung und Verwaltung von Bioproben und daraus gewonnener Materialien für Forschungszwecke, insbesondere für die Erforschung molekulargenetischer Aspekte einer Erkrankung wie Fragestellungen der genetischen Epidemiologie. Das Biobankenmodul wird besonders beschrieben, weil dessen Datenstruktur von den anderen Modulen abweicht. Insbesondere sind Schutzvorkehrungen gegen den Missbrauch genetischer Informationen beschrieben.

Der uns vorliegende Entwurf ermöglicht es, die Anforderungen des Datenschutzes an medizinische Forschungsverbünde bereits in einem sehr hohen Maß umzusetzen. Wir gehen deshalb davon aus, dass wir auch den neu gefassten Leitfaden in Mecklenburg-Vorpommern künftig empfehlen werden können.

6.6.6 Forschungsvorhaben HARMONIC

Mehrere Kliniken und Forschungseinrichtungen unseres Landes erforschen im Projekt HARMONIC Methoden, mit denen Erkrankungen durch multiresistente Erreger, also die bekannten Krankenhauskeime, vermieden bzw. optimal behandelt werden können. Wir haben im letzten Berichtszeitraum das Institut für Community Medicine an der Universitätsmedizin Greifswald, das die Fachgebiete Epidemiologie und Informationstechnik in diesem Projekt verantwortet, zu Fragen des Datenschutzes beraten. Dabei konnte bereits auf bewährte Grundlagen zurückgegriffen werden, wie das Rahmenkonzept Datenschutz und IT-Sicherheit des Institutes (siehe Zehnter Tätigkeitsbericht, Punkt 4.5.1). Den Schwerpunkt der Beratungen bildeten Fragen der Anonymisierung und Pseudonymisierung der Daten von Patientinnen und Patienten sowie vom beteiligten medizinischen Personal, denn das Projekt beinhaltet neben Erhebungen von Patientendaten auch Befragungen von ärztlichem Personal und Pflegekräften.

Es war geplant, die Daten der Patientinnen und Patienten auf der Basis einer informierten Einwilligung einzuholen. Wird die Einwilligung nicht gegeben, so sollten Daten in anonymisierter Form in die Studie einfließen. Gegen diesen Grundansatz hatten wir keine Einwände. Jedoch war technisch keine Anonymisierung, sondern eine Pseudonymisierung vorgesehen. Deshalb haben wir in diesem Punkt eine Nachbesserung verlangt.

Außerdem war vorgesehen, auch die Verarbeitung von Beschäftigtendaten auf eine Einwilligung zu stützen. Wir halten dies rechtlich jedoch für unzulässig, da die Einwilligung nicht freiwillig zu erlangen ist. Würden Beschäftigte nicht einwilligen, so kann nicht ausgeschlossen werden, dass der Arbeitgeber dieses Verhalten negativ bewertet. Unseres Erachtens braucht die teilnehmende Einrichtung eine Rechtsgrundlage für die Verarbeitung der personenbezogenen Beschäftigtendaten. Da im Landeskrankenhausgesetz (LKHG M-V) keine Regelungen zur Verarbeitung solcher Daten existieren, gilt hier allgemeines Datenschutzrecht, je nach Rechtsform des Institutes also das Bundesdatenschutzgesetz (BDSG) oder das Landesdatenschutzgesetz (DSG M-V). Da sich die Fragen an die Beschäftigten auf ihre Arbeitsaufgabe beziehen, kommen als Rechtsgrundlage die Vorschriften zur Verarbeitung von Personaldaten in Betracht. Das sind § 35 DSG M-V für öffentliche Krankenhäuser und § 32 BDSG für private Einrichtungen.

Bei einer solchen Befragung kommt dem Betriebs- oder Personalrat ein Mitbestimmungsrecht zu, da damit eine Leistungskontrolle der Beschäftigten verbunden sein kann. Dies ist in § 70 Abs. 1 Nr. 2 Personalvertretungsgesetz Mecklenburg-Vorpommern (PersVG M-V) für öffentliche Einrichtungen und in § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG) für private Unternehmen geregelt.

Es sei angemerkt, dass im Sozialgesetzbuch Fünftes Buch (SGB V) eine Pflicht von Vertragsärztinnen und Vertragsärzten, Krankenhäusern und anderen Erbringern medizinischer Leistungen zur Qualitätssicherung vorgesehen ist (§§ 135a, 299 SGB V). Verfahren nach diesen Normen erfordern, dass die Daten der Patientinnen und Patienten pseudonymisiert zu erheben sind. Außerdem ist die Erhebung auf eine Stichprobe zu beschränken. Zusätzlich muss der Gemeinsame Bundesausschuss, ein Selbstverwaltungsgremium im Bereich der Sozialversicherung, einen Beschluss oder eine Richtlinie zu dem Untersuchungsgegenstand erlassen haben. Diese Texte enthalten weitere verbindliche Datenschutzregeln für die Verarbeitung personenbezogener Daten. Zu den Daten des medizinischen Personals regeln die oben genannten Vorschriften des SGB V, dass Meldungen auf Leistungserbringer bezogen sind. Leistungserbringer im Sinne des SGB V sind Institutionen und auch Einzelpersonen wie niedergelassene Ärztinnen und Ärzte. Aus den genannten Vorschriften vermögen wir jedoch kein Recht abzuleiten, Einzeldaten von Beschäftigten, also unterhalb der Ebene der Leistungserbringer, zu einrichtungsübergreifender Qualitätssicherung zu nutzen.

Ein wichtiges Element bei der Datenverarbeitung für medizinische Studien sind Treuhandstellen. Sie können - in der Regel als einzige Verfahrensbeteiligte - Pseudonyme und personenidentifizierende Daten einander zuordnen. Auch in dem beschriebenen Projekt wird eine solche Treuhandstelle genutzt, die seit längerem am Institut für Community Medicine besteht. Ist eine Treuhandstelle Teil mehrerer Studien und Projekte, so ist die Datenverarbeitung für die verschiedenen Studien und Projekte wirksam voneinander zu trennen. Wir haben empfohlen, dies in dem Sicherheitskonzept der Treuhandstelle stärker herauszuarbeiten und die Orientierungshilfe Mandantenfähigkeit (http://www.datenschutz-v.de/datenschutz/publikationen/in format/mandant/oh_mandant.pdf) zu berücksichtigen (siehe Punkt 5.1.9).

Über die Umsetzung dieser Hinweise sind wir mit dem Institut für Community Medicine noch im Gespräch.

6.6.7 Krankenhausinformationssysteme (KIS)

Bereits im März 2011 haben die Datenschutzbeauftragten des Bundes und der Länder die Orientierungshilfe „Krankenhausinformationssysteme“ (OH KIS) vorgelegt, in der sie die gesetzlichen Anforderungen an wichtige Teile der Informationstechnik in Krankenhäusern darstellen und Hinweise zur technischen Umsetzung geben (siehe Zehnter Tätigkeitsbericht, Punkt 4.5.2). Im Berichtszeitraum haben wir uns im Rahmen eines Projektes einen Überblick darüber verschafft, ob bzw. wie weit die Vorgaben und Empfehlungen dieser Orientierungshilfe in Krankenhäusern unseres Landes umgesetzt wurden. Die Landeskrankenhausgesellschaft war an diesem Projekt beteiligt. Folgende wesentliche Erkenntnisse haben wir dabei gewonnen:

a) Zum geltenden Recht

Bedingt durch die unterschiedlichen Rechtsformen der Krankenhäuser besteht teilweise Unsicherheit über die anzuwendende Rechtsgrundlage. Dies betrifft insbesondere Krankenhäuser mit öffentlicher Trägerschaft, die in private Trägerschaft mit öffentlicher Beteiligung wechseln. Auf unsere Nachfrage teilte das Ministerium für Arbeit, Gleichstellung und Soziales Mecklenburg-Vorpommern mit, dass für alle Krankenhäuser des Landes Mecklenburg-Vorpommern, die im Landeskrankenhausplan verzeichnet sind, das Landeskrankenhausgesetz Mecklenburg-Vorpommern (LKHG M-V) gilt.

b) Zur Stellung des betrieblichen Datenschutzbeauftragten

IT-Sicherheit und Datenschutz werden in den Krankenhäusern unterschiedlich gewichtet. Es ließ sich ein Zusammenhang zwischen der Position des Datenschutzbeauftragten, seiner fachlichen und organisatorischen Zuordnung und der Wahrnehmung von Datenschutzbelangen in der Krankenhausleitung feststellen.

c) Allgemeine Fragen zur Umsetzung der Orientierungshilfe

Die OH KIS ist in allen Krankenhäusern weitgehend bekannt, wird aber unterschiedlich interpretiert. Die Anforderungen und Empfehlungen der OH KIS sind insgesamt kaum umgesetzt. Dies scheitert insbesondere an zwei Faktoren: Einerseits können die Anforderungen mit den vorhandenen zentralen Systemen zur Verarbeitung der Patientendaten (Patientenaktensysteme - PAS) nur eingeschränkt umgesetzt werden. Andererseits fehlt in den meisten Krankenhäusern entsprechendes Personal. Das führt dazu, dass die Berechtigungen zum Zugriff auf Patientendaten - jedenfalls in allen im Rahmen des Projektes besuchten Einrichtungen - oft zu weit gefasst werden. Ärztliche Leitung sowie Ärztinnen und Ärzte verlangen häufig einen uneingeschränkten Zugriff auf alle Daten der in Behandlung befindlichen Patientinnen und Patienten.

d) Rollen- und Berechtigungskonzept

Mit geeigneten Rollen- und Berechtigungskonzepten und deren konsequenter Umsetzung lässt sich das Datenschutzniveau wirkungsvoll heben, auch wenn die technischen Voraussetzungen in den vorhandenen KIS-Systemen nicht immer optimal sind. Folgende Feststellungen möchten wir in diesem Zusammenhang positiv hervorheben:

- Anmeldungen der Ärztinnen und Ärzte erfolgen immer personalisiert.

- Anmeldungen des medizinischen Personals erfolgen in der Regel personalisiert. In den Fällen, in denen eine Gruppenanmeldung erfolgt, ist die Notwendigkeit einer personalisierten Anmeldung erkannt und in Umsetzung.

- Rollenbezogene Verarbeitungskontexte sind in der Regel in den PAS implementiert.

In den besuchten Einrichtungen haben wir jedoch folgende Defizite festgestellt:

- Die Anmeldungen der Administratoren erfolgen in der Regel über vordefinierte nichtpersonalisierte Administratorenbenutzer.

- Die Konfigurationsmöglichkeit der Benutzerverwaltung lässt nur eingeschränkt die technische Umsetzung der OH KIS zu. Dies resultiert aus der Diskrepanz zwischen den technischen Möglichkeiten der Anwendungen und den organisatorischen Anforderungen an den Behandlungsweg der Patientinnen und Patienten.

- Die Rollen- und Berechtigungskonzepte sind nicht flexibel.

- Es besteht keine Möglichkeit, anwendungsübergreifende Rollen- und Berechtigungskonzepte durch automatisierte Verfahren (Steuerung durch Dienstplan, Personalsysteme) einzusetzen.

- Ungeachtet dessen werden die vorhandenen technischen Möglichkeiten der Anwendungen nicht vollständig ausgenutzt.

- Berechtigungen durch Rollen und über Organisationseinheiten werden in linearer Struktur (i. d. R. Benutzergruppen) abgebildet. Daraus resultiert eine unübersichtliche Anzahl von Benutzergruppen.

- Manuelle Anpassungen der Berechtigungen (Wechsel der Organisationseinheit, Dienste) sind durch personell beschränkte Möglichkeiten in den administrativen Abteilungen nicht möglich. Eine Delegierung der Vergabe von Berechtigungen ist bedingt durch den komplizierten technischen Vorgang der Berechtigungsvergabe und die mangelnden Dokumentationsmöglichkeiten kaum praktikabel.

e) Protokollierung von Zugriffen auf Patientendaten

Schreibende und in unterschiedlichem Umfang lesende Zugriffe auf Patientendaten werden ausschließlich in Systemlogdateien protokolliert. Keines der geprüften Systeme ermöglicht es, Logdateien in der durch die OH KIS beschriebene Form auszuwerten.

Inzwischen haben die Hersteller der Anwendungen jedoch erkannt, wie wichtig die Protokollierung ist. Die Auswertung der Zugriffe auf Patientendaten wird in den neuen Programmversionen optimiert. Darüber hinaus erlauben es einige Anwendungen, Zugriffe über Datenbankabfragen auszuwerten. In diesem Fall können strukturierte Abfragen bereitgestellt werden.

f) Zum Datenschutz in den Funktionseinheiten des Krankenhauses

Im Krankenhausbetrieb ist die Datenübermittlung an Funktionseinheiten innerhalb des Krankenhauses besonders wichtig. Die OH KIS bildet die Komplexität dieser Aufgabe allerdings nur eingeschränkt ab. Wegen der komplexen Anforderungen nach belegloser Dokumentation der Patientendaten sind elektronische Verfahren Standard bei der Übermittlung von Daten innerhalb des Krankenhauses.

Die Datenübermittlung zwischen dem PAS und den nachgestellten Subsystemen ist eine der aufwändigsten und kostenintensivsten Aufgaben, die bei Konzeption und Betrieb von KIS zu lösen sind. Die zur Datenübermittlung verwendeten Kommunikationsschnittstellen basieren zwar oft auf offenen Standards wie HL7. Die individuelle Strukturierung unterschiedlicher Organisations- und Funktionseinheiten in den Krankenhäusern erschwert aber eine durchgehende Darstellung der Zugriffsberechtigungen auf Patientendaten. Dies resultiert insbesondere aus den unterschiedlichen Aufgaben der einzelnen diagnostischen und therapeutischen Funktionseinheiten. Dies gilt selbst in Konzernen mit weitgehend einheitlicher Software-Ausstattung. Nicht einmal dort lassen sich Lösungen aus einem Krankenhaus ohne größeren Aufwand auf ein anderes übertragen. Zugriffe auf Patientendaten lassen sich häufig nur schwer in Abhängigkeit von der Zuordnung der Patientin bzw. des Patienten zur jeweiligen Organisations- und Funktionseinheit einschränken. Das Berechtigungskonzept sollte sich deshalb nicht am Aufenthalt der Patientin bzw. des Patienten, sondern vielmehr an dem Team orientieren, das die Patientin bzw. den Patienten behandelt.

Die Organisation der Übermittlungen zwischen den Stationen und den Funktionseinheiten sollte in allen Krankenhäusern tiefer geprüft werden.

g) Zur Mandantenfähigkeit von KIS

In allen Krankenhäusern sind weitere Leistungserbringer tätig, die als eigenständige verantwortliche Stellen neben dem Krankenhaus selbst zu betrachten sind.

In der Regel sind sich die Verantwortlichen dieses datenschutzrechtlichen Problems nicht bewusst. Die Strukturen der unterschiedlichen Leistungserbringer und damit der verantwortlichen Stellen sind zumeist nur über die betriebswirtschaftlichen Strukturen (Abrechnungsbeziehungen) dargestellt. Deshalb verwundert es nicht, dass in keinem der besuchten Krankenhäuser Mandantenlösungen nach Maßgabe der OH KIS installiert sind.

h) Sperren, Löschen, Archivieren, Verschlüsselung

In allen überprüften Systemen lässt sich eine Auskunftssperre einrichten, wobei auch hier qualitativ unterschiedliche Lösungen anzutreffen sind. Deshalb werden in der Regel über die Sperre im PAS hinaus weitere organisatorische Vorkehrungen in den Krankenhäusern getroffen.

Es sind aber keine Einschränkungen in Bezug auf die Darstellung vorhergehender Behandlungsfälle in der Patientensuche getroffen. Dies gilt für alle Organisation- und Funktionseinheiten der Krankenhäuser. Teilweise sind in verschiedenen Organisations- und Funktionseinheiten medizinische Daten unterschiedlichster Behandlungsfälle einsehbar.

Keines der überprüften Systeme verfügt über die Möglichkeit, Datensätze in geeigneter Form zu sperren oder es ist keine Sperre nach Verlegung oder Abschluss einzelner Fälle konfiguriert. In keinem der besuchten Krankenhäuser ist eine Sperre nach Widerspruch konfigurierbar noch gibt es Regelungen für diesen Fall. Sperren aufgrund von besonderer Stellung der zu behandelnden Patienten (VIP-Sperre) sind nicht konfiguriert. Alternative Lösungen (alias) wurden teilweise getestet und als nicht praktikabel verworfen.

In keinem der überprüften Systeme ist es möglich, Datensätze zu löschen.

Keine der in den besuchten Krankenhäusern installierten Anwendungen verfügt über eine Lösung zur zeitgesteuerten Archivierung der Patientendaten.

In keinem der überprüften Häuser werden Systeme zur Verschlüsselung von Datenbanken oder anderweitig gespeicherten Daten eingesetzt. Soweit geprüft, werden Daten-Backups nicht verschlüsselt.

i) Zum weiteren Vorgehen

Die Landeskrankenhausgesellschaft Mecklenburg-Vorpommern hat einen Arbeitskreis Datenschutz gegründet, der die oben beschriebenen Probleme und weitere Fragen des Datenschutzes klären soll. Bei Bedarf sollen auch externe Experten mit einbezogen werden. Wir begrüßen ausdrücklich, dass die Landeskrankenhausgesellschaft selbst die Initiative zur Verbesserung des Datenschutzes bei ihren Mitgliedsunternehmen ergriffen hat. Im Rahmen unserer Kapazitäten werden wir diesen Arbeitskreis selbstverständlich unterstützen.

6.7 Zensus 2011

Im Zehnten Tätigkeitsbericht, Punkt 5.5, hatten wir über einige Fragen und Probleme zur Volks- und Wohnungszählung (Zensus 2011) sowie über die umfangreichen Vorbereitungsmaßnahmen, die vor allem in den einzurichtenden Erhebungsstellen in unserem Bundesland vorzunehmen waren und in einigen Fällen kontrolliert wurden, berichtet. Die Datenerhebungen und -aufbereitungen zum Zensus 2011 sind im Jahr 2012 weitestgehend abgeschlossen worden. Anfängliche Schwierigkeiten im Hinblick auf den Datenschutz und die Datensicherheit konnten nach und nach ausgeräumt werden, sodass in Bezug darauf die Volkszählung in unserem Bundesland dann unproblematisch verlief.

Anlässlich der Bekanntgabe der im Rahmen des Zensus ermittelten Bevölkerungszahlen hat der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Bilanz gezogen und mit der Pressemitteilung 10/2013 Eckpunkte für eine datenschutzgerechte Ausgestaltung künftiger Volkszählungen veröffentlicht.

Auch aufgrund der bei der Durchführung des Zensus 2011 gesammelten Erfahrungen in unserem und auch in anderen Bundesländern haben sich Aspekte ergeben, die bei der Ausgestaltung der landesrechtlichen Vorschriften für den Zensus 2021 Berücksichtigung finden sollten und die insbesondere folgende Punkte betreffen:

Einsatz von Erhebungsbeauftragten

Wie in § 11 Zensusgesetz 2011 (ZensG 2011) vorgesehen, sind von allen Erhebungsstellen auch externe Erhebungsbeauftragte eingesetzt worden. Die Erfahrung hat gezeigt, dass diese Praxis mit verschiedenen grundsätzlichen Problemen behaftet war, die durch Vorgaben im Zensusrecht für die nächste Erhebung ausgeräumt werden sollten.

Das ZensG 2011 enthält in § 11 Abs. 3 einzelne Anforderungen an die eingesetzten Erhebungsbeauftragten. Diese sollten durch weitere bei allen Beauftragten notwendigen Anforderungen ergänzt werden. So sollte bundesgesetzlich geregelt werden, dass die Beauftragten über die notwendige Fachkunde verfügen müssen, um ihre Aufgaben sachgemäß durchführen zu können.

Für die Erhebungsbeauftragten sollte möglichst bundeseinheitlich ein Ausweismuster vorgegeben werden, um unterschiedliche Gestaltungen zu vermeiden, die geeignet sind, die Akzeptanz der Beauftragten zu verringern. Die Ausweise sollten zudem nur die für eine Identifizierung unabdingbaren Angaben enthalten.

Hinsichtlich der Erreichbarkeit der Erhebungsbeauftragten für die zu befragenden Personen sollte geprüft werden, ob hier nicht zum Schutz der Daten der Beauftragten Regelungen getroffen werden können. Durch Vorgaben für die Erhebungsstellen sollte gewährleistet werden, dass die Erreichbarkeit der Beauftragten - etwa für Terminabsprachen - über die jeweilige Erhebungsstelle sichergestellt ist. Die zusätzliche Offenlegung ihrer privaten Erreichbarkeit sollte den Beauftragten überlassen bleiben.

Zur Gewährleistung der Beachtung des Grundsatzes der Datensparsamkeit sollten die Erhebungsbeauftragten nur einen um den Tag und den Monat der Geburt reduzierten Melderegisterauszug erhalten. Detaillierte Angaben werden für die Durchführung der Erhebung nicht benötigt. Die Erfahrung in den Ländern hat gezeigt, dass die Angabe lediglich des Geburtsjahres zur Identifizierung der zu Befragenden ausreichend ist.

Beim Einsatz der Erhebungsbeauftragten ist darauf zu achten, dass das Risiko, dass Beauftragte Erhebungen bei ihnen bekannten Personen durchführen, weitgehend ausgeschlossen wird. Dies kann durch eine ausreichende Entfernung der Wohnungen der Beauftragten von den Gebieten, in denen sie tätig werden, erreicht werden. Insoweit sollten in den Ausführungsgesetzen der Länder konkretisierende Regelungen geschaffen werden.

Nicht nur eine zu geringe Nähe zwischen dem Wohnort der Erhebungsbeauftragten und ihren Erhebungsgebieten, sondern auch Interessenkollisionen müssen bei der Auswahl der Beauftragten und der Bestimmung ihres Einsatzgebietes möglichst vermieden werden. Die Grundaussagen in § 11 Abs. 3 Satz 4 ZensG 2011 sollten durch bundeseinheitliche Leitlinien für eine einheitliche Schulung und Praxis ergänzt werden.

Durch unsere Kontrolltätigkeit in den Erhebungsstellen wurde deutlich, dass sowohl hinsichtlich des sicheren Transports als auch der Aufbewahrung ausgefüllter Erhebungsbögen durch die Beauftragten Klärungsbedarf besteht. Um ausgefüllte Erhebungsbögen bis zur Ablieferung in der Erhebungsstelle vor unbefugter Einsicht durch Dritte zu schützen, sollte eine einheitliche Verfahrensweise gewährleistet werden. Wichtig sind insoweit Vorgaben für den Transport der Bögen in versiegelten oder in anderer Weise besonders gesicherten Behältnissen (siehe §§ 133 Abs. 1, 136 StGB) durch die Erhebungsbeauftragten und für die Aufbewahrung bei diesen, sodass ein Zugang Dritter zu den Bögen sicher ausgeschlossen werden kann. Ein Transport in schlichten Briefumschlägen ist als nicht ausreichend sicher anzusehen.

Datenübermittlungen
Die Forderung nach einer Verschlüsselung der elektronischen Datenübermittlungen (siehe § 20 Abs. 2 Hs. 2 ZensG 2011) sollte nicht auf allgemein zugängliche Netze beschränkt werden, sondern als Mindestanforderung für alle Datenübermittlungen formuliert werden (zu verschiedenen Übermittlungswegen siehe etwa § 3 ZensG 2011).

Es ist wünschenswert, dass die Landesregierung die vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit angesprochenen Überlegungen in der weiteren Diskussion über den bundesrechtlichen Rahmen für den Zensus 2021 unterstützt und auch die im Rahmen der Durchführung des Zensus 2011 gesammelten Erfahrungen bei der Ausgestaltung der landesrechtlichen Vorschriften für den Zensus 2021 berücksichtigt.

6.8 Finanzwesen

6.8.1 Kartenzahlung per Funk

Bereits im Juni 2011 teilte der Deutsche Sparkassen- und Giroverband (DSGV) mit, dass EC-Karten künftig mit einem Funk-Chip ausgestattet werden. Mit dieser Funktion will der DSGV die seit 1995 auf EC-Karten verfügbare GeldKarten-Funktion attraktiver und somit Bezahlvorgänge für Händler und Geldinstitute kostengünstiger machen. Die Kundinnen und Kunden der Sparkassen können mit der GeldKarten-Funktion der neuen EC-Karten kleine Einkäufe ohne Eingabe einer PIN und ohne Unterschrift bis zu Beträgen von 20 Euro nun kontaktlos bezahlen. Dazu wird die sogenannte NFC-Technologie genutzt (Near Field Communication). Der Funk-Chip der GeldKarte kommuniziert dazu mit einem Lesegerät, das beispielsweise an die Kasse eines Händlers angeschlossen ist, und überträgt die Zahlungsdaten aus der zuvor mit maximal 200 Euro aufgeladenen elektronischen GeldKarte in das Zahlungssystem.

Noch vor dem Start eines Pilotversuchs in Niedersachsen Mitte April 2012 wandte sich ein besorgter Bürger an uns, weil er Sicherheitsrisiken bei der Nutzung der drahtlosen Bezahlfunktion befürchtete. Um die technischen Details des Verfahrens beurteilen zu können, wurden der DSGV und die Verfahrensentwickler gebeten, die neue GeldKarten-Funktion und das dazugehörige girogo-Verfahren im Arbeitskreis „Technische und organisatorische Datenschutzfragen (AK Technik, siehe Punkt 7) vorzustellen. Parallel zur Präsentation technischer Details wurden auch rechtliche Aspekte des Verfahrens beraten. Die AG Kreditwirtschaft des Düsseldorfer Kreises traf sich dazu mehrfach mit Vertretern des DSGV.

Die Präsentation beim AK Technik im Februar 2012 zeigte, dass Datenschutz und Datensicherheit bei der Entwicklung des Verfahrens offenbar eine wichtige Rolle gespielt haben, denn alle Geldtransaktionen werden durch zahlreiche technische Maßnahmen abgesichert. So findet die Kommunikation zwischen GeldKarte, Lesegerät und bankseitiger Infrastruktur immer verschlüsselt statt. Zudem authentisieren sich GeldKarte und Lesegerät gegenseitig, sodass nur spezielle Händler-Lesegeräte Geldbeträge abbuchen können. Wir bemängelten jedoch, dass keine ausreichende Dokumentation des Verfahrens vorlag, die für eine vollständige datenschutzrechtliche Bewertung aber erforderlich ist.

Immerhin kündigte der DSGV in der Sitzung an, für das gesamte girogo-Verfahren ein sogenanntes Privacy Impact Assessment (PIA) durchzuführen und damit auch schriftlich zu dokumentieren, welche Maßnahmen zum Schutz der Privatsphäre der Karteninhaberinnen und Karteninhaber getroffen wurden.

Obwohl die eigentliche Bezahl- und Ladefunktion der GeldKarte offenbar sicherheitstechnisch nicht zu beanstanden war, blieben wichtige datenschutzrelevante Fragen weiterhin offen. Die GeldKarte verfügt nämlich über einen Speicherbereich, der - anders als bei der Bezahlfunktion - von jedem beliebigen RFID-Lesegerät ausgelesen werden kann. In diesem Bereich sind beispielsweise die letzten 15 Bezahlvorgänge und die letzten drei Ladevorgänge sowie die eindeutige Kennung jeder GeldKarte gespeichert. In einem Schreiben an den DSGV kritisierte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder im November 2012, dass diese Daten nicht ausreichend vor dem Zugriff Unbefugter geschützt werden. Die Konferenz forderte einerseits detaillierte Informationen für die Nutzerinnen und Nutzer, damit sie sich bewusst für oder gegen die Nutzung der drahtlosen Zahlfunktion entscheiden können. Zudem wurden technische Maßnahmen wie die Verschlüsselung des Funkverkehrs gefordert, um das unbefugte Auslesen dieser Daten zu verhindern, zumindest jedoch die Bereitstellung von metallischen Schutzhüllen, die jegliche kontaktlose Kommunikation mit der Karte verhindern.

Es dauerte dann noch bis zum April 2013, bis der DSGV das lange angekündigte PIA vorlegte. Wir begrüßten ausdrücklich, dass das Dokument mit einer international anerkannten Methode (PIA-Framework für RFID-Anwendungen der Europäischen Kommission) erstellt wurde. Auch wenn noch immer nicht alle Detailfragen zufriedenstellend beantwortet wurden (bspw. ist die Verschlüsselung der drahtlosen Kommunikation mit dem oben beschriebenen Speicherbereich nach wie vor nicht vorgesehen), brachte das Dokument mehr Transparenz in das Verfahren und ermöglichte erstmals eine umfassendere datenschutzrechtliche Bewertung.

Im November 2013 gaben dann der AK Technik und die AG Kreditwirtschaft eine abschließende Bewertung des girogo-Verfahrens gegenüber dem DSGV ab. Darin wurden die kartenausgebenden Institute verpflichtet, zumindest auf Verlangen der Kundinnen und Kunden die oben erwähnte Schutzhülle auszugeben und den Kundinnen und Kunden ausführliche Hinweise zum Einsatz der GeldKarten mit drahtloser Zahlfunktion zu geben. Darüber hinaus wurde gefordert, den Kundinnen und Kunden zu ermöglichen, die NFC-Funktion ihrer Karte abzuschalten und auch auf diese Weise jegliche Funkkommunikation zu unterbinden. Weiterhin wurden die Institute darauf hingewiesen, dass Zusatzanwendungen auf der Karte das Datenschutz- und Datensicherheitsniveau des girogo-Verfahrens gefährden können und daher immer besonders zu prüfen sind.

Offen ist nach wie vor die Frage der verschlüsselten Kommunikation mit dem frei zugänglichen Speicherbereich der GeldKarte. Obwohl der DGSV die Forderung der Datenschutzbeauftragten nach Verschlüsselung nach wie vor als unangemessen zurückweist, war er bisher nicht in der Lage, die Kosten einer solchen Maßnahme zu beziffern. Daher haben wir diese Forderung zunächst zurückgestellt, erwarten aber, dass weitere Maßnahmen zur technischen Absicherung des NFC-Konzeptes vom DSGV geprüft werden.

6.8.2 Datenschutz beim Abruf elektronischer Lohnsteuerabzugsmerkmale (ELSTAM)

Im Zehnten Tätigkeitsbericht, Punkt 5.6.4, hatten wir darüber berichtet, dass die herkömmliche Papierlohnsteuerkarte von einem elektronischen Verfahren abgelöst werden soll. Nach Verzögerung der Einführung des Verfahrens sind Arbeitgeber seit Ende des Jahres 2013 verpflichtet, die Daten ihrer Arbeitnehmerinnen und Arbeitnehmer, die sie für die Abführung der Lohnsteuer benötigen (ELSTAM), elektronisch bei der Finanzverwaltung abzurufen.

Der Arbeitgeber benötigt mit Beginn einer neuen Beschäftigung für den Abruf der ELSTAM das Geburtsdatum, die Steueridentifikationsnummer und die Angabe, ob es sich um ein Haupt- oder Nebenarbeitsverhältnis handelt. Hat das Arbeitsverhältnis bereits im Jahre 2012 bestanden, sind dem Arbeitgeber diese Daten bereits bekannt.

Nur der jeweilige Arbeitgeber ist zum Abruf der ELSTAM berechtigt. Diese Berechtigung endet mit Ablauf des Arbeitsverhältnisses. Jeder Abruf wird zur Überprüfung der Abrufberechtigung protokolliert. Ein vorsätzlicher oder leichtfertiger Abruf für andere Zwecke als für die Durchführung des Steuerabzugs (z. B. „Neugierabfragen“) stellt eine bußgeldbewehrte Ordnungswidrigkeit dar.

Eine ausdrückliche Zustimmung der Arbeitnehmerin/des Arbeitnehmers zum Abruf ist nicht erforderlich. Zusätzlich kann jede Arbeitnehmerin/jeder Arbeitnehmer aber auch selbst Maßnahmen zum Schutz unberechtigter Steuerdatenabrufe im Lohnsteuerverfahren ergreifen. Hier stehen ihnen verschiedene Rechte zu, die mittels amtlichen Vordrucks geltend gemacht werden können. So kann jede Arbeitnehmerin/jeder Arbeitnehmer auf Antrag beim zuständigen Finanzamt Auskunft über die zur Person gespeicherten Lohnsteuerabzugsmerkmale und über die in den letzten 24 Monaten durch den Arbeitgeber erfolgten Abrufe verlangen.

Außerdem können Arbeitnehmerinnen und Arbeitnehmer, die einen Abruf nicht wünschen oder verhindern wollen, dass zum Beispiel ehemalige Arbeitgeber mit den noch bekannten Daten einen Abruf tätigen, beim zuständigen Finanzamt beantragen, den Abruf ihrer ELSTAM vollständig oder nur für bestimmte Arbeitgeber sperren zu lassen (Vollsperrung oder Negativliste). Ebenso können sie aber auch Arbeitgeber benennen, die zum Abruf von elektronischen Lohnsteuerabzugsmerkmalen berechtigt sein sollen (Positivliste) bzw. den Abruf allgemein freischalten lassen.

Für die entsprechenden Anträge benötigen Arbeitnehmerinnen und Arbeitnehmer die Wirtschaftsidentifikationsnummer des Arbeitgebers, die dieser ihnen mitzuteilen hat.

Kann der Arbeitgeber wegen einer Sperre keine ELSTAM-Daten abrufen, hat dieser die Lohnsteuer allerdings nach Steuerklasse IV zu ermitteln.

6.8.3 Einführung der „Bettensteuer“ in Schwerin?

Anfang des Jahres 2013 haben uns verschiedene Stellen wie Hotelbetreiber der Stadt Schwerin oder der Hotelverband Deutschland um eine datenschutzrechtliche Einschätzung zur Einführung der sogenannten Bettensteuer gebeten. Insbesondere hat ein Vertreter des Hotelgewerbes in Schwerin auf eine Regelung in der entsprechenden Satzung verwiesen, die vor Ort eine Auskunft der Reisenden darüber einfordert, ob der Aufenthalt privater oder beruflicher Natur sei. Hintergrund für diese Bedenken und Anfragen ist, dass die Landeshauptstadt Schwerin offenbar eine Kulturförderabgabe plante, nach der privat veranlasste Übernachtungen zu versteuern, aber beruflich veranlasste Übernachtungen steuerfrei sein sollen.

Da wir die Erhebung der „Bettensteuer“ aus datenschutzrechtlicher Sicht für problematisch halten, haben wir der Stadt Schwerin unsere Bedenken mitgeteilt und die Datenschutzbeauftragte gebeten, sich dafür einzusetzen, dass diese Bedenken bei den sich mit dieser Thematik befassenden Stellen und Gremien Berücksichtigung finden.

Obwohl auch das Innenministerium Mecklenburg-Vorpommern rechtliche Bedenken gegen die Einführung der Kulturförderabgabe geäußert hat, ist im Oktober 2012 die Einführung der „Bettensteuer“ beschlossen worden.

Aus datenschutzrechtlicher Sicht ist eine „Bettensteuer“ nur dann zulässig, wenn das Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) oder eine andere Rechtsvorschrift das Verarbeiten der hierfür benötigten personenbezogenen Daten erlaubt. Als bereichsspezifische Rechtsvorschrift käme hier eine entsprechende Satzung in Betracht. Diese müsste rechtswirksam sein, das heißt, sie dürfte insbesondere nicht gegen höherrangiges Recht verstoßen. Dies dürfte neben dem Landesdatenschutzgesetz Mecklenburg-Vorpommern auch anhand der einschlägigen Vorschriften des Kommunalabgabengesetzes Mecklenburg-Vorpommern (KAG M-V) zu beurteilen sein.

Gemäß § 12 a KAG M-V können die abgabenberechtigten Körperschaften durch Satzung bestimmen, dass Dritte, die in engen rechtlichen oder wirtschaftlichen Beziehungen zu einem Sachverhalt stehen, an den die Abgabenpflicht anknüpft, anstelle der Beteiligten gegen Kostenerstattung verpflichtet sind, ihnen die zur Abgabenfestsetzung oder -erhebung erforderlichen Berechnungsgrundlagen mitzuteilen.

In § 5 Abs. 2 der vorliegenden Fassung der Satzung über die Erhebung einer Kulturförderabgabe in der Landeshauptstadt Schwerin heißt es, dass der Betreiber des Beherbergungsbetriebes für die Kassierung, Abführung und Nachweisführung verantwortlich sei, neben dem Übernachtungsgast für die Abgabe hafte und als Gesamtschuldner betrachtet wird.

Eine solche Formulierung würde sich nicht mit § 12 a KAG M-V decken, denn die Aufbürdung der Steuerschuld und damit das Tragen der Beweislast für die Entstehung der Steuerpflicht zu Lasten der Beherbergungsbetriebe hat eine andere rechtliche Qualität als die Mitteilung der erforderlichen Berechnungsgrundlagen gemäß § 12 a KAG M-V. Letztere kann in Bezug auf die „Bettensteuer“ nur die Mitteilung sein, ob ein Gast aus einem privaten oder beruflichen Anlass übernachtet hat. Diese Erkenntnis ist zur Feststellung der Steuerpflicht ausreichend. Die genannten Regelungen der Satzung sind daher zu weitreichend.

Eine Prüfung der Steuerpflicht an sich mit entsprechenden Erkundigungen oder Nachforschungen durch den Betreiber des Beherbergungsbetriebes kommt auch deshalb nicht in Betracht, da dieser als „verlängerter Arm der Finanzverwaltung“ in Erscheinung treten würde und dies nicht von der Abgabenordnung gedeckt wäre. Auskunftsansprüche über steuerrelevante Daten stehen lediglich den Finanzbehörden zu. Die Prüfung der Steuerpflicht muss daher Aufgabe der Steuer erhebenden Stellen bleiben.

Wir bitten die Landesregierung, diese datenschutzrechtlichen Bedenken im weiteren Verfahren hinsichtlich der Einführung der „Bettensteuer“ zu berücksichtigen und sich für eine satzungsrechtliche Regelung einzusetzen, die den datenschutzrechtlichen Belangen in der beschriebenen Weise entspricht.

6.8.4 Kontendatenabrufe nehmen weiterhin zu

Bereits in unserem Neunten Tätigkeitsbericht, Punkt 2.7.3, hatten wir berichtet, dass die Zahl der Kontendatenabrufe insgesamt deutlich steigt. Auch für den jetzigen Berichtszeitraum kann keine andere Aussage getroffen werden. Immer häufiger wird von Behörden der automatisierte Kontendatenabruf durchgeführt. Insbesondere ist ein Anstieg der Abfragen nach § 93 Abs. 8 Abgabenordnung (AO) im ersten Quartal 2013 zu verzeichnen. Hintergrund hierfür ist vor allem auch die Tatsache, dass der Gesetzgeber die Kontenabrufmöglichkeit inzwischen auch auf andere Zwecke und Behörden ausgedehnt hat. Neben Finanzämtern, Sozialdienststellen und Jobcentern dürfen nun zum Beispiel seit dem 1. Januar 2013 auch Gerichtsvollzieher und das Bundesamt für Justiz für bestimmte Zwecke das Bundeszentralamt für Steuern um einen Kontendatenabruf ersuchen.

Ursprünglich sollten mit Hilfe des Kontendatenabrufverfahrens schwere Verbrechen bekämpft werden und der Terrorismusgefahr entgegengewirkt werden. Mit Schaffung der gesetzlichen Grundlagen sollte es den Finanzbehörden dann möglich sein, nicht bekannte Vermögenswerte zu ermitteln und somit Steuereinnahmen zu erzielen. Nach den in den Bundesländern gesammelten Erfahrungen der Datenschutzbeauftragten werden Kontendatenabrufe jedoch meistens im Vollstreckungsverfahren zur Durchsetzung von Zahlungsansprüchen durchgeführt.

Bei einer Kontendatenabfrage greifen die berechtigten Stellen auf Kontostammdaten wie Namen und Geburtsdatum sowie auf Anzahl und Nummern der bei der Bank geführten Konten zu. Die Einsicht von Kontoständen und Kontobewegungen ist nicht möglich. Betroffene sind grundsätzlich vorab auf die Möglichkeit des Kontendatenabrufs hinzuweisen und über dessen Durchführung zu benachrichtigen. Einige Kontrollbesuche der Datenschutzbeauftragten in anderen Bundesländern haben ergeben, dass gerade auch diese Pflichten nicht immer eingehalten werden.

Um ein detaillierteres Bild von den in den einzelnen Bundesländern durchgeführten Kontendatenabrufen zu erhalten, ist geplant, dass die künftigen vom Bundeszentralamt für Steuern bereitgestellten Jahresstatistiken den Landesbeauftragten in aufgeschlüsselter Form zur Verfügung gestellt werden. Wir gehen davon aus, dass im nächsten Berichtszeitraum, gerade im Hinblick auf Abrufe nach § 93 Abs. 8 AO, genauere Auswertungen, insbesondere zu den Schwerpunkten der Abrufe (Kommunen, Sozialämter usw.) möglich sein werden, sodass gegebenenfalls eine effiziente Planung von Kontrollbesuchen möglich wäre.

6.8.5 IT-Dienstleister – ein datenschutzrechtliches Risiko für Kommunen?

Zunehmend beauftragen Kommunen externe Dritte für die technische Betreuung von IT-Programmen, die den Amtshaushalt der Gemeinden betreffen. So wurde in einem Fall ein Softwareanbieter für Beratungszwecke sowie zur Hilfestellung bei der Fehleranalyse des Programms proDoppik beauftragt. Es wurde unter anderem ein Vertrag über die Pflege von Standardsoftware sowie auch über die Beschaffung von IT-Dienstleistungen geschlossen.

Nach Auftreten eines technischen Fehlers bei der Bilanzaufstellung sind alle vom Amt erhobenen und auch für die Gemeinden zu erhebenden personenbezogenen Daten, die sich auf verschiedenste Abgaben wie Gebühren, Beiträge, Steuern sowie auch Mieten und Pachten beziehen, an die beauftragte Firma auf einem externen Datenträger direkt übergeben worden. Für die Problem- und Fehleranalyse sei nach Aussage des Amtes der gesamte Datenbestand erforderlich gewesen, da sich die Fehler nicht auf einzelne Datenbereiche zuordnen ließen.

Der IT-Dienstleister hat dem Amt dann mitgeteilt, dass aus den Firmenräumen unter anderem ein Laptop entwendet worden sei, auf dem sich die Datenbank des Programms proDoppik befunden habe.

Über diesen Vorfall hat uns das Amt sofort informiert und um entsprechende Empfehlungen zu den ersten einzuleitenden Schritten gebeten. Die erforderlichen Bekanntmachungen und Benachrichtigungen im Verwaltungsgebäude, im amtlichen Mitteilungsblatt sowie im Internet sind daraufhin umgehend erfolgt.

Zur datenschutzrechtlichen Bewertung des Vorfalls ist das Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) heranzuziehen. Es sind hier die Vorschriften über die Verarbeitung von personenbezogenen Daten im Auftrag einschlägig. Danach bleibt der Auftraggeber für die Einhaltung der gesetzlichen Vorschriften über den Datenschutz verantwortlich, wenn personenbezogene Daten durch andere Personen oder Stellen im Auftrag einer öffentlichen Stelle verarbeitet werden. Der Auftraggeber hat also alle in § 4 DSG M-V genannten Voraussetzungen und Anforderungen zu erfüllen.

Demzufolge wurde das Amt zunächst darauf hingewiesen, dass es als auftraggebende Stelle die erforderlichen Weisungen zur Auftragserfüllung schriftlich zu erteilen hat und ein entsprechender Vertrag vorliegen muss. Daraufhin hat das Amt einen Vertragsentwurf vorgelegt, der sich eng an dem von uns empfohlenen Mustervertrag orientiert.

Wir haben abschließend darauf hingewiesen, dass in derartigen Fällen auch vertraglich dargelegt werden sollte, auf welche Art und Weise die Hardware in den Räumlichkeiten sowie die Räume und das Gebäude des Dienstleisters vor unberechtigten Zugriffen gesichert bzw. geschützt werden. In Anbetracht der hochsensiblen Daten haben wir zusätzlich empfohlen, dass die beim Auftragnehmer beschäftigten Personen neben der Verpflichtung auf das Datengeheimnis auch nach dem Verpflichtungsgesetz (VerpflG) verpflichtet werden sollten.

Insgesamt ist es uns ein Anliegen, dass die öffentliche Verwaltung mit personenbezogenen Daten, gerade in besonders sensiblen Bereichen, noch verantwortungsbewusster umgeht. Zwar können Fehler oder unvorhersehbare Situationen nie ausgeschlossen werden. Jedoch sollten beim Umgang mit personenbezogenen Daten zumindest die erforderlichen datenschutzrechtlichen Mindeststandards eingehalten und die entsprechenden Rechtsvorschriften herangezogen werden.

6.9 Bildung

6.9.1 Online-Befragung der Lehrkräfte an öffentlichen Schulen

Das Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern beabsichtigte, die Förderung der Gesundheit der Beschäftigten an öffentlichen Schulen des Landes stärker als bisher in den Focus der Arbeit zu rücken. Zu diesem Zweck sollten zum einen die Lehrerinnen und Lehrer selbst befragt und zum anderen die schulischen Bedingungen analysiert werden. Das Ergebnis der Befragung sollte dann Ausgangspunkt für schulspezifische Präventions- und Interventionsmöglichkeiten werden, um die Gesundheit der Lehrkräfte zu stärken und zu verbessern. Mit der Befragung sollte ein Unternehmen beauftragt werden; das Ministerium übersandte uns die entsprechenden Projektunterlagen mit der Bitte um datenschutzrechtliche Stellungnahme.

In den Projektunterlagen war einerseits ausgeführt, dass die Befragung der Lehrkräfte anonym über das Internet erfolgen sollte. Andererseits wurde in den Unterlagen darauf hingewiesen, dass die Teilnehmerinnen und Teilnehmer zu einem späteren Zeitpunkt nochmals befragt werden sollten. Sofern dies der Fall wäre, handelt es sich nach der datenschutzrechtlichen Terminologie nicht um eine anonyme, sondern um eine pseudonyme Befragung (siehe § 3 Abs. 4 Satz 2 Nr. 8 und 9 DSG M-V). Von zentraler datenschutzrechtlicher Bedeutung war daher die Frage, ob und gegebenenfalls bei welcher Stelle oder Person die identifizierenden Daten einer Lehrerin/eines Lehrers zusammen mit dem Zugangscode gespeichert werden. Außerdem war aus datenschutzrechtlicher Sicht nicht auszuschließen, dass aus der Kombination der Antworten auch die Möglichkeit bestand, auf eine bestimmte Person zu schließen, beispielsweise, wenn die vorwiegend ausgeübte Tätigkeit an der Schule oder spezielle und seltene Fachkombinationen erfasst werden. Auch aus dem Alter könnte im Einzelfall auf eine Person geschlossen werden, wenn es zum Beispiel nur eine weibliche Lehrperson gibt, die 64 Jahre alt ist. Wir haben daher empfohlen, den Datensatz so zu gestalten, dass die Bestimmbarkeit einer Person nicht oder nur mit unverhältnismäßig hohem Aufwand möglich wäre. Außerdem konnten wir den Unterlagen nicht entnehmen, durch welche organisatorischen und technischen Maßnahmen sichergestellt werden sollte, dass jede Teilnehmerin bzw. jeder Teilnehmer nur ihre bzw. seine Daten bearbeiten und zur Kenntnis nehmen kann und ob dem Auftragnehmer personenbezogene Daten der Lehrerinnen und Lehrer übermittelt werden.

Um diese Fragen zu diskutieren, fand ein Gespräch mit dem Ministerium statt. Vom Ministerium war zu erfahren, dass das mit der Durchführung der Studie beauftragte Unternehmen keine Namenslisten der Lehrkräfte erhält, sondern nur den Namen der Schule und die Schulform (Gymnasium, Realschule) sowie die Anzahl der dort beschäftigten Lehrkräfte und die des weiteren Personals.

Zugang zur Befragung erhalten die Lehrkräfte über einen Schulschlüssel plus einer persönlichen PIN, wobei der Schulschlüssel auch dem Ministerium nicht bekannt ist. Die persönliche PIN wird den Schulen in einem Sicherheitskuvert übergeben. Jede Lehrkraft, die an der Befragung teilnimmt, sucht sich einen verschlossenen Umschlag aus, sodass die PIN nur ihr bekannt ist. Der Schule ist somit nicht bekannt, welche Lehrkraft welche PIN besitzt. Für die geplante Folgeerhebung wird dann ein zweiter Code pro Lehrkraft an die Schule gesandt. Diesen kann wieder jede Lehrkraft auswählen, indem sie einen verschlossenen Umschlag zieht. Die Anmeldung zur Befragung kann dann nur über den Schulschlüssel plus erste und zweite PIN erfolgen. Sollte eine Lehrkraft die erste PIN nicht mehr haben, kann sie auch nicht an der Zweitbefragung teilnehmen. Das Ministerium selbst erhält nur das Landesergebnis und das Ergebnis pro Schule.

Im Ergebnis wurden die Projektunterlagen dahingehend geändert, dass keine Angaben mehr erfragt werden, die es erlauben würden, die Antworten eindeutig der Person zuzuordnen, die den Fragebogen bearbeitet hat. Durch die frühzeitige Einbeziehung unserer Behörde schon bei der Projektplanung wurden unsere datenschutzrechtlichen Hinweise für die Durchführung der Befragung entsprechend berücksichtigt.

6.9.2 E-Mail mit unverschlüsselten Personaldaten

Ein Bediensteter einer Universität unseres Landes hat sich 2013 an uns gewandt, weil das Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern ihn betreffende Personaldaten per unverschlüsselter E-Mail an die Universität gesandt hatte. Das Ministerium begründete dies mit der Eilbedürftigkeit der Personalsache. Ähnliche Sachverhalte sind im Geschäftsbereich des Ministeriums bereits öfter aufgetreten. So sind zum Beispiel im Rahmen einer Schulgründung 2012 Personaldaten unverschlüsselt an einen externen Gutachter gesandt worden.

Bei einer Übermittlung von Personalaktendaten per E-Mail sind vor allem die Vertraulichkeit und die Integrität der Daten gefährdet. Für unbeteiligte Dritte ist es möglich, den Inhalt einer unverschlüsselten E-Mail zur Kenntnis zu nehmen. Die E-Mail kann außerdem leicht unbefugt geändert oder gefälscht werden. Mit geeigneten kryptographischen Verfahren können solche Manipulationen erkannt werden. Aus datenschutzrechtlicher Sicht müssen personenbezogene Daten daher verschlüsselt per E-Mail übermittelt werden. Dies gilt insbesondere für Daten, die den Bestimmungen des Landesbeamtengesetzes (LBG M-V) unterliegen und deshalb als besonders schutzbedürftig einzuordnen sind. Personalaktendaten sind wegen ihres sensiblen Inhalts vertraulich zu behandeln und vor unbefugter Einsichtnahme zu schützen (§§ 84 ff. LBG M-V). Die Verantwortung für eine ordnungsgemäße Übertragung trägt die absendende Stelle. Gemäß §§ 21, 22 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) sind die öffentlichen Stellen verpflichtet, erforderliche und angemessene technische und organisatorische Maßnahmen zu treffen. Die unverschlüsselte Übermittlung von Personalunterlagen per E-Mail verstößt gegen die Pflicht, Vertraulichkeit, Integrität und Authentizität der Daten zu gewährleisten (§ 21 Abs. 2 Nr. 1, 2 und 4 DSG M-V).

Der Einsatz asymmetrischer kryptographischer Verfahren zum Schutz von E-Mails mit personenbezogenen Daten entspricht dem Stand der Technik und ist erforderlich, geeignet und angemessen. Kryptographie-Lösungen für E-Mails sind technisch ausgereift, teilweise standardisiert und marktüblich. Sie sind erforderlich, da andere Mittel zum Schutz der E-Mail-Inhalte in der Regel ineffektiv sind.

Wir haben das Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern bereits 2010 in einem anderen Zusammenhang dazu beraten, welche Verschlüsselungsverfahren zum sicheren Versand von Personaldaten per E-Mail über das Internet dem Stand der Technik entsprechen. So hatten wir vorgeschlagen, OpenPGP-kompatible Programme wie das quelloffene GnuPG einzusetzen. Wir haben ausdrücklich darauf hingewiesen, dass die regelmäßige verschlüsselte Übertragung mit solchen Programmen mit geringerem Aufwand und niedrigerer Fehlerrate realisierbar ist als beim Einsatz von Programmen mit symmetrischer Verschlüsselung wie WinZip. Das Ministerium hielt jedoch die symmetrische Verschlüsselung auf der Basis des Algorithmus AES mit Archivierungsprogrammen wie WinZip, 7zip oder WinRAR für ausreichend. Dieser Auffassung konnten wir uns nicht anschließen. Wir haben jedoch erklärt, dass wir den Einsatz der genannten Archivierungsprogramme für eine gewisse Übergangszeit für die gesicherte Übermittlung von Personaldaten für tolerabel halten, wenn hinreichend sichere Passwörter verwendet werden und eine sichere Übermittlung, Aufbewahrung, Nutzung und Vernichtung der Passwörter gewährleistet ist. Falls innerhalb einer angemessenen Frist keine adäquaten zentralen Sicherheitslösungen zur Verfügung stehen, haben wir dem Ministerium empfohlen, selbst eine Lösung zu finden. Das Ministerium hat dann auch eingeräumt, dass die verschlüsselte Übermittlung mithilfe von Archivierungsprogrammen nicht optimal, zudem anfällig und generell verbesserungsbedürftig ist und daher entsprechende Lösungen im Zusammenhang mit der Entwicklung des einheitlichen IT-Grundsystems der Landesregierung angestrebt werden sollten. Es stimmte uns auch zu, dass nur bedingt lange auf eine zentrale Lösung gewartet werden sollte, und es wurde in Aussicht gestellt, dass frühestens 2011 an der Schaffung einer einheitlichen Lösung für das Ministerium begonnen werden könnte.

Offenbar hat die Verwendung von Archivierungsprogrammen mit symmetrischer AES-Verschlüsselung im Ministerium bisher nicht zum angestrebten Erfolg geführt, da es mehrfach zum unverschlüsselten Versand schutzbedürftiger personenbezogener Daten per E-Mail kam.

Angesichts dieser Vorgeschichte haben wir die wiederholte unverschlüsselte Übermittlung von Personaldaten per E-Mail durch das Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern beanstandet.

Das Ministerium hat uns zugesichert, künftig dem Stand der Technik entsprechende Verschlüsselungssoftware auf der Basis asymmetrischer Verfahren an den entsprechenden Arbeitsplätzen im Ministerium sowie in den Hochschulen und in anderen Behörden im Geschäftsbereich des Ministeriums einzusetzen. Die Mitarbeiterinnen und Mitarbeiter sollen im Umgang mit dieser Software unterwiesen werden. Die flächendeckende Installation der Software wird jedoch einige Zeit in Anspruch nehmen. Deshalb hat der Leiter der Hochschulabteilung die Mitarbeiterinnen und Mitarbeiter, die mit Personalangelegenheiten betraut sind, angewiesen, die Anhänge mit Personalaktendaten im E-Mail-Verkehr über das Internet nur noch verschlüsselt zu versenden. Hierzu sind die vorhandenen Archivierungsprogramme mit AES-Verschlüsselung zu nutzen.

Wir empfehlen der Landesregierung, für eine einheitliche Ausstattung der Arbeitsplätze in den Landesbehörden mit Verschlüsselungstechnik zu sorgen, damit ein gesicherter Versand von vertraulichen Nachrichten möglich ist.

6.9.3 Schulinformations- und Planungssystem (SIP)

Das Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern hat mit dem Schulinformations- und Planungssystem (SIP) ein neues System zur Verarbeitung von Daten über Lehrpersonal und Schülerinnen und Schüler an Mecklenburg-Vorpommerns Schulen in Betrieb genommen. Es löst unter anderem das Schulberichtssystem ab (siehe Siebter Tätigkeitsbericht, Abschnitt VII 2).

Wir hatten das Ministerium rechtzeitig vor dem Start des neuen Systems darauf hingewiesen, dass Schülerinnen und Schüler, Eltern und Lehrerinnen und Lehrer angemessen über die Verarbeitung ihrer Daten im SIP zu unterrichten sind. Dennoch kam es Mitte 2012 zu Irritationen unter den Betroffenen. Deshalb hat das Ministerium in seinem Betriebserlass vom 3. Januar 2013 festgelegt, dass Schulleiterinnen und Schulleiter die betroffenen Personengruppen künftig einmal jährlich über die Erhebungsmerkmale unterrichten und über weiteres Informationsmaterial, welches das Ministerium auf seiner Website zur Verfügung stellt, informieren sollen.

Auch zu Fragen der Informationssicherheit im SIP haben wir das Ministerium ausführlich beraten. Dabei war zu beachten, dass im SIP auch sensible personenbezogene Daten verarbeitet werden. Dazu gehören Daten wie Förderbedarf aufgrund von Lese-Rechtschreib-Schwäche oder Rechenschwäche, denn diese Daten lassen einen Rückschluss auf den Gesundheitszustand der Betroffenen zu. Entgegen der Ansicht des Ministeriums gilt das unabhängig davon, ob der Förderbedarf mit pädagogischen oder mit medizinischen Methoden festgestellt wurde.

Aufgrund der Sensibilität der Daten sind hohe Anforderungen an die Informationssicherheit der Systeme und Verfahren zu stellen, insbesondere bei der Datenübertragung zwischen Schulen bzw. anderen beteiligten Stellen und dem zentralen Server. Ursprünglich wurde dazu ein kryptographisch gesichertes Virtual Private Network (VPN) verwendet, also ein verschlüsseltes Netzwerk, das das Internet als Transportmedium für verschlüsselte Datenpakete genutzt. Dieses Produkt funktionierte aber nicht stabil genug.

Als Alternative wird seitdem Transport Layer Security (TLS) genutzt, wie es in jedem modernen Webbrowser eingebaut ist (siehe Zehnter Tätigkeitsbericht, Punkt 4.2.6). Wir haben dieser Alternative unter folgenden Bedingungen zugestimmt:

a) TLS-Version 1.2
Angesichts der sicherheitstechnischen Probleme mit älteren TLS-Versionen ist es erforderlich, TLS 1.2 einzusetzen. Dazu muss Clientsoftware eingesetzt werden, die diese Protokollversion unterstützt. Außerdem muss serverseitig sichergestellt sein, dass Verbindungswünsche mit älteren Protokollversionen abgewiesen werden.

b) Aktuelle kryptographische Primitive
Analog ist auf Client- und Server-Seite sicherzustellen, dass Verbindungen mit aktuellen kryptographischen Primitiven aufgebaut werden. RC4, MD5, DES sowie RSA unter 1536 Bit gehören nicht mehr dazu.

c) Client-Zertifikat
Clients müssen mit eigenen Zertifikaten ausgestattet werden, mit denen sie sich dem Server gegenüber authentifizieren können. Der Server muss eine solche zertifikatsbasierte Authentifizierung zusätzlich zu Benutzername und Passwort verlangen. Dies ist unter anderem deshalb erforderlich, weil in modernen Browsern unüberschaubar viele Zertifizierungsstellen vorgegeben sind, die unmöglich alle auf ihre Vertrauenswürdigkeit und ihr korrektes Arbeiten hin im Auge behalten werden können. Sollte ein gefälschtes, aber vom Browser dennoch akzeptiertes SIP-Zertifikat in Umlauf geraten, könnte ein damit gefahrener Man-in-the-Middle- Angriff am Server erkannt werden.

Mittelfristig sollten überdies individualisierte Zertifikate anstelle eines Gruppen-Zertifikates für alle SIP-Nutzerinnen und -Nutzer benutzt werden.

d) Extended Validation Certificate (EV) für das Schulportal
Für das Schulportal muss ein EV-Zertifikat benutzt werden und es muss den Anwenderinnen und Anwendern auferlegt werden, das Zertifikat in angemessener Weise zu prüfen.

EV-Zertifikate werden aufgrund einer Prüfung der Identität des Zertifikats-Inhabers ausgestellt, die bestimmten Mindestanforderungen genügt. Andere Zertifikate werden schon aufgrund sehr oberflächlicher Prüfmethoden, wie einem einfachen Austausch unverschlüsselter Mails, erzeugt und ausgegeben.

e) Client-Software sicher installieren und administrieren
Client-Software wie Browser oder Terminal-Server-Clients müssen sicher installiert und administriert werden. Dazu gehören auch sichere Update-Prozeduren. Die Installation muss daher einem Administrator obliegen. Updates müssen ebenfalls im administrativen Kontext erfolgen. Nutzerinnen und Nutzer dürfen keinen ändernden Zugriff auf den Programmcode haben. Denkbar sind jedoch automatisierte Update-Prozeduren durch einen System-Dienst mit administrativen Rechten. Solche Verfahren sind beispielsweise bei Virenscannern üblich.

Es ist jedoch darauf hinzuweisen, dass es sich bei TLS um ein sehr komplexes Protokoll handelt. Dadurch kann es leicht zu Fehlern im Protokolldesign und in der Implementation kommen. Dies ist in der Vergangenheit bereits öfter passiert; die oben erwähnten Schwächen der Versionen 1.0 und 1.1 illustrieren dies. Obwohl bei TLS 1.2 zurzeit keine ernstzunehmenden Schwächen bekannt sind, ist es deshalb sinnvoll, mögliche Alternativen und Umstiegsmöglichkeiten auf andere Protokolle im Auge zu behalten. Zu diesen Alternativen gehört IPsec als Standard-Sicherheitsprotokoll für die Internet-Protokollversionen 4 und 6 (siehe Punkt 5.1.5).

Das Ministerium hat diese Auflagen akzeptiert, sich aber eine Übergangszeit für die Client-PC ausgebeten, die noch mit Windows XP laufen. Diese Übergangszeit endet spätestens mit dem Auslaufen der technischen Unterstützung von MicroSoft für dieses Betriebssystem im April 2014.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat für TLS am 8. Oktober 2013 einen Mindeststandard nach § 8 Abs. 1 Satz 1 BSI-Gesetz für den Einsatz des TLS-Protokolls in der Bundesverwaltung herausgegeben (https://www.bsi.bund.de/DE/Publikationen/Mindeststandards/SSL-TLS-Protokoll/SSL-TLS-Protokoll_node.html). Aufgrund einer besonderen kryptographischen Eigenschaft führt die Kompromittierung eines Serverschlüssels nicht dazu, dass frühere Verbindungen, die eventuell von einem Unbefugten aufgezeichnet wurden, entschlüsselt werden können. Diese Eigenschaft wird perfect forward secrecy (PFS – etwa zu übersetzen mit: perfekte vorwärts (oder: in die Zukunft) gerichtete Geheimhaltung) genannt und kommt Verfahren nach dem von Whitfield Diffie und Martin Hellman entwickelten Prinzip zu. Da dieser Standard den aktuellen Stand der Technik widerspiegelt, werden wir ihn auch in unserer Beratungs- und Kontrolltätigkeit zugrundelegen. Demnach sind die Schlüsselaustauschverfahren von TLS auf diejenigen zu beschränken, deren Bezeichnung mit DH oder ECDH beginnt. Damit ist die Auswahl der Krypto-Algorithmen noch weiter eingeschränkt als unter b) beschrieben.

6.9.4 Erhebung von personenbezogenen Stellenplandaten von Hochschulen

Eine Hochschule hat uns darüber informiert, dass das Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern seit einigen Jahren personenbezogene Stellenplandaten von allen Hochschulen des Landes erhebt. So sollen unter anderem Name, Vorname, Geburtsdatum, Geschlecht sowie Angaben über eine Schwerbehinderung der Stellenplaninhaberin/des Stellenplaninhabers und die Entgelt- bzw. Besoldungsgruppe übermittelt werden. Die Hochschule hat uns gebeten zu prüfen, ob die Übermittlung der geforderten personenbezogenen Daten aus datenschutzrechtlicher Sicht zulässig ist.

Auf unsere Anfrage hin, ob der Sachverhalt zutrifft und falls ja, auf welcher Rechtsgrundlage und zur Erfüllung welcher Aufgabe die Daten personenbezogen erhoben werden müssen, begründete das Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern in seiner Stellungnahme die Erhebung der personenbezogenen Stellenplandaten mit seiner Fachaufsicht über die Personalverwaltung der Hochschulen und stützte diese auf § 2 Abs. 3 i. V. m. Abs. 2 Nr. 1 Landeshochschulgesetz (LHG M-V). Das Ministerium hat in seiner Stellungnahme darauf hingewiesen, dass es nur noch ein geringes Maß an Steuerungsmöglichkeiten im Rahmen der Fachaufsicht gibt.

Dieser Rechtsauffassung konnten wir uns nicht anschließen. Das allgemeine Datenschutzrecht erlaubt zwar die Nutzung der für andere Zwecke erhobenen oder erstmalig gespeicherten personenbezogenen Daten unter anderem zu Zwecken der Ausübung von Aufsichts- und Kontrollbefugnissen in dem dafür erforderlichen Umfang. Der Zugriff auf personenbezogene Daten ist aber nach der Rechtsvorschrift insoweit einzugrenzen, als er für die Ausübung der Befugnisse unerlässlich oder unvermeidbar ist, § 10 Abs. 4 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V).

Außerdem ergab sich für uns die Frage, warum die Stellenplandaten überhaupt personenbezogen genutzt werden. Würde auf den Personenbezug (Name, Vorname, Geburtsdatum) verzichtet, wäre nach unserer Auffassung die Nutzung auf die erforderlichen Daten beschränkt und damit zulässig.

Das Ministerium hat daraufhin gebeten, die angesprochenen datenschutzrechtlichen Fragen in einem Gespräch zu erörtern. Das Gespräch fand im Oktober 2010 statt. Im Ergebnis wurde vereinbart, dass das Ministerium unsere Empfehlung, nur die erforderlichen Daten zu erheben, prüft und mit dem Finanzministerium abstimmen wird. Über das Ergebnis des Abstimmungsprozesses sollten wir zu gegebener Zeit unterrichtet werden. Trotz mehrfacher Nachfragen hat sich das Ministerium lange Zeit gelassen, um uns über dieses Ergebnis zu informieren.

Das Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern hat schließlich mitgeteilt, dass es personenbezogene Stellenplandaten von den Hochschulen nicht mehr erheben wird. Es behält sich zukünftig jedoch vor, in begründeten Einzelfällen Stellenplandaten in anonymisierter Form von den Hochschulen zu erheben. Es wird sich dabei um Informationen handeln, die zum Beispiel Auskunft geben zum Umfang der Stellenbesetzung, zum durchschnittlichen Grad der Auslastung der Stellen oder zum Zeitpunkt der Wiederbesetzung frei werdender Stellen. Das Ministerium hat auch zugesichert, die Hochschulen über diese Vorgehensweise zu informieren.

6.9.5 Hochschule übermittelt Personalausweisnummern von Studierenden an Praktikumsbetriebe

Eine Hochschule hatte Studierende bei verschiedenen Betrieben für ein Praktikum angemeldet und dazu eine Liste übersandt, die folgende Angaben enthielt: Name, Vorname, Wohnort, Geburtsort, Geburtsdatum, Telefonnummer, E-Mail-Adresse sowie Personalausweisnummer. Die Studierenden wollten nun wissen, ob es datenschutzrechtlich zulässig sei, die Personalausweisnummern wegen der Teilnahme an einem Praktikum an die Betriebe zu übermitteln.

Auf unsere Anfrage hin hat die Hochschule mitgeteilt, dass die Daten von den Betrieben angefordert würden und dass sie froh sei, den Studierenden ein solches Angebot unterbreiten zu können. Mit anderen Worten: Die Hochschule wollte Auseinandersetzungen mit den Betrieben vermeiden, weil sie befürchtete, dass bei einer Diskussion über die Daten die Betriebe möglicherweise nicht mehr bereit wären, das Praktikum durchzuführen. Dies hätte wiederum gravierende Auswirkungen für die Studierenden, weil sie dann erforderliche Studienabschlüsse nicht erreichen könnten.

Einige Betriebe haben der Hochschule mitgeteilt, dass sie in sicherheitsrelevanten Bereichen tätig sind und zur Wahrnehmung ihres Hausrechts prüfen wollen, ob der Zutritt zu den Arbeitsstätten erlaubt werden kann, wozu eine Legitimation der Studierenden erforderlich sei. Diese Argumentation ist nachvollziehbar. Allerdings ist es für die Legitimation nicht erforderlich, dass bereits einige Zeit vor dem konkreten Zutritt zum Betrieb die Personalausweisnummer erhoben bzw. von der Hochschule an einen Betrieb übermittelt wird.

Vielmehr sollte es ausreichend sein, wenn die Betriebe eine Liste der Studierenden erhalten und sich von diesen für die Identitätsprüfung beim Betreten des Betriebsgeländes den Personalausweis zeigen lassen. Eine Speicherung von Ausweisdaten ist für diese Prüfung nicht erforderlich und damit unzulässig, es sei denn, dass ein Betrieb aufgrund einer gesetzlichen Vorschrift die Identität seiner Besucherinnen und Besucher nachweisen muss. In diesem Fall wären diese darauf hinzuweisen, auf welcher Rechtsgrundlage welche Ausweisdaten für welchen Zweck verarbeitet werden. Eine solche Aufklärungspflicht ergibt sich zum Beispiel aus § 4 Abs. 3 Bundesdatenschutzgesetz (BDSG).

Vor diesem Hintergrund wäre aus datenschutzrechtlicher Sicht nichts dagegen einzuwenden, wenn die Studierenden sich auf freiwilliger Basis in Listen einschreiben, die dann an die Betriebe übermittelt werden, die das Praktikum anbieten. Zu diesem Zweck könnten Name und Vorname sowie Adresse oder Geburtsdatum erhoben werden. Auf der Grundlage dieser Daten ist eine Identitätsprüfung durch die Betriebe möglich. Die Betriebe können außerdem davon ausgehen, dass die Hochschule dafür Sorge trägt, dass in die Liste nur Studierende aufgenommen worden sind, die für das Praktikum aus organisatorischer Sicht in Frage kommen. Es wäre darüber hinaus datenschutzrechtlich nichts dagegen einzuwenden, wenn - wiederum auf freiwilliger Basis - die Studierenden ihre Telefonnummer und/oder ihre E-Mail-Adresse eintragen können, damit die Betriebe mit ihnen gegebenenfalls individuelle Absprachen treffen können. Da diese Daten aber für die Identitätsprüfung nicht erforderlich sind, müsste auf diese Nutzung gesondert hingewiesen werden. Eine Pflicht, auch diese Daten anzugeben, besteht aber nicht.

Die Hochschule sicherte zu, bei der Organisation der nächsten Praktika diese Hinweise zu berücksichtigen.

Im Übrigen ist bei Datenübermittlungen immer zu beurteilen, ob ausreichende Maßnahmen zur Datensicherheit getroffen worden sind. Bei einer Übermittlung einer solchen Liste per E-Mail sollten Verschlüsselungswerkzeuge wie beispielsweise pretty good privacy (PGP) genutzt werden. Wäre dieser Aufwand unverhältnismäßig, weil personenbezogene Daten zwischen den Stellen selten übermittelt werden und ein Verschlüsselungssystem noch nicht implementiert wurde, sollte die Liste per Post versandt werden, was dann auch eine angemessene Maßnahme wäre.

6.9.6 Nutzen von sozialen Netzwerken im Internet für schulische Zwecke

Das Nutzen von sozialen Netzwerken im Internet für schulische Zwecke ist zurzeit auch in Mecklenburg-Vorpommern nicht rechtskonform, da die Nutzungsbedingungen der sozialen Netzwerke nicht mit dem deutschen Datenschutzrecht vereinbar sind. So fehlt es zum Beispiel an einem schriftlichen Datenverarbeitungsauftrag, der gemäß § 4 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) notwendig ist, wenn personenbezogene Daten im Auftrag einer öffentlichen Stelle (hier: Schule) durch eine andere Stelle (hier: Anbieter des sozialen Netzwerks) verarbeitet werden.

Selbst wenn man deutsches Datenschutzrecht aufgrund des Hauptsitzes der Anbieter sozialer Netzwerke nicht für anwendbar hält, so bleiben die Gesetze, die das Lehrer-Schüler-Verhältnis regeln, gültig. Gemäß § 70 Abs. 1 Schulgesetz Mecklenburg-Vorpommern (SchulG M-V) dürfen personenbezogene Daten von Schülerinnen und Schülern nur zur Erfüllung des Unterrichts- und Erziehungsauftrages erhoben und verarbeitet werden. Soziale Netzwerke im Internet jedoch verarbeiten die über das Netz ausgetauschten Daten gemäß ihrer eigenen AGB zu Nutzerprofilen, die später zu Werbezwecken genutzt werden. Eine solche Verarbeitung der Daten von Schülerinnen und Schülern ist nicht zur Erfüllung des Unterrichts- und Erziehungsauftrags erforderlich und ist dementsprechend nicht von § 70 Abs. 1 SchulG M-V gedeckt.

Durch das Einstellen von personenbezogenen Daten einer Schülerin bzw. eines Schülers durch eine Lehrkraft werden mittelbar Daten an den Anbieter des sozialen Netzwerkes übermittelt. Eine solche Übermittlung an Stellen außerhalb des öffentlichen Bereiches ist gemäß § 70 Abs. 2 SchulG M-V nur zulässig, wenn die Schülerin bzw. der Schüler eingewilligt hat. Dies setzt voraus, dass die Schülerin bzw. der Schüler einwilligungsfähig ist und dass so über die Datenverarbeitungsvorgänge unterrichtet wird, dass die Schülerin bzw. der Schüler die Bedeutung und Tragweite der Einwilligung überblicken kann. Bei den großen sozialen Netzwerken werden Datenverarbeitungsvorgänge jedoch so komplex, unvollständig und weitgehend unverständlich dargestellt, dass die Wirksamkeit einer solchen Einwilligung in der Regel ganz offensichtlich nicht angenommen werden kann.

Weiter heißt es in § 70 Abs. 5 SchulG M-V: „Personenbezogene Daten [von Schülern] sind durch geeignete technische und organisatorische Maßnahmen vor unberechtigtem Zugriff zu sichern.“ Die Server der großen sozialen Netzwerke befinden sich in den USA. Die dortigen Datenschutzstandards entsprechen weder den deutschen Standards noch gibt es in unserem Sinne durchsetzbare Möglichkeiten, die Datensicherheit bei der Datenverarbeitung vor Ort durch technische und organisatorische Maßnahmen sicherzustellen.

§ 6 Abs. 2 Satz 2 der Schuldatenschutzverordnung Mecklenburg-Vorpommern (SchulDSVO M-V) verlangt die Sperrung personenbezogener Daten, wenn deren Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist. Bei privaten Datenverarbeitungsanlagen ist dies spätestens ein Jahr, nachdem die Schülerinnen und Schüler nicht mehr von der Lehrkraft unterrichtet werden, der Fall. Was für Daten auf privaten Datenverarbeitungsanlagen - also dem privaten Computer der Lehrkraft - gilt, muss ebenso für Daten gelten, die durch die Veröffentlichung im sozialen Netzwerk gespeichert sind. Wie eine Sperrung von personenbezogenen Daten im sozialen Netzwerk, dessen Verarbeitungsprozesse man derzeit nicht steuern kann, umgesetzt werden soll, bleibt offen.

Insgesamt sollte nicht vergessen werden, dass eine Lehrkraft, die Schülerinnen bzw. Schüler aktiv zur Kommunikation über Facebook und Co. auffordert, diese Schülerinnen und Schüler zur Offenbarung von personenbezogenen Daten in einem unkontrollierbaren und für Börsenzwecke eingerichteten virtuellen Umfeld anhält und damit ein Unternehmen unterstützt, welches mit den Daten der Schülerinnen und Schüler Profite erwirtschaftet. Dies ist mit dem Bildungs- und Erziehungsauftrag der Lehrkräfte nach unserer Meinung nicht vereinbar.

Wir sprechen uns aufgrund rein praktischer Erwägungen trotzdem nicht für ein einfaches Verbot aus, sondern wollen mit unserem Projekt „PeerCon“ (siehe Punkt 2.9) eine rechtssichere, datenschutzfreundliche, für die Nutzerinnen und Nutzer grundsätzlich kostenfreie und nachhaltige Lösung zur schulischen Kommunikation über soziale Netzwerke im Internet anbieten. Dieses Angebot ist dazu geeignet, eine flexible, da individuell anpassungsfähige Alternative „von unten“ zu schaffen, die den Nutzerinnen und Nutzern ihre (informationelle) Selbstbestimmung wiedergibt.

6.10 Weitere Fälle

6.10.1 Zweckbindungsprinzip beim Bodenordnungsverfahren

Eine Petentin hatte uns mitgeteilt, dass sie Eigentümerin eines landwirtschaftlichen Betriebes und eines Wohngrundstückes ist. Mit dem Grundstück des Landwirtschaftsbetriebes ist sie auch Beteiligte in einem Bodenordnungsverfahren (Flurneuordnungsverfahren). Da sie mit den vom zuständigen Amt für Landwirtschaft und Umwelt (StALU) als Ausgleich für ihre alten Flächen vorgesehenen neuen Grundstücken nicht einverstanden war, legte sie gegen die Entscheidung Widerspruch ein. In der Begründung des Widerspruches wurde ihr vom StALU dann die Höhe der ihr bereits gewährten Fördermittel aus dem Programm der privaten Dorferneuerung in den Jahren 2004 bis 2011 vorgehalten. Sie hat uns gebeten, den Sachverhalt datenschutzrechtlich zu prüfen.

Wir haben das StALU über die Petition informiert und darum gebeten, den in der Begründung des Widerspruches dargestellten Zusammenhang zwischen dem Bodenordnungsverfahren und den gewährten Zuwendungen aus dem Programm der privaten Dorferneuerung rechtlich zu begründen. Darüber hinaus war uns bei der Durchsicht der von der Petentin übersandten Unterlagen aufgefallen, dass die Zuwendungsempfänger in dem Antrag um ihr Einverständnis gebeten wurden, ihre persönlichen Daten (Name, gefördertes Vorhaben sowie Höhe der Zuwendungen) in eine Liste aufzunehmen. Diese Liste wird jährlich europaweit veröffentlicht. Auch hierzu haben wir das StALU um eine rechtliche Begründung gebeten. Bereits in unserer Anfrage haben wir darauf hingewiesen, dass die geforderte Einverständniserklärung nicht mehr der Rechtslage entspricht und auf das hierzu vom Europäischen Gerichtshof ergangene Urteil vom 9. November 2010, C-92/09 verwiesen. In dieser Entscheidung wird die Praxis der Veröffentlichung der Daten der Zuwendungsempfänger, soweit es sich um natürliche Personen handelt, für ungültig erklärt. Wir haben daher empfohlen, die Unterlagen der Rechtslage anzupassen.

Das StALU hat daraufhin mitgeteilt, dass es berechtigt sei, die Daten aus dem Dorferneuerungsprogramm im Bodenordnungsverfahren gemeinsam zu nutzen, da es sich in beiden Fällen um die Förderung von investiven Maßnahmen der öffentlichen und privaten Dorferneuerung handele und es in diesem Fall zwischen Teilnehmerin am Bodenordnungsverfahren und Zuwendungsempfängerin eine Personenidentität gibt. Außerdem würde nur die Zuwendungsempfängerin über die Höhe der bereits erhaltenen Fördermittel informiert. Dritte könnten auf diese Information nicht zugreifen.

Diese Begründung war für uns nicht nachvollziehbar, da die datenschutzrechtlichen Bestimmungen zur Zweckbindung personenbezogener Daten nicht beachtet worden sind. Eine Bewilligungsbehörde ist nur befugt, die für das Antragsverfahren und die Einhaltung von Melde- und Veröffentlichungspflichten gegenüber der Europäischen Gemeinschaft erforderlichen Daten zu verarbeiten. Nach unserer Ansicht dürfen Zuwendungen von Mitteln aus dem Dorferneuerungsprogramm, die für Außensanierungen von Gebäuden im Ort vorgesehen sind, nicht im Zusammenhang mit der Entscheidung über die Abfindung von Garten- und Weideland herangezogen werden. Wir haben das StALU daher erneut um eine rechtliche Begründung gebeten.

Diese ließ allerdings lange auf sich warten. Trotz mehrmaliger Aufforderungen waren unsere Fragen zu einer nach unserer Auffassung unkomplizierten datenschutzrechtlichen Angelegenheit auch nach drei Monaten nicht nachvollziehbar beantwortet. Erst nachdem wir gegenüber dem StALU gemäß § 32 Abs. 1 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) eine Beanstandung wegen fehlender Mitwirkung ausgesprochen haben, wurde unser Schreiben beantwortet. Das StALU hat sich dann auch unserer Auffassung angeschlossen, dass gegen die Zweckbindung verstoßen worden ist. Es wurde uns versichert, dass Informationen über die Förderung der Dorferneuerung in Bodenordnungsverfahren zukünftig nicht mehr verwendet bzw. bekanntgegeben werden.

Hinsichtlich der bisher in Zuwendungsbescheiden abverlangten Einverständniserklärung hat sich das StALU an das Ministerium für Landwirtschaft, Umwelt und Verbraucherschutz mit der Bitte gewandt, die Unterlagen der Rechtsprechung anzupassen. Im August 2012 haben wir uns dann den im Internet bereitgestellten ,,Antrag auf Gewährung einer Zuwendung nach der Richtlinie für die Förderung der integrierten ländlichen Entwicklung (ILERL M-V)" angesehen. Die Einverständniserklärung zur Veröffentlichung von Informationen über die Empfänger von Fördermitteln wird nun nicht mehr verlangt.

6.10.2 Fingierte Aktenfunde

Unsere Behörde hatte Mitte des Jahres 2012 mit anonymer Post eine Daten-CD mit ca. 500 Kundendatensätzen erhalten. In dem anonymen Anschreiben wurde behauptet, dass der Absender diese Daten vor einem Altpapiercontainer gefunden, eingescannt und an den Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern übersandt habe. Es handele sich um Unterlagen eines namentlich genannten Kfz-Handelsbetriebs, der laut Mitteilung des anonymen Absenders noch weitere Rechtsverstöße begangen habe. Die Datenkategorien der einzelnen Datensätze enthielten unter anderem Angaben zu Name, Adresse, Geburtsdatum und Familienstand, Einkommen, Bankverbindungen und Personalausweisnummern.

Zusammen mit der zuständigen Polizeidienststelle und dem Kfz-Händler konnten wir klären, dass es sich bei den Dateien nicht um illegal im Müll entsorgte personenbezogene Daten handelte. Vielmehr lag allen Anzeichen nach eine „Racheaktion“ eines ehemaligen Mitarbeiters vor, der die Daten entwendet und nicht nur an den Landesbeauftragten für Datenschutz und Informationsfreiheit, sondern auch an Vertragspartner des Händlers gesandt hatte. Der Kfz-Handelsbetrieb hatte daraufhin bereits im Februar 2012 Strafanzeige bei der Polizei erstattet.

Einzelne Daten waren zudem (ebenfalls mit anonymer Post) mit ähnlicher Behauptung an Kundinnen/Kunden des Autohändlers übersandt worden, die ebenfalls Strafanzeige erstattet hatten. Die zuständige Polizeidienststelle bestätigte uns gegenüber, dass es sich nach den vorliegenden Anzeigen nach ihrem Eindruck um eine Art ,,Rachekampagne" des ehemaligen Mitarbeiters handele.

Entgegen unserer ersten Annahme handelte es sich außerdem nicht um Dateien des Händlers, sondern um die einer Kreditbank, die über den Sachverhalt informiert worden war. Da die Daten sich auf Kredite bei Autokäufen bezogen, waren die Kreditnehmer/innen gleichzeitig Kundinnen/Kunden des Autohändlers. Zu diesen Daten hatte sich der ehemalige Mitarbeiter unberechtigt Zugang verschafft. Wegen der daraus resultierenden Gefahr finanzieller Nachteile für die betroffenen Kundinnen und Kunden des Händlers lag uns vorrangig daran, dass diese darüber informiert wurden. Die Benachrichtigung diente der Sensibilisierung der Betroffenen und gab ihnen insbesondere die Möglichkeit, durch regelmäßige Kontrolle ihrer Bankauszüge einen möglichen Missbrauch schnell zu erkennen und Gegenmaßnahmen zu ergreifen. Der Autohändler war bei unserem Kontrollbesuch kooperativ und hat alle betroffenen Kundinnen und Kunden schriftlich informiert.

Generell besteht nach § 42 a BDSG eine Benachrichtigungspflicht für Firmen und Unternehmen. Stellen diese fest, dass bei ihnen gespeicherte sensible Daten wie Bank- und Kreditkartendaten (aber auch Gesundheitsdaten etc.) unrechtmäßig zur Kenntnis an Dritte gelangt sind, sind sie nach dieser Regelung verpflichtet, die Betroffenen und die Aufsichtsbehörde unverzüglich zu informieren. Voraussetzung ist eine drohende schwerwiegende Beeinträchtigung für die Rechte oder die schutzwürdigen Interessen der Betroffenen. Die Benachrichtigungspflicht besteht auch dann, wenn der Vorfall ohne Verschulden des Unternehmens eingetreten ist. Die Verletzung dieser Pflicht kann ein Bußgeldverfahren nach sich ziehen.

Von den meist anonymen Anzeigeerstattern wird bei fingierten Datenschutzverletzungen verkannt, dass sie sich selbst strafrechtlichen Konsequenzen aussetzen, wenn sie die Daten bei ihren „Racheaktionen“ unbefugt und in Schädigungsabsicht verwenden. Diese selbst inszenierten „Datenschutzverletzungen“ sind auch deshalb ärgerlich, weil sie die ohnehin knappen personellen Ressourcen der Aufsichtsbehörde und der Polizei zu Lasten der Aufklärung wirklicher Datenschutzverletzungen binden.

7 Arbeitskreis „Technische und organisatorische Datenschutzfragen“

7.1 Turnusmäßige Sitzungen des AK Technik

Seit über 20 Jahren leiten wir den Arbeitskreis „Technische und organisatorische Datenschutzfragen“ (AK Technik), der die Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu datenschutztechnischen Fragen unterstützt. Auch in seiner Funktion als Bindeglied zwischen dem IT-Planungsrat (siehe Punkt 4.1) und der Datenschutzkonferenz kommt dem AK Technik eine besondere Rolle zu. Ein wesentliches Anliegen bei der Leitung des Arbeitskreises ist es uns, für ein einheitliches Sicherheits- und Datenschutzniveau sowohl bei bundesweiten E-Government-Verfahren im Zusammenhang mit der Umsetzung der Nationalen E-Government-Strategie als auch bei entsprechenden Verfahren im Bereich des E-Commerce zu sorgen.

In zunehmendem Maße arbeitet der AK Technik mit anderen Arbeitskreisen der Datenschutzkonferenz wie dem AK Sicherheit oder dem Düsseldorfer Kreis zusammen. So war beispielsweise die enge Zusammenarbeit mit der AG Kreditwirtschaft des Düsseldorfer Kreises für die datenschutzrechtliche Bewertung der drahtlosen Zahlverfahren mit EC- und Kreditkarten (siehe weiter unten) zwingend erforderlich.

Es hat sich bewährt, in jedem Jahr zweimal mit den Technikern aller deutschen Datenschutzaufsichtsbehörden zusammenzukommen und dabei auch Kollegen aus den Datenschutzaufsichtsbehörden des benachbarten Auslands wie der Schweiz, Liechtensteins oder Österreichs einzubeziehen. Im Berichtszeitraum haben wir wieder vier Sitzungen des Arbeitskreises organisiert und geleitet.

Zur **58. Sitzung** des Arbeitskreises im Februar 2012 haben wir die Kollegen von Bund und Ländern in das Heinz-Nixdorf-Museumsforum (HNF) nach Paderborn eingeladen. Am Rande unserer Sitzung hatten wir die Möglichkeit, uns mit der Geschichte der Kryptographie vertraut zu machen und in einem Fachvortrag Interessantes über Alan Turing, die Enigma und die Geburt der modernen Kryptographie zu erfahren. Ein Schwerpunkt dieser Sitzung waren die Datenschutzaspekte der „SparkassenCard kontaktlos“. Der Vortrag eines Entwicklers der Sicherheitsinfrastruktur des Verfahrens war Ausgangspunkt der folgenden, langwierigen Beratungen zu diesem Thema (siehe Punkt 6.8.1). Erstmalig befasste sich der AK Technik auf dieser Sitzung mit dem Entwurf der EU-Datenschutz-Grundverordnung (siehe Punkt 3.1) und erarbeitete eine erste Stellungnahme aus technischer Sicht.

Die **59. Sitzung** des Arbeitskreises fand im Oktober 2012 in Schwerin statt. Ein Schwerpunkt dieser Sitzung war die Koordinierung der Beratungstätigkeit im IT-Planungsrat und die Vereinbarung entsprechender Beratungsschwerpunkte in verschiedenen Gremien des IT-Planungsrates (siehe Punkt 4.1). In dieser Sitzung wurde auch die Entschließung zur Übermittlung von Meldedaten erarbeitet, die von der Datenschutzkonferenz im November 2012 verabschiedet wurde (siehe Punkt 6.4.4). Zudem wurden die Beratungen zur „SparkassenCard kontaktlos“ fortgesetzt und Fragen der unverschlüsselten Speicherung von Transaktions- und Kartendaten auf der Karte erörtert. Intensiv beraten wurde zudem über die datenschutzrechtlichen Anforderungen an die Pseudonymisierungsverfahren bei der Führung von Krebsregistern. Die Mitglieder erarbeiteten einen Katalog mit Anforderungen an die Bildung von Kontrollnummern zur Pseudonymisierung von Daten über individuelle Fälle von Krebserkrankungen (siehe Punkt 6.6.4).

Zur **60. Sitzung** des AK Technik hatte die Koordinierungsstelle für IT-Standards (KoSIT) des IT-Planungsrates eingeladen (siehe Punkt 4.5). Da die KoSIT bei der Bremischen Finanzsenatorin angesiedelt ist, fand die Sitzung im Februar 2013 in Bremen statt. Die Vertreter der KoSIT informierten den AK Technik über das breite Aufgabenspektrum und erörterten mit den Mitgliedern des Arbeitskreises die Möglichkeiten der Zusammenarbeit. Mit Blick auf die Anforderungen des IT-Netzgesetzes wurde die künftige Rolle des Standards OSCI-Transport erörtert. Wiederum breiten Raum nahmen die Beratungen zur „SparkassenCard kontaktlos“ ein. Der Arbeitskreis formulierte einen Anforderungskatalog, der dann von der Vorsitzenden der Datenschutzkonferenz an den Deutschen Sparkassen- und Giroverband (DSGV) weitergeleitet wurde und Basis für die weiteren Diskussionen mit der Deutschen Kreditwirtschaft war.

Abgeschlossen wurden die in der 59. Sitzung begonnenen Beratungen zu Pseudonymisierungsverfahren bei der Führung von Krebsregistern. Der AK Technik erarbeitete eine Entschließung, die die Datenschutzkonferenz im März 2013 verabschiedete.

In der **61. Sitzung** im September 2013 in Schwerin musste sich der AK Technik erneut mit den drahtlosen Zahlungsverfahren befassen, diesmal nicht nur mit denen des DSGV, sondern auch mit den Verfahren PayPass von MasterCard und PayWave von VISA. Dazu hatten wir sowohl Vertreter der Deutschen Kreditwirtschaft als auch der beiden Kreditkartenunternehmen eingeladen. Die Beratungen zur „SparkassenCard kontaktlos“ konnten weitgehend abgeschlossen werden. Im Ergebnis formulierte der AK Technik seine abschließende Bewertung, die von der AG Kreditwirtschaft des Düsseldorfer Kreises um einige rechtliche Aspekte ergänzt und anschließend der Deutschen Kreditwirtschaft übermittelt wurde (siehe Punkt 6.8.1). Noch nicht abgeschlossen wurden die Beratungen zu den Verfahren der Kreditkartenunternehmen. Die von den Kreditkartenunternehmen präsentierten Verfahrensdokumentationen konnten die Mitglieder des AK Technik noch nicht überzeugen, da sie für eine datenschutzrechtliche Bewertung der Verfahren nicht aussagekräftig genug waren. Breiten Raum nahm auch die datenschutzrechtliche Bewertung des Umgangs mit nPA-Berechtigungszertifikaten für Identifizierungsdienste in kommunalen Bürgerportalen ein. In einem späteren Gespräch mit dem Bundesverwaltungsamt konnten dann Rahmenbedingungen vereinbart werden, die beim Betrieb dieser Bürgerportale zu berücksichtigen sind (siehe Punkt 6.4.5).

7.2 Workshop des AK Technik

Wie in den vergangenen Jahren (siehe Zehnter Tätigkeitsbericht, Punkt 4.2), haben wir auch in diesem Berichtszeitraum das Konzept des gemeinsamen Workshops von Technikern und Juristen fortgeführt. So kamen auch diesmal wieder Kolleginnen und Kollegen aus den verschiedenen Datenschutzdienststellen von Bund und Ländern zusammen, um sich über ein aktuelles Thema mit Datenschutzbezug zu informieren und Erfahrungen aus der Beratungs- und Aufsichtspraxis auszutauschen.

In diesem Workshop ging es um die datenschutzrechtlichen Aspekte bei der Nutzung mobiler Geräte. Wie aktuell dieses Thema ist, zeigt die Tatsache, dass nicht nur in unserer Behörde (siehe auch Punkt 5.1.8) eine stetig steigende Anzahl von Anfragen aus der öffentlichen Verwaltung zum datenschutzgerechten Einsatz dieser mobilen Endgeräte zu verzeichnen ist.

Mit Unterstützung unserer Kollegen vom Niedersächsischen Landesdatenschutzbeauftragten führten wir den Workshop unter dem Motto „Bring Your Own Device - Einsatz von iPad, iPhone & Co.“ im September 2012 in Hannover durch. Namhafte Referenten vom Fraunhofer Institut für sichere Informationstechnologie (SIT) und vom Bundesamt für Sicherheit in der Informationstechnik (BSI) erläuterten verschiedene technische Aspekte der betreffenden Geräte, beschrieben mögliche Angriffsszenarien und stellten zahlreiche Handlungsempfehlungen vor. Zudem konnten wir den Justiziar des Heise Zeitschriften Verlages gewinnen, die vielfältigen rechtlichen Aspekte der Nutzung von mobilen Geräten differenziert zu beleuchten. Schließlich hatten verschiedene Hersteller die Möglichkeit, ihre Lösungsvorschläge und verfügbaren Produkte zur datenschutzgerechten und datensicheren Nutzung mobiler Geräte vorzustellen.

7.3 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 (siehe Punkt 7) 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, sind wir als ständiger Vertreter der deutschen Landesdatenschutzbeauftragten Mitglied der Technology Subgroup. So ist es uns einerseits möglich, den AK Technik über die laufenden Entwicklungen im europäischen Rahmen zu informieren, und andererseits erlaubt uns die Mitgliedschaft, wichtige nationale Themen und Standpunkte des AK Technik auf internationaler Ebene einzubringen bzw. zu vertreten.

Besonders erwähnenswert sind neben dem gewinnbringenden Austausch und der einheitlichen Meinungsfindung zwischen den Mitgliedsstaaten auch die Erstellung von sogenannten „Opinions“. In diesen Stellungnahmen - vergleichbar mit den Orientierungshilfen auf nationaler Ebene - werden aktuelle technische Themen aus Datenschutzsicht betrachtet und sowohl rechtlich als auch technisch bewertet. Im Berichtszeitraum wurden dabei unter anderem die Themen Cloud-Computing (http://ec.europa.eu/justice/data-protection/article-29/ documentation/opinion-recommendation/files/2012/wp196_en.pdf), Biometrie (http://ec.europa.
eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf), Gesichtserkennung bei online und mobilen Services (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf) sowie App-Anwendungen auf mobilen Endgeräten (http://ec.euro pa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf) ausführlich bewertet.

8 Datenschutz-Fachtagungen

8.1 2012: Datenschutz - Fortschrittsbremse oder Bildungschance?

Die Datenschutz-Fachtagung 2012 zum Thema „Datenschutz - Fortschrittsbremse oder Bildungschance?“ fand am 22. Mai 2012 in der Industrie- und Handelskammer zu Schwerin statt. Das Thema Datenschutz ist schon lange kein reines Insiderthema mehr. Datenschutz als Schutz von Grundrechten zu begreifen, diese Grundrechte auch zu erkennen und wahrzunehmen, erfordert eine entsprechende Kompetenz der Bürgerinnen und Bürger. Diese Kompetenz kann nur durch Bildung erreicht werden. Datenschutz ist daher auch als Bildungsaufgabe zu verstehen, insbesondere schon bei Kindern und Jugendlichen.

Prof. Dr. Hubertus Gersdorf, Lehrstuhlinhaber der Gerd Bucerius-Stiftungsprofessur für Kommunikationsrecht der juristischen Fakultät der Universität Rostock, sachverständiges Mitglied der Enquete-Kommission Internet und digitale Gesellschaft, betonte in seinem Vortrag „Datenschutz im Wandel“, dass Datenschutz uns alle betrifft, insbesondere dann, wenn man im Internet „unterwegs“ ist - schließlich werden im Internet wesentlich größere Mengen an personenbezogenen Daten erhoben und verarbeitet als in der analogen Welt.

Der nahezu unbegrenzte und ständige Datenfluss im Internet und dort insbesondere in sozialen Netzwerken stellt Staat und Gesellschaft vor ungeahnte Herausforderungen. Das Internet birgt große Chancen, aber auch Risiken. Einerseits werden dem Einzelnen durch das Internet Kommunikationsmöglichkeiten eröffnet, die er früher nicht besaß. Ohne großen Kapitalaufwand können kleine und mittelständische Unternehmen ihre geschäftlichen Ideen verwirklichen. Staat und Gesellschaft haben die Möglichkeit, transparenter zu werden. Andererseits besteht unter anderem die Gefahr einer systematischen Erstellung von Persönlichkeitsprofilen durch eine immer intensivere Überwachung des Einzelnen. Der notwendige Interessenausgleich bereitet dem Staat besondere Schwierigkeiten, die sich insbesondere aus der Ungewissheit der Folgeneinschätzung, der Heterogenität und Komplexität des Internet ergeben. Was für den einen ein Risiko ist, ist für den anderen eine Chance. Dem technischen Datenschutz sollte im Rahmen einer künftigen Internetregulierung eine Schlüsselrolle zufallen. Es sollten Anreize zur Entwicklung von Systemen anonymer Datenerhebung und Datenverarbeitung gesetzt werden. Die Entwicklung von Medien- oder besser Netzkompetenz erweist sich als weitere wesentliche Voraussetzung für einen wirksamen Persönlichkeitsschutz im Internet. Nur die mit den Chancen und Risiken vertrauten Nutzerinnen und Nutzer können am Internet selbstbestimmt partizipieren. Informations- und Transparenzpflichten der Internetdiensteanbieter sind wichtig und richtig. Sie bedingen jedoch eine entsprechende Medien- bzw. Netzkompetenz der Nutzerinnen und Nutzer, mit deren Vermittlung bereits in der Schule begonnen werden sollte.

Stephan Micklitz, Tech Lead und Manager -User Facing Privacy Team, Google Germany München, ging in seinem Vortrag „Produktinnovationen im Datenschutz“ darauf ein, dass Transparenz und Kontrollmöglichkeiten als Grundprinzipien immer häufiger im Zusammenhang mit der Entwicklung neuer Web-Applikationen und deren Datenschutzvorkehrungen genannt werden. Um in einer nutzbaren Weise umgesetzt zu werden, müssen diese Grundprinzipien von Anfang an eine starke Bedeutung im Design- und Entwicklungsprozess neuer Web-Dienste einnehmen. Nur so können entscheidend die Akzeptanz, die Sicherheit und das Vertrauen in neue Produkte beeinflusst werden. In Produkten umgesetzt bieten Transparenz und Kontrollmöglichkeiten eine immense Bildungschance: Die Nutzerinnen und Nutzer haben die Möglichkeit, sich umfassend zu informieren, um auf dieser Basis zu einer informierten Entscheidung über die Datenschutz-Einstellungen des von ihnen verwendeten Dienstes zu kommen.

Edgar Wagner, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, erläuterte in seinem Vortrag „Datenschutz und Bildung“, dass die Bürgerinnen und Bürger des digitalen Zeitalters nicht mehr nur Betroffene von Datenverarbeitungsvorgängen sind, sondern dass sie sich zu Aktiven des Web 2.0 entwickelt haben. Im Verbund mit den neuen digitalen Möglichkeiten hat dieser Rollenwechsel dazu beigetragen, dass sie immer mehr Datenspuren hinterlassen und immer tiefere Einblicke in ihr Leben gewähren. Dies ist den Bürgerinnen und Bürgern bewusst, sie klagen auch darüber, dass sie die Kontrolle über ihre Daten verloren hätten. Mit Gesetzen allein wird man an dieser Situation nichts ändern können; notwendig ist es, vor allem den Kindern und Jugendlichen bestimmte Kenntnisse und ein bestimmtes Bewusstsein zu vermitteln. Das Zauberwort heißt „Medienkompetenz“, wozu nicht nur der Umgang mit ethisch fragwürdigen Seiten gehört, sondern auch der verantwortungsvolle Umgang mit den eigenen Daten und der rücksichtsvolle Umgang mit den Daten anderer.

Insoweit schließt Medienkompetenz die Datenschutzkompetenz ein. Datenschutz erschöpft sich deshalb auch nicht mehr im Erlass von Gesetzen und in der Kontrolle ihres Vollzugs, sondern ist auch eine Bildungs- und Erziehungsaufgabe. Auch, wenn die Wahrnehmung dieser Aufgabe nicht nur dem Staat, sondern auch der Zivilgesellschaft und der Wirtschaft obliegt, werden die Schulen diesen Auftrag erfüllen müssen.

Die Beiträge der Datenschutz-Fachtagung sind zu finden unter www.datenschutz-mv.de.

8.2 2013: Intelligente Gebäude - Datenschutz eingebaut?

Die Datenschutz-Fachtagung 2013 zum Thema „Intelligente Gebäude - Datenschutz eingebaut?“ fand am 22. Mai 2013 im Konrad-Zuse-Haus in Rostock, Sitz des Institutes für Informatik der Universität Rostock, statt. Mehr Komfort, mehr Wirtschaftlichkeit, mehr Sicherheit - mit intelligenter Gebäudetechnik ist vieles möglich. Aber welche Daten verarbeitet die Technik über die Menschen, die in so einem Gebäude wohnen oder arbeiten? Welche Risiken ergeben sich daraus für Bewohnerinnen und Bewohner sowie für Nutzerinnen und Nutzer und wie kann man die Risiken minimieren?

Der Tagungsort war nicht zufällig gewählt: Es handelt sich um einen modernen Bau mit komplexer Gebäudetechnik, um den Arbeitsort von Wissenschaftlerinnen und Wissenschaftlern, die selbst auch mehr über diese Technik erfahren wollten. Das Haus ist mit einem sogenannten KNX-Feldbus ausgestattet, welcher quasi für eine Vernetzung der modernen Haus- und Gebäudesystemtechnik sorgt, an das beispielsweise Lichtschalter, Bewegungsmelder, Lampen, Stellmotoren für Jalousien und Fenster und viele andere Geräte angeschlossen sind. Die angeschlossenen Geräte können nun „intelligent“ miteinander kommunizieren, über eine Steuerzentrale zentral kontrolliert oder sogar über das Internet angesteuert werden.

Prof. Dr. Clemens Cap von der Universität Rostock, Fakultät für Informatik und Elektrotechnik, Institut für Informatik, Lehrstuhl Informations- und Kommunikationsdienste, spannte in seinem Einführungsvortrag „Moderne Gebäudetechnik konkret“ den Bogen von allgemeinen Erkenntnissen über die Beeinflussung des Verhaltens von Menschen durch Überwachung bis hin zu Experimenten, bei denen die eigenen Mitarbeiterinnen und Mitarbeiter mit der Gebäudetechnik des Konrad-Zuse-Hauses beobachtet wurden. Die Wissenschaftlerinnen und Wissenschaftler konnten problemlos die Signale des Netzwerkes auslesen und Erstaunliches über ihre Kolleginnen und Kollegen herausfinden: Aus den Daten von Bewegungsmeldern auf den Fluren und Toiletten konnten sie nicht nur Anwesenheitszeiten ermitteln, sondern auch ableiten, wer sich nach der Toilettenbenutzung ausreichend lange die Hände gewaschen hat. Solche und andere Aussagen, die sich dank modernster Gebäudetechnik ableiten lassen, könnten nicht nur neugierige Kolleginnen und Kollegen oder penible Arbeitgeber, sondern auch potenzielle Diebe und andere Dritte interessieren. Möglich waren solche Analysen vor allem, da die Signale auf dem Netzwerk nicht gegen unbefugtes Auslesen geschützt sind; der KNX-Standard sieht keine verschlüsselte Übertragung oder sonstige Zugriffsbeschränkungen vor.

Prof. Dr. Dieter Hutter vom Deutschen Forschungszentrum für Künstliche Intelligenz GmbH (DFKI) Bremen stellte seinen Vortrag unter den Titel „Können Gebäude wirklich intelligent sein?", also können sie rational erkennen, Schlüsse ziehen und handeln? Das DFKI erforscht unter anderem, wie moderne Gebäudetechnik die sogenannten Ambient Assisted Living Systeme (AAL, deutsch: Altersgerechte Assistenzsysteme) unterstützen kann. Dies sind technische Systeme, die dem Menschen helfen, trotz altersbedingter oder anderer gesundheitlicher Defizite ein selbstbestimmtes Leben mit einer hohen Lebensqualität zu führen. Im Mittelpunkt steht das Konzept, dass sich die Technik den Bedürfnissen des Menschen anpasst und nicht umgekehrt. Entsprechend wirken diese Systeme unterstützend, indem sie beispielsweise den Herd automatisch abschalten, die Beleuchtung und die Raumtemperatur kontextabhängig steuern oder externe Dienstleister einbinden und ggf. Notfallmeldungen absetzen. Das DFKI hat eine Laborwohnung mit modernster Sensorik wie Trittsensoren, Kameras für Steuerung durch Gesten, RFID-Technik und mit Aktoren wie automatischen Türen und verstellbaren Möbeln ausgerüstet. In der Wohnung werden auch spezielle Rollstühle getestet, die unter anderem Hindernisse umfahren können. Am DFKI werden Prozesse entwickelt, mit denen die verschiedenen Einzelsysteme sinnvoll zusammenwirken können. Im Rahmen dieser Forschung spielen natürlich auch Fragen der technischen Sicherheit und des Datenschutzes eine wichtige Rolle. So wird nach Mitteln gesucht, welche die in dem System vorhandenen und teils sehr sensiblen Daten über die Nutzerinnen und Nutzer, zum Beispiel über ihren Gesundheitszustand und ihre Lebensgewohnheiten, ausschließlich Berechtigten zugänglich machen. Die Herausforderung besteht darin, dass eine reine Zugangskontrolle zu den Daten allein nicht ausreichend ist, da bereits aus dem Verhalten der einzelnen Geräte Rückschlüsse auf die Lebensumstände der Nutzerinnen und Nutzer gezogen werden können.

Dr.-Ing. Jörg-Ingo Jakob von der T-Systems GEI GmbH analysierte in seiner Rolle als ver.di-Vertreter in seinem Vortrag „Arbeitnehmer-Datenschutz durch Privacy by Design“, wie der Arbeitnehmer-Datenschutz bei der Gebäudetechnik zurzeit umgesetzt wird. Er berichtete davon, dass es in seinem Unternehmen, das Teil der Deutschen Telekom AG ist, bereits zahlreiche Betriebsvereinbarungen zum Thema Datenschutz gibt. Die Gebäudetechnik ist dabei bisher jedoch lediglich in Form von Videoüberwachungsanlagen und Zutrittskontrollsystemen berücksichtigt. In der Regel werden viele Betriebsvereinbarungen jedoch erst abgeschlossen, wenn die Gestaltungsprozesse bereits beendet sind. Dies gilt auch für den Bezug von Gebäuden mit eingebauten technischen Systemen. Die Analysen zahlreicher Betriebsvereinbarungen zeigen, dass gesetzliche Anforderungen des Datenschutzes schlecht in Geschäftsprozessen und Gebäudetechniken umgesetzt werden. Am Beispiel einer Vereinbarung zur Videoüberwachung wurde verdeutlicht, dass Datenschutz durch Technik als sinnvolles Gestaltungselement eingebracht werden sollte. Um der angesprochenen Betriebsvereinbarung gerecht zu werden, musste im Nachhinein unzulässigen Überwachungen durch den Einsatz von physikalischen Sichtblenden, technischen Vorkehrungen zur Einhaltung von Speicherfristen und andere aufwendigen Maßnahmen entgegengewirkt werden. Hätte man bereits im Vorfeld den Datenschutz in die Gesamtkonzeption einbezogen, wäre man damit dem Privacy-by-Design-Konzept gefolgt und hätte sich viele zusätzliche Kosten und umständliche Aufwände erspart.

Prof. Dr. Peter Wedde, Professor für Arbeitsrecht und Recht der Informationsgesellschaft und Direktor der Europäischen Akademie der Arbeit in der Universität Frankfurt am Main, sprach in seinem Vortrag „Beschäftigten-Datenschutz in Gefahr?“ über neue Entwicklungen im Beschäftigten-Datenschutz. Er schilderte zu Beginn einen Fall aus einem Unternehmen, in dem vermeintlich nur neue Rauchmelder installiert wurden. Die Mitarbeiterinnen und Mitarbeiter staunten jedoch nicht schlecht, als sie sich danach auf ihren Notebooks selbst bei der Arbeit zusehen konnten. In die Rauchmelder waren nämlich Videokameras mit WLAN-Anschluss eingebaut. Der Arbeitgeber zeigte sich davon selbst überrascht. Offenbar hatte der Lieferant Rauchmelder mit Zusatzfunktionen geliefert, die der Arbeitgeber aber so gar nicht bestellt hatte. Es bleibt festzuhalten, dass der Einsatz von komplexer Gebäudetechnik bislang nicht eingehend in der Gesetzgebung und Rechtsprechung berücksichtigt worden ist. Auch bei den neuen Entwicklungen zum Thema Beschäftigten-Datenschutzrecht, beispielsweise in der geplanten Datenschutz-Grundverordnung der Europäischen Union und in den neuen Normen im Bundesdatenschutzgesetz, sind derzeit keine Impulse zu erwarten.

Die Beiträge der Datenschutz-Fachtagung sind zu finden unter www.datenschutz-mv.de.

9 Informationsfreiheitsgesetz Mecklenburg-Vorpommern - IFG M-V

9.1 Rechtliche Entwicklungen

In Mecklenburg-Vorpommern gibt es seit Juli 2006 ein Informationsfreiheitsgesetz, welches inzwischen einmal novelliert worden ist. Die Entwicklung in Richtung Transparenz ist auch in anderen Bundesländern positiv. Mittlerweile kann man die Länder, in denen es noch keine Informationsfreiheit gibt, an einer Hand abzählen: es sind Baden-Württemberg, Bayern, Hessen, Niedersachsen und Sachsen. Besonders weit fortgeschritten ist die Freie und Hansestadt Hamburg, welche 2012 ein Transparenzgesetz verabschiedet hat, welches aus der Mitte der Zivilgesellschaft entstanden ist. Das Gesetz hat den Anspruch, Bürgerinnen und Bürger in die Lage zu versetzen, sich im Vorfeld politischer Entscheidungen die notwendigen Informationen zu verschaffen, um sich eine fundiertere Meinung zu bilden und entsprechend qualifizierte Vorschläge zur besseren Gestaltung eines Vorhabens einbringen zu können.

Durch die proaktive Veröffentlichungspflicht wird die demokratische Meinungs- und Willensbildung gefördert, eine Kontrolle staatlichen Handelns sowie Korruptionsprävention ermöglicht. Der Zugang zu Informationen in Hamburg war bisher nur auf Antrag möglich. Jetzt ist im Gesetz zusätzlich eine generelle Veröffentlichungspflicht festgeschrieben worden. Zu diesem Zweck wird ein Informationsregister eingerichtet werden. Zudem werden Ausschlusstatbestände angemessen reduziert und neu strukturiert. Das soll langfristig auch dazu führen, dass individuelle bürokratische Anfragen zurückgehen.

Im Landtag Mecklenburg-Vorpommern ist die Einbringung eines Transparenzgesetzes durch die Fraktion Bündnis 90/DIE GRÜNEN gescheitert.

Dennoch empfehlen wir, die Erfahrungen z. B. Hamburgs berücksichtigend, eine Novellierung des Informationsfreiheitsgesetzes zu prüfen. Wichtig sind dabei insbesondere eine proaktive Veröffentlichungspflicht aller öffentlichen Stellen, die Veröffentlichung von Verträgen, die mit der öffentlichen Hand geschlossen werden, und die Einrichtung eines Open-Data-Portals.

9.2 Open Data/Open Government

Die Bundesregierung hat am 19. Februar 2013 „GovData - Das Datenportal für Deutschland“ im Internet freigeschaltet. Das Portal bietet unter „Daten“ einen zentralen Zugang zu Daten der öffentlichen Hand aus Bund, Ländern und Kommunen.

Diese offenen Daten müssen an ihrem Ursprung gesammelt werden; die Datenkataloge müssen verlinkt werden und über Metadaten weiter erschließbar sein. Sie müssen in offenen Formaten zur Verfügung gestellt werden. Offene Formate sind solche, die plattformunabhängig und maschinenlesbar sind und der Öffentlichkeit ohne Beschränkungen zur Weiterverwendung bereitgestellt werden.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland hat in ihrer Entschließung am 27. Juni 2013 diese Entwicklungen ausdrücklich begrüßt und in einem Positionspapier wesentliche Anforderungen an eine moderne Transparenzgesetzgebung gefordert, abrufbar unter www.lfd.m-v.de/informationsfreiheit/beschluesse/entsch26.

Wir haben bei unserem Ministerium für Inneres und Sport unter Hinweis auf die Entschließung und das Positionspapier angefragt, wie die Open-Data-Strategie der Landesregierung aussieht. Wir haben klargestellt, dass die Informationsfreiheitsbeauftragten für eine kontextgerechte Regelung von Open Data in den jeweiligen Informationsfreiheitsgesetzen der Länder eintreten. Die Ansprüche auf Informationszugang und Veröffentlichung sollten einheitlich dort geregelt werden, um eine weitere Rechtszersplitterung zu vermeiden. Eine Antwort des Ministeriums steht noch aus.

Kategorien von Dokumenten, die quasi automatisch zu veröffentlichen sind, sollten in den Informationsfreiheitsgesetzen möglichst genau beschrieben werden. An dieser Stelle kann das Hamburger Transparenzgesetz als Vorbild dienen. Die im dortigen § 3 geregelte Veröffentlichungspflicht reicht vom Vorblatt und Petitum von Senatsbeschlüssen, von in öffentlicher Sitzung gefassten Beschlüssen - nebst den zugehörigen Protokollen und Anlagen - über Verträge der Daseinsvorsorge bis hin zu den wesentlichen Unternehmensdaten städtischer Beteiligungen.

Bislang werden aus Mecklenburg-Vorpommern lediglich Daten der Stadt Rostock in das Portal eingestellt.

9.3 Einsicht in Verkehrswertgutachten

Immer wieder wird die Einsicht in grundstücksbezogene Unterlagen und hier vor allem in Verkehrswertgutachten begehrt. Aus verschiedenen Gründen wird der Anspruch seitens der Gemeinde oft verwehrt.

So wollte in einem Fall ein Unternehmerverband Einsicht in ein Verkehrswertgutachten für ein zum Verkauf angebotenes Grundstück nehmen. Hierbei unterstützte der Verband ein Mitglied, der dieses Grundstück, welches er für seinen Gewerbebetrieb bereits nutzte, käuflich erwerben wollte. Die Kommune, in deren Eigentum sich das Grundstück befand, lehnte das Informationsbegehren unter Hinweis auf § 8 Informationsfreiheitsgesetz Mecklenburg-Vorpommern (IFG M-V) ab.

Nach § 8 Satz 2 IFG M-V können sich auch das Land und die Kommunen sowie die Unternehmen und Einrichtungen kommunaler Körperschaften bei einer Teilnahme am Wirtschaftsverkehr auf § 8 IFG M-V berufen. Sofern sich eine Behörde (nach durchaus strittiger Ansicht) aufgrund ihrer privatwirtschaftlichen Tätigkeit auf den Schutz von Betriebs- oder Geschäftsgeheimnissen beruft, sind dann die Voraussetzungen des § 8 Satz 1 IFG M-V zu prüfen.

Als Betriebs- oder Geschäftsgeheimnisse werden allgemein alle auf ein Unternehmen bezogene Tatsachen, Umstände und Vorgänge verstanden, die nicht offenkundig, sondern nur einem begrenzten Personenkreis zugänglich sind und an deren Nichtverbreitung der Rechtsträger ein berechtigtes Interesse hat (BverfG, Beschluss vom 14. März 2006 - 1 BvR 2087, 2111/03). Die entscheidende Voraussetzung ist, dass ein objektiv berechtigtes wirtschaftliches Interesse an der Geheimhaltung der Information besteht. Maßgeblich hierfür ist vor allem die wettbewerbsrechtliche Relevanz der Information. Dafür ist entscheidend, inwieweit die Offenbarung der begehrten Information geeignet ist, Konkurrentinnen oder Konkurrenten wirtschaftliche Vorteile zu verschaffen oder die eigene Wettbewerbsfähigkeit zu schwächen. Sofern im Hinblick auf die Aufgabenwahrnehmung eine Monopolstellung besteht, können wettbewerbsbezogene Nachteile aus einer Preisgabe der Informationen grundsätzlich nicht entstehen.

Durch die Stadtverwaltung wurde argumentiert, dass eine Offenlegung der Informationen Rückschlüsse auf kalkulatorische Erwägungen zulassen und dadurch die Verhandlungsführung beeinflusst werden könnte. Inwieweit sich hieraus spürbare Auswirkungen auf die Wettbewerbsfähigkeit ergeben sollten, wurde nicht deutlich. Dieses wäre nur dann der Fall, wenn der Kommune durch die Gewährung des Informationszugangs ein wirtschaftlicher (zumeist finanzieller) Schaden entstehen kann.

Hinzu kam noch, dass die Höhe des Kaufpreisangebotes dem Antragsteller bereits bekannt war und es bei der Einsicht in das Gutachten hauptsächlich darum ging, ob bei der Festlegung der Kaufpreishöhe alle wertbildenden Faktoren berücksichtigt wurden.

Zusätzlich hierzu war durch die Stadtverwaltung nicht berücksichtigt worden, dass sie aufgrund des bestehenden Eigentumsverhältnisses an dem Grundstück eine Monopolstellung inne hatte und sich somit gar nicht auf mögliche Betriebs- oder Geschäftsgeheimnisse berufen konnte.

Nach Information des Antragstellers ist die Verwaltung unserer Empfehlung, den Informationszugang zu gewähren, gefolgt.

9.4 Auskünfte zu Fördermittelanträgen

Vom Landesförderinstitut Mecklenburg-Vorpommern (LFI M-V) wurde der Zugang zu Informationen, die im Zusammenhang mit Fördermittelanträgen stehen, verlangt. Insbesondere wurde hinterfragt, ob bestimmte Unternehmen und Personen innerhalb eines feststehenden Zeitraumes Fördermittelanträge gestellt haben, wann genau dieses erfolgte und wie die Entscheidung dazu ausfiel.

Das LFI M-V lehnte den Antrag zumindest teilweise ab und bezog sich dabei auf den Umstand, dass die Informationen dort nur zum Teil vorhanden sind und Betriebs- oder Geschäftsgeheimnisse nach § 8 IFG M-V dem Informationszugangsanspruch entgegenstehen würden. Nach dieser Vorschrift ist der Antrag auf Informationszugang abzulehnen, soweit der Schutz geistigen Eigentums entgegensteht oder durch die Übermittlung der Informationen ein Betriebs- oder Geschäftsgeheimnis (Begriffserläuterung: siehe Punkt 9.3) offenbart wird und der Betroffene nicht eingewilligt hat.

Für uns war in diesem Fall nicht klar, worin ein berechtigtes wirtschaftliches Geheimhaltungsinteresse liegen sollte, weil es dem Antragsteller gerade nicht um den Zugang zu konkreten Angaben zu der Fördermittelhöhe und damit eventuell vertraulichen Informationen ging. Aus diesem Grund haben wir das LFI M-V gebeten, die Ablehnungsgründe noch einmal näher zu begründen, und gleichzeitig darauf hingewiesen, dass ein Geheimhaltungsinteresse dann besteht, wenn die Aufdeckung der Informationen spürbare Auswirkungen auf die Wettbewerbsfähigkeit des Unternehmens hat oder haben kann. Hierfür genügt zwar schon die Verbesserung der Konkurrenzfähigkeit von Wettbewerbern. Relevant sind aber immer beide Aspekte: die Schwächung des Unternehmens im Wettbewerb durch die Preisgabe der Informationen sowie die Förderung der Wettbewerbsfähigkeit von Konkurrenten. Indikatoren für die Ermittlung der Wettbewerbsrelevanz einer bestimmten Information sind mögliche Rückschlüsse auf die Betriebsführung, auf die Wirtschafts- und Marktstrategie sowie auf die Kostenkalkulation und die Entgeltgestaltung des Unternehmens sowie auf vergleichbare betriebsinterne Umstände (siehe Kommentar zum IFG, F. Schoch, § 6 Randnummer 54).

Das LFI M-V bekräftigte in der Stellungnahme noch einmal seine ablehnende Haltung und begründete dies damit, dass aus den Angaben zur Bewilligung und Auszahlung durchaus Schlüsse auf zeitliche Abläufe der Vorhabensfinanzierung gezogen werden könnten. Nur der Zuwendungsnehmer und die Bewilligungsbehörde würden demnach über Wissen verfügen, welches es potenziellen Mitbewerbern ermöglicht, den Finanzierungsprozess nachzuvollziehen und für eigene Investitionsvorhaben nachzuahmen. Diese Konkurrenten würden Kenntnis besitzen, wann ihnen letztlich Finanzierungsmittel zur Verfügung stünden, und könnten ihre Finanzplanung bereits zur Zeit der Kenntniserlangung hierauf abstellen.

Diese Auffassung teilten wir nicht, sodass eine Beanstandung und dabei die Empfehlung ausgesprochen wurde, den Zugang zu den dort vorliegenden Informationen zu gewähren. Die Beanstandung führte aber auch nicht zu dem gewünschten Erfolg, sodass wir im Ergebnis dem Petenten leider nicht zu einem vollständigen Informationszugang verhelfen konnten.

9.5 Auskunftsrechte der Kommunalverfassung vs. IFG M-V

Der Petitionsausschuss des Landtages Mecklenburg-Vorpommern bat uns um Prüfung und Stellungnahme zu der Frage, ob ein Zugang zu der Tagesordnung einer Kreisausschusssitzung gewährt werden darf.

Problem in diesem Fall war nicht, dass dem Informationszugangsanspruch gegebenenfalls Ablehnungsgründe der §§ 5 bis 8 IFG M-V entgegenstehen, sondern der Umstand, dass das Ministerium für Inneres und Sport Mecklenburg-Vorpommern die Anwendbarkeit des IFG M-V in Frage stellte. Das Ministerium war der Auffassung, dass das IFG M-V hinter die kommunalverfassungsrechtlichen Regelungen zurücktritt, und begründete dieses mit den Regelungen zu § 1 Abs. 3 IFG M-V.

Diese Auffassung teilen wir nicht. Nach § 1 Abs. 3 IFG M-V bleiben besondere Rechtsvorschriften über den Zugang zu amtlichen Informationen, die Auskunftserteilung oder die Gewährung von Akteneinsicht unberührt. Nach dieser Vorschrift ist durch die auskunftsverpflichtete Stelle zu prüfen, nach welcher Rechtsvorschrift für den Antragsteller der am weitestgehende Informationszugangsanspruch besteht. Eine generelle Subsidiarität des IFG M-V gegenüber anderen Zugangsrechten besteht somit nicht.

Die Kommunalverfassung für das Land Mecklenburg-Vorpommern (KV M-V) regelt ein Auskunftsrecht für bestimmte Personengruppen, wogegen nach § 1 Abs. 2 IFG M-V jede natürliche und juristische Person des Privatrechts Anspruch auf Zugang zu den bei einer Behörde vorhandenen Informationen hat.

Im konkreten Fall wäre neben dem IFG M-V gegebenenfalls § 112 Abs. 4 KV M-V als Anspruchsgrundlage für einen Informationszugang in Betracht gekommen. Voraussetzung für die in dieser Vorschrift beschriebene Akteneinsicht wäre allerdings gewesen, dass es sich bei dem Antragsteller um ein Mitglied des Kreistages handeln würde und das der Antrag entweder von einem Viertel aller Kreistagsmitglieder oder von einer einzelnen Fraktion gestellt wird. Ein höchstpersönliches Zugangsrecht ergibt sich aus diesen Bestimmungen jedoch nicht. Somit besteht nach den Regelungen des IFG M-V vorliegend im Vergleich zu den Bestimmungen der KV M-V ein weitergehender Informationszugangsanspruch, da dieser nicht an die in der KV M-V beschriebenen „Hürden“ geknüpft ist.

Der Petitionsausschuss beschäftigte sich in einer Ausschusssitzung mit diesem Thema. Da zwischen dem hiesigen Innenministerium und uns an dieser Stelle kein Konsens hergestellt werden konnte, sollte nach Auffassung des Petitionsausschusses seitens der Landesregierung und der Fraktionen des Landtages über die Aufnahme einer möglichen Klarstellung in das IFG M-V nachgedacht werden.

Wir haben daraufhin dem Petitionsausschuss unsere Bedenken hierzu zum Ausdruck gebracht. Eine mögliche Klarstellung könnte sich negativ auf den gesamten Bereich der Anwendbarkeit des IFG M-V auswirken. Die in § 1 Abs. 3 IFG M-V festgeschriebene „Unberührtheitsklausel“ lässt für die Prüfung des Einzelfalls einen Interpretationsspielraum zu und bedeutet, dass immer mögliche Ansprüche parallel nach dem IFG M-V und anderen Spezialgesetzen geprüft werden müssen.

Wenn man der Sichtweise des Innenministeriums folgen würde, hätte man auch für viele ähnlich gelagerte Fälle von Anspruchskonkurrenzen keinen Anwendungsbereich für das IFG M-V mehr. Das würde einen erheblichen Rückschritt für die Informationsfreiheit und damit auch für direkte Teilhabe der Bürgerinnen und Bürger an demokratischen Prozessen im Land bedeuten.

Wir empfehlen daher dem Landtag, den Gesetzeswortlaut von § 1 Abs. 3 IFG M-V nicht zu ändern.

9.6 Anspruch auf Herausgabe von Kopien

Grundsätzlich lässt sich feststellen, dass die dem Anwendungsbereich des Informationsfreiheitsgesetzes Mecklenburg-Vorpommern (IFG M-V) unterliegenden Stellen (siehe § 3 IFG M-V) die gesetzlichen Regelungen beachten und einhalten. Nichtsdestotrotz konnten wir in einem Fall erleben, dass sogar versucht wurde, aus den gesetzlichen Regelungen Inhalte abzuleiten, die es so überhaupt nicht gibt.

In dem konkreten Fall gewährte eine Behörde dem Antragsteller den Informationszugang, sah sich aber nicht in der Lage, ihm die gewünschten Kopien zu übersenden. Begründet wurde diese ablehnende Haltung damit, dass aufgrund diverser Anträge und des größeren Umfangs der betreffenden Vorgänge dieser Wunsch nicht realisierbar sei und eine „tatsächliche Unmöglichkeit“ zu § 4 Abs. 3 IFG M-V darstellen würde. Alternativ bot man dem Antragsteller an, sich während der Akteneinsicht Notizen zu machen.

Mit der Gesetzesnovellierung im Jahr 2011 ist der Herausgabeanspruch von Kopien gesetzlich klar und voraussetzungslos geregelt worden. Seitdem kann neben den drei in § 4 Abs. 1 IFG M-V beschriebenen Varianten der Informationsgewährung (schriftliche beziehungsweise mündliche Auskunft oder Zugänglichmachen des Informationsträgers) auch die Herausgabe von Kopien verlangt werden. Die Behörde ist grundsätzlich an das Begehren des Antragstellers gebunden, hat also kein Ermessen.

Insofern war die von der Behörde angeführte Argumentation falsch, zumal es eine „tatsächliche Unmöglichkeit“ zu § 4 Abs. 3 IFG M-V gar nicht gibt. Diese gesetzliche Regelung definiert vielmehr eine auf Seiten der Behörde liegende Verpflichtung zur Schaffung der für die Gewährung des Informationszugangs notwendigen Voraussetzungen.
Nach unserer Intervention revidierte die Behörde ihre Entscheidung, sodass dem Antragsteller im Ergebnis doch die gewünschten Kopien übersandt wurden.

9.7 Informationen zu Hinweisgebern

Die öffentliche Verwaltung ist beispielsweise für die Ahndung rechtswidriger Zustände häufig auf Hinweise von Personen angewiesen. Von den Betroffenen wird demgegenüber (auch unter Zuhilfenahme des Informationsfreiheitsgesetzes Mecklenburg-Vorpommern – IFG M-V) versucht, Namen dieser Hinweisgeber herauszubekommen, um in Erfahrung bringen zu können, wer sie „angeschwärzt“ hat.

Da in derartigen Fällen der Zugang zu personenbezogenen Daten begehrt wird, findet § 7 IFG M-V Anwendung. Hiernach ist ein Antrag auf Informationszugang abzulehnen, soweit durch das Bekanntwerden der Informationen personenbezogene Daten (siehe § 3 Abs. 1 Landesdatenschutzgesetz Mecklenburg-Vorpommern – DSG M-V) offenbart werden.

§ 7 IFG M-V führt unter Nr. 1 bis 5 Sachverhalte auf, bei denen der oben genannte Ablehnungsgrund nicht gilt. So kann unter anderem nach § 7 Nr. 5 IFG M-V ein Informationszugang gewährt werden, wenn der Antragsteller ein rechtliches Interesse an der Kenntnis der begehrten Information geltend macht und überwiegende schutzwürdige Belange der oder des Betroffenen der Offenbarung nicht entgegenstehen.

Ein rechtliches Interesse liegt vor, wenn der Antragsteller einen Anspruch verfolgt, der sich aus einer konkreten Rechtsbeziehung zu dem Betroffenen, um dessen Daten es geht, ergibt beziehungsweise ergeben kann. Ein rechtliches Interesse ist aber auch dann gegeben, wenn der Informationszugang möglicherweise größere Klarheit über den Sach- und Streitstand vermittelt und aus Sicht eines verständigen Betrachters die weitere Rechtsverfolgung oder -verteidigung erleichtern wird.

Aus datenschutzrechtlichen Gründen ist die Identität von Hinweisgebern und Informanten aber grundsätzlich vertraulich zu behandeln. Eine Weitergabe derartiger Informationen an Betroffene ist nur dann möglich, wenn der Hinweisgeber damit ausdrücklich einverstanden ist oder wenn die Hinweise sich als falsche Anschuldigungen erweisen, denen mit erheblicher Wahrscheinlichkeit eine Beleidigungs- oder Schädigungsabsicht des Hinweisgebers zugrunde liegt. In diesem Fall wäre ein rechtliches Interesse gegeben.

In den uns vorliegenden Fällen konnte eine solche Absicht und damit ein rechtliches Interesse an der Herausgabe der Informationen nicht stichhaltig begründet werden, sodass (auch mangels Einwilligung der Hinweisgeber auf Herausgabe ihrer personenbezogenen Daten) die Anträge jeweils abgelehnt werden mussten.

9.8 Herausgabe von Informationen zu Öko-Eiern?

Der Antragsteller hatte sich auf das Informationsfreiheitsgesetz bezogen und Zugang zu Informationen über einen Öko-Legehennenstall beantragt. Er wollte wissen, wie einzelne Verfahren zu Kontrollen zur Bio-Legehennenhaltung ausgegangen sind. Das zuständige Landesamt für Landwirtschaft, Lebensmittelsicherheit und Fischerei Mecklenburg-Vorpommern (LALLF M-V) hatte zunächst die Herausgabe von Informationen abgelehnt mit dem Hinweis auf laufende Verfahren (§ 5 Nr. 2 Informationsfreiheitsgesetz (IFG M-V)). Daraufhin hatte der Antragsteller Widerspruch eingelegt und sich an den Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern gewandt und um Unterstützung seines Anliegens gebeten.

Wir haben die Rechtslage wie folgt beurteilt: Gemäß § 5 Nr. 2 IFG M-V ist der Antrag auf Zugang zu Informationen abzulehnen, soweit und solange durch die Bekanntgabe der Informationen der Erfolg eines strafrechtlichen Ermittlungs- oder Strafvollstreckungsverfahrens gefährdet oder der Verfahrensablauf eines anhängigen Gerichts-, Ordnungswidrigkeiten- oder Disziplinarverfahrens erheblich beeinträchtigt würde.

Das LALLF M-V hatte jedoch nicht dargelegt, welche der beiden Alternativen überhaupt einschlägig sein soll. Des Weiteren müsste im Hinblick auf die erste Alternative dargelegt werden, dass der Erfolg des strafrechtlichen Ermittlungsverfahrens durch die Informationspreisgabe gefährdet werden würde. Hinsichtlich der zweiten Alternative müsste der Verfahrensablauf eines anhängigen Gerichtsverfahrens erheblich beeinträchtigt werden. In dem vom Antragsteller mitübersandten Zeitungsartikel ist unter anderem die Rede von Verfahren, die die Staatsanwaltschaft eröffnet hat, und von Verwaltungsverfahren, die die Behörde eingeleitet hat. Soweit es hier um Ordnungswidrigkeitenverfahren geht, die von der Behörde eingeleitet worden sind, ist hier zu prüfen, ob tatsächlich der Verfahrensablauf erheblich beeinträchtigt würde, wenn der Informationszugang gewährt werden würde. Insofern ist also zwischen den einzelnen Verfahren zu differenzieren.

Nach intensiven Gesprächen auf Arbeitsebene hat das LALLF M-V dem Antrag auf Informationszugang stattgegeben.

10 Organigramm

<table>
<tr><td>Stand:
01.09.2013</td><td colspan="3">Landesbeauftragter für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern

Reinhard Dankert</td><td>Vorzimmer
Ute Bache
0385 59494-35</td></tr>
<tr><td>LD 1
Recht, Verwaltung, Informationsfreiheit</td><td>LD 2
Grundsatzfragen, Gesundheit, Soziales</td><td colspan="2">LD 3
Technik, Allgemeine Verwaltung</td><td>LD 4
Wirtschaft</td></tr>
<tr><td>Ina Schäfer
0385 59494-31</td><td>Werner Baulig
0385 59494-46</td><td colspan="2">Gabriel Schulz
0385 59494-37
Stellvertreter des Landesbeauftragten für Datenschutz und Informationsfreiheit</td><td>Rolf Hellwig
0385 59494-42</td></tr>
<tr><td>Thomas Ahrens
0385 59494-32</td><td>Birka Paul
0385 59494-53

Hiltraud Bockholt
0385 59494-43

Antje Kaiser
0385 59494-56</td><td>Technik

René Weichelt
0385 59494-41

Thomas Brückmann
0385 59494-51

Gesine Naab
0385 59494-38</td><td>Allgemeine Verwaltung

Iris Dahlmann
0385 59494-45

Diana Lokatis
0385 59494-52

Katharina Schmidt
0385 59494-57</td><td>Enrico Wilcke
0385 59494-55

Katharina Schmidt
0385 59494-57</td></tr>
<tr><td>Polizei
Justiz
Verfassungsschutz
Ausländerrecht
Religionsgesellschaften
Umweltschutz
Vermessung/Kataster
Geodaten
Kommunales
Einwohnerwesen
Bau-, Wohnungs- und Liegenschaftswesen
Verwaltungsmodernisierung (Recht)
Informationsfreiheit</td><td>Grundsatzfragen
Koordinierungsstelle Landtag, Landesregierung, Bund
Europäischer und internationaler Datenschutz
Rechtsangelegenheiten der Behörde
Bildungsprojekte
Finanzen/Steuern
Statistik
Sozial- und Gesundheitswesen
Personalwesen
Beschäftigtendatenschutz
Bildung/Kultur
Land-, Forst- und Wasserwirtschaft
Wahlen</td><td>AK Technik
IT-Planungsrat
Informations- und Kommunikationstechnik
E-Government
Internet
Betriebssysteme
Netzwerke
Standardsoftware
Verschlüsselung, Signatur
Biometrie
baulicher Datenschutz
Sicherheitskonzepte
Verfahrensverzeichnis
IT der Dienststelle
Telekommunikations- und Medienrecht
Verwaltungsmodernisierung
Europäischer und internationaler Datenschutz
Projekte/Soziale Netze</td><td>Öffentlichkeitsarbeit/ Informationsmaterial
Haushalt/Beschaffung
Personal
Betreuung der Auszubildenden
Schreibdienst
Bibliothek
Registratur</td><td>Banken
Kreditwirtschaft
Versicherungen
Handel/Versandhandel
Auskunfteien
Wohnungswirtschaft
Verkehr
Eigenbetriebe
gewerbliche Dienstleistungen
freie Berufe
Handwerk
Industrie</td></tr>
<tr><td colspan="5">Behördlicher Datenschutzbeauftragter: Thomas Ahrens Gleichstellungsbeauftragte: Ina Schäfer Personalobmann: Thomas Brückmann</td></tr>
</table>

11 Abkürzungsverzeichnis

AAL	Ambient Assisted Living System
AGB	Allgemeine Geschäftsbedingungen
AK Technik	Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Ständigen Konferenz der Datenschutzbeauftragten des Bundes und der Länder
AMG	Arzneimittelgesetz
AO	Abgabenordnung
ARGE	Arbeitsgemeinschaft
ATD	Antiterrordatei
ATDG	Antiterrordateigesetz
BDSG	Bundesdatenschutzgesetz
BEATA	Bezügedaten elektronisch anweisen, transportieren und archivieren
BetrVG	Betriebsverfassungsgesetz
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BMeldDÜV	Datenübermittlungen der Meldebehörden
BMI	Bundesministerium des Innern
BMWi	Bundesministerium für Wirtschaft
BOS	Bremen Online Services
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
BYOD	Bring Your Own Device
BVA	Bundesverwaltungsamt
CDU	Christlich Demokratische Union
CSG	ComputerSpielSchule Greifswald
CN-LAVINE	Corporate Network der Landesverwaltung
CO^2	Kohlenstoffdioxid
DDR	Deutsche Demokratische Republik
DES	Data Encryption Standard
DFKI	Deutsches Forschungszentrum für Künstliche Intelligenz GmbH
DOI	Deutschland Online Infrastruktur e. V.
DSGV	Deutscher Sparkassen- und Giroverband
DSG M-V	Landesdatenschutzgesetz Mecklenburg-Vorpommern
DSK	Konferenz der Datenschutzbeauftragten des Bundes und der Länder
DVZ M-V GmbH	Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH
EDV	elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
eGo-MV	Zweckverband „Elektronische Verwaltung in Mecklenburg-Vorpommern“
eID	elektronischer Identitätsnachweis
ELSTAM	elektronische Lohnsteuerabzugsmerkmale
EPOS	elektronisches Personal-, Organisations- und Stellenmanagementsystem
EU	Europäische Union

EV	Extended Validation Certificate
EVA	elektronischer Vorgangsassistent
FTP	File Transport Protocol
GEKID	Gesellschaft der epidemiologischen Krebsregister e. V.
GeoVermG M-V	Geoinformations- und Vermessungsgesetz Mecklenburg-Vorpommern
GEZ	Gebühreneinzugszentrale
GG	Grundgesetz
GKR	Gemeinsames Krebsregister der neuen Bundesländer und Berlin
GnuPG	GNU Privacy Guard
GovData	Datenportal für Deutschland
HNF	Heinz-Nixdorf-Museumsforum
HTTP	Hypertext Transport Protocol
HTTPS	Hypertext Transport Protocol Secure
ID	Identifikationsnummer
IETF	Internet Engineering Task
IFG M-V	Informationsfreiheitsgesetz Mecklenburg-Vorpommern
ILERL M-V	Richtlinie für die Förderung der integrierten ländlichen Entwicklung Mecklenburg-Vorpommern
INPOL	Informationssystem der Polizei
IP	Internet Protocol
IPv6	Internet Protocol Version 6
IPsec	Internet Protocol Security
ITIL	IT Infrastructure Library
IQMV	Institut für Qualitätsmanagement Mecklenburg-Vorpommern
KAG M-V	Kommunalabgabengesetz Mecklenburg-Vorpommern
Kfz	Kraftfahrzeug
KIS	Krankenhausinformationssysteme
KlinKrebsRG	Klinisches Krebsregistergesetz
KMK	Kultusministerkonferenz
KoSIT	Koordinierungsstelle für IT-Standards
KRG	Gesetz über Krebsregister
KunstUrhG	Kunsturhebergesetz
KV MV	Kassenärztliche Vereinigung Mecklenburg-Vorpommern
KV M-V	Kommunalverfassung für das Land Mecklenburg-Vorpommern
LAKOST	Landeskoordinierungsstelle für Suchtvorbeugung
LALLF M-V	Landesamt für Landwirtschaft, Lebensmittelsicherheit und Fischerei Mecklenburg-Vorpommern
LBesA	Landesbesoldungsamt
LBG M-V	Landesbeamtengesetz Mecklenburg-Vorpommern
LBodSchG M-V	Landesbodenschutzgesetz Mecklenburg-Vorpommern
LFI M-V	Landesförderinstitut Mecklenburg-Vorpommern
LHG M-V	Landeshochschulgesetz Mecklenburg-Vorpommern
LJR M-V	Landesjugendring Mecklenburg-Vorpommern
LKA M-V	Landeskriminalamt Mecklenburg-Vorpommern
LMG	Landesmeldegesetz
LT-Drs.	Landtags-Drucksache

MD5	message-digests 5
MDM	Mobile Device Management
MESTA	Mehrländer-Staatsanwaltschafts-Automation
MfS	Ministerium für Staatssicherheit
MMV	Medienanstalt Mecklenburg-Vorpommern
MPG	Medizinproduktegesetz
MRRG	Melderechtsrahmengesetz
NEGS	Nationale E-Government-Strategie
NFC	Near Field Communication
nPA	neuer Personalausweis
NSA	National Security Agency
OpenPGP	Open Pretty Good Privacy
OSCI	Online Services Computer Interface
OWiG	Gesetz über Ordnungswidrigkeiten
OVG M-V	Oberverwaltungsgericht Mecklenburg-Vorpommern
ÖGDG M-V	Gesetz über den öffentlichen Gesundheitsdienst Mecklenburg-Vorpommern
PAS	Patientenaktensysteme
PAuswG	Personalausweisgesetz
PDF	Portable Document Format - plattformunabhängiges Dateiformat für Dokumente
PeerCon	Peer Connection
PersVG M-V	Personalvertretungsgesetz Mecklenburg-Vorpommern
PFS	perfect forward secrecy
PIA	Privacy Impact Assessment
PIM	Personal Information Manager
PIN	Persönliche Identifikationsnummer
PUK	Personal Unblocking Key
QES	qualifizierte elektronische Signatur
RFID	Radio-Frequency Identification
RSA	Rivest, Shamir und Adleman
RSAG	Rostocker Straßenbahn AG
SchiLF	Schulinterne Lehrerfortbildung
SchulDSVO M-V	Schuldatenschutzverordnung Mecklenburg-Vorpommern
SchulG M-V	Schulgesetz Mecklenburg-Vorpommern
SGB I	Sozialgesetzbuch Erstes Buch
SGB II	Sozialgesetzbuch Zweites Buch
SGB V	Sozialgesetzbuch Fünftes Buch
SGB VIII	Sozialgesetzbuch Achtes Buch
SGB X	Sozialgesetzbuch Zehntes Buch
SIP	Schulinformations- und Planungssystem
SMTP	Simple Mail Transfer Protocol
SOG M-V	Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommern
SPD	Sozialdemokratische Partei Deutschlands
SSL	Secure Sockets Layer
StALU	Staatliches Amt für Landwirtschaft und Umwelt
Steuer-ID	Steueridentifikationsnummer
StGB	Strafgesetzbuch
StPO	Strafprozessordnung

TEO	Tage ethischer Orientierung
TKG	Telekommunikationsgesetz
TLS	Transport Layer Security
TMF	Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V.
TMG	Telemediengesetz
TR	Technische Richtlinie
TR-ESOR	Technische Richtlinie zur Beweiserhaltung kryptographisch signierter Dokumente
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
USA	United States of America
VerpflG	Verpflichtungsgesetz
VPN	Virtual Private Network
VwVfG	Verwaltungsverfahrensgesetz
WLAN	Wireless Local Area Network - drahtloses lokales Netzwerk
WWW	World Wide Web
XML	Extensible Markup Language
ZensG 2011	Zensusgesetz 2011
ZIR	Zentrales Informationsregister
ZKKR	Zentrales Klinisches Krebsregister
ZPO	Zivilprozessordnung

Abgabenordnung 31, 109
Adresse 48
Adressmittlungsverfahren 76
AK Technik 36, 55, 78, 96, 97, 105, 122, 125
AK Wissenschaft 97
Akteneinsicht 133, 134
anonym 30, 111, 126
anonymisiert 42, 68
Anonymisierung 97, 98
Anspruchskonkurrenz 134
Antiterrordateigesetz 70
AO 31
Apotheke 94
Apothekerverband 94
App 22, 125
Arbeitnehmerdatenschutz 98, 128
Arbeitskreis Technische und organisatorische Datenschutzfragen 42, 105, 122
Arbeitslosengeld II 86
Archivierungsprogramm 113
Artikel-29-Gruppe 125
Arzneimittelgesetz 97
Arzt 92
Auftragsdatenverarbeitung 48
Auskunft 66
Auskunfteien 76
Auskunftserteilung 66
Auskunftsrechte 67
Auskunftssperre 78
Auskunftsumfang 67
auskunftsverpflichtete Stelle 133
Ausweis-App 79
Authentisierung 32, 105
Authentizität 44, 52, 84
automatisiertes Verfahren 47
Bagatelldelikt 62
barrierefrei 65
Baustelle 57
Beanstandung 84
BEATA 51
Beherbergungsbetrieb 109
behindertengerecht 65
Behörde 133
Benachrichtigung 72
Benachrichtigungspflicht 122
berechtigtes Interesse 76
Berechtigungszertifikat 79, 124
besonderer Meldeschein 77
Bestandsdatenabfrage 72
Bestandsdatenauskunft 71
Betriebs- und Geschäftsgeheimnis . 47, 131
Betriebskostenabrechnung 43
Betriebsvereinbarung 128
Betroffenenrechte 37
Bettensteuer 108
Beweiswert 52
Bildaufzeichnungsanlage 61
Bildungsministerium 112
Biobank 98
Bio-Legehennenhaltung 135
Biometrie 125
BMWi 45
Bring your own Device 124
BSI 38, 52, 96
BSI-Grundschutz 47
BSI-Grundschutzmethodik 47
Bundesamt für Sicherheit in der Informationstechnik 38, 52, 96
Bundesamt für Verfassungsschutz 73
Bundesdatenschutzgesetz 129
Bundesinnenministerium 79
Bundesministerium für Gesundheit 96
Bundesnetzagentur 33
Bundesverfassungsgericht 27
Bundesverwaltungsamt 80
Bundeswirtschaftsministerium 45
Bundeszentralamt für Steuern 109
Bürgerkonto 82
Bürgerportal 80, 124
Bußgeld 58
BYOD 53
Chaos Computer Club 79
Charta der Grundrechte 74
Chipkarte 84
Clearingstelle 95
Cloud-Computing 44, 45, 46, 125
Cloud-Dienst 46
Cybercrime 20
Cybermobbing 22
Datenkatalog 130
Datenportal 130
Datenschutzgesetz 108
Datenschutzmanagement 55
Datenschutz-Rahmenabkommen 74
Datensicherheit 103
Datensparsamkeit 42
Datenspur 22
Datentrennung 55

Datenübermittlung.....55
Datenverarbeitung im Auftrag 43, 45
DDR 67
De-Mail 40
De-Mail-Diensteanbieter.....31
De-Mail-Gesetz 31
Deutscher Sparkassen- und Giroverband 105
Deutschland Online Infrastruktur.....39
Dienststellenportal.....52
DOI.....39
DOMEA 51, 54
DSGV 105
Düsseldorfer Kreis.....105, 123
DVZ M-V GmbH 14, 48
dynamische IP-Adresse 72
EC-Karte.....105
E-Commerce.....80
eGo-MV 82, 84
E-Government 37, 80
E-Government-Gesetz.....31
E-Government-Masterplan.....52
E-Government-Verfahren.....9, 84, 122
eID-Funktion 79
eID-Strategie 36, 38
eigenhändige Unterschrift 32
Eilfall.....71
Einwilligung 92, 95, 98
elektronische Gesundheitskarte.....33
elektronische Signatur 52
elektronische Verwaltung.....8, 31
elektronischer Vorgangsassistent 69
elektronisches Formular 33
E-Mail.....118
Ende-zu-Ende-Verschlüsselung 34, 40
Epidemiologie 98
epidemiologisches Register.....97
EPOS 54
Erforderlichkeit 75
Erhebungsbeauftragter 103
Erhebungsbögen 104
Erhebungsmerkmal.....114
Erhebungsstelle 103
Ermittlungsverfahren.....69, 136
EU-Datenschutz-Grundverordnung .30, 45, 123, 129
europäischer Binnenmarkt.....45
Facebook 18, 24, 37
Fan-Page.....37
Fernmessen.....43
Finanzbehörde 109
Finanzverwaltung 109
Firewall.....80
Förderbedarf 114
Forschung 97, 98
Forschungsverbund.....97
Fraktion.....133
Friedhof.....59
Friendica 25
Funk-Chip 105
funktionaler Behördenbegriff 75
Funktionsträger 67
G-10-Kommission 71
Gebäudetechnik 127
Gefahrenabwehr.....77
Geheimdienst 73
GeldKarte.....105
Gemeinsamer Bundesausschuss 99
gemeinsames Verfahren.....81
Generalstaatsanwalt 66
Geodaten 76
Geoinfomations- und Vermessungsgesetz M-V.....65
Geo-Portal.....75
Gerichtsverfahren 136
Gesellschaft der epidemiologischen Krebsregister e.V. 96
Gesichtserkennung.....125
Gesundheit 111
Gesundheitsdaten.....96
girogo-Verfahren 105
GnuPG 113
Google.....126
GPS 64
Grunddaten 70
Grundschutz.....85
Grundschutzmethodik.....38
Grundstückseigentümer 76
Gruppierung.....70
Haftbefehl 69
Handy.....22
Heimkinder 67
Herausgabeanspruch 134
Hilfeempfänger 68
Hinweisgeber 134
Hotelgewerbe.....108
iCloud 44
Identifikation.....82
Identifikationsdaten 82
Identifizierung.....80
Identifizierungsdienst 80
Identifizierungsverfahren.....38

Identitätsnachweis 33
Immobilienmakler 76
informationelle Selbstbestimmung...17, 27, 28
Informationsfreiheitsgesetz 129
Informationspreisgabe 136
informierte Einwilligung 98
Integrität 30, 32, 37, 44, 52, 84
intelligente Gebäude 127
Internet 17, 22, 23, 28, 30, 68, 126, 127
Internet-Protokoll 48
Intervenierbarkeit 30
Inverssuche 71
iPad 43, 124
IP-Adresse 48
IPsec 115
IPv6 48
ISO 27001 83
IT-Grundsystem 113
IT-Netzgesetz 123
IT-Planungsrat 33, 36, 85, 122
Jugendamt 67, 90
Jugendhilfeausschuss 67
Jugendwerkhof 67
Kartenleser 79
Kassenärztliche Vereinigung 92
Kennzeichenlesegerät 60
Keylogger 79
Kinderheim 67
Klappbrücke 61
Kneipe 58
KNX-Feldbus 127
Kommunalabgabengesetz 108
kommunale Spitzenverbände 38
Kommunalverfassung 133
Kommunalverwaltung 84
Kommune 38
Kommunikation 72
Kompetenzzentrum Trusted Cloud 45
Konnexitätsprinzip 85
Kontaktperson 70
Kontendatenabrufe 109
Kontoauszüge 88
Kontostammdaten 109
Kontrolleur 69
Koordinierungsstelle für IT-Standards 36
Kopie 134
KoSIT 36, 123
Krankenhaus 99
Krankenhausinformationssystem 99
Krankenkasse 33
Krebsregister 95, 123
Kreisausschuss 133
Kreistag 133
Kriminalitätsbrennpunkt 62
Kryptographie 40, 84, 113
kryptographische Verfahren 113
Kulturförderabgabe 108
Kunsturheberrechtsgesetz 63
Lageerkenntnisse 62
Landesbeamtengesetz 112
Landesbesoldungsamt 51
Landeskriminalamt 70
Landesregierung 16
Landesverfassungsgericht 73
Landkreis 77
Landkreistag 35
Landtag 46
Landtagsverwaltung 43, 46
Landwirtschaft 135
LAVINE 40
Lehrer 111
Leistungserschleichung 62
Leistungskontrolle 99
Leitlinie für die Informationssicherheit .33, 37
Lese-Rechtschreib-Schwäche 114
Lichtbild 69
Liegenschaftsamt 75
Luftbildaufnahme 65
lüfterloses Lesegerät 43
Mail 112
Mandant 54
Mandantenfähigkeit 54, 99
Medienbildung 17
Medienkompetenz 17
medizinische Daten 64
medizinische Forschung 97, 98
Medizinproduktegesetz 97
Meldebehörde 77
Meldedaten 78
Melderegister 78
Meldewesen 38
Metadaten 130
Mitarbeiterdaten 98
Mitbestimmung 99
Mobbing 20
Mobile Device Management 53
mobile Endgeräte 43, 124, 125
Monopolstellung 131
multiresistente Erreger 98
Nachrichtendienst 74

Nationale E-Government-Strategie 38
NEGS 38
neuer Personalausweis.....33, 79, 84, 124
NFC-Technologie.....105
nichtöffentliche Sitzung 47
Nichtverkettbarkeit.....30, 82
nPA.....84
NSA.....73
Nutzungsprofil.....49, 81
Oberverwaltungsgericht Mecklenburg-Vorpommern.....68
Open Source 113
Open-Data 130
OpenPGP 113
Opinion.....125
Optionskommunen 87
Ordnungswidrigkeitsverfahren.....60, 136
Orientierungshilfe.....42, 48, 55, 99, 125
OSCI.....78
OSCI-Transport.....41, 123
Parlamentarische Kontrollkommission ...72
Passwort 24
Patientenaktensystem 100
Patientendaten 91
Patientenunterlagen 92
Personalausweis 79
Personalausweisgesetz 80
Personaldaten 112
personenbezogene Daten.....47, 135
Personenstandswesen 9, 38, 84
persönliche PIN 112
Persönlichkeitsrecht 23
Petitionsausschuss 47, 133
PIA 106
Polizei.....62, 77
Polizeiinspektion 69
Polizeipräsidium.....69
Porträtfoto.....91
Positionspapier 130
Pressemitteilung 103
PRISM.....25, 73
Privacy by Design 52, 128
Privacy Impact Assessment.....106
Private Public Partnership 65
Privatgeheimnis.....85
Profilbildung.....43
Projekt 99
Pseudonym 30, 93, 94, 96
pseudonymisiert 42
Pseudonymisierung 96, 97, 98, 123
qualifizierte elektronische Signatur.....31
Qualitätssicherung 99
Rabattvereinbarung.....94
Rechenschwäche.....114
Recht auf informationelle Selbstbestimmung.....85
rechtliches Interesse.....135
Rehabilitierungsansprüche.....67
Religionszugehörigkeit 78
Restrisiko 79
Revisionsfähigkeit 44
RFID 128
Richtervorbehalt 72
Risikoanalyse.....47, 53
Rollen- und Berechtigungskonzept.....100
Sachbeschädigung.....61
Satzung 108
Schriftform.....31
Schule 111
Schulinformations- und Planungssystem 114
Schutzbedarfsfeststellung 47
Schutzhülle 106
schutzwürdiges Interesse 76
Schweigepflichtentbindungserklärung ...85
Selbstregulierung 37
sensible Daten.....114, 122
Sensorik 128
SGB I 31
Sicherheits- und Ordnungsgesetz 71
Sicherheitsbehörde.....70
Sicherheitskonzept.....47, 54, 91
Sicherheitslücke.....9, 84
Sicherheitsmanagement 55
Signatur.....78
Signaturgesetz.....33, 52
Signaturkarte.....31
Signaturverfahren 38
Signaturverordnung 33
SIP.....114
Smart Meter 41
Smartphone.....22, 53
Social-Plugin.....37
soziales Netzwerk 23, 24, 37
Sozialgeheimnis.....87
SparkassenCard kontaktlos.....123
SSL 79, 114
Staatsanwaltschaft.....66, 67
Städte- und Gemeindetag.....35
Stadtplanungsamt.....75
Steuerpflicht.....108
Strafverfolgung 77

Straßenverkehr 60
Tablet-Computer 43, 53
Tageseinrichtung 90
technisch-organisatorische Maßnahmen .87
Technology Subgroup 125
TEMPORA.....73
temporäres Bürgerkonto.....82
terroristische Vereinigung.....70
TLS 79, 114
TMF.....97
Tracking 64
Transparenz 30, 37, 42, 43, 44, 54, 114, 126, 129
Transparenzgesetz 129
Transport Layer Security.....114
TR-ESOR 52
Treuhandstelle 99
Trusted Cloud.....45
Übermittlung 78
Übermittlungssperre.....78
Überwachung 127
Universität.....56
Unversehrtheit 78
Urheberrecht.....9, 19, 22, 24, 28
Urkunde.....84
Urkundencharakter.....32
Urkundenportal.....83, 84
Verbindungsnetz.....39
Verbrauchsprofil.....43
Verfassungsschutzbehörde.....70
Verfassungswidrigkeit.....70
Verfügbarkeit 30, 37, 44, 47
Verkehrsgefährdung.....61
Verkehrs-Überwachungsanlage 60
Verkehrswertgutachten.....130
Veröffentlichung 68
Veröffentlichungspflicht 129
Verschlüsselung..... 40, 52, 78, 96, 97, 105, 113, 127
Verschlüsselungsgebot 34
Vertraulichkeit ... 30, 37, 44, 47, 52, 54, 72, 78, 84
Verwaltungsverfahrensgesetz 31
Videoaufzeichnung 62
Videokamera..... 56, 129
Videoüberwachung 57, 58, 59, 60
Videoüberwachungsanlage 62
Videoüberwachungsfunktion..... 62
Virenschutzprogramm 80
Virtual Private Network..... 114
Vollauskunft 66
VwVfG 31
Wasserzähler..... 43
Web 2.0..... 126
Webcam 63
Wettbewerbsfähigkeit 131
Whistleblower..... 73
wirtschaftliche Interessen 76
Wirtschaftsverkehr..... 131
WLAN 44, 129
XKeyscore 73
Youtube..... 18
Zensus 2011 103
Zentrales Klinisches Krebsregister 93
Zertifikat 31, 82, 84
Zertifizierung 83
Zertifizierungsverfahren 46
ZIR..... 54
Zugriffsberechtigung 127
Zuständigkeit 86
Zweckbindung 37, 42, 54, 77
Zweckverband..... 80, 84
Zweckverband Elektronische Verwaltung 82
Zwei-Faktor-Authentisierung 47