LANDTAG MECKLENBURG-VORPOMMERN **Drucksache 6/5356**
6. Wahlperiode **19.04.2016**

UNTERRICHTUNG

durch den Landesbeauftragten für Datenschutz und Informationsfreiheit

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

Siebenter Tätigkeitsbericht gemäß § 38 Absatz 1 Bundesdatenschutzgesetz (BDSG)

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

Berichtszeitraum: 1. Januar 2014 bis 31. Dezember 2015

Zugeleitet mit Schreiben des Landesbeauftragten für Datenschutz und Informationsfreiheit vom 14. April 2016.

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 Zwölfte Tätigkeitsbericht gemäß § 33 Abs. 1 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V), der Siebente Tätigkeitsbericht gemäß § 38 Abs. 1 Bundesdatenschutzgesetz (BDSG) und der Fünfte Tätigkeitsbericht nach dem Informationsfreiheitsgesetz Mecklenburg-Vorpommern (IFG M-V) umfassen den Zeitraum vom 1. Januar 2014 bis zum 31. Dezember 2015. 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

Seite

0 Einleitung

Entwicklung des Datenschutzrechts

Mit der Verabschiedung der Europäischen Datenschutzrichtlinie (95/46/EG) durch das Europäische Parlament im Oktober 1995 wurde erstmals der Versuch unternommen, ein einheitliches Datenschutzrecht für ganz Europa zu schaffen. Nicht zuletzt die schnell fortschreitende Technikentwicklung führte dazu, dass schon bald eine Modernisierung des europäischen Datenschutzrechts erforderlich wurde. Mit der Vorstellung des Entwurfs einer EU-Datenschutz-Grundverordnung (EU-DSGVO) durch die Europäische Kommission am 25. Januar 2012 wurde die europaweite Neuregelung des Datenschutzrechtes eingeleitet. Das vorgeschlagene Gesetzgebungspaket hatte von Anfang an die Aktualisierung, die Modernisierung und die Harmonisierung der Datenschutzvorschriften im Fokus.

Die Datenschutzbehörden des Bundes und der Länder haben die Neuregelung intensiv begleitet, siehe Elfter Tätigkeitsbericht, Punkt 3.1. Je konkreter jedoch die Vorschläge für die EU-Datenschutz-Grundverordnung wurden, desto häufiger stellten sich die deutschen Datenschutzbehörden die Frage, ob sie in der Lage sein würden, mit der vorhandenen bzw. teilweise in Aussicht gestellten personellen und finanziellen Ausstattung den massiv wachsenden Anforderungen der Verordnung gerecht werden zu können.

Am 17. Dezember 2015 bestätigte der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) des Europäischen Parlaments in einer außerordentlichen Sitzung die in den Trilogen beschlossenen Texte des Verordnungsentwurfs. Dadurch wurde der Ausschuss der Ständigen Vertreter (AStV) in die Lage versetzt, den endgültigen Kompromisstexten von Verordnung und Richtlinie am 18. Dezember 2015 zuzustimmen. Mit dieser Einigung wurde der Forderung des Europäischen Rates entsprochen, die Verhandlungen über die Datenschutzreform bis Ende 2015 abzuschließen.

Das Regelungspaket beinhaltet zwei Rechtsakte: die EU-Datenschutz-Grundverordnung (mit der die Richtlinie 95/46/EG ersetzt werden soll) und die EU-Datenschutzrichtlinie im Bereich der Strafverfolgung (die den Datenschutz-Rahmenbeschluss von 2008 ersetzen soll).

EU-Datenschutz-Grundverordnung (EU-DSGVO)

Mit der EU-Datenschutz-Grundverordnung (EU-DSGVO) soll das Datenschutzniveau bei der Verarbeitung personenbezogener Daten EU-weit erhöht und das entsprechende Recht harmonisiert werden; gleichzeitig sollen durch eine Verringerung des Verwaltungsaufwandes für die Unternehmen optimierte Geschäftsmöglichkeiten im digitalen Binnen- und Außenmarkt geschaffen werden. Die EU-Datenschutz-Grundverordnung lag zum Redaktionsschluss dieses Berichtes noch nicht in amtlicher deutscher Fassung vor. Im Folgenden werden daher nur die als unstreitig geltenden bzw. unproblematisch übersetzbaren Inhalte zusammengefasst dargestellt:

Erstes Ziel: Besserer Datenschutz für EU-Bürgerinnen und -Bürger
Die Grundsätze und Regelungen für die Verarbeitung personenbezogener Daten müssen im Einklang mit den Grundrechten stehen. Betroffene, das heißt Personen, deren Daten verarbeitet werden, erhalten durch die in der Verordnung vorgesehene Stärkung der Datenschutzrechte grundsätzlich mehr Kontrolle über ihre personenbezogenen Daten.

Damit die für die Verarbeitung Verantwortlichen personenbezogene Daten verarbeiten dürfen, müssen sie spezielle Vorgaben einhalten. In vielen Fällen müssen die Verantwortlichen die Einwilligung der Betroffenen einholen. Betroffene haben künftig umfassende Rechte auf Zugang zu ihren personenbezogenen Daten. Des Weiteren werden sie künftig darüber informiert, was mit den Daten nach ihrer Weitergabe geschieht. Auch sind die Betroffenen in einer klaren und einfachen Sprache über die Datenschutzmaßnahmen zu informieren. Dies kann auch mittels standardisierter Icons erfolgen. Darüber hinaus beinhaltet die Verordnung ein Recht auf Löschung personenbezogener Daten und ein Recht auf „Vergessenwerden“. So ist es Betroffenen beispielsweise möglich, die unverzügliche Entfernung personenbezogener Daten zu verlangen, die etwa in einem sozialen Netzwerk noch während ihrer Kindheit erfasst oder veröffentlicht wurden.

Auch an den Jugendschutz wurde im Verordnungsentwurf gedacht. Wenn ein Jugendlicher unter 16 Jahren Online-Dienste in Anspruch nehmen möchte, muss der Dienstleister sich darum bemühen zu prüfen, ob die Eltern ihre Einwilligung erteilt haben. Die Mitgliedstaaten können diese Altersgrenze gesetzlich bis zum Alter von 13 Jahren herabsetzen.

Zusätzlich besteht in der Verordnung ein Recht auf Übertragbarkeit, sodass personenbezogene Daten leichter von einem Dienstleister, etwa einem sozialen Netzwerk, an einen anderen Dienstleister übermittelt werden können. Ergänzend regeln allgemeine Schutzklauseln unter gewissen Bedingungen die Verarbeitung personenbezogener Daten für die Zwecke der Archivierung sowie für die wissenschaftliche und historische Forschung oder auch für statistische Zwecke.

Um Betroffenen einen möglichst einfachen Zugang zu Rechtsmitteln zu verschaffen, haben sie künftig die Möglichkeit, Entscheidungen ihrer Datenschutzbehörde von ihrem einzelstaatlichen Gericht überprüfen zu lassen, unabhängig davon, in welchem Mitgliedstaat der für die Verarbeitung der Daten Verantwortliche seinen Sitz hat.

Zweites Ziel: Optimierung der wirtschaftlichen Rahmenbedingungen im digitalen (Binnen)markt
Für alle Unternehmen, die (auch oder ausschließlich) Online-Dienstleistungen in der EU anbieten, wird ein unionsweit einheitlicher Rechtsrahmen geschaffen. Damit soll künftig verhindert werden, dass widersprüchliche einzelstaatliche Datenschutzregeln den grenzüberschreitenden Datenaustausch stören oder ganz unterbinden.

Gewünscht und daher in der Verordnung grundsätzlich vorgesehen ist ferner eine intensivere Zusammenarbeit zwischen den Mitgliedstaaten, um insbesondere sicherzustellen, dass die Datenschutzvorschriften EU-weit kohärent angewandt werden. Um Kosten zu senken und Rechtssicherheit zu erleichtern, wird in bedeutenden grenzüberschreitenden Fällen, die mehrere einzelstaatliche Aufsichtsbehörden betreffen, künftig eine einheitliche Aufsichtsentscheidung getroffen.

Durch dieses Prinzip der *zentralen Anlaufstelle* wird es einem in mehreren Mitgliedstaaten tätigen Unternehmen ermöglicht, nur mit der Datenschutzbehörde in dem Mitgliedstaat zu kommunizieren, in dem es seinen Hauptsitz hat. Nach diesem Mechanismus gilt ferner in Streitfällen eine einheitliche Entscheidung für das gesamte Gebiet der Europäischen Union.

Vermutlich nicht nur um die Verwaltungskosten zu senken, sieht die Verordnung zudem künftig einen risikobasierten Ansatz vor. Demnach können die für die Verarbeitung Verantwortlichen (Unternehmen und Behörden) technische und organisatorische Maßnahmen zum Schutz der verarbeiteten Daten von dem Risiko abhängig machen, welches mit den Datenverarbeitungsvorgängen kausal verbunden ist. Die Verordnung sieht demnach keine einheitliche Standardlösung vor: je höher die mit den Tätigkeiten verbundenen Risiken für die personenbezogenen Daten sind, desto strenger sind innerhalb der Verordnung die Anforderungen.

Drittes Ziel: Mehr und effektivere Instrumente zur Durchsetzung der Einhaltung der Datenschutzvorschriften

Die Verordnung sieht mehrere Maßnahmen für eine höhere Verantwortlichkeit und Rechenschaftspflicht der für die Datennutzung Verantwortlichen vor. Die Verantwortlichen müssen eine Reihe von Sicherheitsmaßnahmen anwenden. So sind etwa in bestimmten Fällen Verletzungen des Schutzes personenbezogener Daten zu melden. Um die Verordnung tendenziell zukunftssicher zu machen, gelten formal die Grundsätze des Datenschutzes durch Technik und des Datenschutzes durch datenschutzfreundliche Voreinstellungen. Behörden (regelmäßig) und Unternehmen, die bestimmte riskante Datenverarbeitungen vornehmen, müssen einen *Datenschutzbeauftragten* benennen, der die Einhaltung der Vorschriften überwacht.

Von der Datennutzung Betroffene sowie unter bestimmten Umständen auch Datenschutzorganisationen können bei einer Aufsichtsbehörde eine Beschwerde oder bei Gericht einen Rechtsbehelf einlegen, wenn die Nichteinhaltung von Datenschutzvorschriften angenommen wird. Für die Datenverarbeitung Verantwortliche können mit Geldstrafen von bis zu 20 Millionen Euro oder 4 % ihres gesamten Jahresumsatzes belegt werden.

Viertes Ziel: Garantien für die Übermittlung personenbezogener Daten außerhalb der EU

Die Verordnung regelt die Übermittlung personenbezogener Daten an Drittländer und internationale Organisationen. Diese Übertragungen sind zulässig, sofern eine Reihe von Bedingungen und Garantien erfüllt sind. Neue Angemessenheitsbeschlüsse zur Feststellung von international vergleichbaren Datenschutzniveaus sind mindestens alle vier Jahre zu überprüfen. Bestehende Angemessenheitsbeschlüsse und Genehmigungen bleiben in Kraft, bis sie geändert, ersetzt oder aufgehoben werden.

EU-Datenschutzrichtlinie im Bereich der Strafverfolgung (JI-Richtlinie)

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat sich in der Vergangenheit auch mehrfach zur Europäischen Datenschutzrichtlinie für Polizei und Justiz (JI-Richtlinie) geäußert. Sie bewertet die JI-Richtlinie als einen wichtigen Schritt zur Verbesserung des Datenschutzes in der Europäischen Union und hat in ihrem Papier vom 29. Oktober 2015 einige wichtige Kernpunkte herausgestellt.

Die Richtlinie stellt sicher, dass die Daten von Zeugen, Opfern und Kontaktpersonen nur unter strengeren Voraussetzungen und mit kürzeren Fristen gespeichert werden dürfen als diejenigen von Beschuldigten und Verdächtigen. Allerdings wurde auch ein großer Teil der Kernpunkte der Konferenz nicht berücksichtigt. So wurden wesentliche Entscheidungen häufig dem nationalen Gesetzgeber überlassen. Offen bleibt auch, in welchem Verhältnis bereits bestehende Rechtsakte der polizeilichen und justiziellen Zusammenarbeit zur JI-Richtlinie stehen.

Weiterer Verlauf

Nach der Überarbeitung durch die Rechts- und Sprachsachverständigen (voraussichtlich April 2016) werden die EU-DSGVO und die JI-Richtlinie dem Rat und anschließend dem Parlament zur Annahme vorgelegt. Mit der Veröffentlichung (Verkündung) der EU-Datenschutz-Grundverordnung ist nach derzeitigem Stand (Redaktionsschluss) nicht vor dem Sommer 2016 zu rechnen. Die EU-DSGVO sieht ab dem Zeitpunkt der Verkündung einen zweijährigen Übergangszeitraum vor. Somit werden die EU-DSGVO und die Richtlinie für den Justiz- und Polizeibereich voraussichtlich im Sommer 2018 in Kraft treten.

Schon jetzt weisen wir vorsorglich darauf hin, dass jedes Ministerium sofort nach der Veröffentlichung der Verordnung das geltende Recht in seinem Zuständigkeitsbereich daraufhin überprüfen muss, ob es mit den Bestimmungen der EU-DSGVO vereinbar ist. Schon jetzt steht fest, dass das Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) durch ein entsprechendes Überleitungsgesetz ersetzt werden muss.

Eigene Bewertung

Die obige Zusammenfassung konzentriert sich im Sinne des europäischen Gedankens vor allem auf die (beabsichtigten) grundrechtlichen *Vorteile* der zu erwartenden Verordnung. Insbesondere aus deutscher datenschutzrechtlicher Sicht birgt die EU-DSGVO jedoch auch weitgehende Kompromisse und Enttäuschungen:

So wurde das zentrale Prinzip der *Datensparsamkeit* aufgegeben und auch die Profilbildung anhand einer Zusammenführung und Auswertung von personenbezogenen Daten ist ungenügend geregelt.

Das darüber hinaus in der Europäischen Grundrechtecharta ausdrücklich verankerte Prinzip der *Zweckbindung* wird im jetzigen Text der Verordnung ohne Not und zum einseitigen Nachteil der Grundrechtsträger im Kern aufgegeben.

Des Weiteren findet sich in der Verordnung der „Türöffner“ für eine grundsätzlich datenschutzunfreundliche „Opt-Out-Lösung“. Einwilligungserklärungen, die nunmehr nicht „ausdrücklich“, sondern lediglich „unmissverständlich“ eingeholt werden müssen, sind vor dem Hintergrund der komplexen Verarbeitungsvorgänge im Ergebnis praxisfremd und unzureichend. In Folge dessen ist zu erwarten, dass global agierende Unternehmen auf diese Weise pauschale Datenschutzbestimmungen verwenden und datenschutzunfreundliche Voreinstellungen ohne *ausdrückliche* und informierte Einwilligung der Betroffenen durchsetzen werden.

Darüber hinaus vermissen wir dringend erforderliche Regelungen zum Adresshandel, zu allgemein zugänglichen Daten und nicht zuletzt zur Videoüberwachung.

Zu erwartende Folgen für die Behörde des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern und für das Land Mecklenburg-Vorpommern

Bereits nach einer ersten Rechts- und Strukturfolgenabschätzung ist festzustellen, dass mit der EU-Datenschutz-Grundverordnung (EU-DSGVO) für die Behörde des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern und damit auch für das Land Mecklenburg-Vorpommern sowohl *datenschutzrechtlich* als auch *datenschutzpraktisch* fast nichts mehr so sein wird wie bisher.

Unsere frühzeitigen und eindringlichen Bemühungen, die künftigen Veränderungen gegenüber der Landesregierung und dem Landtag Mecklenburg-Vorpommern ausreichend nachvollziehbar zu machen, führten nur zu spärlichen bis abweisenden Reaktionen auf den sich daraus unmittelbar und mittelbar ergebenden rechtlichen, personellen, finanziellen und strukturellen Handlungsbedarf. Dieser Bedarf gründet sich insbesondere auf die folgenden bereits feststehenden Inhalte der Verordnung:

Die Verordnung lässt in einigen spezifischen Handlungsbereichen nationale Regelungen in den „Grenzen“ der Verordnung zu. Im Übrigen gilt sie als unmittelbares Europarecht. Etwaiges inhaltsgleiches Recht auf nationaler Ebene wird durch die Verordnung überlagert. Daraus resultieren sowohl auf Bundes- wie auch auf Landesebene immense Prüfungs- und Regelungsbedarfe, die in einem ungewöhnlich engen Zeitfenster von nur knapp zwei Jahren durch den Bund und durch das Land vollzogen und konsentiert werden müssen. Sowohl datenschutzrechtliche Regelungen auf Bundesebene - insbesondere das Bundesdatenschutzgesetz - als auch die datenschutzrechtlichen Regelungen auf Landesebene werden erst einmal ganz oder teilweise aufzuheben und je nach verbleibender „Restregelungskompetenz“ (materielle Gesetzgebung oder Vollzugskompetenz) neu zu gestalten sein.

- Die Verordnung regelt nunmehr unmittelbar wesentliche Pflichten, Aufgaben, aktive und passive Klagebefugnisse, das Verwaltungsverfahren, die Abstimmungsverfahren, Fristen und übrigen Befugnisse der Aufsichtsbehörden neu. Aus einer bisherigen „Opportunitätsbehörde“ des Landes mit auch weiterhin unverzichtbaren Beratungs- und Bildungsaufgaben und einer (schon aus Kapazitätsgründen) überwiegend präventiven „Kontrolle“ wird nunmehr eine weitgehend „europäische Behörde“. Diese „neue“ Behörde wird nunmehr viele - auch repressive - Aufgaben haben und sie muss sich mit einem klagebewehrten, aufwendigen sowie einem weitgehend außenbestimmten Verwaltungsprozedere auseinandersetzen, mit der Folge, dass sie nicht mehr wie bisher gegebenenfalls eingreifen kann, sondern durch Gerichte kostenaufwendig einklagbar und in extrem engen Fristen einzugreifen hat, falls Beschwerden oder Rechtsverletzungen im Datenschutz zur Kenntnis kommen.
- Die in der Verordnung vorgesehenen Verfahren und Sanktionen dienen vor allem der Entlastung der Unternehmen und wohl auch der betroffenen Bürgerinnen und Bürger. Vor dem Hintergrund der bisherigen Erfahrungen müssen wir davon ausgehen, dass mit der rasant zunehmenden und breit verfügbaren Informationstechnik auch die Zahl der datenschutzrechtlichen Auseinandersetzungen ähnlich rasant zunehmen wird. Folglich hat die Entlastung der Wirtschaft zwingend die entsprechend dramatisch steigende Belastung der nunmehr für die Rechtsdurchsetzung verantwortlichen Aufsichtsbehörden zur Folge.

In der EU-Datenschutz-Grundverordnung wurde aufgrund dieser wachsenden Anforderungen auch die dadurch naheliegende Problematik gleich mitgeregelt. Demzufolge sind im Lichte der entsprechenden Rechtsprechung des Europäischen Gerichtshofes (EuGH) die Aufsichtsbehörden durch die Mitgliedstaaten (und Bundesländer) als völlig unabhängig zu gestalten und mit dem für die gewachsene Aufgabenfülle erforderlichen Budget auszustatten. *Nur ein an die neuen Aufgaben angepasstes Budget wird es den Aufsichtsbehörden überhaupt ermöglichen, die notwendigen personellen, strukturellen, räumlichen und sonstigen Maßnahmen anzugehen.*

Der in der EU-Datenschutz-Grundverordnung vorgesehene zweijährige Übergangszeitraum ist angesichts der Fülle der möglichen Rechtsfolgen ungewöhnlich knapp. Deshalb müssen die notwendigen Vorbereitungen und Kompetenzaneignungen schon jetzt beginnen. Ein mancherorts diskutiertes „Warten auf das Inkrafttreten der Verordnung“ verbietet sich demnach nicht nur aus rechtlichen Gründen. Die Zeche für jedes unbillige Zuwarten hätten nicht nur die schon jetzt überlasteten Fachkräfte in den Aufsichtsbehörden, sondern auch die Haushalte der Länder in der Folge von Vertragsverletzungsverfahren und wahrscheinlich zahlreichen verlorenen Klageverfahren zu tragen - auf die damit verbundene fatale Signalwirkung für die Rechtstaatlichkeit unseres Landes soll an dieser Stelle nicht näher eingegangen werden.

Schon jetzt - also vor dem Hintergrund einer noch geltenden und vertrauten Rechtsmaterie und einer noch weitgehenden Eigenkontrolle der Verwaltungsabläufe - sieht sich zahlenmäßig ein Mitarbeiter unserer Aufsichtsbehörde rund zehntausend unterschiedlichen datenverarbeitenden Einrichtungen oder Unternehmen gegenüber, deren mittlerweile häufig elektronisches „Datenhandeln“ er theoretisch zu kontrollieren hat.

Die „übrigen“ durchgehend wachsenden Aufgaben wie Beratung, Prävention, Bildungsmaßnahmen, Bearbeitung von Petitionen, Stellungnahmen zu Gesetzentwürfen und anderen Rechtsvorschriften, die aufwendige Analyse des digitalen Status Quo sowie die ständige Sicherung des entsprechenden kurzlebigen Know-Hows sind in diese Rechnung nicht einbezogen. Somit ist jeder Interessierte umstandslos in der Lage, sich ein Bild über die reale präventive Kontrollwirkung und die Funktionsfähigkeit unserer Behörde zu machen.

Der Datenschutz ist jedoch ein *Grundrecht*, welches nicht nur im Grundgesetz (Art. 1 und 2 GG), sondern auch ausdrücklich in der EU-Grundrechtecharta (Artikel 8) und im Vertrag über die Arbeitsweise der Europäischen Union (Artikel 16) verankert ist.

Die entsprechende Gewährleistungsverpflichtung für die Sicherung dieses Grundrechtes trifft vor allem den Staat, in diesem Falle also das Land Mecklenburg-Vorpommern. Sobald der Text der EU-Datenschutz-Grundverordnung in einer amtlichen deutschen Fassung vorliegt, wird unsere Behörde in Kooperation mit den Kollegialbehörden des Bundes und der Länder belastbare und gegebenenfalls auch finanziell spitzgerechnete Folgenabschätzungen erarbeiten und auch dem Landtag unseres Landes zur Verfügung stellen. Das in der Landesregierung für den Datenschutz federführende Ministerium für Inneres und Sport wird hinsichtlich zahlreicher landesrechtlicher Regelungen schon kurzfristig erste Prüfungen durchzuführen haben.

Weitere Tätigkeitsschwerpunkte im Berichtszeitraum

Der vorliegende Bericht zeigt jedoch auch, dass neben den umfangreichen Aufgaben im Zusammenhang mit dem zu erwartenden neuen europäischen Datenschutzrecht die aus dem geltenden Recht resultierenden Aufgaben nach wie vor sehr ernst genommen wurden.

Die dringend erforderlichen *Bildungsprojekte* zu den neuen Medien, zur Medienkompetenz und zum Datenschutz konnten wir erfolgreich weiterführen, siehe Punkt 2.1. Dies war auch in diesem Berichtszeitraum ein wesentlicher Schwerpunkt unserer Tätigkeit.

Ein weiterer Schwerpunkt waren zwei *Projekte*, die uns fast über den gesamten Berichtszeitraum begleitet haben. Mit dem Projekt „Datenschutz an den Schulen in Mecklenburg-Vorpommern“, siehe Punkt 2.1.5, haben wir verschiedene Datenschutzaspekte an den Schulen des Landes untersucht, die daraus resultierenden Handlungsbedarfe bei den verschiedenen Beteiligten im Schulsektor beschrieben und entsprechende Empfehlungen aus datenschutzrechtlicher Sicht gegeben. Mit dem Projekt „Datenschutz und Informationssicherheit in den Kommunen in Mecklenburg-Vorpommern“, siehe Punkt 2.2.1, haben wir den Datenschutz und die Informationssicherheit in den Kommunen geprüft und Empfehlungen aus datenschutzrechtlicher Sicht gegeben. Dieser Bericht gibt nur einen kurzen Überblick über die Ergebnisse beider Projekte. Eine detaillierte Dokumentation der Projekte werden wir im ersten Quartal 2016 vorlegen.

Durch die regelmäßige Teilnahme an den *Sitzungen des IT-Planungsrates* als Vertreter der Datenschutz-Aufsichtsbehörden der Länder konnten wir dazu beitragen, dass bei der Formulierung der Rahmenbedingungen für die Ausgestaltung der bundesweiten Informationstechnik datenschutzrechtliche Aspekte in angemessener Weise berücksichtigt wurden, siehe Punkt 3.

Die rasante *technische Entwicklung* erfordert ein ständiges Nachjustieren der datenschutzrechtlichen Rahmenbedingungen. Der Abschnitt 4 gibt einen Überblick über unserer Aktivitäten in diesem Bereich und soll aufzeigen, dass wir diese Entwicklung nicht nur begleiten, sondern nach Kräften versuchen, sie aktiv mitzugestalten. Eine wichtige Rolle wird dabei künftig das *Standard-Datenschutzmodell* spielen, siehe Punkt 4.1.1. Das Modell soll einerseits zu einer bundesweit abgestimmten, transparenten und nachvollziehbaren Beratungs- und Prüftätigkeit der Datenschutzbehörden führen. Andererseits bekommen auch die verantwortlichen Stellen ein Werkzeug an die Hand, das ihnen helfen soll, ihre personenbezogenen Verfahren nicht nur sicher, sondern auch datenschutzgerecht einzurichten und zu betreiben.

Nach wie vor erfordern die unterschiedlichen Formen der *Videoüberwachung* ein erhebliches Zeitbudget zur Kontrolle und Beratung dieser Verfahren. Der Abschnitt 4.3 gibt einen Überblick über die Rechtsgrundlagen der Videoüberwachung und beschreibt an einigen Beispielen sowohl die Vielfalt und Komplexität dieser Verfahren als auch die Langwierigkeit der Durchsetzung vorhandener Rechtsvorschriften.

In Abschnitt 5 beschreiben wir zahlreiche *Einzelfälle aus verschiedenen Rechtsgebieten*. Allein dieser Abschnitt verdeutlicht eindrucksvoll das umfangreiche Aufgabengebiet des Landesbeauftragten für Datenschutz und Informationsfreiheit, das allein aus dem bisher geltenden Datenschutzrecht resultiert. Dieser Abschnitt macht somit auch klar, welche erheblichen Anstrengungen erforderlich sein werden, um die zusätzlichen Aufgaben bewältigen zu können, die sich aus den neuen europäischen Datenschutzvorschriften ergeben werden.

Auch dieser Bericht umfasst wieder den *Tätigkeitsbericht, den wir nach dem Informationsfreiheitsgesetz Mecklenburg-Vorpommern zu erstellen hatten*. In Abschnitt 8 geben wir einen kurzen Überblick über verschiedene Themen, die im Berichtszeitraum behandelt wurden. Im Jahr 2015 hatte Mecklenburg-Vorpommern turnusmäßig den Vorsitz der Konferenz der Informationsfreiheitsbeauftragten in Deutschland. Damit hatten wir nicht nur die Arbeit der Informationsfreiheitsbeauftragten im laufenden Jahr zu koordinieren, sondern auch die Konferenz der Informationsfreiheitsbeauftragten am 30. Juni 2015 in Schwerin zu organisieren und durchzuführen, siehe Punkt 8.1. Auch unsere Tätigkeit in diesem Bereich wurde überschattet von den zahlreichen neuen Aufgaben im Zusammenhang mit der Europäischen Datenschutz-Grundverordnung (siehe oben). Auf die Herbstkonferenz haben wir daher verzichtet und stattdessen eine Entschließung zum Thema „Informationsfreiheit 2.0 - endlich gleiches Recht in Bund und Ländern!“ im Umlaufverfahren verabschiedet.

1 Empfehlungen

1.1 Zusammenfassung aller Empfehlungen

1. Wir halten an unserer Empfehlung an die Kommunen aus dem Elften Tätigkeitsbericht fest, die Vorgaben der „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ umzusetzen, und erwarten, dass sie für Verfahren zur automatisierten Verarbeitung personenbezogener Daten die Grundschutzmethodik des BSI in vollem Umfang anwenden. Die „Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen“ und der Leitfaden „Informations-Sicherheits-Management-System in 12 Schritten“ sind geeignete Hilfsmittel auf dem Weg dazu, siehe Punkt 3.3.
2. Wir fordern daher die Landeregierung auf, sich für die folgenden Gestaltungsprinzipien bei Bürgerkonten einzusetzen, siehe Punkt 3.5:

   - Es muss auch künftig möglich sein, Verwaltungsdienstleistungen anonym und somit ohne Anmeldung an einem Bürgerkonto zu nutzen, sofern identifizierende Daten nicht erforderlich sind.
   - Bürgerinnen und Bürger müssen die Wahlmöglichkeit haben, etwa bei einmaliger Inanspruchnahme einer Verwaltungsdienstleistung ihre identifizierenden Daten nur temporär im Bürgerkonto zu hinterlegen.
     - Entscheiden sich Nutzerinnen und Nutzer, Daten dauerhaft in einem permanenten Bürgerkonto zu speichern, muss jederzeit nachvollziehbar sein, wer zu welchem Zweck auf diese Daten zugreift.
     - Auf Wunsch der Nutzerinnen und Nutzer muss es jederzeit möglich sein, das Bürgerkonto und alle dort gespeicherten Daten zu löschen.
     - Insbesondere durch technische Maßnahmen muss die oben beschriebene Möglichkeit der Verknüpfung einzelner Nutzeraktivitäten zu einem umfassenden Nutzungsprofil ausgeschlossen werden.

3. Wir empfehlen der Landesregierung, bei der Planung, der Einrichtung und dem Betrieb von Verfahren zur Verarbeitung personenbezogener Daten die im Standard-Datenschutzmodell beschriebene Vorgehensweise evaluierend anzuwenden und uns über die Erfahrungen beim Umgang mit diesem Werkzeug zu berichten, um dadurch die Weiterentwicklung des Standard-Datenschutzmodells zu unterstützen, siehe Punkt 4.1.1.
4. Wir empfehlen unserer Landesregierung schon jetzt, die im Trusted-Cloud-Projekt entwickelten Methoden und Unterlagen bei der Auswahl von Cloud-Diensten zu nutzen, um die Datenschutzkonformität von Cloud-Infrastrukturen bewerten zu können, siehe Punkt 4.1.2.
5. Wir empfehlen den Behörden in unserem Land, den Standard XTA 2.1 in Verbindung mit OSCI-Transport zur sicheren Kommunikation zwischen Behörden einzusetzen, siehe Punkt 4.1.5.
6. Wir empfehlen den Anwendern aus Wirtschaft und Verwaltung in unserem Land, diese Orientierungshilfe zu beachten, siehe Punkt 4.1.6.
7. Wir empfehlen der Landesverwaltung, auf die Durchsetzung der oben genannten Maßnahmen zu dringen. Dem Landtag empfehlen wir, die zu ihrer Durchsetzung gegebenenfalls nötigen Änderungen und Präzisierungen an dem bestehenden Rechtsrahmen vorzunehmen, siehe Punkt 4.1.9.

8. Wir unterstützen diese Vorhaben und empfehlen der Landesregierung insbesondere in Anlehnung an die Forderungen der Datenschutzkonferenz, siehe Punkt 4.1.10:
   - eine einfach bedienbare Verschlüsselungs-Infrastruktur und insbesondere eine sichere Ende-zu-Ende-Verschlüsselung ohne Eingriffsmöglichkeiten Dritter bereitzustellen,
   - die Entwicklung sicherer, transparenter und einfach bedienbarer kryptographischer Verfahren ohne Hintertüren auf allen, insbesondere auch mobilen, Plattformen zu fördern,
   - die Wirtschaft bei der Wahrung der Vertraulichkeit und Integrität ihrer geschäftlichen Kommunikation zu unterstützen und
   - kryptographische Technologien in E-Government-Verfahren standardmäßig zu implementieren.
9. Wir appellieren daher an den Landtag, den Gesetzestext entsprechend den von uns gegebenen Empfehlungen zu ändern, siehe Punkt 5.3.1.
10. Wir empfehlen dem eGo-MV, die erforderlichen personellen Ressourcen bereitzustellen und geeignete Notfallpläne zu entwickeln, um künftig akute Sicherheitsprobleme unverzüglich bewältigen zu können, siehe Punkt 5.4.3.
11. Wir empfehlen dem Ministerium für Inneres und Sport Mecklenburg-Vorpommern den Abschluss eines Vertrages mit dem eGo-MV zum Betrieb des Sicherungsregisters für das Personenstandswesen nach den Vorschriften zur Datenverarbeitung im Auftrag, siehe Punkt 5.4.4.
12. Wir empfehlen der Landesregierung, wesentliche Grundsätze im Melderecht normenklar im LMG und nicht untergesetzlich zu regeln, siehe Punkt 5.4.8.

13. Wir empfehlen den Krankenhäusern, ärztlichen und zahnärztlichen Praxen und anderen Partnern der klinischen Krebsregistrierung unseres Landes, diese Entschließung zu beachten, siehe Punkt 5.6.3.
14. Wir empfehlen der Landesregierung, die flächendeckende Verfügbarkeit von Kartenlesern und Signaturkarten für die qualifizierte elektronische Signatur voranzutreiben und gleichzeitig zu prüfen, welche anderen der in § 3a Abs. 2 VwVfg M-V genannten sicheren Verfahren eingesetzt werden können, siehe Punkt 5.7.2.
15. Wir empfehlen den Verantwortlichen im Bereich Schule, auf die automatisierte Verarbeitung von Daten mit höherem Schutzbedarf mit Hilfe von Verwaltungs- und Lernsoftware zu verzichten, solange dafür keine datenschutzkonforme Software am Markt verfügbar ist. Schon bei der Konzipierung derartiger Softwareprodukte ist in jedem Falle das Gebot der Datensparsamkeit zu berücksichtigen, siehe Punkt 5.10.1.

1.2 Umsetzung der Empfehlungen des Zehnten Tätigkeitsberichtes

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt im 10. TB
1	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.	Die Landesregierung hat mit der Fortschreibung der „Vereinbarung zur Medien-kompetenzförderung in Mecklenburg-Vorpommern“ und dem Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern als neuem Unterzeichner bereits eine gute Handlungsempfehlung auf den Weg gebracht. Jedoch ist es nicht umgesetzt, dass jeder junge Mensch in Mecklenburg-Vorpommern mehrmals qualifizierte Medienbildung (Datenschutz, Privatsphäre, Urheberrecht etc.) erlernen kann. Eine curriculare Verankerung durch alle Klassenstufen und über alle Schularten hinweg fehlt weiterhin.	2.10
2	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.	Die Landesregierung verweist auf die Eigenverantwortung der Kommunen. Außerdem seien die Kommunen bei der Teilnahme an ebenen-übergreifenden Verfahren und Netzinfrastrukturen an entsprechende Regelungen gebunden. Tatsächlich setzen Kommunalverwaltungen die Grundschutzmethodik nach unseren Feststellungen nach wie vor nur in Einzelfällen ein.	4.3

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt im 10. TB
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.	Die Landesregierung verweist auf das Steuerungsprojekt „eID-Strategie“ des IT-Planungsrates. Eigene Aktivitäten der Landesregierung sind uns nicht bekannt.	4.4
4	Wir empfehlen der Landesregierung, bei der elektronischen Übermittlung personenbezogener Daten, insbesondere bei modernen E-Government-Verfahren, regelmäßig Verschlüsselungsverfahren nach dem Stand der Technik einzusetzen und nur in begründeten Ausnahmefällen auf eine Ende-zu-Ende-Verschlüsselung zu verzichten.	Die Landesregierung verweist darauf, dass die jeweiligen Fachverfahrensverantwortlichen zu entscheiden hätten, ob sichere Transportverfahren einzusetzen sind.	4.5
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.	Die Landesregierung gibt an, dass sie sich der Anforderungen bewusst sei und verweist auf die Richtlinie „Öffentliche Aufträge in der Cloud“, die die DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH gemeinsam mit IT-Dienstleistern anderer Bundesländer erstellt hat.	5.1.4
6	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.	Entsprechende Aktivitäten der Landesregierung sind uns nicht bekannt.	5.1.9

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt im 10. TB
7	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 (BMeld-DÜV) gefordert.	Nach Informationen der Landesregierung aus dem Jahr 2014 war geplant, dass ab November 2015 Meldedaten vom Zentralen Informationsregister an die Kirchen mit OSCI-Transport gesichert übermittelt werden sollten. Ziel sei ferner, dieses Protokoll auch bei der Meldedatenübermittlung an die GEZ (jetzt: ARD ZDF Deutschlandradio Beitragsservice) einzusetzen.	6.4.4
8	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.	Der IT-Planungsrat hat empfohlen, ein einheitliches Bürgerkonto für die deutsche Verwaltung zu schaffen. Dies drängt die Nutzung von verschiedenen Berechtigungszertifikaten für jeweils unterschiedliche Stellen und Anwendungen zurück. Auf diese Weise kann die eID-Funktion des nPA nur noch sehr eingeschränkt dazu beitragen, dass verschiedene Nutzungsvorgänge des Bürgerkontos nicht in unzulässiger Weise miteinander verknüpft werden. Dies läuft unserer Empfehlung zuwider. Die Landesregierung hat nach unserer Kenntnis dieser Entwicklung nichts entgegen gesetzt.	6.4.5

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt im 10. TB
9	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.	Der IT-Planungsrat hat empfohlen, ein einheitliches Bürgerkonto für die deutsche Verwaltung zu schaffen. Dies drängt die Nutzung von verschiedenen Berechtigungszertifikaten für jeweils unterschiedliche Stellen und Anwendungen zurück. Auf diese Weise kann die eID-Funktion des nPA nur noch sehr eingeschränkt dazu beitragen, dass verschiedene Nutzungsvorgänge des Bürgerkontos nicht in unzulässiger Weise miteinander verknüpft werden. Dies läuft unserer Empfehlung zuwider. Die Landesregierung hat nach unserer Kenntnis dieser Entwicklung nichts entgegen gesetzt.	6.4.5
10	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.	Die Landesregierung verweist die Kommunalverwaltungen auf den Zweckverband „Elektronische Verwaltung in Mecklenburg-Vorpommern“ und bietet in geringem Umfang organisatorische Hilfen im Informationssicherheitsmanagement. Die Leitlinie Informationssicherheit gilt nach wie vor nicht für Kommunalverwaltungen.	6.4.6

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt im 10. TB
11	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.	Die Landesregierung wird die vom Bundesbeauftragten für den Datenschutz veröffentlichten Eckpunkte für eine datenschutzgerechte Ausgestaltung künftiger Volkszählungen für den Zensus 2021 heranziehen und die im Rahmen der Durchführung des Zensus 2011 gesammelten Erfahrungen bei der Ausgestaltung der landesrechtlichen Vorschriften für den Zensus 2021 berücksichtigen.	6.7
12	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.	Die Stadt Schwerin hat am 8. April 2015 mitgeteilt, dass sie „in Ermangelung von Anhaltspunkten für eine etwaige Rechtswidrigkeit der Satzung und unter Hinweis auf die gegenwärtig vor dem Verwaltungsgericht Schwerin anhängigen Rechtsstreitigkeiten zum jetzigen Zeitpunkt von weitergehenden rechtlichen Einlassungen Abstand nehmen möchte“. Über das Ergebnis der gerichtlichen Befassung würden wir im Weiteren unaufgefordert unterrichtet werden.	6.8.3

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt im 10. TB
13	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.	Die Landesregierung verweist darauf, dass den Landesbehörden und den Kommunalbehörden das Elektronische Gerichts- und Verwaltungspostfach (EGVP) bereitgestellt wird, welches eine Ende-zu-Ende-Verschlüsselung und sogar die Einbindung der qualifizierten Signatur ermöglicht. Nach unserer Kenntnis ist diese Lösung an Verwaltungsarbeitsplätzen nur selten verfügbar. Bemühungen zu einer einheitlichen Ausstattung von Arbeitsplätzen sind insoweit gescheitert. Eine qualifizierte elektronische Signatur wäre nur dann möglich, wenn die Arbeitsplätze mit geeigneten Kartenlesern und die Nutzerinnen und Nutzer mit Signaturkarten ausgestattet wären. Diese Voraussetzungen sind nur sehr selten gegeben.	6.9.2
14	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.	Bisher hat die Landesregierung eine Modernisierung des Informationsfreiheitsgesetzes, die Erfahrungen des Hamburgischen Transparenzgesetzes berücksichtigend, nicht geprüft.	9.1
15	Wir empfehlen dem Landtag, den Gesetzeswortlaut von § 1 Abs. 3 IFG M-V nicht zu ändern.	Weder der Landtag noch die Landesregierung haben im Berichtszeitraum die Initiative ergriffen, um das IFG M-V zu ändern.	9.5

2 Projekte

2.1 Datenschutz und Bildung

Bereits im Elften Tätigkeitsbericht unter Punkt 2 haben wir über unsere Bildungsprojekte zu den neuen Medien, zur Medienkompetenz und zum Datenschutz informiert. Die dort genannten Projekte wurden in diesem Berichtszeitraum weitergeführt.

Ausgehend von der bis heute uneingeschränkt gültigen Rechtsprechung des Bundesverfassungsgerichtes zum Grundrecht auf informationelle Selbstbestimmung und den teilweise darauf zurückgehenden landesrechtlichen Regelungen ist es nach wie vor eine der gesetzlichen Kernaufgaben unserer Behörde, über den Datenschutz und seine praktische Umsetzung zu informieren. Die Art und Weise der Information richtet sich dabei nach den Zielgruppen, die wir erreichen wollen. Angesichts der rasanten Entwicklung unserer medial geprägten Gesellschaft halten wir es für erforderlich, mit diesen Schulungen bereits im Kinder- und Jugendalter zu beginnen. Unsere Auffassungen decken sich somit weitgehend mit der 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.“

Es ist wichtig, Kindern und Jugendlichen Kompetenzen zu vermitteln, die einen selbstbestimmten und reflektierten Umgang mit Medien ermöglichen. In einer digital geprägten Kultur ist Medienbildung unerlässlich, damit Persönlichkeitsentwicklung gelingt, das Demokratieverständnis entwickelt, gesellschaftliche Teilhabe ermöglicht und Ausbildungs- und Erwerbsfähigkeit unterstützt werden. Die digitalen Medien und Anwendungen umgeben inzwischen jeden Einzelnen lückenlos. Deshalb ist es erforderlich, sich immer mehr Kompetenzen im Umgang mit Medien und Wissen über Medien und ihre Funktionsweise anzueignen. Diese „digitale Selbstverteidigung“ ist für alle Bürgerinnen und Bürger, die selbstbestimmt sein oder bleiben möchten, eine dringende Notwendigkeit (siehe dazu http://www.youngdata.de/digitale-selbstverteidigung/allgemeines/). Schon 2011 stellte die 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hierzu in einem Beschluss fest:

„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. 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.“

Die digitalen Medien haben Einzug bis in die Familien und die Zimmer der Heranwachsenden gehalten. Bei unvoreingenommener Betrachtung stellt sich damit nicht mehr die Frage, ob Medienbildung und Medienkompetenzvermittlung ein notwendiger Baustein auf dem Bildungsweg der Kinder und Jugendlichen sein sollte, sondern wie dieser Baustein möglichst nah und in geeigneter Form in die Lebenswelt der Heranwachsenden eingefügt und gleichzeitig auf die Fähigkeiten und den Entwicklungsgrad angepasst werden kann (http://www.kmk.org/bildung-schule/allgemeine-bildung/faecher-und-unterrichtsinhalte/weitere-unterrichtsinhalte/medienbildung-in-der-schule.html).

Wir schließen uns mit dieser breit konsentierten Einschätzung unter anderem der DIVSI Studie (DIVSI Studie U9: https://www.divsi.de/publikationen/studien/divsi-u9-studie-kinder-der-digitalen-welt/) an, wonach eine Vermittlung von digitalen/medialen Kenntnissen notwendig ist, um allen Kindern und Jugendlichen die digitale Teilhabe und Chancengleichheit zu ermöglichen. Dieses Vorhaben sei als eine gesamtgesellschaftliche Aufgabe zu betrachten.

Auch im Bundestag wurde hierzu zuletzt im September 2015 festgestellt: „Standards und Curricula sind den Erfordernissen der Digitalen Bildung anzupassen. Die Bundesregierung muss deshalb darauf hinwirken, dass für die schulische Medienbildung bundesweit einheitliche Mindeststandards zur Medienkompetenz in den verschiedenen Altersstufen entwickelt werden, im besten Fall analog zum Kompetenzstufenmodell von ICILS 2013. Ferner muss Medienbildung in den Prüfungen und Lehrplänen für alle Fächer und im länderspezifischen Qualitätsrahmen zur Schulentwicklung verankert sowie Lehrerinnen und Lehrern angemessene (didaktische) Hilfestellungen und Materialien zur Verfügung gestellt werden. Digitale Bildung muss als ganzheitliche Aufgabe verstanden werden, die auch den außerschulischen Bereich umfasst.“ (Deutscher Bundestag: Drucksache 18/6203 vom 30.09.2015).

Die Vermittlung von Datenschutzbewusstsein und Medienkompetenz gehört nach unserer Auffassung zum staatlichen Bildungsauftrag. Im Einklang mit unseren im Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) festgelegten Aufgaben (unter anderem in § 33) übernehmen wir mit der Umsetzung des Auftrages an die Landesregierung (Koalitionsziffer 390 - 392) einen großen Bereich der Medienbildungsangebote im Land und initiierten ein umfangreiches Angebot in Kooperation mit zahlreichen außerschulischen Partnern.

2.1.1 Vermittlung von Medienkompetenz und Datenschutzbewusstsein an den Schulen

Unsere Schulungsangebote im Bereich Medienkompetenz und Datenschutzbewusstsein werden von den Schulen des Landes in zunehmendem Maße nachgefragt. Im Jahr 2014 wurden ca. 2.200 Schülerinnen und Schüler, Lehrkräfte, Eltern, Fachkräfte der Jugendbildung sowie Erzieherinnen und Erzieher in der Ausbildung bzw. Weiterbildung erreicht. Im Jahr 2015 konnte ein ähnlich gutes Ergebnis erzielt werden. Somit ergab sich im Vergleich zu 2013 (ca. 1.500) eine dem objektiven Bedarf geschuldete Zunahme von über 40 %. Aufgrund des wachsenden Zuspruchs und unserer gleichzeitig nicht gewachsenen personellen Kapazitäten sahen wir uns zur Einführung einer „Warteliste“ veranlasst, die derzeit mehr als sechs Monate beträgt.

Positiv zu werten ist die ständige Kooperation der Partner des Netzwerkes „Medienaktiv M-V“ bei Projekttagen vor Ort und die bewährte Kooperation mit dem im Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern angesiedelten Institut für Qualitätsentwicklung Mecklenburg-Vorpommern (IQ M-V).

Vor Ort arbeiten wir zudem zusammen mit der Landeskoordinierungsstelle für Suchtvorbeugung Mecklenburg-Vorpommern (LAKOST M-V), der Medienanstalt Mecklenburg-Vorpommern (MMV) mit den Medientreckern und den Offenen Kanälen, dem Kompetenzzentrum und der Beratungsstelle für exzessive Mediennutzung und Medienabhängigkeit Schwerin der Evangelischen Suchtkrankenhilfe Mecklenburg-Vorpommern, dem Landeskriminalamt Mecklenburg-Vorpommern (LKA M-V) sowie der ComputerSpielSchule Greifswald (CSG) und dem Filmbüro Wismar. Ohne die ganz wesentlichen Beiträge des Netzwerkes „Medienaktiv M-V“ wäre eine so weitreichende Sensibilisierung und Schulung in unserem Bundesland nicht möglich.

Das Fazit bei allen Schulungen ist nach unseren Erkenntnissen und auf der Grundlage der Rückmeldungen der Teilnehmerinnen und Teilnehmer durchweg positiv. In den Datenschutz-Veranstaltungen geht es um die Gefahren im Netz beim Umgang mit den unterschiedlichen Medien sowie um technische und rechtliche Rahmenbedingungen (Persönlichkeitsrecht, Urheberrecht, Recht am eigenen Bild). Dabei verfolgen wir nicht den Ansatz der Reglementierung, sondern den des gemeinsamen Findens sowohl von Chancen als auch von Risiken im Internet. Das Ziel unserer gemeinsamen Anstrengungen bleibt dabei stets das Erlernen eines selbstbestimmten Umgangs mit digitalen Medien. Denn nur, wer die damit einhergehenden Gefahren kennt, kann diesen kompetent begegnen - und nur, wer die damit verbundenen Chancen kennt, kann diese zielsicher und unter Berücksichtigung Belanger Dritter nutzen.

Auch das Fazit im Erwachsenenbereich ist bisher positiv. Da hier oftmals Kenntnisse über technische und rechtliche Aspekte fehlen und Medienkompetenz und Datenschutzbewusstsein nicht immer didaktisch vermittelt werden, liegt der Schwerpunkt unserer Schulungen in der Vermittlung pädagogischer Fähigkeiten und der Erläuterung von technischem Grundlagenwissen. Alle anfragenden Einrichtungen sind nach eigenen Angaben froh über die Möglichkeit, auf das Fachwissen unserer Behörde zugreifen zu können.

Wir haben auch festgestellt, dass ein steigendes Interesse an der Begleitung der Ausbildung von Erzieherinnen und Erziehern besteht sowie an deren Weiterbildung in den Kindertagesstätten und im Hort. Die Anfragen der freien Träger wie Arbeiterwohlfahrt (AWO), Deutsches Rotes Kreuz (DRK), Diakonie, Pädagogium etc. haben sich von 2014 auf 2015 mehr als verdoppelt. Wir informieren dabei nicht nur über verschiedene Aspekte des Datenschutzrechts in einer Kindertagesstätte (KITA), sondern schulen auch zum gesamten Komplex der Medienbildung und der Medienkompetenzvermittlung im frühkindlichen Bereich. Wir versuchen dabei, oft gestellte Fragen zu beantworten: „Wie können Erzieherinnen und Erzieher auf Medienäußerungen und Medienhandlungen von Kindern eingehen?“, „Wie kann ich Medienkompetenz im frühkindlichen Bereich an die Kinder vermitteln?“, „Welche spielerischen Umsetzungsformen gibt es, die auf die ohnehin wartende digitalisierte `Kinderwelt` vorbereiten können?“. In vielen Fällen gelingt es uns auch, im Rahmen der Elternarbeit Fragen aus dem vorschulischen Bereich mit vergleichbaren Fragen in anderen Altersstufen zu verbinden, etwa indem wir einen Elternabend in einer Kindertagesstätte mit dem in einem Hort kombinieren.

2.1.2 Kooperationsvereinbarung zur Medienkompetenzförderung

Die Landesregierung Mecklenburg-Vorpommern räumt der Förderung von Medienbildung und Medienkompetenz einen hohen Stellenwert ein. Mit der „Kooperationsvereinbarung zur Medienkompetenzförderung in Mecklenburg-Vorpommern“ will sie Impulse für eine vertiefte Zusammenarbeit zwischen medienpädagogischen Einrichtungen, Schulen sowie Kinder- und Jugendeinrichtungen geben. Mit Blick auf unsere breit aufgestellten Bildungsangebote und auf die entsprechend vernetzte Bildungspraxis im Land hat auch unsere Behörde als neuer Partner diese Vereinbarung im April 2015 unterzeichnet (siehe dazu unsere Pressemitteilung vom 21. April 2015 unter https://www.datenschutz-mv.de/presse/2015/pm-koop-teo.html).

Kooperationspartner sind die Staatskanzlei des Landes Mecklenburg-Vorpommern, das Ministerium für Inneres und Sport Mecklenburg-Vorpommern, das Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern, das Ministerium für Arbeit, Gleichstellung und Soziales Mecklenburg-Vorpommern, der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern sowie die Medienanstalt Mecklenburg-Vorpommern. In der Vereinbarung ist dazu ausgeführt: „Medienbildung ist eine Zukunftsaufgabe unseres Landes, Medienkompetenz eine notwendige Schlüsselkompetenz für alle Menschen in unserer Gesellschaft. Allen Bürgerinnen und Bürgern soll die Möglichkeit gegeben werden, sich umfangreiches Wissen über heutige Medien anzueignen und ihre Kompetenzen hierbei kontinuierlich weiterzuentwickeln.“

Aus der Kooperationsvereinbarung gehen zahlreiche Aufgabenschwerpunkte hervor, die in den kommenden vier Jahren umgesetzt werden sollen (https://www.datenschutz-mv.de/presse/2015/koop-teo.pdf). Die Vereinbarung benennt die folgenden zwei Arbeitsgruppen, die sich den neuen Aufgabenbereichen und Herausforderungen stellen sollen:

<u>Arbeitsgruppe „KITA“</u>
Vor allem im frühkindlichen Bereich erkennen wir aufgrund unserer zahlreichen Erfahrungen vor Ort einen steigenden Schulungsbedarf. Auch aus diesem Grunde wurde aufgrund der Kooperationsvereinbarung die Arbeitsgruppe „Kita“ eingerichtet. Die Arbeitsgruppe wird durch die Vertragspartner unter Federführung des fachlich zuständigen Ministeriums für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern initiiert. Die konstituierende Sitzung soll Anfang 2016 stattfinden. Die Arbeitsgruppe wird zudem mit Akteuren der Medienbildung in Mecklenburg-Vorpommern sowie mit Vertretern zuständiger Institutionen und Abteilungen weiterer Ressorts besetzt sein.

Unsere Behörde war aktiv an der Initiierung beteiligt, da wir zum einen im Rahmen unserer zahlreichen Schulungskontakte vor Ort die entsprechenden Bedarfe schnell zuverlässig identifizierten und zum anderen die ganz praktischen Bildungsvorschläge und Erwartungen der betroffenen Erzieherinnen und Erzieher und ihrer Ausbilder in die vernetzende Gruppenarbeit einbringen können. Nicht nur diese unmittelbaren (aber doch auch subjektiven) Erfahrungen und Anfragen, sondern auch die Ergebnisse verschiedener Studien (bspw. Studie „miniKIM 2014“ des Medienpädagogischen Forschungsverbandes Südwest [http://www.mpfs.de/?id=565] oder die „U9-Studie: Kinder in der digitalen Welt“ des Deutschen Instituts für Vertrauen und Sicherheit [https://www.divsi.de/publikationen/studien/divsi-u9-studie-kinder-der-digitalen-welt]) belegen einen steigenden Bedarf zu Schulungs- und Informationsmaßnahmen nicht nur bei Erzieherinnen, Erziehern und Ausbildern, sondern auch bei den Kindern selbst, da die Studienlage zudem eine zunehmende Mediennutzung bei immer jüngeren Kindern nachweist.

Medienbildung im frühkindlichen Bereich möchten wir jedoch nicht in der Form verstanden wissen, dass es zum Beispiel „Tablet-Gruppen“ für 3- bis 4-Jährige geben sollte. Vielmehr sollte an die in diesem Alter vorhandenen kognitiven, motorischen und senso-motorischen Erfahrungen der Kinder angeknüpft werden, um die Funktion und die Wirkung von digitalen Medien zu erklären. So kann und soll von Beginn an ein kritischer Blick auf digitale Medien gefördert werden, damit die Wahrscheinlichkeit steigt, dass sie in gesundem Maß genutzt und die Inhalte und Wirkungsweisen schon früh verstanden werden. Medienkompetenzvermittlung im frühkindlichen Bereich verstehen wir als Medienbildung für Kinder, Eltern, Erzieherinnen und Erzieher mit dem Ziel, zu einer sinnvollen, geregelten und begleiteten Nutzung anzuleiten.

Arbeitsgruppe „Digitale Schule“
Diese zweite Arbeitsgruppe hat das Ziel, der Landesregierung und den kommunalen Schulträgern bis Anfang 2017 einen Orientierungsrahmen für eine nachhaltige Strategie in Bezug auf eine angemessene Ausstattung der Schulen mit Informationstechnik (IT) zu bieten. Es wurden drei Unterarbeitsgruppen eingerichtet, die in den Bereichen „Infrastruktur“, „Datenschutz und Organisation“ und „Medienpädagogik“ Empfehlungen erarbeiten sollen. Wir beteiligen uns in allen drei Unterarbeitsgruppen, da der Datenschutz in allen drei Bereichen eine maßgebliche Rolle spielt.

Im Bereich „Infrastruktur“ soll ein ganzheitliches Konzept entwickelt werden, welches den Anforderungen des Schulalltages in einer multimedialen Welt gerecht werden soll. Es wird davon ausgegangen, dass in der immer komplexer werdenden IT sowohl eine qualifizierte Betreuung der Geräte als auch ein entsprechendes Fortbildungskonzept für die jeweiligen Nutzer notwendig ist. Das Konzept soll sowohl Vorgaben für die Ausstattung der Schulen mit IT als auch Empfehlungen für den Betrieb dieser Technik beinhalten.

Im Bereich „Datenschutz und Organisation“ sollen Vorschläge erarbeitet werden, wie die aktuelle datenschutzrechtliche Rechtslage, die maßgeblich durch das Schulgesetz Mecklenburg-Vorpommern (SchulG M-V) und die Schuldatenschutzverordnung Mecklenburg-Vorpommern (SchulDSVO M-V) geprägt wird, an den Stand der Technik angepasst werden kann. Diese Rechtsgrundlagen sind zurzeit nicht geeignet, angemessene und dem Stand der Technik entsprechende Anforderungen an die IT-Ausstattung zu formulieren.

In der dritten Arbeitsgruppe sollen Anforderungskriterien für eine einheitliche und qualitativ hochwertige, pädagogische Medienversorgung erarbeitet werden. Dabei soll der Tatsache Rechnung getragen werden, dass Datenträger wie DVD oder VHS-Kassetten in den Schulen keine nennenswerte Rolle mehr spielen, sondern künftig Streaming-Dienste im Vordergrund stehen.

Die Arbeitsergebnisse sollen in die nächste Koalitionsvereinbarung einfließen, um ein hohes Maß an Verbindlichkeit zu erreichen und die Umsetzung auf breiter Basis zu gewährleisten. Die Ergebnisse sollen auch dazu beitragen, die Kooperationsvereinbarung zur Medienkompetenzförderung in Mecklenburg-Vorpommern fortzuschreiben.

2.1.3 Netzwerk „Medienaktiv M-V“

Das landesweite Netzwerk für Medienbildung in Mecklenburg-Vorpommern „Medienaktiv M-V“ wird vom Landesjugendring Mecklenburg-Vorpommern (LJR M-V), der Landeskoordinierungsstelle für Suchtvorbeugung Mecklenburg-Vorpommern (LAKOST M-V), dem Landeskriminalamt Mecklenburg-Vorpommern (LKA M-V), dem Kompetenzzentrum und Beratungsstelle für exzessive Mediennutzung und Medienabhängigkeit Schwerin der Evangelischen Suchtkrankenhilfe Mecklenburg-Vorpommern, der Medienanstalt Mecklenburg-Vorpommern (MMV) und unserer Behörde geleitet. Das Netzwerk wird zudem von vielen außerschulischen Partnern der Medienarbeit in Mecklenburg-Vorpommern unterstützt. Dazu gehören beispielsweise Medienwerkstätten, freie Medienpädagoginnen und Medienpädagogen oder Vereine. Das Netzwerk „Medienaktiv M-V“ ist offen gegenüber neuen Mitgliedern. Inzwischen wurde auch eine Kooperation mit dem medienpädagogischen Zentrum des Instituts für Qualitätssicherung des Ministeriums für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern eingegangen.

Grundsätzlich sind alle Mitglieder im Netzwerk kooperationsfördernd gleichberechtigt und bringen ihre Kompetenzen in die Netzwerkarbeit ein. „Medienaktiv M-V“ soll helfen, Partner für neue und vorhandene Projekte, Angebote, Ideen und gemeinsames Auftreten in der Öffentlichkeit zu den Themen des Netzwerkes zu finden. Dazu bringen alle Akteure des Netzwerkes ihre Erfahrungen und ihr Know-How ein und leisten ihren Beitrag, um die Kooperationsvereinbarung zur Förderung von Medienkompetenz in Mecklenburg-Vorpommern, siehe Punkt 2.1.2, umzusetzen. Indem sie die dort aufgeführten Angebote zur Verfügung stellen, leisten sie einen entscheidenden Beitrag zur Medienbildung. Die Präambel der Kooperationsvereinbarung beschreibt dies als „Zukunftsaufgabe unseres Landes“.

Das Netzwerk verdeutlicht die Vielfalt der Medienangebote unseres Bundeslandes und vergrößert die Chance, mit unseren Bildungs- und Informationsangeboten zum Thema Medien verschiedene Zielgruppen zu erreichen. Es ist zugleich ein Wissenspool für seine Mitglieder. Um sich gegenseitig zu qualifizieren und auf dem Laufenden zu halten, treffen sich die Mitglieder zwei Mal im Jahr themenbezogen und schwerpunktorientiert. Dabei stehen fachliche Impulse sowie entsprechende Diskussionen und der fachliche Austausch sowie dessen Nachbereitung im Mittelpunkt. Das Netzwerk greift aktuelle Entwicklungen der Medien auf und regt gemeinsame Strategien an.

Das Netzwerk „Medienaktiv M-V“ berät Politik und Medienwirtschaft bei der Gestaltung der Medienlandschaft in Mecklenburg-Vorpommern. Dabei stehen die Medienkompetenz-Förderung und der Medienschutz für Kinder, Jugendliche, Erwachsene und Senioren im Mittelpunkt.

Dieses Netzwerk ist bundesweit beispielgebend, da sich hier sowohl Suchthilfe, Jugendhilfe, Medienpädagogik, Polizei, Schule und Datenschutz gemeinsam und auf Augenhöhe engagieren. „Medienaktiv M-V“ war auf dem bundesweiten Präventionstag im Juni 2015 präsent. Nach unseren Erkenntnissen aus bundesweiten Arbeitsgruppen zum Thema sind andere Bundesländer ebenfalls auf dem Weg, sich institutionsübergreifend zu vernetzen. Wir unterstützen diesen Wissenstransfer aktiv. Möchte das Land Mecklenburg-Vorpommern jedoch weiterhin diese bundesweite Vorreiterrolle behalten, bedarf es entsprechender Maßnahmen der Landesregierung.

2.1.4 „Medienscouts MV“ und TEO „Protect Privacy“

„Medienscouts MV“
Das Projekt „Medienscouts MV“ haben wir bereits im Juni 2012 gestartet. Im 11. Tätigkeitsbericht haben wir unter Punkt 2.2 über die erste Phase des Projektes berichtet. Das Projekt wird von Beginn an von verschiedenen Institutionen des Landes Mecklenburg-Vorpommern unterstützt: Landeskoordinierungsstelle für Suchtvorbeugung Mecklenburg-Vorpommern (LAKOST M-V), Landesjugendring Mecklenburg-Vorpommern (LJR M-V), Landeskriminalamt Mecklenburg-Vorpommern (LKA M-V), Medienanstalt Mecklenburg-Vorpommern (MMV), Online-Selbsthilfeplattform juuuport, ComputerSpielSchule Greifswald (CSG).

Die Konzeptidee beruht auf dem peer-to-peer-Ansatz. Jugendliche können mit dieser Methode das Wissen, das sie im Laufe der mehrmals im Jahr stattfindenden Medienscouts-Wochenenden erwerben, unmittelbar an andere Jugendliche (und bisweilen auch an Lehrkräfte oder Eltern) weitergeben. Von Freitag bis Sonntag werden Jugendliche im Alter von 14-16 Jahren im konstruktiv-kritischen Umgang mit digitalen Medien fit gemacht.

Sie werden an methodische Konzepte herangeführt, mit denen sie etwa Workshops durchführen, Vorträge halten und Projekttage organisieren können. Beim späteren Anwenden dieser Methoden in der Praxis steht ihnen das Projektteam auch nach der Ausbildung unterstützend zur Verfügung. Einmal jährlich werden zudem alle bereits ausgebildeten Medienscouts zu einem Update-Treffen eingeladen, um sich auszutauschen, neue Themen zu besprechen und aktuelle Trends zu diskutieren.

Seit dem Projektstart im Jahr 2012 wurden an sieben Wochenenden mehr als 170 Medienscouts ausgebildet. Es hat sich bewährt, die Medienscouts-Wochenenden an verschiedenen Orten des Landes durchzuführen. Dies führte zu einer gerechten regionalen Verteilung und ermöglichte es Teilnehmerinnen und Teilnehmern aus allen Regionen Mecklenburg-Vorpommerns, mit vertretbarem Aufwand am Projekt teilzunehmen.

Durch den peer-to-peer Ansatz ist es dem Gemeinschaftsprojekt möglich, das Wissen zu multiplizieren. Somit wurden ca. 8.500 Schülerinnen und Schüler in den vergangenen drei Jahren durch die von uns ausgebildeten Medienscouts geschult. Dazu informieren Medienscouts beispielsweise an den eigenen oder benachbarten Schulen jüngere Klassen oder Gleichaltrige oder werden in außerschulische Einrichtungen eingeladen. Mitunter werden sie auch regulär in einzelne Unterrichtskonzepte (auch jahrgangsübergreifend) eingebunden. Uns sind inzwischen sogar Anfragen bekannt geworden, bei denen die Lehrerschaft selbst von Medienscouts geschult werden möchte.

Dies alles bedeutet für die Jugendlichen neben ihren schulischen Aufgaben einen zusätzlichen Aufwand. Besonders vor diesem Hintergrund freut uns die hohe Nachfrage als spürbarer Nachweis für die hohe Wertschätzung und Anerkennung dieses ehrenamtlichen Engagements. Wir stellen zudem eine steigende Nachhaltigkeit des entsprechenden Wissens und der erworbenen Kompetenzen fest. So ist erfreulich, dass ein Teil der Medienscouts nicht nach der Schule aus dem System „verschwindet“, sondern ihre Schulungstätigkeit beispielsweise in der Ausbildung oder auch im Studium fortsetzt.

Auch in anderen Bundesländern gibt es ähnliche Projekte, die jedoch in der Regel mit weitaus höheren finanziellen Mitteln ausgestattet sind. Das bisher nur in unserem Bundesland praktizierte Kooperationsmodell mit vielen unterschiedlichen (auch) außerschulischen Kooperationspartnern wird inzwischen von den anderen Bundesländern als besonders kostensparend und effizient mit großem Interesse verfolgt. Der weitere Erfolg unseres bundesweit beachteten Projektes setzt jedoch auch weiterhin voraus, dass die strukturelle und organisatorische Basis für diese außerschulische Kooperation erhalten bleibt.

„Tage ethischer Orientierung“ (TEO): Das Modul „protect privacy - Mein Klick, meine Verantwortung!?“
„Tage ethischer Orientierung“ (TEO) ist ein schulkooperatives Modell der Evangelisch-Lutherischen Kirche in Norddeutschland und des Erzbistums Hamburg, das in einer neuen Kooperation mit uns durchgeführt wird. Das Modul „protect privacy - Mein Klick, meine Verantwortung!?“ ist speziell für die 5. und 6. Klassen konzipiert.

Es handelt sich hier ebenfalls um ein Gemeinschaftsprojekt, das von Referenten der Landeskoordinierungsstelle für Suchtvorbeugung Mecklenburg-Vorpommern (LAKOST M-V), dem Kompetenzzentrum und Beratungsstelle für exzessive Mediennutzung und Medienabhängigkeit Schwerin der Evangelischen Suchtkrankenhilfe Mecklenburg-Vorpommern, der ComputerSpielSchule Greifswald (CSG) und der Medientrecker der Medienanstalt Mecklenburg-Vorpommern (MMV) unterstützt wird. Seit 2013 wurden bereits etwa 330 Schülerinnen und Schüler der 5. und 6. Klassen sowie Lehrerinnen und Lehrer unseres Landes geschult.

In dem 4-tägigen Modul befassen sich die Teilnehmerinnen und Teilnehmer mit den Handlungsfeldern „Datenspuren im Netz, soziale Netzwerke, Cybermobbing, Apps, Smartphones, Handys und Computerspiele“. Dabei soll ein Bezug zu den Grundrechten nach Art. 1 und 2 Grundgesetz (GG) hergestellt und die Möglichkeiten verantwortungsbewusster Nutzung digitaler Medien mit Blick auf die eigene Praxis erarbeitet werden.

Diese ebenfalls sehr erfolgreichen Projekte sollen fortgeführt werden. Hierzu bedarf es für die bekannten außerschulischen Partner verlässlicher finanzieller und personeller Rahmenbedingungen, die, soweit es sich um gemeinnützige Träger handelt, seitens der Landesregierung entsprechend zu gewährleisten sind.

Weitere detaillierte Informationen zu diesen Projekten sind im Internet unter www.medienscouts-mv.de und www.teoinmv.de zu finden.

2.1.5 Datenschutz an den Schulen in Mecklenburg-Vorpommern

Im Zusammenhang mit unseren vielfältigen Aktivitäten im Bildungsbereich hatten wir den Eindruck gewonnen, dass die Schulen datenschutzrechtliche Vorgaben mitunter unzureichend berücksichtigen. Um diesen Eindruck mit belastbaren Fakten untermauern zu können, haben wir im ersten Quartal 2014 das Projekt „Datenschutz an den Schulen in Mecklenburg-Vorpommern“ gestartet. Das Projekt hat zum Ziel, den Ist-Zustand im Bereich des Datenschutzes an den Schulen im Land zu erfassen, mögliche Handlungsbedarfe bei den verschiedenen Beteiligten im Schulsektor zu identifizieren und entsprechende Empfehlungen aus datenschutzrechtlicher Sicht zu geben.

Um den datenschutzrechtlichen Ist-Zustand an den Schulen im Land zu erfassen, haben wir zusammen mit dem Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern zunächst eine Online-Befragung aller 593 Schulen Mecklenburg-Vorpommerns durchgeführt. Obwohl die Beantwortung der Fragen freiwillig war, beteiligten sich immerhin 153 Schulen an der Umfrage. Die Auswertung der Ergebnisse zeigte, dass eine umfassendere Befragung nötig war, um belastbarere Ergebnisse zu erhalten. Daher haben wir uns entschieden, weitere Informationen durch persönliche Befragungen an den Schulen im Land einzuholen. Bei 18 Schulen haben wir diese Befragungen im Rahmen eines Kontroll- und Informationsbesuches durchgeführt.

Wir haben von Anfang an ausdrücklich darauf hingewiesen, dass die Besuche in erster Linie dem Zweck dienen, den datenschutzrechtlichen Ist-Zustand an den Schulen zu erfassen, und um eine offene und realistische Schilderung der Zustände gebeten.

Um in der knappen zur Verfügung stehenden Zeit möglichst viele Besuche absolvieren zu können, haben wir - anders als bei den sonstigen Datenschutz-Kontrollen üblich - für die Planung der Besuche und für die jeweiligen Kontrollberichte eine Checkliste in Tabellenform verwendet. Durch diese besondere Form des Berichtes waren wir in der Lage, 18 Schulen in allen Regionen des Landes in relativ kurzer Zeit zu besuchen. Die strukturierte Tabellenform hat zudem die Auswertbarkeit und Vergleichbarkeit der durchgeführten Kontrollen erheblich vereinfacht.

Nach Gesamtschau der durchgeführten Kontroll- und Informationsbesuche haben wir Handlungsbedarfe bei allen Beteiligten im gesamten Schulsektor identifiziert. Mit allen Beteiligten wird beraten, welche Maßnahmen erforderlich sind, um den Datenschutz an den Schulen in angemessener Weise umzusetzen. Bei Redaktionsschluss dieses Berichtes waren diese Beratungen noch nicht beendet, sodass Ergebnisse noch nicht vorliegen. Nach Abschluss der Gespräche, voraussichtlich im Frühjahr 2016, werden wir den Projektbericht „Datenschutz an den Schulen in Mecklenburg-Vorpommern“ in geeigneter Form veröffentlichen.

2.2 Kommunales/Personenstandswesen

2.2.1 Datenschutz und Informationssicherheit in den Kommunen in Mecklenburg-Vorpommern

In diesem Berichtszeitraum waren Datenschutz und IT-Sicherheit in den Kommunen in Mecklenburg-Vorpommern ein Schwerpunkt unserer Tätigkeit. Kommunales E-Government erfordert auch die sorgfältige Umsetzung der Anforderungen an die Informationssicherheit und an den Datenschutz. Die Erfahrungen zeigen jedoch immer wieder, dass viele Kommunen dabei nach wie vor erhebliche Schwierigkeiten haben.

In der ersten Hälfte des Jahres 2014 haben wir stichprobenartige Kontrollen zu datenschutz- und IT-sicherheitsrelevanten Aspekten in den Kommunen in Mecklenburg-Vorpommern mit dem Schwerpunkt im Bereich Personenstandswesen durchgeführt. Dabei haben wir erhebliche Schwierigkeiten bei der Gewährleistung eines angemessenen Datenschutz- und IT-Sicherheitsniveaus festgestellt. Oftmals mangelte es den Kommunen an Personal und Finanzen, nicht selten fehlte aber auch das Bewusstsein für die Bedeutung datenschutzrechtlicher Anforderungen.

Um die Kommunen effektiv unterstützen zu können, haben wir im Rahmen des Projektes „Datenschutz und IT-Sicherheit in den Kommunen in Mecklenburg-Vorpommern“ den Ist-Zustand in Bezug auf Datenschutz und IT-Sicherheit erhoben. Hier ging es einerseits um das Verfahren im Bereich des Personenstandswesens und andererseits um allgemeine datenschutz- und IT-sicherheitstechnische Rahmenbedingungen zur Umsetzung der datenschutzrechtlichen Vorschriften in den jeweiligen Verwaltungen.

Online-Umfrage
Das Projekt begann im dritten Quartal 2014 und endete im 4. Quartal 2015. Zuerst haben wir die Kommunen, die das Fachverfahren Personenstandswesen betreiben, mit Hilfe eines Online-Fragenkatalogs zu verschiedenen Datenschutzaspekten befragt. Den Fragenkatalog haben wir mit dem Ministerium für Inneres und Sport Mecklenburg-Vorpommern abgestimmt, da das Ministerium gleichzeitig eine anonymisierte Online-Erhebung mit dem Schwerpunkt IT-Sicherheit durchführen wollte.

Trotz wiederholter Aufforderung zur Teilnahme und dem Hinweis auf die Mitwirkungspflicht nach § 31 Abs. 1 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) war die Beteiligung der Verwaltungen nicht zufriedenstellend. Zehn Verwaltungen wurde eine Beanstandung wegen fehlender Mitwirkung ausgesprochen.

Ausgewählte Ergebnisse der Online-Umfrage:
- 94 % der Verwaltungen hatten eine/n behördliche/n Datenschutzbeauftragte/n/n bestellt
- 23 % der behördliche/n Datenschutzbeauftragte/n gaben an, mehr als 10 % ihrer Arbeitszeit ihrer Aufgabe widmen zu können
- 24 % der behördliche/n Datenschutzbeauftragte/n empfanden ihren Stellenanteil als ausreichend
- 96 % der Verwaltungen waren der Ansicht, dass die Einführung des Fachverfahrens Personenstandswesen rechtzeitig kommuniziert wurde
- 84 % der Verwaltungen empfanden die Test- und Einarbeitungszeit als ausreichend
- 58 % der Verwaltungen gaben an, über ein verfahrensspezifisches Sicherheitskonzept zu verfügen
- 55 % der Verwaltungen führten eine dokumentierte Vorabkontrolle durch
- 19 % der Verwaltungen standen ein Notfallhandbuch oder eine Notfallanweisung zur Verfügung
- 13 % der Befragten gaben an, noch Windows XP im Einsatz zu haben
- erhöhten Handlungsbedarf sahen die Verwaltungen vor allem bei der Bereitstellung von Checklisten und Formvorlagen sowie Mustern für Dienstanweisungen und Dienstvereinbarungen
- Unterstützung bei der Umsetzung des Datenschutzes erwarteten die Kommunen bei der Erstellung von Sicherheitskonzepten, der Vorgabe von Checklisten für den IT-Grundschutz und bei den Datenschutzschulungen der Mitarbeiterinnen und Mitarbeiter
- zusätzliche Finanzmittel wurden gewünscht

Datenschutzrechtliche Bewertung der Online-Umfrage:
Positiv zu bewerten war, dass sowohl die Informationspolitik als auch die Gestaltung der Test- und Einarbeitungszeiträume rund um die Einführung des Fachverfahrens Personenstandswesen durch die Verwaltungen als sehr gut empfunden wurde. Allerdings verfügten nur 58 % der Kommunen und damit entschieden zu wenig über ein verfahrensspezifisches Sicherheitskonzept für das Verfahren Personenstandswesen, wobei allen Körperschaften durch den Zweckverband „Elektronische Verwaltung in Mecklenburg-Vorpommern“ (eGo-MV) entsprechende Mustervorlagen übergeben worden sind. Obwohl eine Vorabkontrolle für das Personenstandsverfahren vorgeschrieben ist, konnte nur gut die Hälfte der Verwaltungen entsprechende Dokumente vorlegen. Möglicherweise liegt eine Ursache hierfür darin, dass nur 23 % der behördlichen Datenschutzbeauftragten über einen Stellenanteil von mehr als 10 % für diesen Aufgabenbereich verfügen. Die behördlichen Datenschutzbeauftragten müssen über ein ausreichendes Zeitkontingent verfügen, um ihre Aufgaben erfüllen zu können. Insgesamt besteht in vielen Verwaltungen noch Nachholbedarf, wenn es darum geht, ein angemessenes Informationssicherheits- und Datenschutzniveau zu gewährleisten.

Kontroll- und Informationsbesuche
Im Ergebnis der Online-Umfrage haben wir festgestellt, dass weitere detaillierte Erhebungen bei den Kommunen vor Ort erforderlich waren, um die Situation vollständig bewerten und Empfehlungen für Verbesserungen geben zu können. Wir haben daher im zweiten und dritten Quartal 2015 Kontroll- und Informationsbesuche in 40 ausgewählten Kommunen durchgeführt, wobei der Fragenkatalog auf der Grundlage der Erkenntnisse aus der Online-Umfrage erstellt wurde. Inhaltlicher Schwerpunkt der Besuche war neben allgemeinen Fragen zum technischen und organisatorischen Datenschutz die Verarbeitung personenbezogener Daten im Verfahren für das Personenstandswesen. Die Ergebnisse der Kontroll- und Informationsbesuche wurden in tabellarischer Form dargestellt, was sowohl die Lesbarkeit und Verständlichkeit als auch die Vergleichbarkeit der Ergebnisse wesentlich vereinfachte. Diese Vorgehensweise war jedoch nicht dazu geeignet, detaillierte und tiefgreifende Kontrollen durchzuführen.

Im Rahmen der Kontroll- und Informationsbesuche wurden die Ergebnisse aus den Kontrollbesuchen aus dem Jahr 2014, siehe Punkt 5.4.4, sowie die Erkenntnisse aus der Online-Umfrage aus dem Jahr 2015 weitgehend bestätigt. Während der Besuche wurden Gespräche über Einzelfragen der Informationssicherheit und des technischen und organisatorischen Datenschutzes und zum Betrieb des automatisierten Verfahrens für das Personenstandswesens geführt. Darüber hinaus wurden verschiedene Unterlagen gesichtet, etwa Sicherheitskonzepte und ausgewählte Vertragswerke. Abschließend wurden wichtige Infrastruktureinrichtungen in Augenschein genommen.

Ausgewählte Ergebnisse der Kontroll-und Informationsbesuche:
- 77 % der Verwaltungen hatten eine/n behördliche/n Datenschutzbeauftragte/n bestellt,
- 35 % hatten eine Stellvertreterin/einen Stellvertreter der/des behördliche/n Datenschutzbeauftragte/n bestellt,
- keine der kontrollierten Verwaltungen verfügte über ein qualifiziertes und aktuelles Rahmensicherheitskonzept,
- 7 % konnten ein qualitativ gutes Sicherheitskonzept vorlegen, sie versäumten es allerdings, es systematisch zu aktualisieren,

- 72 % konnten ein verfahrensspezifisches Sicherheitskonzept in einer sehr guten Qualität vorlegen,
- praktisch alle Kommunen nutzen die Software „TeamViewer“, um Fernwartungszugriffe zu ermöglichen,
- 63 % der Standesamt-PC entsprachen nur teilweise den datenschutzrechtlichen Anforderungen,
- 32% der Kommunen hatten die Aufbewahrung der Signaturkarten und PINs vollständig den datenschutzrechtlichen Anforderungen entsprechend geregelt,
- die physische Sicherheit der Verwaltungsgebäude entsprach in 62 % vollständig, zu 13 % weitgehend und zu 25 % nur teilweise den Anforderungen,
- 75 % der Verwaltungen hatten die Anforderungen an die Sicherung der Verfügbarkeit der Daten (Datensicherung) vollständig umgesetzt.

Datenschutzrechtliche Bewertung der Kontroll- und Informationsbesuche:
Die Gesamtverantwortung für die Ausführung der Vorschriften zu Informationssicherheit und Datenschutz liegt stets bei der jeweiligen öffentlichen Stelle, hier bei der Behördenleitung, siehe § 19 Abs. 1 DSG M-V.

Allein die Ankündigung der Kontroll- und Informationsbesuche hat die Verantwortlichen in fast allen Verwaltungen dazu veranlasst, eine Überprüfung der Dokumentation und der technischen und organisatorischen Maßnahmen durchzuführen. Im Zuge der Vorbereitungen wurden viele datenschutzrelevante Hinweise der behördlichen Datenschutzbeauftragten umgesetzt, die schon seit längerer Zeit zur Umsetzung anstanden. Dies verfälschte zwar ein wenig den vorgefundenen Ist-Zustand, führte aber zur Vervollständigung und Aktualisierung der Dokumentation in den jeweiligen Kommunen, was aus unserer Sicht sehr positiv zu bewerten ist.

Die Verwaltungen, die durch die externen behördlichen Datenschutzbeauftragten des Zweckverbandes „Elektronische Verwaltung in Mecklenburg-Vorpommern“ (eGo-MV) betreut werden, waren in der Regel besser vorbereitet und umfassender mit den geforderten Unterlagen ausgestattet worden als andere Verwaltungen.

Schlussbetrachtungen und Ausblick
Im kommunalen Bereich werden sehr viele und zum Teil sehr schutzbedürftige Daten automatisiert verarbeitet. Durch die zunehmend automatisierte Verarbeitung sind die Anforderungen an die Informationssicherheit und an den Datenschutz im Bereich der Kommunen in den letzten Jahren erheblich gestiegen. Fachaufgaben, die die Kommunen in der Vergangenheit auf dem Papier oder mit einfachen, lokalen Datenverarbeitungsanlagen erledigt haben, werden inzwischen mit komplexen, oftmals zentral organisierten IT-Verfahren bearbeitet.

Die neuen Strukturen der IT-Verfahren resultieren zum Teil auch aus bundesgesetzlichen Vorgaben. Als Beispiele sollen hier nur das Meldewesen, die Beantragung und Ausstellung von Reisepass und Personalausweis, das elektronische Grundbuch oder das Personenstandswesen genannt werden.

Die meisten Verfahren sind als Verbund-, Abruf- oder gemeinsame Verfahren ausgestaltet und bestehen daher aus zentralen und dezentralen Komponenten, die - insbesondere wegen der oftmals an einer Stelle konzentrierten großen Datenmengen und der mitunter bundesweiten Vernetzung -erhebliche Sicherheits- und Datenschutzrisiken in sich bergen. Diese Risiken müssen durch entsprechende Schutzbedarfsfeststellungen und Risikoanalysen benannt und durch technische und organisatorische Maßnahmen auf ein hinnehmbares Maß reduziert werden.

Um einschätzen zu können, welche Sicherheits- und Datenschutzmaßnahmen erforderlich und angemessen sind, ist eine systematische und konzeptionelle Vorgehensweise erforderlich. Diese Maßnahmen müssen vor der Inbetriebnahme des Verfahrens umgesetzt werden.

Ein Sicherheitskonzept kann seine Wirkung jedoch nur entfalten, wenn es in ein Informationssicherheits- und Datenschutz-Management-System eingebettet ist. Der Betrieb eines solchen Management-Systems erfordert einerseits eine angemessene finanzielle Ausstattung, um die erforderlichen Maßnahmen umsetzen zu können, und andererseits qualifiziertes Fachpersonal, um den Betrieb des Informationssicherheits- und Datenschutz-Management-Systems sicherzustellen.

Der Betrieb der zentralen Komponenten eines Verfahrens erfolgt in der Regel durch gut ausgebildete und erfahrene Fachleute in Rechenzentren des Landes oder des Bundes und wird durch IT-Sicherheitsbeauftragte und behördliche bzw. betriebliche Datenschutzbeauftragte fachlich kompetent begleitet. Dort stehen in der Regel auch angemessene finanzielle Mittel zur Verfügung, um die Sicherheitskonzepte zu erstellen und vor allem umzusetzen.

Aber auch die kommunale Ebene muss in derartige Management-Prozesse eingebunden werden, weil die Sicherheits- und Datenschutzanforderungen sich uneingeschränkt auch auf die dezentralen Komponenten der eingesetzten IT-Verfahren erstrecken. Die dezentralen Komponenten in den Kommunen müssen das gleiche IT-Sicherheits- und Datenschutzniveau aufweisen wie die zentralen Komponenten, denn ein IT-Verfahren ist nur so sicher wie seine schwächste Stelle.

Im März 2013 hat der IT-Planungsrat die „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ verabschiedet und damit zwischen Bund und Ländern erstmals ein verbindliches Mindestsicherheitsniveau der IT-gestützten ebenenübergreifenden Zusammenarbeit in der Verwaltung vereinbart. Den Kommunen wird die Anwendung der Leitlinie für die Informationssicherheit lediglich empfohlen. Damit ignorierte der IT-Planungsrat die weitergehenden Empfehlungen sowohl der kommunalen Spitzenverbände als auch der Datenschutzbeauftragten von Bund und Ländern.

Wir haben den Kommunen unseres Bundeslandes dennoch frühzeitig empfohlen, die Vorgaben der Leitlinie umzusetzen und für die Planung und Umsetzung eines angemessenen IT-Sicherheitsniveaus die Grundschutzmethodik des Bundesamtes für Sicherheit in der Informationstechnik (BSI) anzuwenden, siehe Elfter Tätigkeitsbericht, Punkt 4.3.

Im Ergebnis dieses Projektes ist festzustellen, dass der Einsatz von elektronischen Verfahren in der Verwaltung auch die Umsetzung einer durchgängig hohen Informationssicherheit und eines umfassenden Datenschutzes erfordert. Um die komplexen IT-Infrastrukturen dauerhaft sicher und datenschutzgerecht betreiben zu können, bedarf es der Etablierung eines Management-Prozesses für Informationssicherheit und Datenschutz, der Erstellung, Umsetzung und regelmäßigen Aktualisierung von Sicherheitskonzepten, ausreichend finanzieller Mittel für Ausstattung und Personal, qualifizierten Fachpersonals sowie Maßnahmen zur Aufrechterhaltung der Informationssicherheit und des Datenschutzes. Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern wird bei diesen Prozessen auch weiterhin unterstützen.

3 IT-Planungsrat

3.1 Die Rolle der Datenschutzbeauftragten von Bund und Ländern

Der IT-Planungsrat wurde im Jahr 2010 als zentrales Gremium des Bundes und der Länder für die föderale Zusammenarbeit in der Informationstechnik eingerichtet. Er steuert die Zusammenarbeit von Bund und Ländern in der Informationstechnik und im E-Government. Mitglieder im IT-Planungsrat sind die Beauftragten für Informationstechnik (CIO) der Länder und des Bundes. Der IT-Planungsrat hatte beschlossen, zusätzlich sowohl die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit als auch einen Vertreter der Landesbeauftragten für den Datenschutz zu seinen Sitzungen mit beratenden Stimmen hinzuzuziehen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erteilte uns in unserer Eigenschaft als Vorsitzendem des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ (AK Technik - siehe Punkt 6) das Mandat zur Beratung des IT-Planungsrates aus der Sicht der Landesbeauftragten für den Datenschutz.

Im Berichtszeitraum haben wir sowohl an allen sechs turnusmäßigen Sitzungen des IT-Planungsrates als auch in verschiedenen Beratungen auf Arbeitsebene teilgenommen. In zahlreichen Arbeitsgremien des IT-Planungsrates haben uns weitere Kolleginnen und Kollegen aus dem Kreis der Landesbeauftragten für den Datenschutz unterstützt.

In den folgenden Abschnitten berichten wir über einige ausgewählte Aspekte unserer Beratungstätigkeit. Einen vollständigen Überblick über die Arbeit des IT-Planungsrates und dessen Projekte, Anwendungen und Entscheidungen können sich interessierte Leserinnen und Leser auf dessen Internetpräsentation verschaffen (http://www.it-planungsrat.de/DE/Home/home_node.html).

3.2 Cloud-Richtlinie der Datenzentralen

Angesichts der zunehmenden Verbreitung von Cloud-Computing-Technologien befasste sich der IT-Planungsrat in seiner 13. Sitzung am Rande der CeBIT 2014 in Hannover mit dem Thema und insbesondere mit den damit im Zusammenhang stehenden Fragen der IT-Sicherheit und des Datenschutzes. Die auf dieser Sitzung beschlossene Umfrage zur Cloud-Nutzung in den Bundesländern erbrachte insgesamt 85 Rückläufe, wovon 50 auf Dienststellen des Bundes, 31 auf Dienststellen der Länder und 4 auf Kommunen entfielen. Bei 26 der rückmeldenden Organisationen waren bereits Cloud-Technologien im Einsatz. Dieser Anteil verteilte sich gleichmäßig auf Einrichtungen im Bereich des Bundes und der Länder. 9 Organisationen bereiteten die Nutzung von Cloud-Diensten gerade vor, 1 plante deren Einsatz. Rund die Hälfte der rückmeldenden Organisationen erklärte, Cloud-Computing nicht einzusetzen. Der IT-Planungsrat zog aus der Umfrage den Schluss, dass den Behörden zusätzliche Hilfestellungen bei der Ausschreibung von Cloud-Diensten gegeben werden sollten, und griff einen Vorschlag des Arbeitskreises der Leiter der Datenzentralen der verschiedenen Bundesländer auf.

Der Arbeitskreis der Datenzentralen hatte auf Initiative der Datenzentralen aus Mecklenburg-Vorpommern und Rheinland-Pfalz (DVZ M-V GmbH und LDI R-P) eine Richtlinienempfehlung für die Ausschreibung, die Vergabe und den Betrieb von öffentlichen Aufträgen in der Cloud erarbeitet (http://www.it-planungsrat.de/SharedDocs /Downloads/DE/ Entscheidungen/16.%20Sitzung/08_Cloud-Handlungsempfehlungen. html?nn=1299858). Das Papier war vor der Präsentation im IT-Planungsrat dem AK Technik, siehe Punkt 6, mit der Bitte um Stellungnahme vorgelegt worden. Der AK Technik befürwortete die Richtlinienempfehlung Technik und begrüßte den Ansatz, personenbezogene Daten nur in solchen Cloud-Strukturen zu verarbeiten, die in nationalen, zertifizierten Hochsicherheitsrechenzentren betrieben werden und somit den Datenschutzregeln in der Europäischen Union unterliegen.

Der IT-Planungsrat nahm das Papier in seiner 16. Sitzung zur Kenntnis und sprach sich dafür aus, bei der Nutzung von Cloud-Computing durch die öffentliche Verwaltung in Bund, Ländern und Kommunen abgestimmte Kriterien und Vorgehensweisen zu nutzen. Er beauftragte den Bund sowie die Länder Rheinland-Pfalz und Mecklenburg-Vorpommern, zusammen mit weiteren Ländern hierzu Vorschläge zu erarbeiten. Zu diesem Zweck wurde im September 2015 eine Arbeitsgruppe eingerichtet, die Vorschläge zum weiteren Vorgehen entwickeln und dem IT-Planungsrat als abgestimmten Bericht zur Beschlussfassung vorlegen soll. Ziel ist ein Positionspapier zur Cloud-Strategie der Bundes- und Landesverwaltungen.

In der Arbeitsgruppe vertritt der Landesbeauftragte für den Datenschutz Rheinland-Pfalz die Interessen der Datenschutzbeauftragten der Länder. Er wird sich unter anderem dafür einsetzen, dass sich im Positionspapier auch die datenschutzrechtlichen Anforderungen wiederfinden, die die Datenschutzkonferenz in der Orientierungshilfe Cloud-Computing (https://www.datenschutz-mv.de/datenschutz/publikationen/informat/cloud/oh_cloud.pdf) formuliert hat.

3.3 Informationssicherheit in den Kommunen

Im Jahr 2014 hat sich der IT-Planungsrat erneut mit der Frage befasst, wie die Informationssicherheit in den kommunalen Verwaltungen und Einrichtungen verbessert werden kann. Damit wurde die Diskussion um die 2013 beschlossene Informationssicherheitsleitlinie fortgesetzt. Diese definiert die Ziele der Bundes- und Landesverwaltungen in Bezug auf die Informationssicherheit und berücksichtigt dabei auch die Gewährleistungsziele des Datenschutzes. Die Leitlinie ist für die Kommunalverwaltungen nicht verbindlich, siehe 11. Tätigkeitsbericht, Punkt 4.3.

Auch auf seiner 14. Sitzung im Juli 2014 folgte der IT-Planungsrat dem Vorschlag der kommunalen Spitzenverbände nicht, die Informationssicherheitsleitlinie auch für Kommunen verpflichtend einzuführen.

Dennoch zeigt der IT-Planungsrat den Kommunen Wege zu einer verbesserten Informationssicherheit auf, indem er in seiner 16. Sitzung im März 2015 den Kommunalverwaltungen die „Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen“ für den Aufbau und Betrieb kommunaler Informationssicherheits-Management-Systeme (ISMS) empfiehlt. Darüber hinaus stellt er fest, dass der in der Handreichung erwähnte Leitfaden „Informations-Sicherheits-Management-System in 12 Schritten“ kleinen und mittelgroßen Kommunen ein pragmatisches und skalierbares Vorgehensmodell zur Einführung eines Informations-Sicherheits-Management-Systems darstellt, das die entsprechenden Mindestanforderungen des IT-Planungsrates abdeckt. Diesen Beschluss unterstützen wir.

Die übersichtliche und gut strukturierte Handreichung haben mehrere Verbände und Vereine aus dem kommunalen Bereich gemeinsam herausgegeben. Sie vergleicht die bekannten und etablierten Methoden BSI-Grundschutz, ISO27001 und den Leitfaden „Informations-Sicherheits-Management-System in 12 Schritten“. Kommunalen Verwaltungen, die mit dem Aufbau eines Rahmenwerks der Informationssicherheit beginnen, wird im Ergebnis empfohlen, mit ISO27001 bzw. dem Leitfaden zu beginnen und Grundschutz als Erweiterungsoption zu sehen. Dies erscheint uns gerade für kleinere und mittelgroße Verwaltungen durchaus nachvollziehbar. Anschließend erläutert die Handreichung, wie ein ISMS eingeführt wird und welche Struktureinheiten zu beteiligen sind und welche Rollen sie dabei einnehmen und wie ein Sicherheitsprozess in Gang gesetzt wird.

Dem Leitfaden „Informations-Sicherheits-Management-System in 12 Schritten“ des Bayerischen IT-Sicherheitscluster e. V. gelingt es, einen Mittelweg zwischen dem umfangreichen BSI-Grundschutz und der abstrakten ISO27001 zu finden. Zur Etablierung eines ISMS werden zwölf Schritte empfohlen, die nacheinander abzuarbeiten sind. Der Maßnahmenkatalog hat etwa ein Zehntel des Umfangs der BSI-Grundschutzkataloge. Der Leitfaden wendet sich ebenfalls an kleine und mittelgroße Verwaltungen (und auch Unternehmen dieser Größe), die zunächst die grundlegenden Gefährdungen für die Informationssicherheit beherrschen wollen. Damit werden die Grundlagen zur späteren vollständigen Anwendung des BSI-Grundschutzes gelegt.

Wir halten an unserer Empfehlung an die Kommunen aus dem Elften Tätigkeitsbericht fest, die Vorgaben der „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ umzusetzen, und erwarten, dass sie für Verfahren zur automatisierten Verarbeitung personenbezogener Daten die Grundschutzmethodik des BSI in vollem Umfang anwenden. Die „Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen“ und der Leitfaden „Informations-Sicherheits-Management-System in 12 Schritten“ sind geeignete Hilfsmittel auf dem Weg dazu.

3.4 Die Nationale E-Government-Strategie

Der IT-Planungsrat hat bereits in seiner 3. Sitzung im September 2010 die Nationale E-Government-Strategie (NEGS) für den Zeitraum 2010 bis 2015 beschlossen. Die NEGS strebt die gemeinsame strategische Ausrichtung von Bund, Ländern und Kommunen in der Weiterentwicklung von E-Government an und möchte das Handeln der Beteiligten koordinieren, um Interoperabilität und Wirtschaftlichkeit zu sichern. Hierfür formuliert sie ein Leitbild und gemeinsame Ziele für die Weiterentwicklung des E-Government, an denen sich Bund, Länder und Kommunen in ihrem jeweiligen Handlungs- und Zuständigkeitsbereich ausrichten können und sollen. In der NEGS wird davon ausgegangen, dass Datenschutz, Datensicherheit und Transparenz wichtige Voraussetzungen sind, damit die Bürgerinnen und Bürger dem E-Government vertrauen, es akzeptieren und auch intensiv nutzen.

Mit Auslaufen des Geltungszeitraums Ende 2015 war es erforderlich, die NEGS zu überarbeiten und den aktuellen rechtlichen und technischen Gegebenheiten anzupassen. Der IT-Planungsrat beauftragte daher seine Kooperationsgruppe Strategie mit der Überarbeitung der NEGS. Um datenschutzrechtliche Aspekte in angemessener Form einfließen zu lassen, haben wir uns an der Arbeitsgruppe beteiligt und zahlreiche Vorschläge zur datenschutzgerechten Ausgestaltung der NEGS unterbreitet. Bei der Überarbeitung konnten wir uns erfolgreich dafür einsetzen, dass die aktuellen Erkenntnisse aus der Tätigkeit der Datenschutzbehörden in das Dokument einfließen.

In der NEGS wird nun beispielsweise die Förderung der Medienkompetenz für Bürgerinnen und Bürger als Handlungsfeld ausdrücklich festgeschrieben (Ziel 1). Ein weiteres Handlungsfeld betrifft den sicheren elektronischen Austausch von Daten und die sichere Identifizierung der Anbieter und der Nutzer unter Beachtung des Datenschutzes (Ziel 4).

Von besonderer datenschutzrechtlicher Bedeutung ist der sogenannte Zielbereich C der NEGS, der Fragen der Informationssicherheit und des Datenschutzes anspricht. Dort wird in Anlehnung an die Leitlinie Informationssicherheit des IT-Planungsrats, siehe Punkt 3.3, die Etablierung eines ebenenübergreifenden Informationssicherheitsmanagements gefordert (Ziel 9). Darüber hinaus wurde festgeschrieben, dass sich technische und organisatorische Maßnahmen zur Gewährleistung des Datenschutzes künftig auf die Schutzziele Verfügbarkeit, Vertraulichkeit, Integrität, Transparenz, Nichtverkettbarkeit (als technische Sicherung der Zweckbindung) und Intervenierbarkeit (als technische Gestaltung von Verfahren zur Ausübung von Betroffenenrechten) beziehen sollen (Ziel 10).

Sie decken sich somit sowohl mit den Forderungen der Datenschutzkonferenz für ein modernes Datenschutzrecht für das 21. Jahrhundert (https://www.datenschutz-mv.de/datenschutz/themen/beschlue/Eckpunkte.pdf) als auch mit dem neuen Konzept der Datenschutzaufsichtsbehörden zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, siehe Standard-Datenschutzmodell unter Punkt 4.1.1.

Mit der Forderung, nur diejenigen personenbezogenen Daten zu erheben und zu verarbeiten, die für die Erfüllung der jeweiligen Verwaltungsaufgabe benötigt werden und zudem die anonyme oder pseudonyme Inanspruchnahme von Verwaltungsdienstleistungen ermöglichen, wird auch das Gewährleistungsziel der Datensparsamkeit in der NEGS verankert.

Der IT-Planungsrat hat in seiner 18. Sitzung die überarbeitete NEGS für den Zeitraum 2016 bis 2020 beschlossen (http://www.it-planungsrat.de/SharedDocs/Downloads/DE/NEGS/NEGS_ Fortschreibung.pdf?_blob=publicationFile&v=4) und die Kooperationsgruppe Strategie unter anderem damit beauftragt, die Umsetzung der Nationalen E-Government-Strategie durch Erarbeitung und Vorlage des jährlichen Aktionsplanes vorzubereiten. Wir begrüßen die datenschutzfreundliche Ausgestaltung der NEGS ausdrücklich und werden uns auch an den Arbeiten am Aktionsplan beteiligen.

3.5 Die Umsetzung der eID-Strategie - Schwerpunkt Bürgerkonten

Bereits im Herbst 2013 hatte der IT-Planungsrat die „Strategie für eID und andere Vertrauensdienste im E-Government (eID-Strategie)“ verabschiedet (http://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/12._Sitzung/eID-Strategie.pdf?__blob=publication-File). Im Rahmen der Umsetzung der Strategie hat der IT-Planungsrat erklärt, dass nach seiner Auffassung ein flächendeckender Einsatz von Bürgerkonten und deren Vernetzung untereinander erhebliche Mehrwerte und Nutzen für Bürgerinnen und Bürger bedeutet und jedem die Möglichkeit bietet, sich über sein persönliches, einmal eingerichtetes Bürgerkonto einfach bei allen Verwaltungsdienstleistungen auf kommunaler, Länder- und Bundesebene zu identifizieren. Der IT-Planungsrat hat sich in seiner 17. Sitzung im Juni 2015 für eine flächendeckende Verbreitung von Bürgerkonten ausgesprochen und empfohlen, für Bürgerinnen und Bürger ein einheitliches Benutzerkonto für die deutsche Verwaltung zu schaffen, bei dem die Identifizierung mit der eID-Funktion des Personalausweises möglich ist.

In unserem 11. Tätigkeitsbericht haben wir unter Punkt 6.4.5 ausführlich erläutert, welche datenschutzrechtlichen Auswirkungen es haben kann, wenn Bürgerinnen und Bürger mit einer einmaligen Anmeldung an einem Bürgerportal mit Hilfe der eID-Funktion des Personalausweises viele verschiedene E-Government-Anwendungen zur Nutzung freischalten und benutzen. So ist zu befürchten, dass das durchdachte Konzept der Berechtigungszertifikate zum Auslesen von Daten aus dem Personalausweis *(siehe Kasten)* unterlaufen wird und somit nicht sicher ausgeschlossen werden kann, dass die verschiedenen Aktivitäten der Ausweisinhaber zu einem aussagekräftigen Nutzungsprofil verknüpft werden. Zudem werden Betroffene kaum noch nachvollziehen können, wer die im Portal hinterlegten personenbezogenen Daten für welche Zwecke nutzt. Und es ist fast vorherzusehen, dass auch die Verwaltungsdienstleistungen, die eigentlich anonym genutzt werden könnten, künftig nur noch personalisiert in Anspruch genommen werden können.

Die von uns im 11. Tätigkeitsbericht formulierten Anforderungen bezogen sich bisher auf Bürgerportale unseres Bundeslandes. Angesichts der Bestrebungen, verteilte Bürgerportale der Bundesländer durch entsprechende Schnittstellen miteinander kompatibel zu machen, gelten unsere Empfehlungen umso mehr für alle Bürgerportale, die der IT-Planungsrat empfiehlt. Besondere Risiken für die Transparenz und die Zweckbindung sind insbesondere dann zu erwarten, wenn das zurzeit nur als Gedankenspiel existierende bundesweite Bürgerportal Realität werden würde.

Werden zentral an einer Stelle Daten von Bürgerinnen und Bürgern permanent vorgehalten, entstünde ein bundesweiter Datenbestand, der weit über den Umfang eines bundesweiten Melderegisters hinausgehen würde. Welche Risiken ein solcher Datenbestand im Zeitalter von Big Data und umfassenden Verknüpfungsmöglichkeiten hat, muss sicher nicht weiter erläutert werden.
Immerhin weist der IT-Planungsrat darauf hin, dass die rechtlichen Rahmenbedingungen das Recht auf informationelle Selbstbestimmung und sämtliche sonstige datenschutzrelevanten Belange zu berücksichtigen haben. Aber auch die technische und organisatorische Ausgestaltung von Bürgerkonten muss datenschutzrechtlichen Grundprinzipien genügen, beispielsweise den Prinzipien der Datensparsamkeit, der Transparenz und der Nichtverkettbarkeit.

Wir fordern daher die Landeregierung auf, sich für die folgenden Gestaltungsprinzipien bei Bürgerkonten einzusetzen:

- **Es muss auch künftig möglich sein, Verwaltungsdienstleistungen anonym und somit ohne Anmeldung an einem Bürgerkonto zu nutzen, sofern identifizierende Daten nicht erforderlich sind.**

- **Bürgerinnen und Bürger müssen die Wahlmöglichkeit haben, etwa bei einmaliger Inanspruchnahme einer Verwaltungsdienstleistung ihre identifizierenden Daten nur temporär im Bürgerkonto zu hinterlegen.**

- **Entscheiden sich Nutzerinnen und Nutzer, Daten dauerhaft in einem permanenten Bürgerkonto zu speichern, muss jederzeit nachvollziehbar sein, wer zu welchem Zweck auf diese Daten zugreift.**

- **Auf Wunsch der Nutzerinnen und Nutzer muss es jederzeit möglich sein, das Bürgerkonto und alle dort gespeicherten Daten zu löschen.**

- **Insbesondere durch technische Maßnahmen muss die oben beschriebene Möglichkeit der Verknüpfung einzelner Nutzeraktivitäten zu einem umfassenden Nutzungsprofil ausgeschlossen werden.**

Was ist ein Berechtigungszertifikat?
Ein Berechtigungszertifikat ist eine elektronische Bescheinigung, die es einem Diensteanbieter ermöglicht, seine Identität dem Personalausweisinhaber nachzuweisen und die Übermittlung personen- und ausweisbezogener Daten aus dem Personalausweis anzufragen. Diensteanbieter erhalten auf schriftlichen Antrag die Berechtigung, die für die Wahrnehmung ihrer Aufgaben oder Geschäftszwecke erforderlichen Daten im Wege des elektronischen Identitätsnachweises beim Inhaber des Personalausweises mittels eines Berechtigungszertifikats anzufragen. Für die Erteilung der Berechtigungszertifikate ist das Bundesverwaltungsamt zuständig.

4 Technik und Organisation

4.1 Neue Technologien

4.1.1 Das Standard-Datenschutzmodell

Das Bundesdatenschutzgesetz und die Datenschutzgesetze der verschiedenen Bundesländer basieren auf der Europäischen Datenschutzrichtlinie 95/46/EG vom Oktober 1996. Darüber hinaus gibt es zahlreiche bundesweit geltende Rechtsvorschriften, die auch den Datenschutz betreffen. Man könnte daher annehmen, dass alle Datenschutzaufsichtsbehörden von Bund und Ländern aus diesen rechtlichen Vorgaben für vergleichbare Verfahren zur Verarbeitung personenbezogener Daten auch vergleichbare technische und organisatorische Anforderungen ableiten. Das war in der Vergangenheit nicht immer der Fall. Nicht immer war transparent, warum welche Maßnahme von der einen Aufsichtsbehörde gefordert und von einer anderen möglicherweise nicht oder nur in abgeschwächter Form gefordert wurde. Es ist nachvollziehbar, dass dies mitunter zur Verunsicherung der verantwortlichen Stellen sowohl im öffentlichen als auch im nicht-öffentlichen Bereich geführt hat.

Zudem war im Rahmen von Datenschutzkontrollen in zunehmendem Maße zu beobachten, dass verantwortliche Stellen zwar recht umfassende IT-Sicherheitskonzepte etwa nach der BSI-Grundschutzmethodik erarbeitet hatten, aber erstaunt waren, wenn die Kontrolleure sich nach einem vergleichbaren Dokument zu Fragen des Datenschutzes erkundigten, auch wenn der Datenschutzbaustein der Grundschutzkataloge vollständig abgearbeitet worden war. Dass neben den Anforderungen an die Informationssicherheit vergleichbar hohe Anforderungen an den Datenschutz existieren und datenschutzspezifische Maßnahmen erfordern, die über die der Grundschutzkataloge weit hinausgehen, war verantwortlichen Stellen oft nicht bewusst.

Vor diesem Hintergrund hat die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz) den AK Technik, siehe Punkt 6, beauftragt, das Standard-Datenschutzmodell (SDM) zu entwickeln. Das SDM soll einerseits zu einer bundesweit abgestimmten, transparenten und nachvollziehbaren Beratungs- und Prüftätigkeit der Datenschutzbehörden führen. Andererseits bekommen auch die verantwortlichen Stellen ein Werkzeug an die Hand, das ihnen helfen soll, ihre personenbezogenen Verfahren nicht nur sicher, sondern auch datenschutzgerecht einzurichten und zu betreiben.

Auch bei der Anwendung des SDM bleibt es dabei, dass die Soll-Vorgaben einer Datenschutzprüfung sich aus dem Datenschutzrecht ergeben. Dabei haben die Datenschutzanforderungen einen sehr viel höheren Verpflichtungsgrad als Anforderungen der Informationssicherheit, wie sie beispielsweise vom IT-Grundschutz des BSI oder von ISO-Standards formuliert werden. Ohne eine Rechtsgrundlage dürfen Organisationen keine personenbezogenen Daten verarbeiten. Auch jede Datenschutzprüfung mit Hilfe des SDM beginnt daher mit der Prüfung der Rechtsgrundlagen. Existiert eine solche Rechtsgrundlage, können Soll-Vorgaben an eine datenschutzgerechte Datenverarbeitung mit technisch-organisatorischen Schutzmaßnahmen formuliert und mit den Ist-Feststellungen einer Bestandsaufnahme vor Ort verglichen und beurteilt werden. Genau an diesem Punkt hilft das SDM.

Das SDM verwendet zur Modellierung von Datenschutzanforderungen sieben Schutzziele, die im SDM als Gewährleistungsziele bezeichnet werden. Die wissenschaftliche Forschung der letzten Jahre, die maßgeblich von Professor Andreas Pfitzmann (TU Dresden) vorangetrieben wurde, kam zu dem Ergebnis, dass sich mit den sechs elementaren Schutzzielen Verfügbarkeit, Vertraulichkeit, Integrität, Intervenierbarkeit (als technische Gestaltung von Verfahren zur Ausübung der Betroffenenrechte), Transparenz und Nichtverkettbarkeit (als technische Sicherung der Zweckbindung) die datenschutzrechtlichen Anforderungen an ein Verfahren zur Verarbeitung personenbezogener Daten vollständig modellieren lassen. Die Diskussion des Modells im Kreis der Datenschutzaufsichtsbehörden führte noch zur Ergänzung der sechs Schutzziele um das allgemeine Schutzziel Datensparsamkeit. Mit Hilfe dieser sieben Gewährleistungsziele lassen sich aus den rechtlichen Anforderungen also die konkreten Maßnahmen zur Gewährleistung eines angemessenen Datenschutzes ableiten. Da sich das SDM methodisch an den IT-Grundschutz anlehnt, können auch Maßnahmen zur Gewährleistung der Informationssicherheit ausgewählt und auf ihre Datenschutzkonformität hin bewertet werden. Damit ergänzen sich IT-Grundschutz und SDM in idealer Weise.

Wichtigstes Werkzeug für den Anwender des SDM soll der Schutzmaßnahmen-Referenzkatalog mit einer Sammlung von datenschutzspezifischen Bausteinen und Einzelmaßnahmen werden. Sofern vorhanden referenzieren diese Maßnahmen auf den Maßnahmenkatalog des IT-Grundschutzes, auf einige technische Richtlinien des BSI und des DIN sowie auf die Orientierungshilfen und Handreichungen einzelner Datenschutzaufsichtsbehörden. Der Maßnahmenkatalog wird zurzeit von den Datenschutzbehörden erarbeitet.

Das SDM berücksichtigt die Anforderungen der Datenschutzgesetze von Bund und Ländern nach Angemessenheit von einzelnen Maßnahmen in Bezug auf den unterschiedlichen Schutzbedarf personenbezogener Daten. Der Katalog wird Maßnahmen für normalen und hohen Schutzbedarf ausweisen. Bei sehr hohem Schutzbedarf müssen - ähnlich wie in der Grundschutzmethodik des BSI - zusätzliche Maßnahmen erdacht und getroffenen werden. Das SDM orientiert sich somit auch hier systematisch an der Grundschutzmethodik. Dabei behält es aber im Blickfeld, dass Datenschutz natürlichen Personen und nicht der Sicherheit von Geschäftsprozessen dient. Die Schutzbedarfsdefinitionen des IT-Grundschutzes wurden daher für die Nutzung im SDM entsprechend angepasst.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz) hat das vom AK Technik erarbeitete SDM-Handbuch im Oktober 2015 zustimmend zur Kenntnis genommen und seine Mitglieder gebeten, in Prüfungs- und Beratungsvorgängen die im Modell beschriebene Vorgehensweise evaluierend anzuwenden. Die Aufsichtsbehörden haben das SDM-Handbuch und den Tagungsband zum entsprechenden Workshop des AK Technik, siehe Punkt 6.2, auf ihren Web-Seiten veröffentlicht (https://www.datenschutz-mv.de/datenschutz/sdm/SDM-Handbuch_V09a.pdf ; https://www.datenschutz-mv.de/datenschutz/sdm/Tagungsband.pdf), um Erfahrungen mit der Methode zu sammeln, eine Kommentierung durch die breite Fachöffentlichkeit zu vereinfachen und dadurch die Weiterentwicklung zu unterstützen.

Wir haben das SDM im Oktober 2015 erstmalig angewendet, um die technischen und organisatorischen Maßnahmen zu beschreiben, die zur datenschutzgerechten Ausgestaltung einer zentralen Schulverwaltungssoftware erforderlich sind - siehe Punkt 5.10.1.

Wir empfehlen der Landesregierung, bei der Planung, der Einrichtung und dem Betrieb von Verfahren zur Verarbeitung personenbezogener Daten die im Standard-Datenschutzmodell beschriebene Vorgehensweise evaluierend anzuwenden und uns über die Erfahrungen beim Umgang mit diesem Werkzeug zu berichten, um dadurch die Weiterentwicklung des Standard-Datenschutzmodells zu unterstützen.

4.1.2 Das Technologieprogramm Trusted Cloud

Das Bundesministerium für Wirtschaft und Energie (BMWi) hat Ende 2010 das Technologieprogramm Trusted Cloud gestartet, mit dem die Innovations- und Marktpotenziale von Cloud-Computing insbesondere für den Mittelstand erschlossen werden sollen. Eine Expertenjury hat aus den 116 Projektvorschlägen 14 Projekte ausgewählt und mit einem Fördervolumen von 50 Millionen Euro unterstützt. Zur wissenschaftlichen Begleitung der Projekte wurde im BMWi das Kompetenzzentrum Trusted Cloud gegründet. Teil des Kompetenzzentrums war die Arbeitsgruppe „Rechtlicher Rahmen für Cloud-Computing“, in der Experten aus der Wirtschaft, der Anwaltschaft, der Wissenschaft und der Datenschutzbehörden unter anderem ein Konzept zur Zertifizierung von Cloud-Strukturen erarbeitet haben. An der Erarbeitung dieses Konzeptes haben wir uns im Zeitraum zwischen November 2013 und April 2015 intensiv beteiligt.

Ausgangspunkt für die Erarbeitung eines Zertifizierungskonzeptes war das Thesenpapier „Datenschutzrechtliche Lösungen für Cloud-Computing“ (http://www.trusted-cloud.de/media/content/140228_Thesenpapier_Datenschutz_gesamt_RZ.pdf). Dort wird klargestellt, dass Cloud-Computing in der Regel eine Form der Datenverarbeitung im Auftrag ist und der Cloud-Nutzer als Auftraggeber für die Verarbeitung personenbezogener Daten in der Cloud die rechtliche Verantwortung trägt. Damit wird deutlich, dass die gesetzlichen Anforderungen der Auftragsdatenverarbeitung (§ 11 BDSG, § 4 DSG M-V) auch für Cloud-Strukturen gelten. Der Cloud-Nutzer muss also prüfen, ob der Cloud-Anbieter in der Lage ist, angemessene technische und organisatorische Maßnahmen zu treffen. Das Thesenpapier geht davon aus, dass diese Kontrollpflicht auch dadurch erfüllt werden kann, indem unabhängige Dritte den Cloud-Dienst auf der Basis eines vorgegebenen Kriterienkatalogs prüfen und das Ergebnis einer bestandenen Prüfung mit einem Testat dokumentieren.

Ein Schwerpunkt der Arbeiten war die Erstellung dieses Kriterienkatalogs, dem sogenannten Trusted-Cloud-Datenschutzprofil (TCDP - http://www.trusted-cloud.de/media/content/Publikation_TCDP.pdf). Das TCDP beschreibt die gesetzlichen Anforderungen an die Auftragsdatenverarbeitung und konkretisiert diese zu prüffähigen Normen. Es baut auf dem ISO/IEC-Standard 27018 auf *(siehe Kasten)*, der die international anerkannten ISO/IEC-Standards 27001 und 27002 um Cloud- und insbesondere datenschutzspezifische Anforderungen erweitert. Das TCDP bezieht diese Standards durch entsprechende Verweisungen ein, soweit sie geeignet sind, die gesetzlichen Anforderungen des BDSG zu konkretisieren. Maßstab und Leitbild des TCDP bleiben somit die gesetzlichen Anforderungen des BDSG an die Auftragsverarbeitung. Der Kriterienkatalog enthält zahlreiche Anforderungen und Umsetzungsempfehlungen zu vertraglichen Regelungen der Auftragsdatenverarbeitung, zum Verhältnis zwischen Cloud-Anbieter und Cloud-Nutzer und vor allem zu den technischen und organisatorischen Maßnahmen, die der Cloud-Anbieter zu gewährleisten hat. Das TCDP ist somit ein geeigneter Kriterienkatalog, um die Datenschutzkonformität von Cloud-Diensten prüfen zu können.

Was ist die ISO/IEC-27018?
Die ISO/IEC 27018 ist ein neuer internationaler Standard für den Datenschutz in der Cloud (http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498). Der im August 2014 verabschiedete Standard befasst sich ausschließlich mit der Regulierung der Verarbeitung von personenbezogenen Daten in der Cloud, indem er datenschutzrechtliche Anforderungen für Cloud-Dienste formuliert. Der Standard bietet damit einen nützlichen Rahmen für Datenschutzbestimmungen und richtet sich im Wesentlichen nach den Schutz- und Überwachungspflichten sowohl der geltenden europäischen Datenschutzgesetze als auch der künftig geltenden Europäischen Datenschutz-Grundverordnung, siehe Einleitung.

Für die Auswahl geeigneter Maßnahmen ist der Schutzbedarf der zu verarbeitenden Daten ein entscheidendes Kriterium. Der Cloud-Nutzer ist für die Festlegung des Schutzbedarfs seiner Daten verantwortlich. Da die Zertifizierung eines Cloud-Dienstes jedoch vor der ersten Nutzung des Dienstes abgeschlossen sein muss und dennoch für die Gesamtheit aller künftigen Nutzer des Dienstes gelten soll, kann sich die Zertifizierung nicht auf einen konkreten Datenverarbeitungsvorgang beziehen, sondern muss verallgemeinerbar sein. Um dieses Problem zu lösen, haben wir gemeinsam mit anderen Projektbeteiligten ein Schutzklassenkonzept entwickelt (http://www.trusted-cloud.de/media/content/150402_ Arbpapier_Nr_9_ Schutzklassen_Datenschutz_ gesamt_RZ_Ansicht_EZ.pdf). Mit diesem Konzept kann einerseits die Eignung eines Dienstes für ein bestimmtes Niveau von Sicherheitsanforderungen geprüft werden. Andererseits kann der Nutzer eines Dienstes seinen individuellen Schutzbedarf in Schutzklassen einordnen und somit einen Cloud-Dienst auswählen, dessen Datenschutz- und Sicherheitsniveau der von ihm benötigten Schutzklasse entspricht. Die Schutzklasse nimmt damit eine Doppelfunktion ein. Zum einen beschreibt sie den Schutzbedarf der zu verarbeitenden Daten und zum anderen beschreibt sie das Schutzniveau, das ein Cloud-Dienstleister gewähren kann. Stimmen Schutzbedarf der Daten des Nutzers und Schutzstufe des Angebots des Dienstleisters überein, darf der Cloud-Dienst verwendet werden. Das Schutzklassenkonzept ist insofern verallgemeinerbar, als dass es für fast alle Formen der Datenverarbeitung im Auftrag anwendbar ist.

Die Arbeitsgruppe „Rechtsrahmen für Cloud-Computing“ des Trusted-Cloud-Projektes hat ihre Tätigkeit mit dem Abschlusskongress am 13. April 2015 erfolgreich beendet. Neben dem Kriterienkatalog und dem Schutzstufenkonzept wurden weitere Unterlagen erarbeitet, die für die rechtskonforme Ausgestaltung von Cloud-Strukturen hilfreich sind, etwa zu den Themen Vertragsgestaltung, Lizensierungsbedarf, Schweigepflicht oder Haftungsrisiken. Das Projekt wird Anfang 2016 mit der Musterzertifizierung eines Cloud-Dienstes fortgesetzt, in der die Praxistauglichkeit des Zertifizierungsverfahrens nachgewiesen werden soll.

Wir empfehlen unserer Landesregierung schon jetzt, die im Trusted-Cloud-Projekt entwickelten Methoden und Unterlagen bei der Auswahl von Cloud-Diensten zu nutzen, um die Datenschutzkonformität von Cloud-Infrastrukturen bewerten zu können.

4.1.3 Digitale Selbstvermessung

Getreu dem Motto „Meine Dienstleistung für deine Daten“ werden in der heutigen Gesellschaft immer mehr Angebote zur Verfügung gestellt, die Rabatte oder günstige Tarife gegen Daten in Aussicht stellen. Jedoch handelt es sich hierbei nicht um einfache Daten, die, wie es in aller Regelmäßigkeit gerne suggeriert wird, bedenkenlos und ohne Risiken geteilt werden können, vielmehr sind es Daten mit zum Teil sehr sensiblem Inhalt.

So haben es ganz besonders die Krankenkassen darauf abgesehen, ihre Klienten zu digitalisieren. Weitere Interessenten, wie beispielsweise Kfz- oder Lebensversicherungen, sind aber ebenfalls schon in der Warteschleife oder auf der Beschleunigungsspur, wenn es darum geht, die Daten der Kundin bzw. des Kunden zu erfassen.

Alle Anbieter haben dabei ein Ziel gemeinsam: das Ökonomisieren von Lebensdaten. So sollen mit einem möglichst großen und lückenlosen Datenpool die Kundinnen und Kunden in diverse Risikogruppen unterteilt oder es soll ihnen ein „Health Score“ zugewiesen werden. Dies führt zwangsläufig zu einer schonungslosen Individualisierung und am Ende entscheiden Algorithmen und Risikoberechnungen, wer in ein gutes Raster passt und damit profitiert. Wird dieser Entwicklung nicht Einhalt geboten, werden künftig in einer entsolidarisierten Gesellschaft diejenigen mit teuren Tarifen bestraft, die schlechte Werte liefern oder die sich weigern, als gläserne Patienten Daten einer solchen Sammlung hinzuzufügen.

Bei den Krankenkassen lässt sich der angesprochene Datenpool besonders einfach mit modernen Messwerkzeugen, den sogenannten digitalen Selbstvermessern, füllen. So ist es für diese Geräte heutzutage ohne Weiteres möglich, den gesamten Tagesablauf zu vermessen. Die kleinen Chips, unter anderem getragen als Smartwatch oder Armband am Körper oder auch eingenäht in die Kleidung, sind auch unter dem Begriff „Wearables“ bekannt. Sie sind in der Lage, die unterschiedlichsten Daten zu erfassen, angefangen von zurückgelegten Schritten, Blutdruck, Körperfettanteil, Puls und Herzfrequenz bis hin zur Schlafdauer und -tiefe. Besonders populär sind die Wearables in Verbindung mit einer von über 100.000 Gesundheits- oder Fitness-Apps für das Smartphone, welche in erster Linie Aufschluss über den eigenen körperlichen Zustand liefern und dabei helfen sollen, von Algorithmen vorgegebene Ziele im Bereich von Sport und Gesundheit zu erreichen.

Es gibt inzwischen zahlreiche solcher Apps, kostenlos oder im Abo. Alle haben eines gemeinsam: die Verarbeitung von zum Teil sehr sensiblen Daten, welche als Gesundheitsdaten eingestuft werden müssen und daher besonders schützenswert sind. Alle gesammelten und miteinander kombinierten Daten lassen somit nicht nur erkennen, zu welcher Tageszeit man sich wo regelmäßig aufhält, sondern gewähren auch Rückschlüsse auf den eigenen Gesundheitsstatus und wie dieser sich im Laufe der Zeit verändert.

Ähnlich verhält es sich mit den „Pay as you drive“ (PAYD) -Angeboten der Kfz-Haftpflichtversicherungen. Die Anbieter solcher Tarife berechnen die Prämienhöhe auf Grundlage der Fahrzeugnutzung und des Fahrstils. Hierzu werden im Fahrzeug sehr umfangreiche und teils sekundengenaue Daten, wie beispielsweise Geschwindigkeit, Anfahr- oder Bremsverhalten, Auffahrdichte, Tageszeit und Fahrtendauer, erhoben und an den Versicherungsanbieter übermittelt.

Dass diese riesigen Datenmengen Begehrlichkeiten in privaten und öffentlichen Bereichen wecken, ist naheliegend. Es bedarf nicht sonderlich viel Phantasie, um sich vorzustellen, dass beispielsweise im Zusammenhang mit strafrechtlichen oder steuerrechtlichen Untersuchungen gerne auf diese Daten zurückgegriffen würde oder dass Arbeitgeber, siehe auch Punkt 5.5.3, oder Fahrzeugvermieter ihr Interesse an diesen Daten bekunden.

Wir können daher nur empfehlen, sich genau zu überlegen, ob kurzfristige Vorteile wirklich die leichtfertige Preisgabe sensibler, teils intimer Daten rechtfertigen. Denn am Ende zahlen diejenigen drauf, die nicht (mehr) in ein perfektes Muster passen.

4.1.4 Risiken der Fernwartung

Viele öffentliche und nicht-öffentliche Stellen in Mecklenburg-Vorpommern lassen ihre Informationssysteme von Dienstleistern fernwarten. Davon sind auch hoch schutzbedürftige Verfahren im kommunalen und im medizinischen Bereich betroffen. Im Berichtszeitraum haben wir erfahren, dass einige Stellen dazu die Software TeamViewer verwenden. Wir hatten deshalb zu prüfen, ob dies datenschutzrechtlich zulässig ist.

Nach den Veröffentlichungen des Herstellers dieser Lösung werden Fernwartungsverbindungen mit TeamViewer kryptographisch gesichert. Im Einzelnen werden folgende Sicherheitsmechanismen verwendet:

Die Verbindung zwischen dem Kundenrechner und dem Rechner des Dienstleisters werden mit einem hybriden Verfahren aus RSA-2048 und AES-256 gesichert. Zu Beginn der Verbindung werden dabei die öffentlichen Teile dieser Schlüssel über einen vom Hersteller betriebenen Masterserver ausgetauscht. Die Nachrichten für diesen Schlüsselaustausch werden vom Masterserver signiert. Der zur Prüfung dieser Nachrichten nötige öffentliche Schlüssel des Masterservers wird bei der Installation des Fernwartungsprogramms mit installiert. Der geheime Teil des Kundenschlüssels und des Dienstleisterschlüssels verlassen dabei nicht die Rechner von Kunden und Dienstleister.

Außerdem prüfen Kunde und Dienstleister zu Verbindungsbeginn mithilfe ihrer Software ein gemeinsames Passwort. In den uns vorliegenden Fällen wird dieses Passwort beim Kunden angezeigt und muss telefonisch dem Dienstleister mitgeteilt und dort eingegeben werden. Dieses Passwort wird mit einem Protokoll namens Secure Remote Password Protocol (SRP) geprüft. Ist zwischen den Rechnern von Kunden und Dienstleistern keine direkte Verbindung möglich, so läuft auch der nachfolgende Datenaustausch verschlüsselt über eine vom Hersteller bereitgestellte Infrastruktur. Ferner wird SRP auch bei der Anmeldung an Konten von Dienstleistern und Kunden in der Infrastruktur des Herstellers genutzt. Zur Anmeldung an solche Konten kann zusätzlich eine Zwei-Faktor-Authentisierung genutzt werden.

Darüber hinausgehende Informationen haben wir von den Anwendern nicht erhalten.

Beim Einsatz kryptographischer Verfahren kommt es nicht nur auf die richtigen Algorithmen und Parameter wie Schlüssellängen an, sondern auch auf deren korrekte Implementation oder technische Umsetzung einschließlich einer sinnvollen Kombination verschiedener Verfahren sowie auf die Schlüsselverwaltung. In jedem dieser Bereiche können Fehler dazu führen, dass die Gesamtlösung als unsicher zu betrachten ist.

Die kryptographischen Verfahren RSA-2048, AES-256 und SRP entsprechen jedes für sich genommen dem Stand der Technik. In den uns vorliegenden Unterlagen ist jedoch nicht beschrieben, wie sichergestellt wird, dass der vom Masterserver übermittelte öffentliche Schlüssel tatsächlich zum vermuteten Kunden oder Dienstleister gehört. Dienstleister und Kunde können dies nämlich nicht anhand weiterer Informationen, beispielsweise mit Zertifikaten von unabhängigen Stellen, prüfen. Sie sind in diesem Punkt vollständig auf den Hersteller von TeamViewer angewiesen. Bei Anwendungen mit hohem Schutzbedarf ist dies nicht hinnehmbar. Es entspricht nicht dem Stand der Technik. Kunde und Dienstleister müssten sich von der Echtheit der übermittelten öffentlichen Schlüssel überzeugen können, ohne auf den Hersteller angewiesen zu sein. In Betracht kommen hierzu beispielsweise der manuelle Vergleich von sogenannten Fingerprints (dies sind geeignete Prüfdaten der Schlüssel) oder die Nutzung einer eigenen oder selbst gewählten Public-Key-Infrastruktur.

Diese Sicherheitslücke könnte durch das Protokoll SRP geschlossen werden. Damit kann der Kunde prüfen, ob der Dienstleister im Besitz eines vorher vereinbarten Passwortes ist. Gleichzeitig entsteht bei beiden Teilnehmern weiteres Schlüsselmaterial, welches sie beispielsweise zur Verbindungsverschlüsselung nutzen könnten. Den uns vorliegenden Unterlagen ist jedoch nicht zu entnehmen, dass TeamViewer das mit SRP produzierte Schlüsselmaterial zur Absicherung der Fernwartungsverbindung nutzt. Außerdem genügt die telefonische Übermittlung von Passwörtern nicht dem hohen Schutzbedarf der geprüften Anwendungen. Unter diesen Bedingungen kann auch SRP das beschriebene Problem nicht lösen.

Die oben genannte Zwei-Faktor-Authentisierung hat keinen Einfluss auf die Sicherheit der Fernwartungsverbindung selbst und wurde deshalb nicht weiter betrachtet.

Rechtlich ist eine datenverarbeitende Stelle, die Wartungsleistungen für ihre Informationstechnik in Anspruch nimmt, Betroffenen gegenüber für die datenschutzgerechte Ausführung dieser Leistungen verantwortlich. Es handelt sich hierbei um Datenverarbeitung im Auftrag (§ 4 DSG M-V, § 11 BDSG).

Die Stelle muss insbesondere sicherstellen, dass bei der Fernwartung keine Unbefugten auf personenbezogene Daten zugreifen können (§ 21 DSG M-V, § 9 BDSG). Dabei haftet die Stelle auch für Datenschutzverstöße der von ihnen beauftragten Stelle einschließlich eventueller Fehlentscheidungen bei der Auswahl von Fernwartungslösungen.

Die vom Hersteller der Fernwartungslösung TeamViewer bereitgestellten Sicherheitsmechanismen erfüllen nach derzeitigem Kenntnisstand nicht die bestehenden datenschutzrechtlichen Anforderungen für hoch schutzbedürftige Verfahren zur Verarbeitung personenbezogener Daten. Solche Verfahren dürfen mit diesem Produkt nur dann ferngewartet werden, wenn die dazu genutzten Verbindungen ausreichend gesichert sind, beispielsweise mit einem kryptographischen Virtual Private Network (VPN).

4.1.5 XTA - sicherer Datentransport in der öffentlichen Verwaltung

Im Berichtszeitraum waren wir gemeinsam mit anderen Datenschutzbehörden an der Entwicklung eines Standards zum sicheren Datentransport in der öffentlichen Verwaltung (XÖV-Transport-Adapter - XTA) beteiligt.
Bei der Kommunikation zwischen verschiedenen Behörden sind immer Anforderungen des Datenschutzes und der Informationssicherheit zu beachten. Deshalb werden vielfach spezielle, sichere Transportdienste, beispielsweise auf der Basis des Standards OSCI-Transport, siehe Elfter Tätigkeitsbericht, Punkt 4.5, eingesetzt. Diese Dienste sind häufig komplex und werden bei Dienstleistern meistens für eine größere Zahl von Behörden gemeinsam betrieben. Insbesondere die Hersteller überregional eingesetzter Fachverfahren müssen in der Lage sein, mehrere verschiedene Transportdienste zu unterstützen. Deshalb ist es sinnvoll, einen geeigneten Zubringerdienst zwischen den Fachverfahren der öffentlichen Verwaltung und diesen sicheren Transportdiensten einzusetzen. Dieser kann für durchgehende Sicherheit vom Fachverfahren bis zum Endpunkt der Kommunikation sorgen und gleichzeitig die Fachverfahrenshersteller davon entlasten, Schnittstellen zu mehreren verschiedenen Transportdiensten entwickeln zu müssen. Als Standard für einen solchen kryptographisch gesicherten Zubringerdienst hat der IT-Planungsrat, siehe auch Punkt 3, XTA entwickeln lassen. Im Berichtszeitraum wurde Version 2.1 fertiggestellt.

XTA 2.1 ist ein sehr gut ausgereifter Standard, mit dem sich die Anforderungen des Datenschutzes an die sichere Kommunikation zwischen Behörden sehr gut beschreiben und umsetzen lassen. Die Datenschutzaspekte dieses Standards orientieren sich an den Gewährleistungszielen des Standard-Datenschutzmodells, siehe Punkt 4.1.1. Damit wird sichergestellt, dass die technischen Anforderungen, die sich aus dem geltenden Datenschutzrecht ergeben, vollständig umgesetzt werden. Typische Bündel solcher Anforderungen können in XTA 2.1 zu sogenannten Schutzprofilen zusammengefasst werden. Der IT-Planungsrat kann diese Schutzprofile standardisieren und zentral aktualisieren. Darauf können sich dann Fachstandards beziehen. Sie werden dadurch übersichtlicher und lassen sich besser pflegen.

Wir empfehlen den Behörden in unserem Land, den Standard XTA 2.1 in Verbindung mit OSCI-Transport zur sicheren Kommunikation zwischen Behörden einzusetzen.

4.1.6 Neue Norm zur Datenträgervernichtung

Im Oktober 2012 wurde die neue DIN 66399 „Büro- und Datentechnik - Vernichten von Datenträgern“ veröffentlicht. Der zuständige DIN-Ausschuss hat damit einen Standard erarbeitet, der den heutigen Stand der Technik in der Datenträgervernichtung abbildet und die mittlerweile veraltete Norm DIN 32757 ablöst, siehe Achter Tätigkeitsbericht, Punkt 2.8.10.

Um die Anwendung dieser Norm zu erleichtern, haben wir im Berichtszeitraum eine Orientierungshilfe unter dem Titel „Ermittlung des Schutzbedarfs personenbezogener Daten für den Prozess der Datenträgervernichtung“ veröffentlicht.

Durch das Vernichten von Datenträgern, auf denen personenbezogene Daten gespeichert sind, können datenverarbeitende Stellen ihrer Verpflichtung zum Löschen dieser Daten nachkommen. Personenbezogene Daten sind insbesondere dann zu löschen, wenn ihre Speicherung unzulässig oder ihre Kenntnis für die Aufgabenerfüllung bzw. zur Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist, siehe beispielsweise § 13 Abs. 2 DSG M-V. Unter dem Begriff „Löschen“ wird dabei das dauerhafte Unkenntlichmachen gespeicherter personenbezogener Daten verstanden, § 3 Abs. 4 Nr. 6 DSG M-V. Der Prozess muss dauerhaft und irreversibel dazu führen, dass die betreffenden Informationen nicht mehr aus den gespeicherten Daten gewonnen werden können. Das Vernichten von Datenträgern ist gleichzeitig eine technisch-organisatorische Maßnahme zur Gewährleistung der Datensicherheit, insbesondere zur Verhinderung der Kenntnisnahme personenbezogener Daten durch Unbefugte, § 21 Abs. 2 Nr. 1 DSG M-V. Die Maßnahme muss dem Stand der Technik entsprechen und angemessen sein, § 21 DSG M-V.

Die DIN 66399 benennt Grundlagen und Begriffe (Teil 1) sowie Anforderungen an Maschinen zur Vernichtung von Datenträgern (Teil 2) und beschreibt einen sicheren Prozess der Datenträgervernichtung (Teil 3). Der Standard empfiehlt jeder datenverarbeitenden Stelle, alle im Geschäftsverkehr vorkommenden oder anfallenden Informationen (Daten) bzw. die sie speichernden Datenträger zunächst hinsichtlich des Schutzbedarfs zu klassifizieren und definiert hierfür drei Schutzklassen. Darüber hinaus beschreiben sieben Sicherheitsstufen Anforderungen an die Wirksamkeit der Vernichtung. Die Norm bestimmt dazu insbesondere Grenzwerte für Teilchengrößen, die bei der Vernichtung eines Datenträgers eingehalten werden müssen. Die Grenzwerte werden für diverse Materialklassen (wie Papier, Mikrofilm, magnetische Festplatten, optische Datenträger, Halbleiterspeicher) separat festgelegt. Anschließend empfiehlt die DIN, Datenträger bestimmter Schutzklassen nur nach bestimmten Sicherheitsstufen zu vernichten.

Die Orientierungshilfe gibt konkrete Anregungen für die Praxis, welche Überlegungen bei der Vernichtung von Datenträgern mit Daten unterschiedlicher Sensitivität anzustellen sind. Im Mittelpunkt stehen hierbei Ausführungen zur Ermittlung des Schutzbedarfs von Daten und Datenträgern, zur Zuordnung von Schutzklassen und zu den Eigenschaften der Sicherheitsstufen gemäß DIN 66399 sowie zur Auswahl geeigneter und angemessener Sicherheitsstufen für die datenschutzgerechte Vernichtung von Datenträgern mit personenbezogenen Daten. Weiterhin werden für eine Reihe konkreter Arten von Daten bzw. Unterlagen die vorgeschriebenen Aufbewahrungsfristen sowie Empfehlungen zur Einstufung in Schutzklassen gegeben.

Wir empfehlen den Anwendern aus Wirtschaft und Verwaltung in unserem Land, diese Orientierungshilfe zu beachten.

4.1.7 Digitale Fernmesswasser- und Fernmesswärmezähler

Bereits im Zehnten Tätigkeitsbericht haben wir unter Punkt 5.1.2 über eine Petition berichtet, in der Bedenken gegen den Austausch des alten analogen Wasserzählers gegen ein neues digitales Modell mit wesentlich größerem Funktionsumfang geäußert wurde. Im Rahmen unserer Untersuchung bei der zuständigen Wohnungsgesellschaft stellte sich heraus, dass die Sorgen durchaus berechtigt waren. Es fehlte an technischen und organisatorischen Maßnahmen zum Schutz der verarbeiteten Verbrauchsdaten. Dies betraf nicht nur die neuen Funkwasser-, sondern auch die neue Generation der Funkwärmezähler.

So lieferten die Funkzähler in kurzen Zeitabständen ihre Tageswerte an einen sogenannten Masterdatensammler, der die gesammelten Daten der angeschlossenen Funkzähler dann an das Rechenzentrum des Dienstleisters weitervermittelte. Es war somit ohne Weiteres möglich, ein Profil über das Verhalten der Kundinnen und Kunden zu erstellen.

Im Ergebnis unserer Untersuchung forderten wir eine Umgestaltung des eingesetzten Verfahrens, sodass nur noch einmal im Monat ein konsolidierter und verschlüsselter Verbrauchswert als Monatsendwert an das Rechenzentrum des Dienstleisters übertragen wird. Eine Profilbildung wäre unter diesen Umständen dann nicht mehr möglich.

Im Laufe des Jahres 2014 haben wir die notwendige Umgestaltung des Verfahrens begleitet. Dabei stellte sich heraus, dass die Umsetzung der datenschutzrechtlichen Anforderungen nur unter erheblichem zeitlichen und finanziellen Aufwand realisiert werden konnte. So konnte die Umstellung alle Masterdatensammler erst zum Ende des Jahres 2014 abgeschlossen werden. Dieses Beispiel verdeutlicht erneut, dass die frühzeitige Berücksichtigung datenschutzrechtlicher Forderungen, also die Berücksichtigung des Gestaltungsprinzips „Privacy by Design“, viel Zeit und Geld sparen kann.

4.1.8 QR-Code im Sichtfenster von Briefumschlägen

Ein Kreuzfahrtunternehmen übersandte an Kundinnen und Kunden Buchungsbestätigungen postalisch. Hierbei war neben den gängigen Adressdaten zusätzlich ein QR-Code im Sichtfenster des Briefes abgedruckt. Problematisch war, dass der QR-Code auch die Buchungsnummer für die Reise enthielt.

Die Kundinnen und Kunden benötigen die Datensätze Vorname, Name und Buchungsnummer, um sich online auf der Internetplattform des Kreuzfahrtunternehmens anzumelden, um dort weitere benötigte Daten, beispielsweise im Schiffsmanifest, einzutragen. Das Schiffsmanifest enthält auch Daten zu Behinderungen oder auch Personalausweisdaten. Diese Daten werden benötigt, um entsprechenden besonderen Belangen der Behinderten auf der Kreuzfahrt gerecht zu werden, die Personalausweisdaten werden unter anderem für die Passagierlisten und die Anmeldung in fremden Häfen benötigt.

Diese Daten werden nach der Kreuzfahrt im System gesperrt. Bucht eine Kundin oder ein Kunde erneut, wird der Datensatz reaktiviert und die Daten im Schiffsmanifest sind bei neuer Anmeldung (neue Buchungsnummer, Name und Vorname) bereits im System hinterlegt. Dies soll der Vereinfachung dienen, soll Fehler bei der Eintragung im Schiffsmanifest verhindern und wird durch das Unternehmen als Kundenservice gesehen.

Datenschutzrechtlich bedenklich war allerdings, dass unberechtigte Dritte ohne größeren Aufwand zu den benannten Datensätzen, wie denen im Schiffsmanifest, Zugang hätten nehmen können, da alle benötigten Daten für die Online-Anmeldung im Sichtfenster des Briefes vorhanden waren. Ohne größere Probleme hätten unbefugte Dritte sich alle Daten beschafft, die beispielsweise nötig sind, um einen Identitätsdiebstahl vorzunehmen.

Dies war dem Kreuzfahrtunternehmen nicht aufgefallen und wohl auch nicht bewusst. Der betriebliche Datenschutzbeauftragte des Unternehmens hat allerdings sofort nach unserem Hinweis entsprechend reagiert und veranlasst, dass der QR-Code nicht mehr im Sichtfenster der Briefe gedruckt wird. Der QR-Code befindet sich jetzt innerhalb des verschlossenen Briefes, der auch die Buchungsbestätigung mit der Buchungsnummer enthält.

Als weitere - aus unserer Sicht erforderliche - Maßnahme integriert das Kreuzfahrtunternehmen ein Passwort für die Online-Anmeldung, welches die Kundinnen und Kunden selbst wählen und ändern können. Damit ist es unbefugten Dritten grundsätzlich nicht mehr möglich, wie oben beschrieben Zugriff auf das Schiffsmanifest zu nehmen. Die Installation des Passwortschutzes soll nach Mitteilung des Unternehmens bis Ende 2015 abgeschlossen sein.

4.1.9 Gewährleistung der Menschenrechte bei der elektronischen Kommunikation

Die Enthüllungen des Whistleblowers Edward Snowden haben ein Ausmaß an geheimdienstlicher Überwachung aufgezeigt, das viele zuvor nicht für möglich gehalten hatten. In der Folge haben nicht nur die Datenschutzbeauftragten des Bundes und der Länder gefordert, auf diese neue Qualität der Überwachung rechtlich und politisch zu reagieren, siehe 11. Tätigkeitsbericht, Einleitung und Punkt 6.3.3.

Schnell wurde aber auch deutlich, dass rechtliche und politische Reaktionen allein nicht ausreichen würden, um der tendenziell unbegrenzten und kaum kontrollierbaren Überwachung der elektronischen Kommunikation durch Geheimdienste etwas entgegenzusetzen. Es bestand Einigkeit, dass auch technische und organisatorische Schutzmaßnahmen erforderlich sind, um den Schutz der informationellen Selbstbestimmung der in Deutschland lebenden Menschen sowie die Vertraulichkeit und Integrität informationstechnischer Systeme wieder herzustellen und dauerhaft zu sichern.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat auf Anregung und nach entsprechender Vorarbeit des AK Technik, siehe auch Punkt 6, im März 2014 eine Entschließung verabschiedet (https://www.datenschutz-mv.de/datenschutz/themen/beschlue/87_DSK/Ent_ElKom.pdf). Die Konferenz forderte die Prüfung und Umsetzung folgender Maßnahmen:

- sichere Verschlüsselung beim Transport und bei der Speicherung von Daten,
- Bereitstellung einer einfach bedienbaren Verschlüsselungs-Infrastruktur,
- Einsatz von Ende-zu-Ende-Verschlüsselung in Kombination mit Verfahren zur Verbindungsverschlüsselung,
- sichere und vertrauenswürdige Bereitstellung von Internetangeboten,
- Weiterentwicklung innovativer Vorkehrungen zum Schutz von Verkehrsdaten,
- Ausbau der Angebote und Förderung anonymer Kommunikation,
- Angebot für eine Kommunikation über kontrollierte Routen,
- sichere Verschlüsselung der Mobilkommunikation und Einschränkung der Möglichkeiten der Geolokalisierung,
- Beschränkung des Cloud-Computing mit personenbezogenen Daten auf vertrauenswürdige Anbieter mit zertifizierter Informationssicherheit,
- Förderung der Vertrauenswürdigkeit informationstechnischer Systeme durch Zertifizierung,
- Sensibilisierung von Nutzerinnen und Nutzern moderner Technik und
- ausreichende Finanzierung von Maßnahmen der Informationssicherheit.

Der AK Technik hat einen Anforderungskatalog formuliert, der die hier genannten Maßnahmen konkretisiert (https://www.datenschutz-mv.de/datenschutz/themen/beschlue/87_DSK/Ent_ElKom_Anl.pdf).

Wir empfehlen der Landesverwaltung, auf die Durchsetzung der oben genannten Maßnahmen zu dringen. Dem Landtag empfehlen wir, die zu ihrer Durchsetzung gegebenenfalls nötigen Änderungen und Präzisierungen an dem bestehenden Rechtsrahmen vorzunehmen.

4.1.10 Verschlüsselung ohne Einschränkungen

Als Reaktion auf die Terroranschläge im Januar 2015 in Paris wurde erneut weltweit die Reglementierung von Verschlüsselungsverfahren diskutiert. Am 16. Januar 2015 forderte Großbritanniens Premier Cameron entsprechende Befugnisse für die Geheimdienste. Ähnliche Forderungen stellten US-Präsident Obama und der Anti-Terror-Koordinator im Rat der Europäischen Kommission. Auch Bundesinnenminister de Maizière forderte, dass deutsche Sicherheitsbehörden in die Lage versetzt werden müssen, verschlüsselte Kommunikation zu entschlüsseln oder zu umgehen.

Diese Diskussion wurde in Deutschland schon einmal Ende der 90er Jahre unter dem Stichwort „Kryptokontroverse“ geführt. Sie wurde jedoch am 2. Juni 1999 beendet, nachdem das Bundeskabinett die Eckpunkte der deutschen Kryptopolitik verabschiedet hatte. Die 58. Datenschutzkonferenz begrüßte die Eckpunkte mit einer entsprechenden Entschließung, siehe Vierter Tätigkeitsbericht, Punkt 3.16.2.

Diese neuerlichen Diskussionen waren Anlass für die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, in einer Entschließung auf die Bedeutung des Brief-, Post- und Fernmeldegeheimnisses hinzuweisen (https://www.datenschutz-mv.de/datenschutz/themen/beschlue/89_DSK/Ent_Verschluesselung.html).

Die Konferenz hat Forderungen abgelehnt, den Einsatz kryptographischer Verfahren durch staatliche Regulierungen zu unterbinden oder zumindest einzuschränken. Sie hat darauf hingewiesen, dass solche Regulierungen leicht umgangen werden könnten, kaum kontrollierbar wären, Grundrechte einschränken würden, den Schutz von Berufs- und Geschäftsgeheimnissen gefährden und Schwachstellen schaffen würden, die auch von Kriminellen ausgenutzt werden können. Im Ergebnis wäre dann der erhoffte Nutzen bei der Bekämpfung des internationalen Terrorismus äußerst fraglich.

Im November 2015 hat sich die Bundesregierung zur Stärkung der vertrauenswürdigen Kommunikation insbesondere durch Ende-zu-Ende-Verschlüsselung bekannt. In der Berliner Erklärung zum 9. IT-Gipfel (http://www.bmwi.de/BMWi/Redaktion/PDF/IT-Gipfel/it-gipfel-2015-berliner-erklaerung,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf) stellt die Bundesregierung klar, dass die Gewährleistung von IT-Sicherheit und der Schutz der Privatsphäre zentrale Erfolgsfaktoren für die Digitalisierung in Deutschland und in Europa und damit zwei tragende Säulen der digitalen Souveränität sind. In der Charta zur Stärkung der vertrauenswürdigen Kommunikation (https://www.telekom.com/static/-/293840/3/151118-charta-si), die anlässlich des 9. IT-Gipfels unter anderem vom Bundesinnenminister unterschrieben wurde, formulieren Bundesregierung und führende IT-Unternehmen Deutschlands gemeinsam Rahmenbedingungen, durch die vertrauenswürdige Kommunikation gestärkt werden soll und die Deutschland „zum Verschlüsselungsstandort Nr. 1 auf der Welt“ machen soll.

Wir unterstützen diese Vorhaben und empfehlen der Landesregierung insbesondere in Anlehnung an die Forderungen der Datenschutzkonferenz

- **eine einfach bedienbare Verschlüsselungs-Infrastruktur und insbesondere eine sichere Ende-zu-Ende-Verschlüsselung ohne Eingriffsmöglichkeiten Dritter bereitzustellen,**
- **die Entwicklung sicherer, transparenter und einfach bedienbarer kryptographischer Verfahren ohne Hintertüren auf allen, insbesondere auch mobilen, Plattformen zu fördern,**
- **die Wirtschaft bei der Wahrung der Vertraulichkeit und Integrität ihrer geschäftlichen Kommunikation zu unterstützen und**
- **kryptographische Technologien in E-Government-Verfahren standardmäßig zu implementieren.**

4.1.11 Cloud-Nutzung - oft ohne Wissen der Nutzenden

Im Zeitalter von Smartphone, Tablet und Co. spielt die Nutzung von sogenannten Clouds, siehe auch Punkt 4.1.2 und Punkt 3.2, eine immer größere Rolle. Die Motivation hierfür ist durchaus nachvollziehbar. Die heutzutage fast ununterbrochen verfügbare Internetanbindung erlaubt Nutzenden, nicht nur Unmengen von Daten, sondern auch aufwendige Rechenoperationen auf extern verfügbaren Speichersystemen kostengünstig oder gar kostenlos auszulagern. Die Geräte können so in ihrem Funktionsumfang deutlich erweitert werden und es gibt faktisch keine Speicherplatzprobleme mehr. Bedenklich ist jedoch die Tatsache, dass oft nicht nachvollziehbar ist, wo die Daten landen und wer auf diese zugreifen kann. Oft haben die Cloud-Anbieter ihren Sitz außerhalb der Europäischen Union oder des Europäischen Wirtschaftraumes, wo nicht von einem ausreichenden Datenschutzniveau ausgegangen werden kann.

Mittlerweile sind aber auch schon die Betriebssysteme mit derartigen Cloud-Funktionen ausgestattet. Datenschutzrechtlich bedenklich ist hierbei insbesondere die Tatsache, dass diese Funktionen oft standardmäßig aktiviert sind. Die Hersteller haben somit „per default“ Zugriff auf eine Vielzahl von personenbezogenen Daten. Da der von Herstellern empfohlene Standard-Installationsvorgang die Möglichkeit der Datenschutzeinstellungen regelmäßig überspringt, wissen die Nutzenden oft nichts von der späteren Auslagerung ihrer Daten in die Cloud. So ist es ihnen kaum möglich, die Datenübertragungen kritisch zu hinterfragen oder gar abzustellen. Nutzenden wird somit das Recht auf informationelle Selbstbestimmung genommen. Der Hersteller erhält stattdessen viele Informationen, die es ihm erlauben, das Verhalten der Nutzenden detailliert nachzuvollziehen und zu analysieren.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz) hat daher am 30. September 2015 in einer Entschließung auf die Datenschutzrisiken von Cloud-unterstützten Betriebssystemen hingewiesen (https://www.datenschutz-mv.de/datenschutz/themen/beschlue/90_DSK/Ent_CloudOS Risiken.html). Die Konferenz fordert die Hersteller solcher Betriebssysteme auf, die Software mit datenschutzfreundlichen Voreinstellungen, also mit „Privacy by Default“, auszuliefern. Darüber hinaus fordert sie, die Anwender detailliert und fortlaufend darüber zu informieren, welche Daten unter welchen Voraussetzungen zu welchen Zwecken übertragen werden. Nur so können sie einschätzen, ob sie die Software unter den gegebenen Umständen erwerben bzw. verwenden wollen. Zudem müssen Anwender die Möglichkeit haben, auf einfache Weise selbst festzulegen, welche Daten lokal gespeichert bleiben sollen und welche Daten in die Cloud bzw. an den Hersteller übermittelt werden.

4.1.12 Regelungen in der GGO I zum E-Mail-Verkehr

Wegen der besonderen Risiken beim Umgang mit vertraulichen Schriftstücken enthielt die Gemeinsame Geschäftsordnung I der Ministerien und der Staatskanzlei des Landes Mecklenburg-Vorpommern (GGO I) über viele Jahre hinweg eine Regelung zur Übermittlung dieser Schriftstücke per E-Mail. § 32 Abs. 3 der GGO I schrieb vor, dass Dokumente mit personenbezogenen oder anderen sensiblen Daten nicht per E-Mail versandt werden dürfen, solange die technischen Voraussetzungen wie digitale Unterschrift und Verschlüsselung nicht realisiert sind. Diese Vorschrift konkretisierte in anwenderfreundlicher Form die datenschutzrechtlichen Anforderungen, die in allgemeiner Form im Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) normiert sind, § 21 DSG M-V.

Im Laufe des Jahres 2014 wurde die GGO I überarbeitet und trat am 1. Januar 2015 in Kraft. Wir mussten zur Kenntnis nehmen, dass § 32 Abs. 3 der alten Fassung ersatzlos gestrichen war. Unsere Nachfrage beim Ministerium für Inneres und Sport Mecklenburg-Vorpommern ergab, dass diese Änderung eingehend im Ausschuss für Organisationsfragen beraten worden war und dass sich auch die Al.1-Konferenz mit dem Thema befasst hatte. Obwohl die Änderung den Umgang mit personenbezogenen Daten betraf, waren wir in die Beratungen nicht einbezogen worden mit der Begründung, bei der GGO I handele es sich um eine reine Verwaltungsvorschrift und keine Rechtsvorschrift im Sinne des § 4 Abs. 3 der GGO II, die die Einbeziehung des Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern erfordert hätte.

Das Ministerium begründete den Wegfall der besagten Regelung mit dem im Landtag anhängigen E-Government-Gesetz des Landes, siehe Punkt 5.4.1. Das Gesetz würde eine Verordnungsermächtigung enthalten, nach der das Ministerium für Inneres und Sport eine verbindliche IT-Richtlinie erlassen könne, in der als Landesstandard vergleichbare Forderungen zum sicheren Datenaustausch aufgenommen werden sollen. Wann diese Standards verabschiedet und somit verbindlich werden sollen, blieb offen.

Wir halten es für nicht sinnvoll, eine wichtige Regelung in der GGO I zum Umgang mit sensiblen personenbezogenen Daten zu streichen, bevor eine neue, vergleichbare Regelung in Kraft tritt. Denn es ist zu befürchten, dass ein relativ langer Zeitraum zu erwarten ist, in dem die Anforderungen des Landesdatenschutzgesetzes Mecklenburg-Vorpommern nicht anwenderfreundlich in Verwaltungsvorschriften umgesetzt sind. Der zunächst ersatzlose Wegfall der oben genannten Regelung hat schon jetzt zu Verunsicherungen bei Mitarbeiterinnen und Mitarbeitern der Verwaltung geführt. Mitunter wird angenommen, dass ohne diese Regelung in der GGO I die Übermittlung personenbezogener Daten per E-Mail nunmehr auch ohne zusätzliche Datensicherheitsmaßnahmen zulässig wäre.

Unabhängig von konkretisierenden Verwaltungsvorschriften bleibt jedoch festzuhalten, dass die Anforderungen des Landesdatenschutzgesetzes in Bezug auf angemessene Maßnahmen zum Schutz personenbezogener Daten insbesondere bei ihrer Übermittlung in unsicheren Netzen unverändert gelten und von uns auch eingefordert werden. So verlangt § 21 DSG M-V technische und organisatorische Maßnahmen, um beispielsweise die Vertraulichkeit personenbezogener Daten gewährleisten zu können.

Wir weisen deshalb nochmals ausdrücklich darauf hin, dass das Verbot der Übermittlung personenbezogener Daten per E-Mail ohne entsprechende Schutzvorkehrungen weiterhin auch nach Streichung des § 32 Abs. 3 GGO I gilt.

4.2 Kommunikation/neue Medien

4.2.1 Google - Recht auf Vergessenwerden im Internet?

Am 13. Mai 2014 urteilte der Europäische Gerichtshof (EuGH, Urteil vom 13.05.2014 - C-131/12), dass das Unternehmen Google zur Entfernung von bestimmten Links (URLs) aus den Google-Suchergebnissen verpflichtet ist. Demnach können sich Bürgerinnen und Bürger der Europäischen Union an Google wenden und das Löschen bestimmter Suchergebnisse verlangen. Dieser Anspruch bezieht sich jedoch nur auf die direkt angezeigten Links zur Namenssuche einer bestimmten Person in der Suchmaschine von Google. Ausgenommen von der Möglichkeit zur Löschung sind dabei Inhalte, bei denen das Interesse der Allgemeinheit an dem fraglichen Inhalt dem Löschinteresse der Betroffenen überwiegt.

Da es sich bei der Entscheidung, den Eintrag zu löschen, um einen zivilrechtlichen Anspruch handelt, obliegt es im ersten Schritt dem Unternehmen Google, dem Löschanspruch zu entsprechen. Erst bei der Ablehnung des Löschersuchens ist der Weg frei, sich an die für Google zuständige Datenschutzaufsichtsbehörde zu wenden. Zuständig für abgelehnte Löschanträge für das Unternehmen Google ist in Deutschland der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit.

Durch das Urteil, an dem sich im Übrigen alle Suchmaschinenbetreiber orientieren müssen, gibt es nun erstmals für den Einzelnen die Möglichkeit, bestimmte Sachverhalte zu seiner Person, zumindest in Europa, aus den Suchergebnislisten von Suchmaschinenbetreibern zu löschen.

Auf die richtungsweisende Bedeutung des Urteils des Europäischen Gerichtshofes wurde bereits in der Entschließung „Zum Recht auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen“ der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. und 9. Oktober 2014 in Hamburg hingewiesen (https://www.datenschutz-mv.de/datenschutz/themen/beschlue/88_DSK/Ent_Suche.pdf). Dort wurde jedoch bewusst darauf verzichtet, ein „Recht auf Vergessen“ zu thematisieren. Denn in der medialen Nachbetrachtung des Urteils verbreitete sich schnell die gesellschaftliche Auffassung, dass mit dem genannten Urteil ein so genanntes Recht auf Vergessen im Internet einhergeht. Dem müssen wir widersprechen, denn wir haben schon oft darauf hingewiesen, dass einmal im Internet verbreitete Daten praktisch nie vollständig gelöscht werden können. Das Internet vergisst nicht oder nicht so leicht, wie mit dem Ausspruch „Recht auf Vergessen“ suggeriert wird. Denn klarzustellen ist in diesem Zusammenhang, dass die Informationen, die „vergessen“ werden sollen, keinesfalls aus dem Netz gelöscht werden, wenn diese aus den Ergebnislisten einer Suchmaschine entfernt wurden. Der Inhalt ist ab diesem Zeitpunkt lediglich schwerer im Netz auffindbar. Daher sollte das Löschersuchen beim Suchmaschinenbetreiber nicht das alleinige Mittel zur Wahl sein, einen bestimmten Inhalt im Internet unzugänglich zu machen. Wir empfehlen, im ersten Schritt immer an den eigentlichen Verbreiter des fraglichen Inhaltes heranzutreten und dort den Anspruch auf Löschung des Inhaltes durchzusetzen.

Auch hier zeigt sich wieder, wie wichtig der sorgsame Umgang mit personenbezogenen Daten im Zusammenhang mit der Nutzung des Internet ist. Wer das Prinzip der Datensparsamkeit berücksichtigt und immer sehr sorgfältig prüft, bevor er Daten im Internet veröffentlicht, kann sich selbst und anderen Betroffenen die aufwendigen Bemühungen sparen, einen unerwünschten Inhalt aus dem Internet zu löschen.

4.2.2 Aktivitäten zu Google und Facebook und Microsoft

Immer wieder stehen weltweit agierende Softwareanbieter in der Kritik der deutschen Datenschutzaufsichtsbehörden, weil ihre Angebote oft mit deutschem Datenschutzrecht kollidieren (siehe bspw. Neunter Tätigkeitsbericht, Punkt 3.14, Zehnter Tätigkeitsbericht, Punkte 2.2 und 4.2.2, Elfter Tätigkeitsbericht, Punkt 2.9). Auch in diesem Berichtszeitraum hat sich daran nicht viel geändert. Obwohl wir in den meisten Fällen nicht die jeweils zuständige Aufsichtsbehörde sind, berichten wir im Folgenden über einige Bestrebungen verschiedener Gremien, diese Unternehmen zu datenschutzkonformen Verhalten zu veranlassen.

Google

Urteil des Europäischen Gerichtshofes

Wie schon erwähnt, erging im Berichtszeitraum ein bedeutendes Urteil des Europäischen Gerichtshofes (EuGH, Urteil vom 13.05.2014 – C-131/12) in Bezug auf das Unternehmen Google. Den Inhalt sowie die Folgen des Urteils erläutern wir unter Punkt 4.2.1.

Anordnung gegen Google
Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat im September 2014 eine Anordnung gegen das Unternehmen Google erlassen. Mit dieser Anordnung wird Google aus gegebener Veranlassung ausdrücklich verpflichtet, Daten, die bei der Nutzung unterschiedlicher Google-Dienste anfallen, zukünftig streng unter Beachtung der gesetzlichen Vorgaben zu verarbeiten. Grund für diese Maßnahme war die Feststellung, dass Google bei der Erstellung von Nutzerprofilen weit über das zulässige Maß hinaus in die Privatsphäre der Google-Nutzer eingriff.

In der Folge dieser Anordnung konzipierte Google eine Einwilligungslösung für seine Dienste. Sowohl registrierte als auch nichtregistrierten Nutzer durchlaufen nun vor der Nutzung der Google-Dienste ein Einwilligungsprozedere. Seit Google diese Einwilligungslösung anbietet, kommt es bei den Nutzern verstärkt zu Fragen. Deshalb veröffentlichte der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit auf seiner Homepage einige weitergehende Informationen zum Umgang mit dieser neuen Einwilligungslösung (https://www.datenschutz-hamburg.de/uploads/media/Information_zur_Einwilligungs-loesung_von_Google.pdf).

Google hat gegen diese Anordnung eine Anfechtungsklage vor dem Verwaltungsgericht Hamburg erhoben. Der Rechtsstreit ist noch nicht entschieden.

Facebook
Anordnungen gegen Facebook
Ebenfalls in diesem Berichtszeitraum hat der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit gegenüber dem Unternehmen Facebook eine Anordnung erlassen. Facebook wird hierin aufgefordert, seinen Kunden die pseudonyme Nutzung des sozialen Netzwerks zu ermöglichen. Bisher werden Kunden von Facebook vor die Wahl gestellt, ihren Klarnamen zu benutzen oder das Netzwerk zu verlassen. Außerdem wurde Facebook dazu aufgefordert, auf digitale Ausweiskopien zu verzichten. Gegen die Anordnung hat das Unternehmen Facebook Klage eingereicht. Das Verfahren ist anhängig.

Privatrechtliche Klageverfahren des Maximillian Schrems
Ungültigkeit von Safe-Harbor:
Ein bedeutendes Urteil des Europäischen Gerichtshofes (C-362/14 vom 06.10.2015) erging in dem Rechtsstreit zwischen Maximillian Schrems und der Irischen Datenschutzaufsicht (Data Protection Commissioner Ireland). In diesem Urteil erklärte der Europäische Gerichtshof das sogenannte Safe-Harbor-Abkommen (siehe Entscheidung der Kommission 2000/520/EG vom 26.07.2000,
http://www.bfdi.bund.de/SharedDocs/ExterneLinks/SafeHarbor/SafeHarborEntscheidung2000_520_EG.pdf?__blob=publicationFile&v=1) für ungültig. Das Safe-Harbor-Abkommen enthielt nicht verhandelbare und die entsprechenden amerikanischen Unternehmen verpflichtende Grundsätze zum transatlantischen Datentransfer zwischen Europa und den Vereinigten Staaten von Amerika (USA).

Hintergrund der Entscheidung des Europäischen Gerichtshofes war (siehe auch dazu Pressemitteilung des Europäischen Gerichtshofes Nr. 117/15 vom 06.10.2015), dass Schrems bei der irischen Datenschutzaufsicht eine Beschwerde einlegte, weil er im Hinblick auf die von Edward Snowden enthüllten Tätigkeiten der Nachrichtendienste der USA, insbesondere der National Security Agency, der Ansicht war, dass das Recht und die Praxis der Vereinigten Staaten keinen ausreichenden Schutz der in dieses Land übermittelten Daten vor Überwachungstätigkeiten der dortigen Behörden böten. Schrems bezog sich dabei auf Datenübermittlungen des Unternehmens Facebook von Europa in die USA. Die irische Behörde wies jedoch die Beschwerde insbesondere mit der Begründung zurück, die Kommission habe in ihrer Entscheidung 2000/520/EG festgestellt, dass die USA im Rahmen des Safe-Harbor-Abkommens ein angemessenes Schutzniveau der übermittelten personenbezogenen Daten gewährleisteten.

Im vorliegenden Urteil entschied nun der Europäische Gerichtshof, dass die Kommission in der Entscheidung 2000/520/EG gerade nicht nachgewiesen habe, dass die USA aufgrund ihrer innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen tatsächlich ein angemessenes Schutzniveau gewährleisten würden. Damit verstoße die Entscheidung der Kommission gegen den Grundsatz, dass personenbezogene Daten nur in andere Länder außerhalb Europas übermittelt werden dürfen, wenn dort ein angemessenes Schutzniveau der Daten, ähnlich wie in Europa, gewährleistet werden kann.

Die Artikel-29-Gruppe, ein europäischer Zusammenschluss der Datenschutzaufsichtsbehörden, hat mit einem Statement auf das Urteil des Europäischen Gerichtshofes reagiert (siehe https://www.datenschutz-mv.de/datenschutz/themen/beschlue/90_DSK/SH-StatementA29.pdf).
Unter anderem werden darin die Unternehmen in Europa aufgefordert, im Lichte des Urteils die Risiken eingehend zu reflektieren, die sie bei der Datenübermittlung eingehen. Ihnen wird empfohlen, rechtliche und technische Lösungen zu ergreifen, mit denen diese offenkundigen Risiken minimiert werden können und die dem europäischen Datenschutzniveau entsprechen.
Auch die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat in einem Positionspapier auf das richtungsweisende Urteil des Europäischen Gerichtshofes reagiert (siehe https://www.datenschutz-mv.de/datenschutz/themen/beschlue/90_DSK/Positions_ papier.html). Die Konferenz fordert die Kommission auf, in ihren Verhandlungen mit den USA auf die zeitnahe Schaffung ausreichend weitreichender Garantien zum Schutz der Privatsphäre zu drängen. Dies betreffe insbesondere das Recht auf gerichtlichen Rechtsschutz, die materiellen Datenschutzrechte und den Grundsatz der Verhältnismäßigkeit.

Auch sei im Lichte des Urteils, die weitere Zulässigkeit der Datentransfers in die USA auf der Grundlage der anderen hierfür eingesetzten Instrumente, etwa Standardvertragsklauseln oder verbindliche Unternehmensregelungen (Binding Corporate Rules), in Frage gestellt.
Es gelte nunmehr, die Entscheidungen zu den Standardvertragsklauseln kurzfristig an die in dem Urteil genannten Vorgaben anzupassen.

Verbraucherklage in Österreich:
In einem anderen anhängigen Verfahren von Maximillian Schrems gegen das Unternehmen Facebook geht es unter anderem darum, inwieweit eine Verbraucher-Sammelklage gegen Facebook in Europa zulässig ist. Mit dieser Frage beschäftigt sich in zweiter Instanz nun der Oberste Gerichtshof in Österreich. Mit Spannung wird erwartet, ob in dieser Frage der Europäische Gerichtshof durch den Obersten Gerichtshof Österreichs angerufen wird.

Facebook möchte in dem Rechtsstreit verhindern, dass Verbraucher ihre Rechte in Form einer Sammelklage, vertreten durch einen Verbraucher, geltend machen können. Dies hätte dann die Folge, dass über die Ansprüche der Verbraucher in dessen Wohnsitzland verhandelt werden könnte. Das Unternehmen müsste in diesem Fall seine beanstandete Datenschutzpraxis vor europäischen Gerichten verantworten.

Bundesverwaltungsgericht
In einem anderen Verwaltungsrechtsstreit geht es nicht direkt um das Unternehmen Facebook, sondern um die Möglichkeit, eine Fanpage auch als privatwirtschaftliche Organisation auf Facebook zu betreiben. Es soll nun abschließend höchstrichterlich geklärt werden, ob eine Fanpage einer Organisation datenschutzrechtlich zugerechnet werden kann.

In dem in Rede stehenden Verwaltungsrechtsstreit zwischen dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein und der Wirtschaftsakademie Schleswig-Holstein GmbH geht es um eine Anordnung gegenüber der Wirtschaftsakademie Schleswig-Holstein GmbH. In dieser Anordnung verlangt das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein von der Wirtschaftsakademie Schleswig-Holstein GmbH, dessen Facebook-Fanpage zu deaktivieren.

Nach Auffassung der Kollegen aus Schleswig-Holstein verstößt der Betrieb der fraglichen Facebook-Fanpage gegen europäisches und nationales Datenschutzrecht. Begründet wird dies unter anderem damit, dass die Betreiberin als verantwortliche Stelle für die Datenverarbeitung auf dieser Fanpage beispielsweise nicht die erforderliche Einwilligung eines Nutzers in die umfangreiche Datenverknüpfung, welche bei einem Besuch auf der fraglichen Fanpage erfolgt, einholt.

Die Wirtschaftsakademie Schleswig-Holstein GmbH hat gegen die Anordnung Klage eingereicht. Der Rechtsstreit, der bereits das Schleswig-Holsteinische Verwaltungsgericht und das Schleswig-Holsteinische Oberverwaltungsgericht beschäftigt hat, liegt nun zur Entscheidung beim Bundesverwaltungsgericht. Die Verhandlung vor dem Bundesverwaltungsgericht ist vorläufig für den 25. Februar 2016 angesetzt.

Microsoft
Im Berichtszeitraum veröffentlichte das Unternehmen Microsoft ein neues Betriebssystem, welches nicht nur nach unserer Auffassung einen Paradigmenwechsel in der Funktionsweise darstellt. Die bisherigen Betriebssysteme der Firma Microsoft greifen nicht in dem Maße auf internetbasierte Cloud-Services zurück, wie dies bei dem neuen Betriebssystem Windows 10 offensichtlich der Fall ist.

Diese Entwicklung veranlasste unter anderem die 90. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, die Entschließung „Cloud-unterstützte Betriebssysteme bergen Datenschutzrisiken“ zu verabschieden (siehe dazu ausführlich Punkt 4.1.11).

Auch auf internationaler Ebene nimmt man sich dieser Problematik an. Die „Artikel-29-Gruppe“, ein europäischer Zusammenschluss der Datenschutzaufsichtsbehörden, gründete eine Arbeitsgruppe zur Untersuchung von Windows 10. Dort arbeiten Mitarbeiter der Datenschutzaufsichtsbehörden Spaniens, Frankreichs, Ungarns, Irlands, Italiens, Großbritanniens, der Niederlande und Deutschlands (vertreten durch das LDA-Bayern) zusammen. Mit ersten Analyseergebnissen ist in Kürze zu rechnen.

4.2.3 Smart-TV

Schaut man sich die im Handel verfügbaren Fernsehgeräte an, stellt man fest, dass diese allesamt „smart“ sind. „Smart“ bedeutet in diesem Zusammenhang, dass die Fernsehgeräte neben dem normalen TV-Empfang weitere Zusatzfunktionen bieten. Die wichtigste Funktion ist die Fähigkeit der Geräte, sich mit dem Internet zu verbinden. Durch Einbau von hochleistungsfähigen Prozessoren und Festplatten haben diese Fernsehgeräte inzwischen fast schon die Leistungsfähigkeit herkömmlicher Tablets oder Personalcomputer. Das Skypen, Surfen und Shoppen gehört für die modernen Fernsehgeräte genauso zum standardmäßigen Leistungsumfang wie das Herunterladen verschiedener Anwendungen (sogenannter Apps) aus diversen App-Stores, wie man es vom Smartphone und Tablet her kennt. Beim Nutzen dieser Fernsehgeräte fallen aber auch zahlreiche personenbezogene Daten der Nutzer an und es ist nicht verwunderlich, dass viele Begehrlichkeiten zur Verwendung dieser Daten geweckt werden.

So hat das Bayerische Landesamt für Datenschutzaufsicht bei einer Untersuchung von 13 Smart-TV-Geräten diverser Hersteller zahlreiche Datenschutzmängel aufgedeckt. Die Datenschützer stellten regelmäßige Datenflüsse an diverse Akteure fest, beispielsweise an Gerätehersteller, App- oder TV-Anbieter. Es wurde vermutet, dass das individuelle Nutzungsverhalten erfasst und ausgewertet werden soll (https://www.datenschutz-mv.de/presse/2015/pm-smarttv.html). Schon das Umschalten auf ein anderes Fernsehprogramm löst offenbar Datenflüsse über das Internet aus. Ermöglicht wird dies durch das so genannte HbbTV (Hybrid Broadcasting Broadband TV), das Nutzer an der „Red Button“-Funktion ihres Fernsehgerätes erkennen können. HbbTV ermöglicht die Verzahnung des Rundfunksignals (Broadcasting) mit dem Internet (Broadband). Auf diese Weise können dem Zuschauer neben dem Fernsehangebot weitere Zusatzinformationen geliefert werden. So kann er beispielsweise auf Mediatheken, soziale Netzwerke oder elektronische Programmzeitschriften zugreifen. Warum aber schon eine Kommunikation mit dem TV-Anbieter stattfindet, bevor der Nutzer überhaupt den „Red Button“ geklickt hat, bleibt aus datenschutzrechtlicher Sicht fragwürdig.

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) und die Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten haben im Mai 2014 ihre gemeinsame Position zu diesem Thema veröffentlicht (https://www.datenschutz-mv.de/presse/2015/Anlage2.pdf). Insbesondere wird dort gefordert, dass eine anonyme Nutzung von Fernsehangeboten auch bei der Smart-TV-Nutzung gewährleistet sein muss. Ferner sollten die Geräte dem „Privacy by Default“-Prinzip folgen. Sie sollen also mit datenschutzfreundlichen Grundeinstellungen ausgeliefert werden.

Diese Einstellungen sollen unter anderem bewirken, dass die mit dem Aufruf der Web-Dienste einhergehende wechselseitige Kommunikation mit Geräteherstellern, TV-Anbietern oder sonstigen Akteuren per Internet erst gestartet wird, nachdem der Nutzer umfassend über Details der Datenübermittlungen informiert wurde und seine Zustimmung erteilt hat. Keinesfalls dürfen Daten schon beim Einschalten des Gerätes oder beim Umschalten auf andere Sender fließen.

Im September 2015 hat der Düsseldorfer Kreis seine Anforderungen an einen datenschutzgerechten Betrieb mit der „Orientierungshilfe zu den Datenschutzanforderungen an Smart-TV-Dienste“ (https://www.datenschutz-mv.de/datenschutz/publikationen/informat/smart-tv/oh_smart.pdf) weiter konkretisiert. Sie richtet sich gezielt an die Anbieter von Smart-TV-Diensten und -Produkten und beschreibt konkrete datenschutzrechtliche und technisch-organisatorische Anforderungen.

4.3 Videoüberwachung

4.3.1 Rechtsgrundlagen der Videoüberwachung

Auf sehr hohem Niveau liegt weiterhin die Zahl der Eingaben zu Videokameras. Die rechtlichen Voraussetzungen für die Nutzung von Videokameras sind häufig entweder nicht bekannt oder sie werden nicht beachtet.

Maßgebliche Zulässigkeitsnorm ist § 6b Bundesdatenschutzgesetz (BDSG), der die Videoüberwachung von öffentlich zugänglichen Räumen regelt. Dabei umfasst der Begriff der Videoüberwachung sowohl die Videobeobachtung (Live-Übertragung der Bilder auf einen Monitor) als auch die Videoaufzeichnung, bei der Aufnahmen gespeichert werden.

Bei Kamera-Attrappen kommt das Bundesdatenschutzgesetz nicht zur Anwendung, weil es sich nicht um „optisch-elektronische Einrichtungen“ handelt und deshalb de facto keine personenbezogenen Daten erhoben werden. Weil das Fehlen der Funktionsfähigkeit von außen nicht erkennbar ist, kann der bei den Betroffenen entstehende (subjektive) Überwachungsdruck eine Beeinträchtigung des Persönlichkeitsrechts darstellen und daher zivilrechtliche Abwehransprüche auslösen, die gegebenenfalls auf dem zivilrechtlichen Klageweg durchgesetzt werden müssen.

Zu den von der Vorschrift erfassten öffentlich zugänglichen Räumen zählen Straßen, Verkaufsräume, Biergärten, Gasträume von Gaststätten, Hotelfoyers etc. Handelt es sich um eine Videoüberwachung in nicht öffentlich zugänglichen Räumen, so ist die Rechtmäßigkeit nach ähnlichen Kriterien gemäß § 28 BDSG zu beurteilen.

Nach § 6b Abs. 1 BDSG ist die Videoüberwachung nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder berechtigter Interessen für konkrete Zwecke erforderlich ist und zusätzlich keine Anhaltspunkte für das Vorliegen überwiegender schutzwürdiger Interessen der Betroffenen bestehen. Grundsätzlich kann ein berechtigtes Interesse angenommen werden, wenn der Zweck im Schutz vor Einbrüchen, Vandalismus oder Diebstählen besteht, sofern eine tatsächliche Gefahrenlage nachgewiesen wurde.

Voraussetzung ist, dass die Videoüberwachung tatsächlich für die Erreichung des festgelegten Zwecks geeignet und auch erforderlich ist. Die Erforderlichkeit ist nur dann gegeben, wenn der Zweck nicht genauso mit einem „milderen“ (also in die Rechte des Betroffenen weniger einschneidenden) Mittel erreicht werden kann. Nicht selten ist es für den Zweck ausreichend, die Überwachung auf Zeiträume außerhalb der Geschäftszeiten oder auf die Nachtstunden zu begrenzen. Alternativen können auch im zusätzlichen Einbau von Sicherheitsschlössern, dem Einsatz von Überwachungspersonal oder einer Umzäunung bestehen, sofern diese Mittel wirtschaftlich und organisatorisch zumutbar sind.

Auch wenn nach diesen Maßstäben eine Erforderlichkeit gegeben ist, ist die Videoüberwachung nur dann zulässig, wenn zusätzlich in einer Abwägung zwischen den berechtigten Interessen der verantwortlichen Stelle und den schutzwürdigen Interessen der Betroffenen letztere nicht überwiegen. Grundsätzlich unzulässig sind Überwachungsmaßnahmen, die die Intimsphäre verletzen, zum Beispiel im Fall von Saunen, Toiletten oder Duschkabinen. Schutzwürdige Interesse überwiegen zudem häufig dort, wo Menschen kommunizieren, essen und trinken oder sich erholen, beispielsweise in den Sitzbereichen von Restaurants, Parks etc. Nach § 6b Abs. 2 BDSG ist Videoüberwachung außerdem durch geeignete Maßnahmen (z. B. Schilder oder Piktogramme) erkennbar zu machen, die so anzubringen sind, dass die Betroffenen die Überwachung noch vor dem Betreten des überwachten Bereiches erkennen können.

Nach § 6b Abs. 5 BDSG sind die Daten unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind. Bei Aufzeichnungen zu Beweiszwecken ist das in der Regel nach 48 Stunden der Fall (in begründeten Einzelfällen, z. B. an Wochenenden, nach 72 Stunden). Beim Einsatz von Webcams, die Live-Aufnahmen ins Internet übertragen und dadurch einer unbestimmten Zahl von Personen weltweit zugänglich machen, sind die Vorschriften des Kunsturheberrechtsgesetzes zu beachten. Der Einsatz von Webcams ist nur dann datenschutzrechtlich zulässig, wenn auf den Bildern ein Personenbezug nicht herstellbar ist.

Bei der Videoüberwachung von Beschäftigten ist zusätzlich § 32 BDSG zu beachten. Eine durchgängige Überwachung von Beschäftigten während ihrer gesamten Arbeitszeit ist nicht zulässig. Bei der Überwachung von besonders gefahrträchtigen Arbeitsbereichen ist der Erfassungsbereich auf diesen Bereich zu beschränken. Die Beschäftigten sind soweit wie möglich auszublenden. Eine Überwachung allein zum Zweck der Überprüfung der Einhaltung eines planmäßigen Dienstablaufs ist unzulässig.

4.3.2 Videoüberwachung einer Großbaustelle

In unserem Sechsten Bericht der Aufsichtsbehörde für den nicht-öffentlichen Bereich hatten wir unter Punkt 5.2.2 über eine unzulässige Videoüberwachung auf einer Großbaustelle berichtet. Hier wurden die angestellten Bauarbeiter auf dem jeweils oberen Stockwerk des Rohbaus während der gesamten Arbeitszeit durch Videokameras überwacht. Wir hatten das Unternehmen darauf hingewiesen, dass eine lückenlose Videoüberwachung von Arbeitnehmern während der gesamten Arbeitszeit nach der Rechtsprechung des Bundesarbeitsgerichtes unzulässig ist.

Trotz bestehender Alternativlösungen hat das Unternehmen in Kenntnis der Rechtswidrigkeit die Videoüberwachung bis zum Abschluss der Großbaustelle fortgesetzt. Das Unternehmen stellte sich auf den Standpunkt, dass hier keine personenbezogenen Daten von den Arbeitern erhoben werden, da diese auf den Bildern nicht zu erkennen seien. Wir haben daher ein Bußgeld im fünfstelligen Bereich festgesetzt. Gegen den Bußgeldbescheid hatte das Unternehmen Rechtsmittel eingelegt, sodass das zuständige Amtsgericht mit der Angelegenheit befasst war.

Durch das Amtsgericht wurde in der Verhandlung festgestellt, dass es sich bei den von der Videoüberwachung betroffenen Arbeitern um bestimmbare natürliche Personen i. S. d. § 3 Abs. 1 Bundesdatenschutzgesetz (BDSG) handelt, da die Personen durch Zusatzwissen, z. B. des Poliers, bestimmbar sind. Daraufhin erklärte sich das Unternehmen in der Verhandlung bereit, mit dem Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern in Kontakt zu treten, um für alle seine Baustellen, die in Zukunft mit Videokameras überwacht werden sollen, eine datenschutzgerechte Lösung zu finden.

Aus Sicht des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern war in diesem Fall eine Videoüberwachung der obersten Baustellenplattform vom Kran aus wegen der hier dargelegten speziellen Begründung bzw. des berechtigten Interesses des Unternehmens grundsätzlich möglich, wenn nur alle 30 Minuten ein anlassbezogenes Bild von der Baustelle aufgenommen wird. Ausnahmsweise haben wir es hier bei einigen besonders gefahrenträchtigen Bauphasen, die einer besonderen Begründung bedürfen und auch im Verfahrensverzeichnis festgehalten werden müssen, für zulässig gehalten, den Abstand der Aufnahmen der Bilder von 30 Minuten auf 8 Minuten zu reduzieren, sodass nicht zwei, sondern sieben bis acht Bilder pro Stunde aufgenommen werden. Die aufgenommenen Bilder sollten maximal 72 Stunden gespeichert werden. Durch den betrieblichen Datenschutzbeauftragten ist eine Vorabkontrolle durchzuführen, auch wenn gegebenenfalls eine Betriebsvereinbarung mit dem Betriebsrat über die Videoüberwachung abgeschlossen wurde.

Unabhängig davon wurde auch von anderen Bauunternehmen angefragt, inwieweit Aufnahmen einer Baustelle zum Zweck der Dokumentation des Baufortschrittes zulässig sind. Generell halten wir für diese Zwecke zwei bis drei Bilder pro Tag für ausreichend, die möglichst zu Tageszeiten aufgenommen werden sollten, wenn sich keine Personen in den überwachten Bereichen aufhalten (z. B. vor Arbeitsbeginn, nach Arbeitsende oder in den Pausenzeiten). Nur Bilder, die nicht personenbeziehbar sind, sind aus datenschutzrechtlicher Sicht grundsätzlich unbedenklich.

4.3.3 Webcambilder von der Strandpromenade

Der Eigentümer eines Grundstückes mit Ferienwohnungen hatte auf seinem Grundstück in exponierter Lage eines Kurortes an der Ostsee zwei Videokameras installiert, von denen Teile der Strandpromenade, eines Fahrradweges und des Bootshafens (Marina) erfasst wurden. Bei den beiden Kameras handelte es sich um Webcams, die die Aufnahmen live ins Internet übertragen.

Durch die Kameras war es möglich, Personen insbesondere auf dem Fahrradweg und der - gerade im Sommer - viel genutzten Strandpromenade zu erkennen und zu identifizieren, was einen Verstoß gegen § 6b Bundesdatenschutzgesetz (BDSG) sowie gegen § 23 Abs. 1 Nr. 2 Kunsturheberrechtsgesetz (KunstUrhG) darstellt, siehe auch Punkt 5.3.1. Wir haben den Betreiber der Kameras deshalb aufgefordert, die Kameras so einzustellen, dass keine Personen oder personenbeziehbaren Merkmale beobachtet, aufgenommen und ins Internet übertragen werden.

Der Betreiber der Kameras reagierte darauf lediglich mit dem Hinweis, es handelte sich nur um Panorama-Aufnahmen, die die Landschaft und das aktuelle Wetter zeigen sollten. Die zufällig miterfassten Personen seien unkenntlich, da die Bilder klein gehalten seien und eine niedrige Auflösung gewählt worden sei.

Nachdem der Betreiber sich weiterhin uneinsichtig zeigte, haben wir eine Anordnung mit Androhung eines Zwangsgeldes in Höhe von 1.000,00 Euro pro Kamera erlassen und die sofortige Vollziehung angeordnet.

Auf die Klage des Betreibers der Kameras gegen diese Anordnung hat das Verwaltungsgericht Schwerin in einem Beschluss klargestellt, dass es nach § 6b Abs. 1 Nr. 3 BDSG nicht zulässig ist, wenn Webcams zum Zwecke der Werbung und Information potentieller Urlaubsgäste öffentlich zugängliche Bereiche aufzeichnen, in denen sich bestimmbare Personen aufhalten und gleichzeitig der Abruf dieser Aufzeichnungen über das Internet (per Livestream) ermöglicht wird. Dabei hat das Gericht die Kriterien für die Bestimmbarkeit von Personen und die Zulässigkeit solcher Aufnahmen klar eingegrenzt und unter anderem betont, dass unabhängig von einer Erkennbarkeit von Gesichtern auch zusätzliche Kriterien zu einer Bestimmbarkeit führen können (Körperbild einer Person, Körperhaltung, Kleidung oder mitgeführte Gegenstände).

Erst wenn - etwa durch technische Vorkehrungen - die Anonymität der möglicherweise aufgezeichneten Personen gewährleistet ist, fehlt es am Erheben personenbeziehbarer Daten. Auf den Bildern erkennbare Personen sind - anders als etwa bei einer bloßen Panoramaaufnahme - auch nicht lediglich nebensächlich oder Beiwerk gemäß § 23 KunstUrhG. Vielmehr handelt es sich schon wegen des regen Publikumsverkehrs in den von den Kameras erfassten Bereichen und im Hinblick auf ihre Erkennbarkeit um wesentliche Bestandteile der Aufnahmen.

Zudem werden - wie das Gericht weiter ausführte - diese Eingriffe erheblich dadurch verstärkt, dass zugleich die Abrufbarkeit der Bilder über das Internet ermöglicht wird, sodass es weltweit beliebigen Dritten überlassen bleibt, wie diese mit den Videoaufnahmen verfahren und in welchem Umfang sie diese speichern oder auswerten, ohne dass die Betroffenen etwas darüber erfahren. Nach Feststellung des Verwaltungsgerichtes bestanden nach diesen Grundsätzen ganz erhebliche Anhaltspunkte für ein Überwiegen der schutzwürdigen Interessen der von der Videoüberwachung betroffenen Personen.

Auf den Beschluss des Verwaltungsgerichts Schwerin hin hat der Betreiber seine beiden Webcams nunmehr nach den in unserer Anordnung genannten datenschutzrechtlichen Vorgaben korrekt eingestellt.

4.3.4 Dashcams

Im Rahmen einer Petition wurde bei einem Taxi- und Fuhrunternehmen festgestellt, dass dieses Dashcams in seinen Fahrzeugen am Rückspiegel installiert hatte. Diese Kameras waren in Fahrtrichtung ausgerichtet und mit einem sogenannten Event-(Shock)-Modus ausgestattet. Dashcams filmen in aller Regel den öffentlich zugänglichen Raum vor dem Fahrzeug.

Nach der technischen Beschreibung der Dashcam zeichnet die Kamera im Event-(Shock)-Modus auf einen Ringspeicher 15 Sekunden auf, der automatisch immer wieder überschrieben wird. Erst wenn ein Event wie eine hohe Beschleunigung durch z. B. einen Aufprall eintritt, werden die 15 Sekunden der Aufzeichnungen im Zwischenspeicher „fest“ gespeichert. Weiterhin werden ab dem Event weiterhin 15 Sekunden danach gespeichert, sodass bei einem eingetretenen Event insgesamt 30 Sekunden Bildmaterial fest gespeichert und ausgewertet werden können.

Diese Kameras wurden als datenschutzrechtlich unzulässig gewertet, da nach der Systematik des Bundesdatenschutzgesetzes (BDSG) zunächst die Beobachtung durch die Kamera gemäß § 6b Abs. 1 BDSG bewertet wird. Erst wenn die Beobachtung als zulässig bewertet werden kann, kann eine danach erfolgende Speicherung der Aufnahmen gemäß § 6b Abs. 3 BDSG zulässig sein.

Auch im Event-(Shock)- Modus wird permanent öffentlicher Raum, nämlich der Straßenverkehr und somit andere Verkehrsteilnehmer, nicht anlassbezogen beobachtet. Die durchgängige Beobachtung des öffentlichen Raumes ist unabhängig von der Speicherdauer unzulässig, da die schutzwürdigen Interessen der anderen Verkehrsteilnehmer, nicht permanent heimlich beobachtet zu werden, grundsätzlich überwiegen. Die Bilder werden auch im Event-(Shock)-Modus zusätzlich für 15 Sekunden gespeichert und danach automatisch überschrieben. Die Möglichkeit der Auswertung der Bilder nach einem Event mag gegebenenfalls anlassbezogen sein, die vorher stattfindende permanente Beobachtung ist allerdings nicht anlassbezogen und daher unzulässig.

Nach unserer datenschutzrechtlichen Bewertung unter Verweis auf die einschlägige Rechtsprechung des Verwaltungsgerichtes Ansbach, des Amtsgerichtes München und des Landgerichtes Heilbronn wurde durch das Taxi- und Fuhrunternehmen bestätigt, dass dieses die Kameras ausgebaut hat.

Ein weiteres Problem von Dashcams ist, dass die gemäß § 6b Abs. 2 BDSG erforderliche Kenntlichmachung der Kamera nicht möglich ist und dadurch eine heimliche Videoüberwachung von öffentlichem Raum erfolgt. Für die betroffenen Verkehrsteilnehmer ist nicht erkennbar, dass sie gefilmt werden. Alle Dashcams, die durchgängig beobachten und zusätzlich die Aufnahmen auch speichern, sind daher datenschutzrechtlich unzulässig.

4.3.5 Videoüberwachung im Behandlungszimmer einer Arztpraxis

Einem Petenten ist bei seinem Besuch in einer Praxis für Gastroenterologie aufgefallen, dass in dem Behandlungszimmer und in den Fluren der Praxis Videokameras installiert waren. Er hat uns gebeten, ihm mitzuteilen, ob dies datenschutzrechtlich zulässig sei.

Der Praxisinhaber hat uns auf unsere Anfrage hin mitgeteilt, dass die Videokameras aus sicherheitstechnischen Gründen installiert worden seien. Die Praxis sollte damit vor Diebstahl und Vandalismus geschützt werden. Mit der Videoüberwachung in den Behandlungsräumen sollte verhindert werden, dass Patienten, die noch unter dem Einfluss von Medikamenten stehen, unbeaufsichtigt durch die Praxis irren und sich oder andere gefährden. Es wurde Tag und Nacht aufgezeichnet und die Aufnahmen nach zwei Tagen automatisch gelöscht.

Bei der datenschutzrechtlichen Bewertung war zu unterscheiden, ob die Räume allgemein zugänglich sind oder nicht.

Der Tresen-/Flur- und der Wartebereich gehören - wie der gesamte allgemein zugängliche Bereich der Praxis - zum sogenannten öffentlich zugänglichen Raum. Rechtsgrundlage für die Überwachung öffentlich zugänglicher Räume ist § 6b Abs. 1 Bundesdatenschutzgesetz (BDSG). Danach ist dies nur zulässig, wenn die Überwachung, insbesondere zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen, für konkret festgelegte Zwecke erforderlich ist und zusätzlich keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Erforderlich wäre eine Videoüberwachung in diesen Bereichen nur dann, wenn es kein milderes (gleich geeignetes) Mittel gäbe, um hier eine angemessene Sicherheit zu gewährleisten. Hieran bestanden in Anbetracht der ständigen Anwesenheit von Arzthelferinnen und der Möglichkeit, bei Gefahr jederzeit die Polizei zu rufen, begründete Zweifel. Auch können diese Straftaten bereits durch automatisierte Türöffnungssysteme weitgehend ausgeschlossen werden. Eine Installation von Videoüberwachungsanlagen in diesen Bereichen allein damit zu begründen, dass dies aus „sicherheitstechnischen Gründen“ erforderlich sei, ist nach den Grundsätzen des § 6b BDSG nicht zulässig.

Bei der Videoüberwachung im Ruheraum bzw. im Raum für Infusionen kann man davon ausgehen, dass diese Räume in einem Bereich liegen, der nicht allgemein zugänglich ist. Damit wäre § 6b BDSG nicht anwendbar, sodass hier als Rechtsgrundlage vor allem eine schriftliche Einwilligung der Patientin oder des Patienten gemäß § 4a BDSG in Betracht kommt. Da hier medizinische Daten (§ 3a Abs. 9 BDSG) erhoben werden sollen, muss die Einwilligung sich ausdrücklich auch auf diese Daten beziehen, § 4a Abs. 3 BDSG. Zudem kann nicht von einem überwiegenden Interesse der Patientinnen und Patienten ausgegangen werden, in einer Arztpraxis während oder nach einer Behandlung nicht von einer Kamera überwacht zu werden. Die seitens des Praxisinhabers vorgebrachten Gefährdungssituationen können grundrechtsneutral durch innerorganisatorische Maßnahmen umgangen werden.

Wir haben daher empfohlen, die öffentlich zugänglichen Räume lediglich während der Nachtzeit durch Videokameras zu überwachen. Nur, wenn es in den Räumen wiederholt zu nicht selbst verursachten Zwischenfällen kommen sollte und die Aufnahmen für Beweiszwecke erforderlich sein sollten, wäre eine längere Speicherung zulässig. Wir haben daher vorgeschlagen, die Aufzeichnungen im Aufnahmebereich bereits früher zu löschen.

Unsere Hinweise wurden in der Praxis ausgewertet. Im Ergebnis wurde auf eine Videoaufzeichnung während der Praxiszeiten verzichtet. Die Videoaufzeichnungen wurden auf die Zeiten außerhalb der Sprechzeiten beschränkt und auch die Speicherfrist der Aufzeichnungen wurde verkürzt.

5 Datenschutz in verschiedenen Rechtsgebieten

5.1 Rechtswesen

5.1.1 Bundesnotarordnung - Gesetz zur Neuordnung der Aufbewahrung von Notariatsunterlagen

Von einem unserer Länderkollegen haben wir erfahren, dass der Entwurf eines Gesetzes zur Neuordnung der Aufbewahrung von Notariatsunterlagen und Errichtung eines elektronischen Urkundenarchivs erarbeitet worden ist. Wir haben dazu gegenüber unserem Justizministerium wie folgt Stellung genommen:

Datenschutzrechtlichen Bedenken begegnet die „Befreiung“ von der Pflicht, einen behördlichen Datenschutzbeauftragten zu bestellen. So ist der Datenschutzbeauftragte nicht nur für das elektronische Urkundenarchiv, sondern auch etwa für Mitarbeiterdaten und andere, nicht originär der Notartätigkeit zuzuordnenden Verfahren (Webseite, Internetzugang, Telefonanlage etc.), zuständig. Zudem bedeutet die als Begründung angegebene Unabhängigkeit und Weisungsfreiheit des Notars nicht, dass datenschutzrechtliche Vorschriften nicht ebenso einzuhalten sind und auf deren Einhaltung nicht ebenso hinzuwirken ist, wie bei anderen öffentlichen Stellen.

Nicht akzeptabel ist aus unserer Sicht die Änderung des § 92 Bundesnotarordnung-Entwurf (BNotO-E). Ausweislich der Begründung soll damit bezweckt werden, dass die Notare nicht mehr der Kontrolle der Landesdatenschutzbeauftragten unterliegen. Die Gründe hierfür sind nicht überzeugend. Notare sind öffentliche Stellen und damit dem Geltungsbereich des Landesdatenschutzgesetzes Mecklenburg-Vorpommern (DSG M-V) unterworfen (vgl. § 2 DSG M-V). Eine unterschiedliche Behandlung öffentlicher Stellen wäre mit dem Recht auf informationelle Selbstbestimmung in diesem Kontext nicht zu vereinbaren und den Betroffenen kaum vermittelbar. Ebenso unterfallen die Notare in Mecklenburg-Vorpommern unserer Kontrollkompetenz gemäß § 30 DSG M-V. In diesem Rahmen berücksichtigt der Datenschutzbeauftragte selbstverständlich auch die bereichsspezifischen Vorschriften der BNotO.

Im Übrigen erscheint es auch fraglich, ob die beabsichtigte Datenschutzaufsicht ausschließlich durch die in § 92 BnotO genannten Stellen der Justizverwaltung mit den Vorgaben des Urteils des Europäischen Gerichtshofs (EuGH) vom 9. März 2010 - C-518/07 - übereinstimmt. Die Große Kammer hatte in dem Urteil festgestellt, dass die EU-Datenschutzrichtlinie die völlige Unabhängigkeit der Arbeit der zuständigen datenschutzrechtlichen Kontrollstellen vorschreibe. Die Stellen der Justizverwaltung unterstehen in Ausübung ihrer Funktion selbst der Dienstaufsicht durch die übergeordneten Organe der Justizverwaltung. Eine völlige Unabhängigkeit in der Wahrnehmung der Aufgaben der Datenschutzkontrolle ist daher bei diesen nicht gewährleistet.

Auch die weitere Begründung, eine parallele und damit doppelte Kontrolle durch Dienstaufsicht und den Landesdatenschutzbeauftragten sei unnötig und im Hinblick auf das Recht auf informationelle Selbstbestimmung problematisch, überzeugt nicht. Die Kontrolle durch den Landesbeauftragten betrifft die Datenverarbeitung der Notare und dient damit gerade dem Schutz der Betroffenen hinsichtlich ihres Rechts auf informationelle Selbstbestimmung. Zudem dürften die mit der Dienstaufsicht betrauten Stellen der Justizverwaltung ihren Fokus der Aufsicht regelmäßig auf andere Gesichtspunkte der Notartätigkeit legen, wohingegen der Landesdatenschutzbeauftragte sich speziell und ausschließlich mit Gesichtspunkten des Datenschutzes befasst.

Erhebliche Bedenken bestehen auch gegen die Regelung, dass Auskunfts- und Einsichtsrechte in einer Rechtsverordnung geregelt werden sollen. Das Auskunftsrecht der Betroffenen ist wesentlicher Bestandteil des Rechts auf informationelle Selbstbestimmung. Wenn es dazu Beschränkungen geben soll, muss der Rahmen dazu im Gesetz selbst geregelt sein, vergleiche hierzu die vom Bundesverfassungsgericht entwickelte Wesentlichkeitstheorie, BVerfGE 49,168,181. In der jetzigen Form erscheint die Verordnungsermächtigung nicht verfassungskonform.

Wir haben unser Justizministerium darum gebeten, die Anregungen und Empfehlungen bei den anstehenden Gesetzesberatungen mit zu berücksichtigen. Das Ministerium hat uns mitgeteilt, dass es in den Arbeitsgruppensitzungen zunächst darum gegangen sei, ein Scheitern des Vorhabens aus finanziellen Gründen zu verhindern. Man werde jedoch die Belange des Datenschutzes berücksichtigen.

5.1.2 Forschungsprojekt zum Warnschussarrest

Das Kriminologische Forschungsinstitut Niedersachsen (KFN) ist vom Bundesjustizministerium beauftragt worden, die neue jugendstrafrechtliche Sanktionsmöglichkeit des Jugendarrestes neben einer Jugendstrafe umfassend zu untersuchen.

Das Forschungsinstitut hat die Datenschutzbeauftragten des Bundes und der Länder um Stellungnahme gebeten. Wir haben uns wie folgt geäußert:

Die Auswertung der Verfahrensakten soll vor Ort durch Rechtsreferendare erfolgen. Bei früheren Justizforschungsvorhaben haben wir uns damit einverstanden erklärt, dass eine aufwendige Anonymisierung durch einen Mitarbeiter des Forschungsinstituts erfolgen darf. Voraussetzung ist, dass der betreffende Mitarbeiter nicht an der weiteren Durchführung des Forschungsvorhabens beteiligt ist und vor der Aufnahme seiner Tätigkeit die erforderliche Verpflichtungserklärung auf das Datengeheimnis abgibt. Grund hierfür ist der Umstand, dass dieses von der aktenführenden Stelle wegen der ohnehin schon bestehenden Arbeitsbelastung der Justiz nicht geleistet werden kann. Diese Verfahrensweise wird auch bei dem vorliegenden Forschungsprojekt befürwortet.

Unklar war zunächst, in welcher Form die Auswertung der Akten erfolgen soll, das heißt, welche Daten - personenbezogen - aus den Jugendstrafakten konkret erhoben werden. Bei der schriftlichen Fragebogenerhebung sind sämtliche Probanden ausdrücklich in einem Informationsanschreiben darauf hinzuweisen, dass die Teilnahme an der Befragung freiwillig ist. Eine Rechtsgrundlage für eine Pflicht zur Teilnahme an der Befragung besteht nicht.

Die Auskünfte der Experten haben ohne jeden Bezug zu bestimmten Personen zu erfolgen. Die Freiwilligkeit der Teilnahme und die schriftliche Aufklärung darüber gelten insbesondere auch für die schriftliche Befragung von Warnschussarrestanten sowie für die geplante persönliche Befragung von Inhaftierten.

Das KFN hat mitgeteilt, dass die Daten aus den persönlichen Interviews mit Bediensteten und Inhaftierten der Arrestanstalten, die in den gezogenen Landgerichtsbezirken liegen, hinreichend anonymisiert werden, sodass Rückschlüsse auf einzelne Personen nicht mehr möglich seien. Unsere Hinweise zur Freiwilligkeit der Teilnahme und die informierte schriftliche Einwilligungserklärung wurden akzeptiert. Hinsichtlich der Auswertung der Strafverfolgungsstatistik seien die Einzeldatensätze bereits anonymisiert. Eine De-Anonymisierung soll lediglich auf Ebene der Landgerichtsbezirke erfolgen; eine Identifizierbarkeit auf Personen-Ebene sei weiterhin ausgeschlossen.

Mit dieser Vorgehensweise waren wir einverstanden.

5.1.3 Öffentlichkeitsfahndung in sozialen Netzwerken im Internet

Die Justizministerkonferenz hat in ihrer 84. Sitzung im Juni 2013 einen Beschluss zur Öffentlichkeitsfahndung in sozialen Netzwerken im Internet gefasst. Sie befürwortet ebenso wie die Innenministerkonferenz grundsätzlich die Nutzung sozialer Netzwerke zu diesem Zweck. Zur Umsetzung dieses Beschlusses wurde im Jahr 2014 der Entwurf für die Änderung der Anlage B der Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) zu Ziffer 3.2 „Nutzung des Internets“ vorgelegt.

Die Justizministerkonferenz hat ihren Strafrechtsausschuss gebeten, vor einer Umsetzung der Empfehlungen die Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu beteiligen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich auf ihrer Sitzung am 27. und 28. März 2014 in einer Entschließung (https://www.datenschutz-mv.de/datenschutz/themen/beschlue/87_DSK/Ent_Fahndung.pdf) kritisch geäußert. Sie hat darauf hingewiesen, dass eine Nutzung sozialer Netzwerke privater Betreiber wie Facebook zur Öffentlichkeitsfahndung aus datenschutzrechtlicher Sicht sehr problematisch ist. Durch die weltweit recherchierbare Veröffentlichung von Fahndungsdaten wird in weitaus schwerwiegenderer Weise in die Grundrechte Betroffener (Tatverdächtiger oder auch Zeugen) eingegriffen, als dies bei der Nutzung klassischer Medien der Fall ist. So sind im Internet veröffentlichte Daten einer Fahndungsausschreibung praktisch nicht mehr zu löschen.

Auch der Strafrechtsausschuss geht davon aus, dass soziale Netzwerke nur dann für Zwecke der Fahndung genutzt werden sollten, wenn im Einzelfall eine schwerwiegende Straftat aufgeklärt werden soll und andere Maßnahmen, die den Tatverdächtigen oder andere Betroffene weniger beeinträchtigen würden, keinen Erfolg versprechen. Es müssen jedoch auch verfahrensrechtliche Vorkehrungen dazu getroffen werden. Durch entsprechende Umsetzungsregelungen müssen Staatsanwaltschaften verpflichtet werden, bereits im Antrag auf richterliche Anordnung der Maßnahme die Art, den Ort, den Umfang und die Dauer der Öffentlichkeitsfahndung konkret anzugeben. Dies umfasst insbesondere die ausdrückliche Angabe, ob und warum die Anordnung auch die Öffentlichkeitsfahndung in sozialen Netzwerken umfassen soll.

In dem Vorschlag des Strafrechtsausschusses heißt es weiter, dass „insbesondere auch zu prüfen ist, ob von der Bereitstellung etwaiger Kommentierungsfunktionen abzusehen ist“. Diese Formulierung ist den Datenschutzbeauftragten zu schwach. Geben Nutzer und Nutzerinnen in Nutzerkommentaren öffentlich Spekulationen, Behauptungen und Diskriminierungen ab, beeinträchtigt dies die Persönlichkeitsrechte der Betroffenen erheblich. Derartige Kommentarfunktionen sind in den von den Ermittlungsbehörden betriebenen Angeboten weder geeignet noch erforderlich, um die behördlichen Aufgaben zu erfüllen. Wir fordern daher, die Kommentarfunktion abzuschalten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert sicherzustellen, dass
- die zur Öffentlichkeitsfahndung verwendeten personenbezogenen Daten von den Strafverfolgungsbehörden ausschließlich auf im eigenen Verantwortungsbereich stehenden Servern gespeichert und verarbeitet werden, nicht hingegen auf Servern privater Anbieter,
- die Weitergabe und der automatisierte Abruf der personenbezogenen Daten aus dem Internet durch Web-Crawler und ähnliche Dienste soweit als technisch möglich verhindert werden,
- die Kommunikation zwischen den Strafverfolgungsbehörden und den Nutzern nur außerhalb der sozialen Netzwerke erfolgt.

Um Fragen der Öffentlichkeitsfahndung in sozialen Netzen auch aus medienwissenschaftlicher Seite bewerten zu lassen, haben wir das Institut für Sprache und Kommunikation des Fachgebietes Medienwissenschaft bei der Technischen Universität Berlin Mitte 2014 gebeten, das Thema aus wissenschaftlicher Sicht zu untersuchen. Die Forscher legten ihre Ergebnisse Anfang Oktober 2014 vor (https://www.datenschutz-mv.de/datenschutz/publikationen/informat/onlinefahnd/onlinefahnd.pdf). Der Bericht kommt zwar zum Ergebnis, dass Öffentlichkeitsfahndung in sozialen Netzwerken aufgrund verschiedener Netzwerkeffekte durchaus geeignet ist, um Fahndungserfolge zu erzielen, und dass sie auch wirkungsvoller als Offline-Fahndung sein kann. Der Bericht bestätigt aber auch die Bedenken der Datenschutzbeauftragten von Bund und Ländern, indem er die Angemessenheit derartiger Fahndungsmethoden angesichts der damit verbundenen Risiken für die Betroffenen in Frage stellt. Die 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer Sitzung im Oktober 2014 den Forschungsbericht zur Kenntnis genommen und festgestellt, dass die datenschutzrechtliche Bewertung der Öffentlichkeitsfahndung in sozialen Netzen durch die Argumente des Gutachtens weiter unterstützt wird. Der Konferenzvorsitzende hat daraufhin das Gutachten dem Strafrechtsausschuss der Justizministerkonferenz zur Verfügung gestellt und darum gebeten, auch die dort vorgebrachten Argumente bei der Neuregelung der Ziffer 3.2. „Nutzung des Internets" der Anlage B zu den RiStBV zu berücksichtigen.

Nach derzeitigem Kenntnisstand soll die Änderung der Anlage B der RiStBV zu Ziffer 3.2 „Nutzung des Internets“ im Frühjahr 2016 in der Fassung des Entwurfs von 2014 verabschiedet werden. Weder die Empfehlungen der Datenschutzbeauftragten noch die Hinweise aus wissenschaftlicher Sicht wurden bisher ausreichend berücksichtigt.

5.1.4 Anti-Doping-Gesetz

Zur Stellungnahme lag uns der Entwurf zum Gesetz zur Bekämpfung von Doping im Sport vor. Mit dem Gesetz soll eine Gesetzesgrundlage für die informationellen Maßnahmen bei der Durchführung von Doping-Kontrollen in Deutschland geschaffen werden. In einer gemeinsamen Stellungnahme der Datenschutzaufsichtsbehörden von Berlin, Mecklenburg-Vorpommern, Rheinland-Pfalz und Schleswig-Holstein stellten wir folgende Kritikpunkte fest:

- Der Gesetzgeber verweist bezüglich der Verarbeitung von personenbezogenen Daten der Sportlerinnen und Sportler lediglich auf ein „Dopingkontrollsystem“. Die Ausgestaltung dieses Systems wird vollständig nichtstaatlichen Organisationen wie der National Anti Doping Agentur Deutschland (NADA) und der World Anti-Doping Agency (WADA) überlassen, sodass diese die Datenverarbeitung nahezu ohne gesetzliche Vorgaben steuern können.
- Es besteht keine Regelung zu zwingend erforderlichen Datenübermittlungen.
- Es ist keine strenge Zweckbindung der erhobenen Gesundheitsdaten und der anderen sensiblen Daten vorgesehen, auch an der verfassungsrechtlich geforderten Transparenz für die Betroffenen fehlt es.
- Verfahrensrechtliche Sicherungen der Betroffenenrechte (Auskunft, Berichtigung, Sperrung, Löschung, Benachrichtigung, Widerspruch) fehlen - insbesondere auch gegenüber NADA und WADA und beim globalen Datenaustausch.
- Für die vorgesehene internationale Verarbeitung der sensiblen personenbezogenen Daten fehlen technisch-organisatorische Maßnahmen zur Sicherung.

Zwar wird die Notwendigkeit eines internationalen Doping-Kontrollsystems durch die Datenschutzbehörden anerkannt, jedoch muss dieses den rechtsstaatlichen Anforderungen, die in Deutschland bestehen, genügen. Dementsprechend muss das Anti-Doping-Gesetz die Persönlichkeitsrechte, die Würde und die Intim- und Privatsphäre der Sportlerinnen und Sportler wahren.

Der Staat hat gegenüber den Sportlerinnen und Sportlern eine Schutzpflicht, aus der sich ergibt, dass wesentliche datenschutzrechtliche Fragen der Dopingbekämpfung rechtsstaatlich und unter Achtung der Privatsphäre der Betroffenen geregelt werden.

Das Gesetz wurde mittlerweile vom Bundestag verabschiedet und soll ab dem 1. Januar 2016 in Kraft treten. Die Hinweise der Datenschutzbehörden wurden in dem Gesetz jedoch nicht berücksichtigt.

5.1.5 Auskunft an Datenschutz-Aufsichtsbehörde ist verpflichtend

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern kontrolliert nach § 38 Abs. 1 Bundesdatenschutzgesetz (BDSG) die Einhaltung des Bundesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz. Daher haben die der Kontrolle der Aufsichtsbehörde unterliegenden Stellen der Aufsichtsbehörde gemäß § 38 Abs. 3 BDSG auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen.

Im Berichtszeitraum wurden neun Ordnungswidrigkeitsverfahren eingeleitet, weil von verantwortlichen Stellen keine bzw. nicht ausreichende Auskunft erteilt wurde. Zumeist handelte es sich dabei um Auskünfte über Videoüberwachungsanlagen.

Den Beteiligten ist oft nicht klar, dass die Nichterteilung von Auskünften ebenso wie eine unvollständige und verspätete Auskunft gegenüber der Aufsichtsbehörde den Bußgeldtatbestand nach § 43 Abs. 1 Nr. 10 BDSG erfüllt und damit eine Ordnungswidrigkeit darstellt.

Nachdem die Auskunft vollständig nachgereicht worden war, konnten sechs der eingeleiteten Ordnungswidrigkeitsverfahren wieder eingestellt werden.

Bei drei Ordnungswidrigkeitsverfahren dagegen musste ein Bußgeld verhängt werden.

In einem Verfahren wurde gegen den Bußgeldbescheid Einspruch eingelegt und die Sache daher an das zuständige Amtsgericht abgegeben.

5.2 Polizei

5.2.1 Gemeinsame Telekommunikationsüberwachung der norddeutschen Küstenländer

Das Ministerium für Inneres und Sport Mecklenburg-Vorpommern hat uns den Entwurf des Gesetzes zum Staatsvertrag über die Einrichtung und den Betrieb eines Rechen- und Dienstleistungszentrums zur Telekommunikationsüberwachung der Polizeien im Verbund der norddeutschen Küstenländer und den Staatsvertrag selbst zur Stellungnahme übersandt.

Vertragspartner sind die Freie Hansestadt Bremen, die Freie und Hansestadt Hamburg, das Land Mecklenburg-Vorpommern, das Land Niedersachsen und das Land Schleswig-Holstein.

Die Vertragspartner verpflichten sich, ein gemeinsames Rechen- und Dienstleistungszentrum (RDZ) einzurichten als eigenständige Organisationseinheit des Landeskriminalamts Niedersachsen. Das RDZ soll für die Vertragspartner die technische Umsetzung strafprozessualer Telekommunikationsüberwachungs-Maßnahmen durchführen. Weiterhin soll das RDZ die Vertragspartner bei der Erhebung und Verarbeitung von Inhalts-, Verkehrs- und Bestandsdaten unterstützen. Entsprechendes gilt für Maßnahmen zur Gefahrenabwehr, soweit es das jeweilige Landesrecht erlaubt.

Anlass für den Staatsvertrag sind laut dessen Präambel die mit der progressiven Verwendung digitaler Medien verbundenen besonderen Herausforderungen für die Sicherheitsbehörden. Wegen des technischen, finanziellen, personellen und organisatorischen Aufwands sei die Schaffung kooperativer Strukturen notwendig, um künftig Maßnahmen der Telekommunikationsüberwachung durch die Polizeien der norddeutschen Küstenländer durchführen zu können.

Da alle Datenschutzbeauftragten der norddeutschen Küstenländer gleichermaßen betroffen sind, haben sie eine gemeinsame Stellungnahme abgegeben. Es geht im Wesentlichen um folgende Punkte:

Anbindung des RDZ beim Landeskriminalamt Niedersachsen
Die vorgesehene Einbindung des RDZ als eigenständige Organisationseinheit in das Landeskriminalamt (LKA) Niedersachsen ist aus datenschutzrechtlicher Sicht mit größeren Herausforderungen verbunden als die Errichtung einer eigenständigen Behörde. Letztere würde bereits organisatorisch eine größere Neutralität bieten können. Durch die vorgesehene Struktur wird das LKA Niedersachsen faktisch über sämtliche Daten aus Telekommunikationsüberwachungen der beteiligten Länder verfügen. Hier muss nicht nur technisch, sondern auch organisatorisch eine strikte Trennung zwischen dem LKA Niedersachsen und dem gemeinsamen RDZ sichergestellt sein. Umso wichtiger ist bei der vorgesehenen Organisationsstruktur die Bedeutung der Beteiligung der Länder an der Errichtung, Ausgestaltung und dem Betrieb des gemeinsamen RDZ. Hier räumt der Staatsvertrag den Ländern Beteiligungsrechte bei den wesentlichen Gestaltungsentscheidungen ein, etwa beim Betriebskonzept, dem Personalkonzept, einschließlich Bestellung von Leitung und Stellvertretung, beim Budget für Investitionen und Betriebs- und Personalkosten, dem Datenschutzkonzept und dem Konzept zur Informationssicherheit. Hierüber entscheiden die Länder teilweise einstimmig, teilweise mehrheitlich.

Anders ist die Ausgestaltung der Kontrolle durch die Länder zu beurteilen. Auffällig ist, dass den Entscheidungsbefugnissen der Länder bei der Errichtung und Gestaltung keine Beteiligungsrechte bei der Umsetzung dieser Konzepte und Maßnahmen gegenübergestellt sind. Die Fach- und Rechtsaufsicht über das RDZ ist im Staatsvertrag nicht geregelt. Die Weisungsbefugnis der Länder als Auftraggeber des RDZ kann die fehlende Aufsicht nicht ersetzen.

Einbindung der Landesbeauftragten für Datenschutz
Die Regelung in Artikel 3 des Entwurfs für den Staatsvertrag wird so verstanden, dass das RDZ unmittelbar der Kontrolle durch die Landesdatenschutzbeauftragten aller beteiligten Länder unterliegt, soweit es für diese Länder Maßnahmen durchführt.
Die Landesbeauftragten für Datenschutz regen an, dass im Staatsvertrag in Artikel 8 eine Regelung über ihre Beteiligung bei geplanten Entscheidungen des Beirats aufgenommen wird, die Auswirkungen auf Datenschutz und Datensicherheit haben können. Die Beteiligung sollte in Form einer Unterrichtung mit der Gelegenheit zur Stellungnahme erfolgen.

Informationssicherheit
Die Landesbeauftragten für Datenschutz begrüßen, dass für das RDZ ein hoher Standard für die Datensicherheit festgelegt werden soll und die bisherigen zahlreichen Hinweise und Anregungen der Datenschutzbehörden zu rechtlichen und technisch-organisatorischen Fragen der Verfahrensgestaltung des bisherigen TKÜ-Verfahrens des LKA Niedersachsen aufgegriffen wurden bzw. werden sollen. Um Flexibilität für künftige Änderungen des vorgesehenen Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bzw. die Einführung gänzlich neuer Standards zu schaffen, sollte jedoch eine neutrale Formulierung gewählt werden. Der konkrete BSI-Standard sollte lediglich in der Begründung als Erläuterung des aktuellen Stands der Technik angeführt werden.

Inzwischen ist der Entwurf des Staatsvertrages überarbeitet worden und enthält nunmehr alle Empfehlungen der Datenschutzbeauftragten. Endgültig ist der Vertragstext jedoch noch nicht. Voraussichtlich wird das Kabinett im Januar 2016 über den Staatsvertrag entscheiden sowie nach dessen Zeichnung über das dazugehörige Zustimmungsgesetz mit anschließender Zuleitung an den Landtag.

5.2.2 Neue Richtlinien für die erkennungsdienstliche Behandlung

Das Landeskriminalamt Mecklenburg-Vorpommern (LKA M-V) hatte uns im Mai 2015 den Entwurf der Erkennungsdienstlichen Richtlinien des Landes Mecklenburg-Vorpommern (ED-Richtlinien) übersandt. Wir haben uns dazu wie folgt geäußert:

Eine erkennungsdienstliche Behandlung (ED-Behandlung) nicht tatverdächtiger Kinder zur Identitätsfeststellung, wenn und soweit dies zur Aufklärung einer Straftat geboten ist, halten wir generell für datenschutzrechtlich höchst bedenklich und unverhältnismäßig. Sie kann auch nicht davon abhängig gemacht werden, ob Kinder sich dagegen aussprechen oder nicht. Wir haben daher vorgeschlagen, dass der Punkt gestrichen wird.

Bei der Zusammenstellung der Wahllichtbildvorlage (WLV) kann - anstatt ein Lichtbild der betroffenen/beschuldigten Person aus der Zentralen Lichtbilddatei des Landes (ZLD) zu verwenden - auch ein Passbild des Beschuldigten verwandt werden. Zu einem solchen Fall hatten wir in der Vergangenheit eine Petition. Es verhielt sich so, dass anderen Zeugen innerhalb einer WLV mehrere Fotos aus dem ZLD vorgelegt wurden, zum Beschuldigten jedoch ein Passbild. Der Petent war der Auffassung, dass das Foto zu seiner Person (Passbild) optisch aus der WLV heraussteche (anderer Hintergrund, anderer Gesichtsausdruck). Er sah darin eine Beeinflussung des Zeugen. Seitens der Polizei wurde argumentiert, dass es sich bei der Verwendung des Passbildes um ein milderes Mittel im Verhältnis zur erkennungsdienstlichen Behandlung handele.

Im konkreten Fall wurde das Passbild durch das zuständige Einwohnermeldeamt „im Rahmen der Amtshilfe“ übermittelt und für die Erstellung der Wahllichtbildvorlage in das Täterlichtbildsystem (TLBS) eingepflegt. Das TLBS sei dabei so eingerichtet, dass in solchen Fällen das eingepflegte Lichtbild nach 24 Stunden automatisch gelöscht werde. Auch wenn die Polizei meint, bei dieser Vorgehensweise handele es sich um „ein milderes Mittel“, so ist dies aus datenschutzrechtlicher Sicht durchaus problematisch, da der Beschuldigte nichts davon erfährt, dass er in einer Wahllichtbildvorlage auftaucht. Dies hatte er erst dadurch erfahren, dass sein Rechtsanwalt Einblick in die Ermittlungsakte genommen hatte.

Bei einer erkennungsdienstlichen Behandlung kann der Betroffene in etwa abschätzen, was auf ihn zukommt. Zudem sehen wir die Gefahr der Beeinflussung von Zeugen aufgrund der unterschiedlichen optischen Wirkung des Passbildes. Des Weiteren war fraglich, ob sich das Einwohnermeldeamt auf eine zulässige Rechtsgrundlage zur Datenübermittlung stützen konnte. Insofern hatten wir das LKA M-V darum gebeten, den Punkt noch einmal zu überprüfen.

Hinsichtlich der Berichtigung, Sperrung und Löschung der ED-Daten hatten wir empfohlen, die einschlägigen Regelungen der Strafprozessordnung (StPO) und des Sicherheits- und Ordnungsgesetzes (SOG M-V) in der Richtlinie konkret zu benennen.

Die Richtlinie wird erst im Jahr 2016 in Kraft gesetzt werden.

5.2.3 Neue Richtlinie zur Funkzellenabfrage

Das Landeskriminalamt Mecklenburg-Vorpommern (LKA M-V) hat uns im Oktober 2014 den Entwurf der Richtlinie zur Funkzellenabfrage und -auswertung durch die Polizei übersandt.

Die Funkzellenabfrage ist eine verdeckte, unter grundsätzlichem Richtervorbehalt stehende Ermittlungsmaßnahme zum Zweck der Strafverfolgung, die nur im Fall einer Straftat von erheblicher Bedeutung in Betracht kommt. Unter Beachtung der strengen Voraussetzungen des § 100 g Strafprozessordnung (StPO) können mit einer Funkzellenabfrage alle Verkehrsdaten von den Telekommunikations-Diensteanbietern angefordert werden, die in einem räumlichen und zeitlich hinreichend bestimmten Telekommunikationsbereich angefallen sind. Ziel der Abfrage ist es, durch die Auswertung der übermittelten Verkehrsdaten Täterhinweise zu erlangen.

Die Funkzellenabfrage ist damit eine Maßnahme mit einer großen Streubreite, in die auch viele Unbeteiligte hineingeraten können. Daher kam es uns bei der Stellungnahme darauf an, auf Folgendes aufmerksam zu machen:

- Schon vor der Abfrage von Funkzellendaten ist grundsätzlich eine Funkzellenbestimmung/-vermessung durchzuführen. Sie darf nur unterbleiben, wenn ihre Durchführung tatsächlich unmöglich ist oder wenn wegen der Unaufschiebbarkeit der Maßnahme ansonsten ein Beweismittelverlust droht. Unterbleibt eine Funkzellenbestimmung/-vermessung, ist die räumliche Ausdehnung durch eine möglichst exakte Bezeichnung der Örtlichkeit auf das nach dem Grundsatz der Verhältnismäßigkeit unabdingbare Mindestmaß zu beschränken.
- Eine vermutete Fahrtstrecke als Kriterium für eine Funkzellenabfrage zu werten, ist aus datenschutzrechtlicher Sicht nicht mit den in der Richtlinie angeführten Verhältnismäßigkeitserwägungen zu vereinbaren. Es bestünde die Gefahr, dass - je nachdem, wie viele Kilometer eine Fahrtstrecke beträgt - unter Umständen mehrere Funkzellen großflächig abgefragt und hinsichtlich der Verkehrsdaten ausgewertet werden.
- In der Richtlinie ist vorgesehen, dass im Ergebnis der Auswertung der Funkzellendaten durch die sachbearbeitende Dienststelle ein Auswertebericht in Papierform gefertigt werden soll, der dann Gegenstand der Verfahrensakte der Staatsanwaltschaft sein soll. Aus datenschutzrechtlichen Erwägungen halten wir es für erforderlich, dass die sachleitenden Staatsanwaltschaften in Abstimmung mit den datenverarbeitenden Polizeidienststellen frühzeitig Konzepte zur frühestmöglichen Reduzierung von durch nichtindividualisierte Funkzellenabfragen erhobenen Verkehrsdaten auf das zur Strafverfolgung erforderliche Maß zu erstellen und zukünftig anzuwenden.
- Zusätzlich könnten Kriterien, die nach kriminalistischer Erfahrung auf die Durchführung von Straftaten hindeuten, entwickelt werden, um den Restdatenbestand zu verkleinern, vergleiche § 5 Abs. 1 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V). Die zur Strafverfolgung nicht erforderlichen, das heißt die nach einer Verkleinerung des Datenbestandes überzähligen Verkehrsdaten, sind unverzüglich zu löschen. Sie sind nach § 101 Abs. 8 Satz 1 StPO „zur Strafverfolgung und für eine etwaige gerichtliche Überprüfung der Maßnahme nicht mehr erforderlich“. Wegen der Gefahr einer „Konfliktverteidigung“ im Gerichtsverfahren könnte eine Rohdatendatei, deren Daten gesperrt werden müssen und die physisch getrennt zu halten und besonders zu sichern ist, weiterhin der Staatsanwaltschaft zur Verfügung stehen.

Die Richtlinie ist bis jetzt noch nicht in Kraft gesetzt worden.

5.2.4 Verschlüsselung bei Anfragen der Polizei nach dem Telekommunikationsgesetz (TKG)

Ein E-Mail-Dienste-Anbieter hat sich bei uns darüber beschwert, dass die Landespolizei Mecklenburg-Vorpommern eine Anfrage nach § 113 Telekommunikationsgesetz (TKG) als unverschlüsselte E-Mail an den Provider gestellt hat. Außerdem war diese Anfrage nicht über die polizeieigene Domain @polmv.de erfolgt, sondern über die Domain eines privaten Anbieters.

Anbieter von Telekommunikationsdiensten sind nach § 113 TKG verpflichtet Ermittlungsbehörden im Sinne von § 113 Abs. 3 TKG Auskunft über gespeicherte Daten zu den Nutzern auf Anfrage mitzuteilen.

Diese Anfragen sind jedoch so zu stellen, dass die in der E-Mail vorkommenden personenbezogenen Daten keinem Unbefugten zugänglich werden können. Da die E-Mail an sich keine sichere Kommunikationsart darstellt, käme sie nur mit einer Verschlüsselung in Betracht, siehe dazu auch Punkt 4.1.12.

Eine solche Anfrage enthält in der Regel personenbezogene Daten wie Vor- und Zunamen oder die IP-Adresse des Gerätes, welches der Betroffene genutzt hat. Auch die Tatsache, dass die Person unter Verdacht steht, eine Straftat begangen zu haben, stellt ein schützenswertes Datum dar.

Da die Landespolizei Mecklenburg-Vorpommern auch dem Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) unterliegt, hat sie gemäß § 21 DSG M-V allgemeine Maßnahmen zur Datensicherheit durchzuführen. Diese Maßnahmen haben sich nach dem Stand der Technik, der Schutzbedürftigkeit der Daten und der Zweck-Mittel-Relation zu richten. Besonders im Hinblick auf die hohe Schutzbedürftigkeit der Daten der Betroffenen stellt die verschlüsselte E-Mail ein angemessenes Mittel dar.

Eine nichtverschlüsselte Anfrage kann nicht nur den Betroffenen in seinen Rechten verletzen, sondern auch unter Umständen die durchgeführten Ermittlungen gefährden.

Der E-Mail-Dienste-Anbieter bot auf seiner Internetseite die Möglichkeit zur verschlüsselten Kommunikation an. Nachdem die betreffende Polizeidienststelle zur Stellungnahme aufgefordert wurde, wurde uns mitgeteilt, dass die erste Anfrage an den E-Mail-Dienste-Anbieter zwar unverschlüsselt, eine zweite jedoch verschlüsselt erging. Der Beamte hatte die angebotene Verschlüsselung auf der Webseite zunächst nicht erkannt. Er versuchte den E-Mail-Dienste-Anbieter vorab telefonisch zu erreichen, um mögliche Schlüssel zu erfragen, erreichte jedoch niemanden. Nachdem er das Angebot der Verschlüsselung auf der Webseite des E-Mail-Dienste-Anbieters entdeckte, stellte er seine Anfrage erneut verschlüsselt.

Die Nutzung einer E-Mail-Adresse eines privaten Anbieters begründete der Polizeibeamte damit, dass eine Verschlüsselung über seine polmv.de-Adresse aufgrund der Abgeschlossenheit des Polizeinetzwerks nur unter großem Aufwand möglich ist. Nachdem wir auf das Problem aufmerksam gemacht hatten, wurde die betreffende Polizeidienststelle mit domaineigenen E-Mail-Konten durch das Landesamt für zentrale Aufgaben und Technik der Polizei, Brand- und Katastrophenschutz Mecklenburg-Vorpommern (LPBK M-V) ausgestattet, die eine Verschlüsselung auf einfache Weise zulassen.

Auch das Ministerium für Inneres und Sport Mecklenburg-Vorpommern wurde durch uns auf diesen Vorfall aufmerksam gemacht. Dieses teilte mit, dass bisher keine Hinweise auf vergleichbare Fälle vorliegen und versicherte uns, die Beamtinnen und Beamten der kriminalpolizeilichen Dienststellen erneut für den richtigen Umgang mit personenbezogenen Daten zu sensibilisieren.

5.2.5 Falsche Daten im Elektronischen Vorgangsassistenten (EVA)

Ein Petent berichtete darüber, dass er im Zuge einer allgemeinen Verkehrskontrolle durch die Polizei darauf hingewiesen wurde, dass gegen ihn eine Eintragung wegen eines Betäubungsmittelverstoßes (BTM-Verstoßes) vorliegen würde. Der Grund dieser Eintragung wurde ihm nicht benannt. Außerdem bestritt der Betroffene, einen solchen BTM-Verstoß begangen zu haben. Lediglich an einen BTM-Verstoß eines Freundes, in dessen Zusammenhang er als Auskunftsperson von der Polizei vorgeladen wurde, könne er sich erinnern.

Auf Nachfrage teilte uns das zuständige Polizeipräsidium mit, dass der Betroffene (wie dieser selbst vermutete) in einem Fall als Auskunftsperson zu einem BTM-Verstoß aus dem Jahr 2014 geführt wird. Zu einem anderen Sachverhalt wurde er jedoch auch als Beschuldigter geführt. Dieses Strafverfahren stammt jedoch schon aus dem Jahr 2012.

Zu beiden Fällen hinterlegte die Polizei im Elektronischen Vorgangsassistenten (EVA) personenbezogene Daten. Da das betreffende Strafverfahren gegen den Betroffenen selbst im Jahr 2014 eingestellt wurde und seine personenbezogenen Daten im zweiten Fall (als Nicht-Beschuldigter) Mitte des Jahres 2015 anonymisiert wurden, konnte die Polizei ein Fehlverhalten der Polizeibeamten zum Zeitpunkt der Verkehrskontrolle nicht ausschließen. Vermutet wurde dabei, dass die personenbezogenen Daten des Petenten in unzulässiger Weise aus dem damals noch im Vorgangs- und Auskunftssystem EVA geführten aktuellen Vorgang, bei dem die Anonymisierung erst 2015 erfolgte, stammen und der Petent bei der Verkehrskontrolle damit konfrontiert wurde.

Der Polizeipräsident des verantwortlichen Polizeipräsidiums hat den Vorgang zum Anlass genommen, seine Mitarbeiter hinsichtlich des Umgangs mit EVA weiter zu sensibilisieren.

5.3 Verfassungsschutz

5.3.1 Änderung des Landesverfassungsschutzgesetzes

Das Gesetz zur Änderung des Landesverfassungsschutzgesetzes und des Sicherheitsüberprüfungsgesetzes - LT-Drucksache 6/4430 - wird wohl erst im Jahr 2016 verabschiedet werden. Am 12. November 2015 fand im Landtag eine öffentliche Anhörung dazu statt. Wir haben zu dem Gesetzentwurf wie folgt Stellung genommen:

Der hier vorliegende Gesetzentwurf lehnt sich in zentralen Punkten an den auf Bundesebene beschlossenen Gesetzentwurf „Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes“ an. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat in ihrer Entschließung am 30. September/1. Oktober 2015 in Darmstadt die beschlossene Verfassungsschutzreform abgelehnt (https://www.datenschutz-mv.de/datenschutz/themen/beschlue/90_DSK/Ent_VSReform.html).

Sie hält die Gesetzesänderungen in zentralen Punkten für verfassungsrechtlich äußerst bedenklich. Das betrifft insbesondere die praktisch unbegrenzten Befugnisse der Verfassungsschutzbehörden, personenbezogene Daten in umfassenden zentralen Dateien zu speichern. Insofern setzen sich die verfassungsschutzrechtlichen Bedenken auch im vorliegenden Gesetzentwurf fort.

Generell ist hinsichtlich der verdeckten Ermittlungsmethoden zu kritisieren, dass nicht differenziert wird, dass bestimmte besonders eingriffsintensive Mittel nur gegen einen eng begrenzten Kreis von Betroffenen eingesetzt werden dürfen und mit unterschiedlichen Schwellen ausgestattet werden müssen. Bereits in früheren Stellungnahmen wurde von uns kritisiert, dass der Schutz des Kernbereichs privater Lebensgestaltung fehlt.

Eine aus datenschutzrechtlicher Sicht wesentliche Neuerung ist ein „verdecktes Beobachten und sonstiges Aufklären des Internet, ohne dass der Schutzbereich des Artikel 10 des Grundgesetzes (Brief-, Post-und Fernmeldegeheimnis) berührt ist, insbesondere die verdeckte Teilnahme an den Kommunikationseinrichtungen des Internet und der Suche nach ihnen“. Positiv zu werten ist die Formulierung, dass der Schutzbereich des Artikel 10 Grundgesetz (GG) nicht tangiert werden darf. Jedoch setzt sich der Gesetzentwurf nicht damit auseinander, dass auch das Recht auf informationelle Selbstbestimmung eingeschränkt sein kann.

Das Bundesverfassungsgericht hat in seinem Urteil vom 28. Februar 2008 - Entscheidung zur Online-Durchsuchung - für den Polizeibereich festgestellt, dass Ermittlungstätigkeiten in das Recht auf informationelle Selbstbestimmung eingreifen können, „wenn Informationen, die durch die Sichtung allgemein zugänglicher Inhalte gewonnen wurden, gezielt zusammengetragen, gespeichert und gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet werden und sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt“. Insbesondere handelt es sich um einen Grundrechtseingriff, „wenn die gewonnenen Informationen einzelnen Personen zugeordnet werden können“. Zwar handelt es sich hier nicht um eine Online-Durchsuchung durch die Verfassungsschutzbehörde. Die in dem Urteil dargelegten Entscheidungsgründe sind jedoch auch hier entsprechend heranzuziehen.

Ein Grundrechtseingriff kann nur in solchen Fällen verneint werden, in denen der Staat allgemein zugängliche Inhalte wie jeder Dritte zur Kenntnis nimmt, ohne diese zielgerichtet zu sammeln. Ausweislich der Gesetzesbegründung soll die Verfassungsschutzbehörde jedoch befugt werden, „Erkenntnisse durch die Nutzung des Internet zu sammeln, auch ohne von den Berechtigten hierzu als Kommunikationsteilnehmerin oder Kommunikationsteilnehmer autorisiert zu sein“. Insofern soll gerade zielgerichtet gesammelt werden. Das Sammeln soll verdeckt beziehungsweise unter Pseudonym erfolgen, ohne dass die Kommunikationspartner wissen, dass sich ein Mitarbeiter des Verfassungsschutzes dahinter verbirgt. Das Spektrum dürfte sich auf Internetforen, Chaträume und soziale Netzwerke beziehen. Fraglich ist jeweils, wann ein Vertrauen in einen Gesprächspartner schutzwürdig ist. Es muss anhand der Umstände des Einzelfalls entschieden werden, wann Nutzeraktivitäten besonderes Vertrauen genießen. Folgende Umstände können dafür maßgeblich sein:

- Der Personenkreis, dem Informationen zugänglich werden, ist durch bestimmte Merkmale eingegrenzt.
- Die Anzahl der Personen, denen die Informationen zugänglich werden, ist gering.

Solange der Verfassungsschutz keine positiven Anhaltspunkte dafür hat, dass der Nutzer oder die Nutzer auf Vertrauen verzichten, muss er davon ausgehen, dass ein schutzwürdiges Interesse in die Identität der Kommunikationspartner besteht. Dies gilt umso mehr, je sensibler die Informationen sind, die in diesem Kreis ausgetauscht werden, und je schutzwürdiger der betroffene Personenkreis ist.

Hinsichtlich der Schwere eines solchen Eingriffs ist zu bedenken, dass eine verdeckte Überwachung im Internet gravierender sein kann als eine verdeckte Telekommunikationsüberwachung, die es laut Gesetzestext gerade nicht geben soll. Bei einer Telekommunikationsüberwachung können Inhalte überwacht werden, solange der Telekommunikationsvorgang andauert. Bei einer verdeckten Teilnahme an Internetforen, Chaträumen oder in sozialen Netzwerken können zeitlich weit darüber hinausgehende Inhalte erfasst werden, da die dort eingestellten Inhalte in der Regel nicht flüchtig sind.

Wir haben darauf hingewiesen, dass erhebliche datenschutzrechtliche Bedenken hinsichtlich der Normenklarheit der Gesetzesänderung bestehen. Es wird nicht klar, unter welchen eingrenzenden Voraussetzungen, hinsichtlich welchen Personenkreises die Verfassungsschutzbehörde personenbezogene Daten in Chaträumen, Internetforen oder sozialen Netzwerken erheben, speichern und auswerten darf.

Wir haben daher empfohlen, die Vorschrift tatbestandlich einzugrenzen.

Zwar wurden im Gesetzentwurf die Übermittlungsbefugnisse durch die Verfassungsschutzbehörde an Polizei und Staatsanwaltschaften insgesamt etwas konkreter gefasst. Dabei wurden die Grundsätze des Urteils des Bundesverfassungsgerichts zur Antiterrordatei (BVerfG Urteil vom 24.04.2013) insofern nicht beachtet, als dieses vorgegeben hat, dass die Datenübermittlungen zwischen Nachrichtendiensten und Polizei nicht an vergleichbar niedrigschwellige Voraussetzungen wie der bloßen „Erforderlichkeit“ geknüpft werden dürfen. Genau dies wurde im vorliegenden Entwurf jedoch getan.

Schlussendlich haben wir die Beschränkung der Auskunftsverpflichtung der Verfassungsschutzabteilung kritisiert.

In unserer Kritik, insbesondere hinsichtlich des „verdeckten Beobachtens und sonstigen Aufklären des Internet, ohne dass der Schutzbereich des Artikels 10 des Grundgesetzes (Brief-, Post- und Fernmeldegeheimnis) berührt ist, insbesondere die verdeckte Teilnahme an den Kommunikationseinrichtungen des Internet sowie die Suche nach ihnen“ durch die Verfassungsschutzbehörde, wurden wir durch die Sachverständigen Prof. Dr. Fredrik Roggan, Fachhochschule der Polizei des Landes Brandenburg, und Prof. Dr. Hartmut Aden, Hochschule für Wirtschaft und Recht Berlin, inhaltlich unterstützt. Beide Sachverständige kamen ausweislich des Wortprotokolls der 83. Sitzung des Innenausschusses des Landtages ebenfalls zu dem Ergebnis, dass die neuen Regelungen zur Internetüberwachung viel zu unbestimmt, viel zu unpräzise und auch hinsichtlich der Begrifflichkeiten, die gewählt wurden, irreführend seien im Hinblick auf die Grundrechte, die dort betroffen sind.

Wir appellieren daher an den Landtag, den Gesetzestext entsprechend den von uns gegebenen Empfehlungen zu ändern.

5.4 Kommunales/Meldewesen

5.4.1 Das E-Government-Gesetz des Landes

Im April 2014 hatten wir Gelegenheit, zum „Entwurf des Gesetzes zum Einsatz der Informationstechnologie für die elektronische Verwaltungstätigkeit sowie zur Änderung des Landesverwaltungsverfahrensgesetzes“ Stellung zu nehmen. Mit diesem Gesetz will die Landesregierung die rechtlichen Rahmenbedingungen in der öffentlichen Verwaltung an die fortschreitende Digitalisierung der Gesellschaft anpassen, damit Verwaltungstätigkeiten künftig vollständig elektronisch und effizienter durchgeführt werden können. Das vergleichbare Gesetz auf Bundesebene trat bereits am 1. August 2013 in Kraft.

Damit die Regelungen des entsprechenden Bundesgesetzes auch bei Landesgesetzen angewendet werden können, müssen die Bundesregelungen in Landesrecht überführt werden. Deshalb wurden im Gesetzentwurf des Landes zahlreiche Regelungen des Bundesgesetzes wortgleich übernommen. Unsere Kritik am Bundesgesetz gilt somit in gleicher Weise für das Landesgesetz. Dies betrifft beispielsweise die Nutzung von De-Mail durch die öffentliche Verwaltung und die Änderungen des Verwaltungsverfahrensgesetzes im Bereich der elektronischen Kommunikation. Unsere datenschutzrechtlichen Bewertungen dazu sind im Elften Tätigkeitsbericht unter Punkt 3.2 nachzulesen.

In unserer Stellungnahme zum Landesgesetz haben wir auf folgende weitere Aspekte hingewiesen:

Bei der Nutzung elektronischer Verwaltungsverfahren, die eine Identifizierung der beteiligten Personen erfordert, soll die Identifizierungsfunktion des neuen Personalausweises genutzt werden. Die dafür aus datenschutzrechtlicher Sicht erforderlichen Rahmenbedingungen haben wir ebenfalls im Elften Tätigkeitsbericht, Punkt 6.4.5, ausführlich erläutert. In unserer Stellungnahme haben wir begrüßt, dass dem Zweckverband „Elektronische Verwaltung in Mecklenburg-Vorpommern“ (eGo-MV) ermöglicht wird, eine wesentliche Rolle als Dienstleister zu spielen. Wir haben empfohlen, dass zumindest in der Gesetzesbegründung darauf hingewiesen wird, dass die Aufgabe der Identitätsfeststellung an den eGo-MV nur im Rahmen eines gemeinsamen Verfahrens gemäß § 3 Abs. 10 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) übertragen werden kann. Diese Aufgabe kann als Teilverfahren ausgegliedert werden und in eigener datenschutzrechtlicher Verantwortung des eGo-MV betrieben werden.

Da mit dem neuen Gesetz die Behörden aufgefordert werden, ihre Akten elektronisch zu führen, haben wir darauf hingewiesen, dass insbesondere die datenschutzrechtlichen Anforderungen zu beachten sind, die unter anderem in § 22 Abs. 4 DSG M-V formuliert sind. Dies betrifft insbesondere die Protokollierung der Verarbeitung der Daten. Wir haben vorgeschlagen, in der Gesetzesbegründung auf diese Anforderungen hinzuweisen.

Ein Paragraf des Gesetzentwurfes ist überschrieben mit „Akteneinsicht durch Beteiligte“. Auch wenn die Vorschrift lediglich nur die Art und Weise der Akteneinsicht regelt und kein eigenes Akteneinsichtsrecht schafft, könnte mit dieser Überschrift suggeriert werden, dass dieses Einsichtsrecht lediglich für einen bestimmten Personenkreis, nämlich die an einem Verfahren Beteiligten, gilt. Dieses entspricht jedoch nicht der Intention des durch das Informationsfreiheitsgesetz Mecklenburg-Vorpommern (IFG M-V) definierten Informationszugangsrechts.

Gemäß § 1 Abs. 2 IFG M-V hat jede natürliche und juristische Person des Privatrechts Anspruch auf Zugang zu den bei einer Behörde vorhandenen Informationen. Um etwaige Unklarheiten hinsichtlich der Frage der Anspruchsberechtigung zu vermeiden, haben wir empfohlen, für den entsprechenden Paragrafen die Überschrift „Akteneinsicht“ zu wählen. Dieses würde im Übrigen auch mit den bundesgesetzlichen Regelungen übereinstimmen.

Im Dezember 2015 wurden wir erneut in das Gesetzgebungsverfahren einbezogen. Wir wurden gebeten, eine Stellungnahme zum Gesetzentwurf, nunmehr als „Gesetz zur Förderung der elektronischen Verwaltungstätigkeit in Mecklenburg-Vorpommern und zur Änderung des Landesverwaltungsverfahrensgesetzes (E-Government-Gesetz M-V)“ bezeichnet, abzugeben und an der öffentlichen Anhörung zu diesem Gesetz im Innenausschuss des Landtages Mecklenburg-Vorpommern teilzunehmen.

In diesem Zusammenhang haben wir festgestellt, dass ein Teil unserer oben beschriebenen Empfehlungen im nunmehr vorliegenden Entwurf auf Drucksache 6/4636 vom 27. Oktober 2015 bereits berücksichtigt wurden. So wird in der Begründung zu § 2 Abs. 2 auf die Risiken von De-Mail hingewiesen und die Behörden werden aufgefordert, bei der Übermittlung schützenswerter Daten De-Mail nur mit zusätzlicher Verschlüsselung zu verwenden. Ausdrücklich werden hier Verfahren mit einer standardmäßigen Ende-zu-Ende-Verschlüsselung gefordert. Auf unsere Anregung hin wurde ein Hinweis auf die Handreichung der Bundesdatenschutzbeauftragten zum datenschutzgerechten Umgang mit De-Mail eingefügt. Darüber hinaus wurde unserer Empfehlung gefolgt, in der Begründung zu § 10 Abs. 1 auf die besonderen Anforderungen an die Protokollierung der Verarbeitung elektronisch gespeicherter Daten hinzuweisen, die sich aus § 22 Abs. 4 DSG M-V ergibt.

Im Gesetzestext selbst wurden schließlich unsere Vorschläge zur Rolle des gemeinsamen Verfahrens bei der Identitätsfeststellung bei der Nutzung des neuen Personalausweises und zur Überschrift des Paragrafen Akteneinsicht umgesetzt.

Es blieben jedoch einige Kritikpunkte, die wir im Rahmen der öffentlichen Anhörung wie folgt erläutert haben:

Vom Geltungsbereich dieses Gesetzes werden Hochschulen und Schulen ausgenommen. In Hochschulen und Schulen werden jedoch in zunehmendem Maße Verwaltungsabläufe in elektronischer Form abgebildet. So hat der Bildungsminister angekündigt, eine einheitliche Schulverwaltungssoftware entwickeln zu lassen und den Schulen in Mecklenburg-Vorpommern anzubieten. Es ist somit absehbar, dass die Mehrzahl von Verwaltungstätigkeiten (Erteilung von Zensuren, Erstellung von Zeugnissen, Aussprechen von Verweisen usw.) sowie die Kommunikation zwischen Schülerinnen und Schülern, Eltern und Lehrkräften künftig in elektronischer Form erfolgen werden. Hierfür sind gesetzliche Regelungen erforderlich. Einige dieser Regelungen enthält bisher das Verwaltungsverfahrensgesetz (VwVfG M-V) des Landes. So regelt § 3a Abs. 1 VwVfG M-V Fragen der Eröffnung eines Zugangs zur Übermittlung elektronischer Dokumente, § 3b VwVfG M-V den Umgang mit elektronischen Akten und § 3c VwVfG M-V das Übertragen und Vernichten des Papieroriginals, sofern Akten elektronisch geführt werden.

Diese Regelungen werden mit Artikel 2 des Gesetzentwurfs aufgehoben und praktisch wortgleich in das neue E-Government-Gesetz aufgenommen (§§ 2, 10 und 11). Werden nun Hochschulen und Schulen aus dem Geltungsbereich des E-Government-Gesetzes herausgenommen, gelten die für die übrige Verwaltung als erforderlich angesehenen Regelungen beispielsweise für die geplanten Schulverwaltungssysteme nicht. Wir haben daher empfohlen, dass das Gesetz auch für Hochschulen und Schulen gelten soll.

5.4.2 Nutzung des ePost-Briefes in der Kommunalverwaltung

Aus dem kommunalen Bereich erhielten wir die Anfrage, ob der von der Deutschen Post AG (DPAG) angebotene ePost-Brief in der Kommunalverwaltung verwendet werden darf.

Beim ePost-Brief nimmt die DPAG Sendungen auf elektronischem Wege an. In Abhängigkeit von der Erreichbarkeit der Adressatin oder des Adressaten versendet die DPAG den Brief entweder elektronisch oder sie druckt ihn aus, kuvertiert ihn und stellt ihn auf herkömmliche Weise per Briefkasten zu.

Die Anfrage bezog sich auf diesen klassischen Zustellweg und ausdrücklich auch auf Sendungen aus sensiblen Bereichen, wie dem Steueramt oder dem Sozialamt.

Bei der Bearbeitung der Sendungen können Mitarbeiterinnen und Mitarbeiter der DPAG die übergebenen Sendungen einsehen. Unterliegt die Sendung einem besonderen Berufs- oder Amtsgeheimnis, wie dem Steuergeheimnis oder dem Sozialgeheimnis, so muss das entsprechende Fachrecht eine solche Einsichtsmöglichkeit zulassen.

So ist bei kommunalen Abgaben gemäß § 12 Kommunalabgabengesetz (KAG) die Abgabenordnung (AO) das maßgebliche Verfahrensrecht und damit auch die Vorschriften zum Steuergeheimnis nach § 30 AO. Diese Vorschrift sieht eine Offenbarungsmöglichkeit an Dienstleister nicht vor. Bei Daten, die dem Sozialgeheimnis, § 35 Sozialgesetzbuch Erstes Buch (SGB I), unterliegen, ist § 80 Sozialgesetzbuch Zehntes Buch (SGB X) zu beachten. Diese Vorschrift gestattet Sozialleistungsträgern die Datenverarbeitung im Auftrag durch nicht-öffentliche Stellen insbesondere nur dann, wenn beim Auftraggeber sonst Störungen im Betriebsablauf auftreten können oder die übertragenen Arbeiten beim Auftragnehmer erheblich kostengünstiger erledigt werden können.

Ob dies zutrifft, wurde uns in der Anfrage nicht mitgeteilt.

Zusätzlich muss ein Vertrag zur Datenverarbeitung im Auftrag nach § 4 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) geschlossen werden. Darüber hinaus sind die Mitarbeiterinnen und Mitarbeiter der DPAG, die Einsicht in die Sendungen nehmen können, auf das Datengeheimnis nach § 6 DSG M-V und auf die Einhaltung der berührten Berufs- und Amtsgeheimisse zu verpflichten.

Nach den uns vorliegenden Informationen ist die DPAG nur zu einer Verpflichtung gemäß § 6 DSG M-V bereit. Damit darf die Dienstleistung nur für solche Sendungen genutzt werden, die keinem besonderen Berufs- oder Amtsgeheimnis unterliegen.

Inzwischen bietet die DPAG auch einen Dienst an, mit dem Sendungen vollständig elektronisch zugestellt und dabei verschlüsselt übertragen werden, sodass Beschäftigte der DPAG keinen Einblick in die Inhalte nehmen können. Die DPAG bietet dazu die Möglichkeit, Anhänge mithilfe eines asymmetrischen kryptographischen Verfahrens mit dem Schlüssel des Empfängers zu verschlüsseln und einem E-Postbrief beizufügen. Zur Verwaltung der Schlüssel unterhält die DPAG einen eigenen Verzeichnisdienst.

Dieser Zustellweg darf auch für Sendungen genutzt werden, für die besondere Berufs- oder Amtsgeheimnisse gelten. Er wird derzeit jedoch nur größeren Geschäftskunden angeboten. Andere Kundinnen und Kunden können solche Sendungen bislang nur empfangen. Ohne die asymmetrische Verschlüsselung kann bei elektronischer Zustellung ein Zugriff durch DPAG-Beschäftigte nicht ausgeschlossen werden. Deshalb gelten in diesem Fall die oben für den ePost-Brief mit klassischer Zustellung beschriebenen Rahmenbedingungen.

5.4.3 Lücke in Personenstandssoftware wird zu langsam geschlossen

Bereits Ende 2013 haben wir eine schwerwiegende Sicherheitslücke im Verfahren für das Personenstandswesen beanstandet, siehe Elfter Tätigkeitsbericht, Punkt 6.4.6. Durch diesen Mangel konnte es zu besonders schwerwiegenden Auswirkungen bei der unbefugten Nutzung des Verfahrens kommen.

Verantwortlich für den Betrieb der zentralen Teile dieses Verfahrens und somit auch für den fehlerhaft gestalteten Verfahrensteil ist im Wesentlichen der kommunale „Zweckverband elektronische Verwaltung in Mecklenburg-Vorpommern“ (eGo-MV). Zur Behebung des Mangels mussten zentrale Infrastrukturkomponenten ausgetauscht und einzelne Systemteile in allen Standesämtern neu konfiguriert werden. Die zentralen Komponenten mussten im Rahmen einer öffentlichen Ausschreibung neu beschafft werden. Im August 2015 informierte uns der eGo-MV darüber, dass die zentralen Komponenten betriebsbereit wären und erste Standesämter an die neue sichere Infrastruktur angeschlossen worden sind. Bis zum Ende dieses Berichtszeitraumes ist die Umstellung jedoch immer noch nicht in allen Städten und Gemeinden des Landes abgeschlossen.

Es hat somit über eineinhalb Jahre gedauert, eine schwerwiegende Sicherheitslücke in den zentralen Verfahrensteilen des Personenstandswesens zu schließen. Zwei Jahre nach Feststellung des Fehlers gibt es immer noch Standesämter, die von der Sicherheitslücke betroffen sind. Solche Zeiträume sind nicht akzeptabel.

Der eGo-MV berichtete uns davon, dass in mehreren Kommunen die Verantwortlichen für die Verwaltung von kryptographischen Zertifikaten, siehe Elfter Tätigkeitsbericht, Punkt 6.4.6, von Firewallregeln oder von anderen sicherheitskritischen Komponenten und Einstellungen nicht aufzufinden waren oder verzögert reagierten, siehe hierzu auch Punkte 2.2.1 und 3.3. Ferner hätten einige Kommunen noch das völlig veraltete Betriebssystem Windows XP im Einsatz, weshalb sie die neue Lösung nicht nutzen könnten. Solche Missstände müssen in den betroffenen Verwaltungen dringend abgestellt werden.

Die lange Bearbeitungsdauer begründete der eGo-MV auch damit, dass die DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH (DVZ M-V GmbH) als Auftragnehmerin des eGo-MV neue Gerätetechnik in einem Ausschreibungsverfahren beschaffen musste. Außerdem habe der Hersteller des Fachverfahrens für das Personenstandswesen, der Verlag für Standesamtswesen, umfangreiche Updates herausgegeben, die zu bestimmten Stichtagen den Standesämtern zur Verfügung gestellt hätten werden müssen. Solche Umstellungen jeweils zum Jahreswechsel sind in Fachverfahren der öffentlichen Verwaltung durchaus üblich und beanspruchen je nach Umfang einige Tage oder Wochen.

Mit diesen Umständen allein ist die Verfahrensdauer jedoch nicht zu erklären. Wir sind deshalb der Ansicht, dass der eGo-MV nicht genügend personelle Ressourcen zur Verfügung stellt, um ungeplant auftretende Probleme bei Informationssicherheit und technischem Datenschutz in akzeptablen Zeiträumen lösen zu können. Solche Situationen können aber selbst bei sorgfältigster Arbeitsweise und Planung auch künftig nicht vollständig vermieden werden. Wir möchten an dieser Stelle aber ausdrücklich erwähnen, dass die mit dem geschilderten Vorfall befassten Mitarbeiterinnen und Mitarbeiter im eGo-MV und in der DVZ M-V GmbH sehr konstruktiv und engagiert an der Fehlerbeseitigung gearbeitet haben.

Wir empfehlen dem eGo-MV, die erforderlichen personellen Ressourcen bereitzustellen und geeignete Notfallpläne zu entwickeln, um künftig akute Sicherheitsprobleme unverzüglich bewältigen zu können.

5.4.4 Kontrollserie Personenstandswesen

Im Frühjahr und im Sommer 2014 haben wir eine Serie von Kontroll- und Informationsbesuchen durchgeführt, um die Verarbeitung personenbezogener Daten im Personenstandswesen zu prüfen. Der Schwerpunkt lag dabei auf technischen und organisatorischen Datenschutzfragen. Ziel war eine Bestandsaufnahme in einem Verfahren, bei dessen Realisierung die Städte und Gemeinden nicht auf sich allein gestellt waren, sondern umfangreich fachlich unterstützt wurden. An dem Verfahren wirken insbesondere das Ministerium für Inneres und Sport Mecklenburg-Vorpommern, der Zweckverband „Elektronische Verwaltung in Mecklenburg-Vorpommern“ (eGo-MV) als Betreiber zentraler Teile dieses Verfahrens und die landeseigene DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH (DVZ M-V GmbH) als wichtige Auftragnehmerin des eGo-MV mit.

Bereits bei der Konzeption des Verfahrens haben wir diese Stellen beraten, siehe Zehnter Tätigkeitsbericht, Punkt 4.4.4, auch zu den Details des Verfahrens und der Rechtsverhältnisse. Wir besuchten insgesamt vier unterschiedlich große Stadtverwaltungen, den eGo-MV und die DVZ M-V GmbH. Ein konkreter Anlass für diese Besuche bestand nicht. Unsere Aktivitäten im Zusammenhang mit einer schweren Sicherheitslücke im Verfahren des Personenstandswesens, siehe Punkt 5.4.3, liefen nur zufällig parallel. Erkenntnisse aus dieser Besuchsreihe sind in die Planung unseres Projektes „Datenschutz und Informationssicherheit in den Kommunen in Mecklenburg-Vorpommern“, siehe Punkt 2.2.1, eingeflossen.

Während der Kontroll- und Informationsbesuche haben wir einige gravierende Mängel im Verfahrensbetrieb in den besuchten Kommunalverwaltungen festgestellt. Es folgt eine Auswahl aus verschiedenen Bereichen:

- Organisatorischer Datenschutz: Sicherheitskonzepte, Verfahrensbeschreibungen, Freigabeerklärungen und Dienstanweisungen zum Datenschutz waren oft nicht vorhanden, unvollständig oder fehlerhaft, obwohl der eGo-MV den Kommunalverwaltungen umfangreiches Referenzmaterial zur Verfügung gestellt hatte. Verwaltungsweit geltende Rahmensicherheitskonzepte waren nur selten vorhanden.
- Technischer Datenschutz: Es waren Signaturkartenleser mit gebrochenem Siegel im Einsatz. Dies ist unzulässig, denn in solchen Fällen sind Manipulationen nicht sicher auszuschließen. Außerdem wurden Fernwartungszugriffe nicht revisionssicher protokolliert. Teilweise entsprachen Firewalls nicht dem Stand der Technik und Fernwartungssitzungen konnten gestartet werden, ohne dass Nutzerinnen und Nutzer dies bestätigen mussten.
- Baulicher Datenschutz: Serverräume waren unzureichend gegen Einbruch gesichert. Wir fanden beispielsweise Räume mit Leichtbauwänden, ungesicherten Fenstern oder einfachen Bürotüren. Außerdem fanden wir in diesen Räumen immer wieder zu viel brennbares Material, wasserführende Leitungen und Heizkörper oder es fehlten Brand- und Einbruchmeldeanlagen. Darüber hinaus wurden Signaturkarten, Sperrdaten, Backups und weitere sicherheitsrelevante Datenträger nicht immer in ausreichend sicheren Stahlschränken verwahrt.

Unsere Feststellungen und Empfehlungen haben wir den betroffenen Verwaltungen mitgeteilt. Dabei haben wir von Beanstandungen abgesehen, weil der Landtag der Landesregierung im April 2014 bereits einen Prüfauftrag erteilt hatte, der auf die Verbesserung der Informationssicherheit im kommunalen Bereich abzielt, siehe Punkt 2.2.1, und wir den Ergebnissen dieser Prüfung nicht vorgreifen wollten.

Im Rahmen der Besuchsserie haben wir auch erfahren, dass das Ministerium für Inneres und Sport Mecklenburg-Vorpommern bisher keinen Vertrag mit dem eGo-MV zum Betrieb des Sicherungsregisters für das Personenstandswesen geschlossen hat. Hierzu ist das Ministerium aber nach § 1 Sicherungsregisterverordnung (SiRegVO M-V) in Verbindung mit § 4 DSG M-V verpflichtet. Dieser Missstand ist nach unserer Kenntnis zum Ende dieses Berichtszeitraumes immer noch nicht beseitigt.

Wir empfehlen dem Ministerium für Inneres und Sport Mecklenburg-Vorpommern den Abschluss eines Vertrages mit dem eGo-MV zum Betrieb des Sicherungsregisters für das Personenstandswesen nach den Vorschriften zur Datenverarbeitung im Auftrag.

5.4.5 Datenpanne bei der Erstellung eines Adressbuches

Eine Stadt hat ein Adressbuch herausgegeben. In diesem Zusammenhang haben sich einige Bürgerinnen und Bürger dieser Kommune an uns gewandt und um Aufklärung hinsichtlich der Zulässigkeit von Übermittlungen von Meldedaten für dieses Adressbuch gebeten. Hierbei spielte insbesondere das in § 35 Abs. 3 Landesmeldegesetz (LMG) ausgewiesene Widerspruchsrecht eine Rolle. Nach dieser Vorschrift haben Betroffene das Recht, der Übermittlung ihrer Daten (Vor- und Familienname, Doktorgrad und Anschrift) an Adressbuchverlage zu widersprechen. In den betreffenden Fällen wurde denjenigen, die sich an uns gewandt hatten, geraten, von diesem Widerspruchsrecht für künftige Übermittlungen von Meldedaten an Adressbuchverlage Gebrauch zu machen.

Unabhängig hiervon mussten wir einem Zeitungsartikel entnehmen, dass es bei der Auflage des Adressbuches zu einer Datenpanne gekommen ist. Konkret soll das besagte Adressbuch auch personenbezogene Daten von Bürgerinnen und Bürgern enthalten haben, für die eine zweijährige Auskunftssperre eingetragen war und deren Angaben nach § 35 Abs. 4 i. V. m. § 34 Abs. 5 LMG nicht hätten übermittelt und in der Folge im Adressbuch veröffentlicht werden dürfen. Eine solche Auskunftssperre wird beispielsweise dann eingetragen, wenn Tatsachen vorliegen, die die Annahme rechtfertigen, dass dem Betroffenen oder einer anderen Person durch eine Melderegisterauskunft eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnlicher schutzwürdiger Interessen erwachsen kann. Da im Ergebnis einer solchen Eintragung keinerlei Melderegisterauskünfte über Einwohner an private Personen erteilt werden dürfen, sind an die Eintragung strenge Voraussetzungen zu stellen. Hieraus wird die Bedeutung dieser Auskunftssperre deutlich, die im vorliegenden Fall für die Betroffenen ausgehebelt wurde.

Die Stadtverwaltung reagierte nach Bekanntwerden des Fehlers sofort und übersandte den Betroffenen ein Informationsschreiben, in dem man sich auch für den Fehler entschuldigte. Gleichzeitig wurden die notwendigen technischen Änderungen in der Bearbeitungssoftware veranlasst.

Die Stadtverwaltung stoppte den weiteren Verkauf des bereits herausgebrachten Adressbuches. Problematisch war dabei allerdings, dass eine Vielzahl an Exemplaren bereits verkauft war.

Da der Adressbuchverlag auf seinem vertraglichen Recht einer Neuherausgabe des Stadtadressbuches bestand, wurde die kommunale Vermögensschadenshaftpflichtversicherung hinzugezogen, die auch bereit war, einen Neudruck zu bezahlen.

Im Ergebnis dieser auch durch die Medien publizierten Datenpanne legten über 800 Bürgerinnen und Bürger Widerspruch gegen eine Meldedatenübermittlung nach § 35 Abs. 3 LMG ein.

5.4.6 Sparsamer Umgang mit Angaben von Antragstellern bei Beschlussvorlagen

Immer wieder tauchen Fragen auf, inwieweit und in welchem Umfang personenbezogene Daten in Beschlussvorlagen von kommunalen Gremien verarbeitet werden dürfen. So hat sich beispielsweise eine Petentin an uns gewandt und mitgeteilt, dass im Zuge eines von ihr gestellten Bauantrages ohne ihre Einwilligung Vorname, Familienname und Wohnadresse veröffentlicht wurden. Dieses erfolgte im Zusammenhang mit der Veröffentlichung der Beschlussvorlage im Internet. Nach entsprechendem Hinweis wurde die Beschlussvorlage aus der Internetveröffentlichung herausgenommen. Was blieb, war allerdings die Veröffentlichung des Vor- und Familiennamens im Zusammenhang mit der Bekanntmachung der Einladung zu der betreffenden Sitzung im Internet, da auch die Tagesordnung personenbezogene Daten von Antragstellern enthielt.

Grundsätzlich ist es zu begrüßen, dass Bauanträge im öffentlichen Teil einer Gemeindevertretersitzung behandelt und beschlossen werden, da dieses dem in § 29 Abs. 5 Kommunalverfassung Mecklenburg-Vorpommern (KV M-V) ausgewiesenen Grundsatz der Öffentlichkeit von Gemeindevertretersitzungen entspricht.

Sofern eine Einladung beziehungsweise Beschlussvorlage personenbezogene Daten enthält, liegt eine Datenverarbeitung vor. Aus datenschutzrechtlicher Sicht ist hierbei der Grundsatz der Erforderlichkeit zu beachten und einzuhalten. Nicht alle entscheidungserheblichen Angaben, zu denen unter anderem personenbezogene Angaben der Bauantragsteller gehören könnten, sind gleichzeitig erforderliche Daten, die an die Öffentlichkeit beziehungsweise an die Gemeindevertreter zu übermitteln wären. Vielmehr sind nur diejenigen Daten im Vorwege zur Verfügung zu stellen, die auf Seiten der Gemeindevertreter zur Bildung einer (vorläufigen) Meinung und gegebenenfalls zur Vorbesprechung in der Fraktion benötigt werden beziehungsweise zu einer sachgemäßen Entscheidung unbedingt notwendig sind. Hierzu gehören grundsätzlich nicht die personenbezogenen Daten des Bauantragstellers, sondern vielmehr die grundstücksbezogenen Angaben (Gemarkung, Flur, Flurstück).

Von daher sollte jede Kommune genau prüfen, ob die Angabe von personenbezogenen Daten in Beschlussvorlagen und Einladungen zu Gremiensitzungen erforderlich ist. Sollte dies beispielsweise bei Bauangelegenheiten der Fall sein oder aufgrund der geringen Größe der Gebietskörperschaft auch durch grundstücksbezogene Angaben sich eine Personenbeziehbarkeit ableiten lassen, sollte unter Berücksichtigung der in § 29 Abs. 5 KV M-V festgelegten Ausnahmen zum Grundsatz der Öffentlichkeit eine Beratung und Beschlussfassung dieser Angelegenheiten im nicht-öffentlichen Sitzungsteil erfolgen.

5.4.7 Internetveröffentlichung einer Vorschlagsliste ehrenamtlicher Richter

Im Frühsommer 2015 waren für die Wahlperiode 2015 bis 2020 die ehrenamtlichen Richterinnen und Richter für das Oberverwaltungsgericht und die Verwaltungsgerichte Greifswald und Schwerin zu wählen. Die Wahl erfolgt nach den Vorschriften der Verwaltungsgerichtsordnung (VwGO).

Nach § 28 VwGO stellen die Landkreise und kreisfreien Städte hierzu eine Vorschlagsliste auf. Uns lag hierzu eine Petition vor, in der sich darüber beschwert wurde, dass in einem Landkreis die Vorschlagsliste für die ehrenamtlichen Richterinnen und Richter in dem Ratsinformationssystem online veröffentlicht wurde. In dieser Liste waren die Namen, Vornamen, Adressen, Geburtsdaten und der Geburtsort der infrage kommenden ehrenamtlichen Richterinnen und Richter enthalten.

§ 28 VwGO sieht zwar vor, dass die Vorschlagsliste die vorgenannten personenbezogenen Daten (sowie zusätzlich noch die Angabe über den Beruf) enthalten soll, trifft jedoch keine Regelungen zur Veröffentlichung dieser. Im letzten Satz der betreffenden Vorschrift heißt es, dass die Vorschlagslisten dem Präsidenten des zuständigen Verwaltungsgerichts zu übermitteln sind.

Da gemäß § 28 Satz 5 VwGO die jeweiligen Regelungen zur Beschlussfassung der Vertretungskörperschaft unberührt bleiben, haben wir geprüft, ob sich gegebenenfalls eine Veröffentlichung aus den Bestimmungen der Kommunalverfassung Mecklenburg-Vorpommern (KV M-V) ergeben könnte.

Der Beschluss über die Vorschlagslisten wurde im öffentlichen Sitzungsteil beraten. Diese entspricht dem in § 107 Abs. 5 KV M-V verankerten Öffentlichkeitsgrundsatz. Das schließt jedoch nicht automatisch die Veröffentlichung der betreffenden personenbezogenen Daten für die Öffentlichkeit ein. Gemäß der vorgenannten kommunalrechtlichen Bestimmung sind lediglich Zeit, Ort und Tagesordnung der Sitzung des Kreistages rechtzeitig vor der Sitzung öffentlich bekanntzumachen.
Unter Berücksichtigung datenschutzrechtlicher Aspekte haben wir dem Landkreis empfohlen zu prüfen, ob nicht der „geschlossene Teil“ des Ratsinformationssystems bei einer zwingend erforderlichen Übermittlung dieser Vorschlagsliste an die Kreistagsmitglieder zu nutzen wäre. Dieser Bereich ist für einen bestimmten Personenkreis (Mitglieder des Kreistages beziehungsweise der jeweiligen Ausschüsse) nach vorheriger Anmeldung (Nutzerkennung und Passwort) nutzbar. Hiermit wäre zum einen gewährleistet, dass die Beschlussvorlage weiterhin im öffentlichen Sitzungsteil beraten werden kann, und zum anderen würde den schutzwürdigen Interessen der Betroffenen entsprochen werden. Außerdem wäre damit den Vorschriften des § 28 Satz 5 VwGO in Verbindung mit § 107 KV M-V genüge getan, da durch die Übermittlung der personenbezogenen Daten an einen bestimmten Personenkreis (Kreistagsmitglieder) die Wirksamkeitsvoraussetzungen für die Beschlussfassung gegeben wären.

Der Landkreis hat uns mitgeteilt, dass das Innenministerium unseres Landes sich mit uns und dem Justizministerium in dieser Angelegenheit abstimmen will. Ein Ergebnis hierzu liegt noch nicht vor.

5.4.8 Landesgesetz zur Ausführung des Bundesmeldegesetzes

Im Zuge des am 1. November 2015 in Kraft getretenen Bundesmeldegesetzes (BMG) wurde uns durch das Innenministerium unseres Landes der Entwurf eines Ausführungsgesetzes des Landes Mecklenburg-Vorpommern zur Stellungnahme übersandt. Schwerpunkt hierbei war die Neufassung des Landesmeldegesetzes (E-LMG). Grund dieser gesetzlichen Neufassung ist die nicht mehr bestehende Befugnis der Länder, in eigener Kompetenz melderechtliche Regelungen zu erlassen. Das BMG ermächtigt jedoch die Länder zumindest in einem bestimmten Umfang, eigene Regelungen zu erlassen.

Gegen den vorgelegten Gesetzentwurf hatten wir insbesondere zu zwei Punkten erhebliche Bedenken. Dieses betrifft erstens die in § 4 Abs. 1 E-LMG vorgesehene Erweiterung der bundesmelderechtlichen Regelungen bezüglich der Übermittlung von Meldedaten an öffentlich-rechtliche Religionsgesellschaften um die Angabe zu Staatsangehörigkeiten von Familienmitgliedern. In der Gesetzesbegründung wurde hierzu angegeben, dass dieses Datum für entsprechende seelsorgerische und karitative Aufgaben und Angebote relevant sei. Dieses Argument war für uns nicht schlüssig genug, um für diese Datenverarbeitung eine Erforderlichkeit herleiten zu können, da hierbei weniger die Staatsangehörigkeit, sondern der Aspekt der Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgesellschaft im Vordergrund stehen dürfte. Die Frage, welche Staatsangehörigkeit der Betroffene hat, dürfte aufgrund der Vielfältigkeit der Glaubensrichtungen auch unter Personen derselben Staatsangehörigkeit nur eine nachrangige Funktion haben. Wir haben daher empfohlen, auf die Übermittlung der Angabe zur Staatsangehörigkeit an dieser Stelle zu verzichten.

Als zweiten Punkt - und aus unserer Sicht wesentlich problematischer - sahen wir das Bestreben, dass durch § 8 Nr. 3 E-LMG beispielsweise die Möglichkeit geschaffen werden soll, der Verfassungsschutzbehörde des Landes über den Erlass einer Rechtsverordnung das Recht einzuräumen, weitere Daten als im BMG vorgesehen im automatisierten Verfahren abzurufen, wenn und soweit dies für die Aufgabenerfüllung erforderlich ist.

Ursprung dieser Bestrebungen ist offensichtlich ein Beschluss des Arbeitskreises IV der Innenministerkonferenz vom 22. August 2014, der auf Regelungsbedarfe „aller Verfassungsschutzbehörden“ Bezug nimmt. Wir haben das Innenministerium darauf hingewiesen, dass (sofern derartige Regelungswünsche auf Landesebene bestehen) diese Bestimmungen auch im LMG und nicht untergesetzlich normiert werden müssen. Nur eine normenklare gesetzliche Vorschrift, die dem Grundsatz der Verhältnismäßigkeit entspricht, käme dafür in Betracht. Eine untergesetzliche Regelung, die sich im Übrigen einer parlamentarischen Auseinandersetzung mit diesem Thema entziehen dürfte, halten wir im Hinblick auf das Volkszählungsurteil des Bundesverfassungsgerichts vom 15.12.1983 (BVerfGE 65, 1 ff.) für nicht möglich. Das Bundesverfassungsgericht hat seinerzeit festgelegt, dass Beschränkungen des Rechts auf informationelle Selbstbestimmung einer (verfassungsmäßigen) gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben, bedürfen. Diese Vorgaben sind ebenfalls aufgrund der vom BVerfG entwickelten Wesentlichkeitstheorie (BVerfG 49, 168 (181)) zu beachten, die besagt, dass im Bereich der untergesetzlichen Normsetzung „wesentliche Entscheidungen“ durch das Parlament selbst getroffen werden müssen. Dies betrifft insbesondere Grundrechtseingriffe.

Wir empfehlen der Landesregierung, wesentliche Grundsätze im Melderecht normenklar im LMG und nicht untergesetzlich zu regeln.

5.4.9 Was verdienen Geschäftsführer kommunaler Unternehmen?

Eine Kommune in Mecklenburg-Vorpommern beabsichtigte, den Gesellschaftsvertrag einer kommunalen Wohnungsbaugesellschaft unter der Beachtung der Festlegungen der Kommunalverfassung zu ändern. Diese Änderung des Gesellschaftsvertrages sollte unter anderem dazu führen, dass das Gehalt des Geschäftsführers der Wohnungsbaugesellschaft offenzulegen ist. Hier stellte sich die Frage, ob das Persönlichkeitsrecht des Geschäftsführers das Informationsinteresse des Landes und der Bürgerinnen und Bürger überwiegt.

Angaben über das Einkommen bestimmter oder bestimmbarer Personen sind personenbezogene Daten im Sinne des Datenschutzrechtes. Hier lässt sich der Personenbezug aufgrund der öffentlichen Stellung des Geschäftsführers ohne Weiteres für jedermann herstellen, womit der Anwendungsbereich des Landesdatenschutzgesetzes Mecklenburg-Vorpommern (DSG M-V) eröffnet ist.

Mit dem Volkszählungsurteil vom 15.12.1983 wurde zwar das Recht auf informationelle Selbstbestimmung gestärkt, jedoch wird dieses Recht nicht schrankenlos gewährt. Das Bundesverfassungsgericht sagt, dass der Einzelne grundsätzlich Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen muss. Diese bedürfen jedoch einer gesetzlichen Erlaubnisnorm. Daher ist nach § 7 Abs. 1 Nr. 2 i. V. m § 14 Abs. 1 DSG M-V zu prüfen, ob eine Rechtsvorschrift eine Veröffentlichung der Daten über das Gehalt eines Geschäftsführers zulässt.

Gemäß § 73 Abs. 1 Kommunalverfassung Mecklenburg-Vorpommern (KV M-V) ergeben sich für Gemeinden unterschiedliche Kontroll- und Prüfungsrechte für Unternehmen, an denen sie mittelbar oder unmittelbar beteiligt sind. Ein kommunales Unternehmen hat gemäß § 73 Abs. 1 Nr. 2 KV M-V einen Jahresabschluss und einen Lagebericht nach den Vorschriften des Dritten Buches des Handelsgesetzbuches für große Kapitalgesellschaften aufzustellen. Dies beinhaltet ebenfalls die Beachtung von § 285 HGB. Gemäß § 285 Nr. 9 HGB sind im Anhang des Jahresabschlusses für Geschäftsführungsorgane die Gesamtbezüge, also Gehälter, Gewinnbeteiligung, Bezugsrechte und sonstige aktienbasierende Vergütungen, Aufwandsentschädigungen, Versicherungsentgelte, Provisionen und Nebenleistungen jeder Art, aufzuführen. Grundsätzlich können gemäß § 286 Abs. 4 HGB die Angaben nach § 285 Abs. 9 HGB ausbleiben, wenn es sich nicht um eine börsennotierte Aktiengesellschaft handelt.

Dies wird jedoch in der Kommunalverfassung Mecklenburg-Vorpommern als Spezialgesetz in § 73 Abs. 1 Nr. 8 KV M-V ausdrücklich ausgeschlossen.

Diese Regelung fand erst mit Novellierung der KV M-V im Jahre 2011 den Weg in das Gesetz. Der Ausschluss des § 286 Abs. 4 HGB wurde ausdrücklich aus Gründen der Transparenz gewollt.

Eine Offenlegung erfolgt nicht nur gegenüber der Gemeindevertretung, sondern ebenfalls gemäß § 73 Abs. 1 Nr. 2 KV M-V i. V. m. § 70b Abs. 2 KV M-V und § 14 Abs. 5 S. 2 Kommunalprüfungsgesetz Mecklenburg-Vorpommern (KPG M-V) gegenüber der Öffentlichkeit. Gemäß § 14 Abs. 5 KPG M-V sind der Jahresabschluss und der Lagebericht sieben Tage öffentlich auszulegen.

Über die Auslage ist in einer Bekanntmachung hinzuweisen. Demzufolge erhält nicht nur die Gemeindevertretung, sondern auch die Öffentlichkeit die Möglichkeit der Kenntnis über die Gesamtbezüge eines Geschäftsführers eines kommunalen Unternehmens.

Demnach besteht eine Erlaubnisnorm, die die Einschränkung der informationellen Selbstbestimmung zulässt, und auch einer Änderung des Gesellschaftsvertrages der Wohnungsbaugesellschaft steht nichts entgegen.

5.4.10 Erneuter Meldedatenabgleich für den Beitragsservice der Rundfunkanstalten

Der Rundfunkstaatsvertrag (RStV) enthält die grundlegenden Regelungen für den öffentlich-rechtlichen und den privaten Rundfunk in dem dualen Rundfunksystem der Länder Deutschlands. Mit Inkrafttreten der 15. Änderung des Rundfunkstaatsvertrages am 1. Januar 2013 wurde ein vollständiger Meldedatenabgleich durchgeführt, um den Wechsel von einer gerätebezogenen Abgabe zu einem wohnungs- bzw. betriebsbezogenen Beitrag zur Finanzierung des öffentlich-rechtlichen Rundfunks zu ermöglichen. Dazu wurden die Daten des Beitragsservices der bisher Beitragspflichtigen mit den Daten aller volljährigen Personen, die bei den Einwohnermeldeämtern in Deutschland gemeldet sind, verglichen. Dabei ging es um Angaben zum Namen, Doktorgrad, Familienstand, Geburtsdatum sowie zur aktuellen und vorherigen Anschrift der Haupt- und Nebenwohnungen und zum Tag des Einzugs.

Die Datenschutzbeauftragten von Bund und Ländern hatten ihre damalige Kritik zu diesem Meldedatenabgleich (siehe Beschluss vom 11. Oktober 2010 - https://www.datenschutz-mv.de/datenschutz/themen/beschlue/rundfunk.html) jedoch zurückgestellt, weil die Rundfunkanstalten nachweisen konnten, dass ein solcher Eingriff in das Recht auf informationelle Selbstbestimmung der betroffenen Beitragspflichtigen erforderlich war.

Während des Berichtszeitraumes wurde nun eine erneute Änderung des Rundfunkstaatsvertrages initiiert. Im Vorschlag zur 19. Änderung des Rundfunkstaatsvertrages ist ein nochmaliger, vollständiger Meldedatenabgleich aller meldepflichtigen Personen in Deutschland vorgesehen. Die Rundfunkanstalten begründen dies mit sonst drohenden Einnahmeverlusten. Nur durch diesen erneuten Abgleich würden auch die Beitragspflichtigen erfasst, die den Wohnsitz geändert haben oder für die eine Beitragspflicht neu entstanden ist, etwa bei Jugendlichen.

Der erneute Meldedatenabgleich ist nach unserer Auffassung jedoch nicht erforderlich. Die Rundfunkanstalten konnten nicht zufriedenstellend aufzeigen, wie hoch der jährliche Beitragsverlust etwa durch Umzüge, Scheidungen oder durch den Tod von Beitragspflichtigen tatsächlich ist. Aus unserer Sicht ist somit der Eingriff in das Recht auf informationelle Selbstbestimmung der betroffenen Beitragspflichtigen nicht hinreichend legitimiert.

Wir haben daher unserer Landesregierung empfohlen, dem Abschnitt zum erneuten vollständigen Meldedatenabgleich im 19. Rundfunkänderungsstaatsvertrag nicht zuzustimmen.

5.5 Soziales/Arbeitnehmerdatenschutz

5.5.1 Datenschutz bei der Förderung des Europäischen Sozialfonds

Über Petitionen einzelner Betroffener, Anfragen von privaten (gemeinnützigen) Trägern sowie im Rahmen von sich daraus entwickelnden Beratungsgesprächen mit Vertretern des Ministeriums für Arbeit, Gleichstellung und Soziales Mecklenburg-Vorpommern sind wir auf zahlreiche datenschutzrechtliche Fragen im Zusammenhang mit der Förderung des Europäischen Sozialfonds (ESF) gestoßen. Dabei handelte es sich insbesondere um die bisherige Praxis der Datenerhebung, der Datenverarbeitung, der Datennutzung und der Datenübermittlung.

Das Erheben von personenbezogenen Daten gehört seit vielen Jahren zu den zentralen Verpflichtungen gegenüber der Europäischen Kommission, denen das Land Mecklenburg-Vorpommern (und somit auch die betroffenen Träger und Behörden) bei der Umsetzung der ESF-Förderung unterliegt. Die ESF-Mittel werden mit einem breiten Spektrum von Förderrichtlinien bzw. Förderinstrumenten umgesetzt. Gefördert werden zum Beispiel Maßnahmen in der Schule, der Aus- und Weiterbildung, Existenzgründungen, die Aktivierung von Arbeitslosen, die Qualifizierung von Strafgefangenen oder auch Forschungsprojekte. In der Regel sind dabei die Teilnehmenden einer Maßnahme nicht mit den Zuwendungsempfängern identisch. Zuwendungsempfänger sind insbesondere Bildungsträger, sonstige Träger oder Unternehmen.

In der aktuellen Förderperiode bis 2020 werden in nahezu allen Förderbereichen (insbesondere jedoch im Bereich der Schulsozialarbeit) bei den Teilnehmenden Daten zum Zeitpunkt des Eintritts und des Austritts aus der Förderung sowie sechs Monate nach Austritt aus der Förderung erhoben. Hierzu werden Fragebögen genutzt, deren Umfang nach unserer Einschätzung über das zur erfolgreichen Durchführung der Förderprogramme erforderliche Maß deutlich hinausgeht. Die Landesbehörden in Mecklenburg-Vorpommern verweisen auf verschiedene Verordnungen der Europäischen Union (EU) und darauf, dass ein Rückschluss auf einzelne Personen letztendlich anhand der an die EU übermittelten Daten nicht möglich sei.

Wir haben zahlreiche Gespräche zur Erforderlichkeit der umfangreichen Erhebungen und Auswertungen sowie zur Freiwilligkeit etwaiger Einverständniserklärungen von Betroffenen im Zusammenhang mit der Eingehung einer beruflichen Tätigkeit bzw. im Zusammenhang mit bestehenden Abhängigkeitsverhältnissen geführt. Zudem haben wir erläutert, dass die beschriebene Praxis nach unserer Auffassung deutschem Datenschutzrecht widerspricht. Im Ergebnis war man seitens des Ressorts zu Detailänderungen bei Datenschutzerklärungen, bei den Einwilligungserklärungen und bei der inhaltlichen Gestaltung der Bögen bereit und setzte diese auch sukzessive um. Hinsichtlich der „monitoringbedingten“ sowie der Maßnahmen nachweisenden Datenströme vom Träger zu den Kommunen, von dort zu den Ministerien und EU-Bewirtschaftungseinheiten sowie Kontrolleinrichtungen und von dort zu der Kommission berief man sich jedoch auf die EU-seitigen „Bindungen und Erfordernisse“, die ein datenschutzfreundliches Handeln des Landes bzw. der Kommunen im Ergebnis verhindere.

Dabei wird auch uns gegenüber angeführt, dass die Europäische Kommission die beanstandete Datenpraxis im gesamten Umfang verbindlich abfordere und ansonsten Rückforderungen bzw. Nichtzahlungen erfolgten. Im Zuge dessen beriefe sich die Kommission auf verschiedene Verordnungen und Richtlinien, die - so die Schlussfolgerung der Landesbehörden - gegebenenfalls den Vorschriften des Bundesdatenschutzgesetzes (BDSG) oder des Landesdatenschutzgesetzes Mecklenburg-Vorpommern (DSG M-V) vorgingen.

Im Interesse der Zuwendungsempfänger und der Teilnehmenden der zu fördernden Maßnahmen sollte unseres Erachtens die Situation geprüft und optimiert werden. Deshalb haben wir uns zur Klärung der wesentlichen Fragen an den europäischen Datenschutzbeauftragten gewandt. Zwar ist dieser nach seiner Aussage nicht bei allen in Rede stehenden Verordnungen sowie eventuell vorliegenden fondsspezifischen Regelungen beteiligt worden. Da er allerdings gewisse Kontrollrechte innehat, wird er den Datenschutzbeauftragten der Europäischen Kommission kontaktieren, um für eine solche Prüfung zunächst um Klärung bestimmter Datenverarbeitungsvorgänge durch die Europäische Kommission im Rahmen von Projektförderungen durch den Europäischen Sozialfonds zu bitten.

5.5.2 Datenerhebung durch den Träger einer Kindertagesstätte

Eltern, deren Kinder eine Kindertagesstätte besuchen, haben bei uns angefragt, ob es aus datenschutzrechtlicher Sicht unbedenklich wäre, wenn der Träger der Einrichtung beim Abschluss eines Betreuungsvertrages auch den Geburtsort und das Geburtsdatum der Eltern erheben würde. Auf Nachfrage der Eltern hat der Träger der Kindertagesstätte die Datenerhebung damit begründet, dass die Angaben erforderlich seien, um Personen im Falle eines gerichtlichen Mahnverfahrens besser zuordnen zu können.

Wir haben den Träger der Kindertagesstätte gebeten, uns die Rechtsgrundlage mitzuteilen, nach der Eltern verpflichtet sind, die geforderten Angaben zu machen.

Der Träger der Kindertagesstätte hatte seine Datenerhebung auf die Freiwilligkeit der Angaben gestützt. Die Eltern konnten nach Auskunft des Trägers frei entscheiden, ob sie die Daten angeben. Die Erforderlichkeit der Angaben begründete der Träger damit, dass diese bei einem eventuell stattfindenden Mahn- und Vollstreckungsverfahren notwendig seien, um mögliche Verwechslungen auszuschließen.

Diese Begründung genügte nach unserer Auffassung nicht, um die gewünschten Daten zu erheben. Nach den datenschutzrechtlichen Bestimmungen dürfen personenbezogene Daten nur erhoben werden, sofern eine Rechtsgrundlage dafür besteht oder die Betroffenen eingewilligt haben. Eine weitere Voraussetzung ist, dass die Daten zur Aufgabenerfüllung der datenverarbeitenden Stelle erforderlich sind. Selbst wenn die Datenerhebung und -speicherung hier auf eine Einwilligung der Betroffenen gestützt wurde, hatten wir Zweifel an der Verhältnismäßigkeit der Datenerhebung.

Richtig ist, dass die verantwortlichen Stellen mit einer Einwilligung den ihnen nach § 28 Bundesdatenschutzgesetz (BDSG) zustehenden Verarbeitungsspielraum erweitern können. Die verantwortliche Stelle bleibt also berechtigt, die jeweils erforderlichen Daten zu erheben (§ 28 Abs. 1 Nr. 1 BDSG), darf aber die Teilnahmebereitschaft (Einwilligung) nicht dazu nutzen, um auf zusätzliche, im aktuellen Verarbeitungskontext nicht benötigte Angaben, zuzugreifen. Nicht zuletzt muss die Einwilligung auf der freien Entscheidung der Betroffenen beruhen. Dies bedeutet auch, dass sie über den Zweck aufgeklärt und auf die Freiwilligkeit der Datenerhebung hingewiesen werden müssen.

Auf dem uns vorliegenden Exemplar eines Betreuungsvertrages fehlte der notwendige Hinweis darauf, dass diese Angaben freiwillig sind. Dabei ist es ebenso erforderlich, dass denjenigen, der nicht einwilligt, keine Sanktion trifft. Im vorliegenden Fall konnte eine solche Verbindung nicht ausgeschlossen werden.

Da personenbezogene Daten nur erhoben werden dürfen, wenn sie zur Erfüllung einer aktuellen Aufgabe der verantwortlichen Stelle erforderlich sind, dürfen nur die zur aktuellen Aufgabenerfüllung benötigten Daten erhoben werden. Es ist nicht zulässig, Daten „auf Vorrat“ zu erheben, das heißt Daten, die zu einem späteren Zeitpunkt benötigt werden könnten und deshalb bereits beim Abschluss des Betreuungsvertrages erhoben werden.

Außerdem wurde bei diesem Vorgehen der datenschutzrechtlich Grundsatz der Verhältnismäßigkeit nicht beachtet, da personenbezogene Daten (Geburtsort, Geburtsname) von einer unverhältnismäßig großen Personengruppe erhoben wurden. Der Träger der Einrichtung schließt mit den Eltern einen Vertrag über die Betreuung der Kinder ab. Soweit die Eltern die sich aus dem Vertrag für sie ergebenden Pflichten, wie zum Beispiel die fristgerechte Zahlung der Elternbeiträge, erfüllen, sind die für ein mögliches Mahnverfahren erforderlichen Daten der Eltern nicht erforderlich. Erst wenn sich Eltern nicht vertragsgerecht verhalten und ein Mahnverfahren eingeleitet werden soll, sind die in Rede stehenden Daten für den Träger der Einrichtung erforderlich und dürfen auch erst dann erhoben werden. Dies dürfte nach unserer Einschätzung nur einen begrenzten Teil der Eltern betreffen.

Wir haben dem Träger der Kindertagesstätte empfohlen, die in Rede stehenden Daten nur von den Eltern und auch erst dann zu erheben, wenn ein Mahnverfahren eingeleitet werden soll. Der Träger der Kindertagesstätte hat sich unserer rechtlichen Argumentation angeschlossen. Die Angaben Geburtsdatum und Geburtsort der Eltern werden nicht mehr in dem Betreuungsvertrag gefordert.

5.5.3 GPS-Überwachung von Mitarbeiter-Kfz

Vermehrt entscheiden sich Unternehmen dazu, ihre Dienstfahrzeuge mittels GPS (Global Positioning System) zu überwachen. Mitarbeiter fühlen sich dadurch oft verunsichert und in ihrer Arbeitsleistung überwacht. Daher haben wir zunehmend Anfragen oder Beschwerden zu dieser Thematik.

Die Überwachung von Dienstfahrzeugen mittels GPS ist nur unter strengen Voraussetzungen möglich.

Im vorliegenden Fall beschloss ein Fuhrparkunternehmen aus Mecklenburg-Vorpommern, die Dienstfahrzeuge der Mitarbeiter (nicht jedoch die zu vermietenden Fahrzeuge) mit GPS-Ortungsgeräten auszustatten. Da die Mitarbeiter die Fahrzeuge auch privat nutzen konnten, war es möglich, für diese Zeit das GPS-Ortungsgerät in den „Privat-Modus“ zu stellen, sodass lediglich die gefahrenen Kilometer aufgezeichnet wurden. Wurde das Fahrzeug jedoch dienstlich genutzt, wurden durch den Arbeitgeber das Kennzeichen des Fahrzeugs, das Einsatzdatum, die Einsatzzeit, der Ort (Abfahrt, Ziel, Routenaufzeichnung inklusive Geschwindigkeit), die gefahrenen Kilometer, der Anlass des Einsatzes, Kundendaten (Name, Anschrift, Zweck des Besuchs) und die GPS-Koordinaten gespeichert.

Deshalb waren die GPS-Ortungsgeräte in diesem Fall dazu geeignet, das Arbeitsverhalten der Mitarbeiter zu kontrollieren. Dies ist jedoch datenschutzrechtlich nicht zulässig, da die Mitarbeiter keinem permanenten Kontrolldruck ausgesetzt sein dürfen.

Auch eine Einwilligung des Mitarbeiters zur GPS-Ortung ist aufgrund des Abhängigkeitsverhältnisses zum Arbeitgeber nicht als freiwillig zu werten und damit nicht wirksam.

Daher darf der Arbeitgeber ein GPS-Ortungssystem nur unter den Voraussetzungen des § 32 Bundesdatenschutzgesetz (BDSG; Arbeitnehmerdatenschutz) in den Dienstwagen installieren. Dabei kommt es auf den Zweck der Datenverarbeitung, die technischen Möglichkeiten des Systems und dessen tatsächlichen Gebrauch an. So wäre es datenschutzrechtlich unproblematisch, wenn die Ortung durch das System erst nach einem Diebstahl des Fahrzeuges einsetzen würde. Ein berechtigtes Interesse kann auch bestehen, wenn die GPS-Ortung in den zu vermietenden Fahrzeugen angebracht worden wäre.

Das GPS-Ortungssystem muss insbesondere für die angegebenen Zwecke geeignet und erforderlich sein. Das bedeutet, dass es keine milderen Mittel zur Erreichung des angegebenen Zwecks geben darf. Außerdem muss der Grundsatz der Datensparsamkeit eingehalten werden.

Die Prüfung der angegebenen Zwecke (anlassbezogene Positionsabfrage für Abholungsplanung) und der hierzu erhobenen Daten hat im hier genannten Fall ergeben, dass die Erhebung unverhältnismäßig bzw. nicht erforderlich und damit nicht zulässig war.

Daher haben wir dem Unternehmen Folgendes empfohlen:

- Es werden keine Namen, Anschriften, Telefonnummern, E-Mail-Adressen und Fähigkeiten von Mitarbeitern im Zusammenhang mit der GPS-Ortung erhoben.
- Es werden keine Angaben zum Fahrverhalten (beispielsweise Geschwindigkeit) erhoben.
- Auch im Privat-Modus werden keine gefahrenen Kilometer erhoben.
- Der Zugriff auf die GPS-Daten erfolgt durch koordinierende Mitarbeiter und nicht durch die Geschäftsführung.
- Es werden keine Daten der Kunden erhoben.
- Es erfolgt keine Routenaufzeichnung, sondern eine anlassbezogene Bestimmung der Echtzeitposition des Dienstfahrzeuges.

Da das Unternehmen die von uns gesetzten Vorgaben technisch nicht zeitnah umsetzen konnte, wurde das GPS-Ortungssystem abgeschaltet. Weiterhin versicherte uns das Unternehmen, uns vor einer erneuten Inbetriebnahme darüber in Kenntnis zu setzen.

5.6 Gesundheitswesen

5.6.1 Patientendaten auf dem Flur einer Station im Krankenhaus

Ein Petent hatte in einer Klinik (Abteilung für Neurochirurgie) festgestellt, dass vor den Patientenzimmern Krankenüberwachungsbögen angebracht waren, sodass Besucher der Station den Vornamen, den Nachnamen, das Geburtsdatum und die Aufnahmenummer sowie auch Angaben zum Gesundheitszustand (z. B. Bewusstsein eingeschränkt, Schmerzen nach neurochirurgischer Operation, nach Schlaganfall, Patient kann spontan Urin, Stuhl lassen) der Patienten zur Kenntnis nehmen konnten. Außerdem war zu sehen, ob der Patient pflichtversichert ist. Da der Petent erhebliche Zweifel an der Zulässigkeit dieses Vorgehens hatte, hat er uns um Unterstützung gebeten.

Wir haben die Anfrage zum Anlass genommen, bei der Klinik nachzufragen, ob der Sachverhalt zutrifft und wenn ja, auf welcher Rechtsgrundlage und zu welchem Zweck die Patientendaten in der geschilderten Weise Dritten offenbart werden.

Der Leiter der Klinischen Abteilung bestätigte uns, dass es gängige Praxis sei, neben der Eingangstür zum Patientenzimmer sogenannte Überwachungsbögen auszuhängen. Eine Rechtsgrundlage, nach der die Übermittlung zulässig gewesen wäre, hatte uns die Klinik nicht genannt. Die Klinik hatte ihr Vorgehen auf das Einverständnis der Patienten gestützt, das heißt, die Patienten wurden jeweils mündlich auf diese Praxis hingewiesen, ohne jedoch eine schriftliche Einverständniserklärung einzuholen.

Bei dem hier geschilderten Sachverhalt sind neben der durch § 203 Strafgesetzbuch (StGB) strafbewehrten ärztlichen Schweigepflicht zur Beurteilung des Sachverhaltes die Bestimmungen des Landeskrankenhausgesetzes Mecklenburg-Vorpommern (LKHG M-V) heranzuziehen. Im Datenschutzrecht spricht man hier von einer Übermittlung von Patientendaten an Dritte, das heißt an Stellen außerhalb des Krankenhauses. Das LKHG M-V enthält in § 35 Abs. 1 einen Katalog mit den Fällen, in denen eine Übermittlung an Dritte zulässig ist. So ist zum Beispiel die Übermittlung von Patientendaten an Dritte zulässig zur Erfüllung des Behandlungsvertrages, zur Durchführung einer Mit- oder Nachbehandlung oder zur Abwehr einer gegenwärtigen Gefahr für Leben, körperliche Unversehrtheit oder persönliche Freiheit der Patienten oder Dritter, wenn diese Rechtsgüter das Geheimhaltungsinteresse der Patienten wesentlich überwiegen. Allein die Tatsache, dass eine Person, die durch Name und Vorname identifiziert ist, in einem Krankenhaus behandelt wird, qualifiziert diese Daten als Patientendaten im Sinne von § 32 Abs. 1 Satz 2 LKHG M-V. Patientendaten unterliegen einer strengen Zweckbindung. Eine Norm, nach der die Übermittlung von Patientendaten an Besucher einer Station zulässig ist, enthält das LKHG M-V nicht, sodass die geschilderte Praxis aus datenschutzrechtlicher Sicht nicht zulässig war.

Die Klinik hat unseren Hinweis zum Anlass genommen, dieses Verfahren umgehend zu ändern, sodass die Krankenhausüberwachungsbögen nicht mehr für Dritte zugänglich sind.

5.6.2 Datenübermittlung von der Ärzteversorgung an Gutachter

Eine Petentin hat uns geschildert, dass sie im Zusammenhang mit ihrem Berufsunfähigkeitsverfahren durch die Ärzteversorgung mehrfach aufgefordert worden sei, sich bei einem Gutachter vorzustellen. Nachdem der Petentin im Zusammenhang mit einer Nachbegutachtung Name und Anschrift der Gutachterin mitgeteilt worden seien, habe sie mit der Praxis einen Termin abstimmen wollen. Bei diesem Telefonat habe sie erfahren, dass der Gutachterin neben ihren Kontaktdaten bereits ihre Diagnosen in Form von ICD-Schlüsseln - (Internationale Klassifizierung von Krankheiten) vorlägen, obwohl sie der Ärzteversorgung keine Schweigepflichtentbindungserklärung erteilt habe. Über dieses Vorgehen habe sie sich bereits bei der Ärzteversorgung beschwert, die aber in der Übermittlung der ICD-Schlüssel keine Verletzung der ärztlichen Schweigepflicht gesehen habe. Die Petentin hat uns daher um Unterstützung gebeten.

Die Ärzteversorgung ist die berufsständische Pflichtversorgungseinrichtung für Ärzte, Zahnärzte und Tierärzte, die in Mecklenburg-Vorpommern beruflich tätig sind. Sie ist beitrags- und leistungsrechtlich als gleichwertige Alternative zur Rentenversicherung anzusehen.

Nach den allgemeinen datenschutzrechtlichen Bestimmungen ist die Verarbeitung personenbezogener Daten nur zulässig, wenn die Vorschriften des Landesdatenschutzgesetzes Mecklenburg-Vorpommern (DSG M-V) sie zulässt, eine andere Rechtsvorschrift sie erlaubt oder zwingend voraussetzt oder die betroffene Person eingewilligt hat, § 7 Abs. 1 DSG M-V. Wir haben daher bei der Ärzteversorgung nachgefragt, welche der genannten gesetzlichen Voraussetzungen in dem geschilderten Fall vorlagen.

Die Ärzteversorgung konnte uns keine Rechtsgrundlage mitteilen, nach der sie berechtigt war, ärztliche Diagnosen an die Gutachterin zu übermitteln. Ohne Rechtsgrundlage hätten die Daten nur übermittelt werden dürfen, wenn die Petentin ihr Einverständnis (ärztliche Schweigepflichtentbindungserklärung) gegeben hätte.

Das Ergebnis unserer datenschutzrechtlichen Prüfung haben wir der Ärzteversorgung mitgeteilt. In unserer Stellungnahme haben wir darauf hingewiesen, dass sich strafbar macht, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis, offenbart, das ihm als Arzt anvertraut worden oder sonst bekannt geworden ist, § 203 Abs. 1 Strafgesetzbuch (StGB). Die ärztliche Schweigepflicht umfasst alle Tatsachen, die nur einem bestimmten, abgrenzbaren Personenkreis bekannt sind und an deren Geheimhaltung der Patient ein verständliches, also sachlich begründetes und damit schutzwürdiges Interesse hat. Dies ist bei Gesundheitsdaten regelmäßig anzunehmen. Die ärztliche Schweigepflicht ist grundsätzlich auch gegenüber anderen Ärzten zu beachten. Dies bedeutet, dass beispielsweise auch zwei Fachärzte keine Patientendaten austauschen dürfen, wenn dies nicht durch eine vorherige informierte Einwilligung oder durch eine konkrete Gesetzesnorm gedeckt ist. Auch die Berufsordnung für die Ärztinnen und Ärzte in Mecklenburg-Vorpommern (BOÄ M-V) regelt in § 9 Abs. 4, dass, sofern mehrere Ärzte gleichzeitig oder nacheinander denselben Patienten untersuchen bzw. behandeln, diese nur dann untereinander von der Schweigepflicht befreit sind, wenn das Einverständnis des Patienten vorliegt bzw. anzunehmen ist. Diese Voraussetzungen waren vorliegend nicht erfüllt.

Im Ergebnis hat uns die Ärzteversorgung Mecklenburg-Vorpommern mitgeteilt, dass künftig ohne ausdrückliche schriftliche Einverständniserklärung keinerlei Daten an zu beauftragende Gutachterinnen/Gutachter im Rahmen eines Berufsunfähigkeitsrentenantragsverfahrens oder eines Nachbegutachtungsverfahrens weitergegeben werden.

5.6.3 Sichere Übermittlung von Krebsregisterdaten

In Mecklenburg-Vorpommern gibt es - wie auch in anderen Bundesländern - klinische Krebsregister, die umfangreiche medizinische Daten über krebskranke Menschen speichern. Diese Daten sollen dazu beitragen, deren Behandlung zu verbessern. Diese Register arbeiten auf der Grundlage von § 65c Sozialgesetzbuch Fünftes Buch (SGB V) und entsprechenden Landesgesetzen, wie dem Klinischen Krebsregistergesetz, siehe Zehnter Tätigkeitsbericht, Punkt 3.3.4. Die Daten der klinischen Krebsregistrierung sind äußerst schutzbedürftig. Deshalb sind angemessene technische und organisatorische Maßnahmen zu deren Schutz zu ergreifen.

Kommunikationspartner der Krebsregister sind insbesondere alle Krankenhäuser und ärztliche und zahnärztliche Praxen, die krebskranke Patientinnen und Patienten behandeln. Verantwortlich für die Übermittlung der Patientendaten an die klinischen Krebsregister sind die Behandlungseinrichtungen. Sie müssen deshalb ausreichende Schutzvorkehrungen treffen. Welche dies sind, haben die Datenschutzbehörden des Bundes und der Länder Ende 2014 in einer gemeinsamen Entschließung „Anforderungen an den Schutz der Datenübermittlungen zwischen medizinischen Leistungserbringern und klinischen Krebsregistern“ festgestellt (https://www.datenschutz-mv.de/datenschutz/themen/beschlue/89_DSK/ent_krebsregister.html). Darunter finden sich zusammengefasst folgende Punkte:

- Sollen die medizinischen Daten mit einer Web-Anwendung erfasst werden, so müssen die Praxisnetze die „Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze“ (Beschluss des Düsseldorfer Kreises vom 4./5. Mai 2011) erfüllen. Wegen der hohen Sicherheitsanforderungen wird davon abgeraten, dass Patientendaten für Tumorkonferenzen und andere Formen der einrichtungsübergreifenden Zusammenarbeit mithilfe von Web-Anwendungen abgerufen werden können (Nummern 1-3).
- Zur Sicherung der Übermittlung sind sichere kryptographische Verfahren einzusetzen. Maßstab ist hier die Technische Richtlinie BSI-TR 03107-1 des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Darüber hinaus muss auch die Schlüsselverwaltung dem Stand der Technik entsprechen (Nummern 4-7).
- Die Übertragungssicherung muss als Ende-zu-Ende-Sicherheit ausgestaltet sein. Es muss sichergestellt sein, dass nur befugte Personen Zugriff auf Patientendaten erlangen können. Gegebenenfalls muss eine Zwei-Faktor-Authentisierung der Zugriffsberechtigten stattfinden (Nummern 8-18).
- Ambulante Leistungserbringer müssen die „Empfehlungen zu Datenschutz und Datensicherheit in der Arztpraxis“ der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung beachten. Auf Geräten, mit denen unverschlüsselte medizinische Daten verarbeitet werden, darf kein allgemeiner Internetzugriff möglich sein. Webanwendungen der Krebsregister bedürfen besonderer Maßnahmen zum Schutz vor Manipulationen (Nummern 19-26).

- Darüber hinaus muss sichergestellt sein, dass die Herkunft von Daten, die der weiteren medizinischen Behandlung zugrunde liegen, nachvollzogen werden kann. Hierzu dienen insbesondere Signaturverfahren (Nummern 27-28).
- Schließlich muss anhand geeigneter Protokolle nachvollzogen werden können, wer medizinische Daten welcher Patientin oder welches Patienten abgerufen hat (Nummern 29-31).

Wir empfehlen den Krankenhäusern, ärztlichen und zahnärztlichen Praxen und anderen Partnern der klinischen Krebsregistrierung unseres Landes, diese Entschließung zu beachten.

5.6.4 Mangelhafter Schutz von Patientendaten

Mangelhafte technische und organisatorische Maßnahmen beim Umgang mit Patientendaten können die Datensicherheit nicht gewährleisten. Folgende Beispiele zeigen dies recht deutlich.

In einem Fall hat uns eine öffentliche Stelle den Verlust eines Datenträgers mit Patientendaten angezeigt. Der Datenträger mit Gesundheitsdaten von 48 Patienten war auf dem Postweg verlorengegangen. In der Regel werden diese Datenträger zusammen mit anderen Unterlagen in einem Paket verschickt. In diesem Fall hatte man vergessen, den entsprechenden Datenträger mit zum Teil unverschlüsselten Patientendaten beizulegen, sodass dieser per Brief nachgesandt werden sollte. Der Datenträger wurde in zwei Briefumschläge, die mit einem Klebeband zusätzlich verschlossen wurden, gelegt und per Kurier zur Post gebracht. Beim Empfänger kam allerdings nur ein verschmutzter offener Briefumschlag an. Die Verlustanzeige war verbunden mit der Bitte um datenschutzrechtliche Beratung.

Da bekannt war, von welchen Personen Gesundheitsdaten auf dem Datenträger gespeichert waren, haben wir empfohlen, die Betroffenen in einem Brief über den Verlust und auch über die Maßnahmen zu informieren, die eingeleitet wurden, um den Verbleib des Datenträgers aufzuklären. So sollte bei der Post ein Antrag auf Nachverfolgung gestellt werden, um den Verbleib des Datenträgers zu klären. Des Weiteren sollte geprüft werden, welche technischen und organisatorischen Maßnahmen einzuleiten sind, um eine Wiederholung eines solchen Vorfalls zu verhindern. Eine einfache und sichere Maßnahme ist zum Beispiel, nur verschlüsselte Daten auf dem Datenträger zu speichern, sodass unberechtigte Dritte keinen Zugriff auf diese Daten nehmen können.

In einem anderen Fall haben wir den anonymen Hinweis bekommen, dass man über einen Weblink Patienten- sowie Mitarbeiterdaten einer öffentlichen Stelle zur Kenntnis nehmen kann. Wir sind diesem Hinweis nachgegangen und konnten aus der angegebenen Zip-Datei unproblematisch mehrere Lotus-Notes-Dateien extrahieren. Es stellte sich dabei heraus, dass es sich um Datenbanken handelt, die zum Teil sehr sensible Gesundheitsdaten von Versicherten sowie diverse Mitarbeiterdaten beinhalten. Den Zugang auf diese Datenbanken haben wir ohne große Schwierigkeiten über eine einfache Lotus-Notes-Client-Installation erzielen können. Es war daher davon auszugehen, dass ein Zugriff auf die Daten ohne Weiteres von nicht berechtigten Dritten erfolgen konnte.

Wir haben die öffentliche Stelle aufgefordert, den angegebenen Link sowie gegebenenfalls weitere vorhandene Links zu Dateien mit personenbezogenen Daten unverzüglich zu sperren. Außerdem sollte geprüft werden, wie es dazu kommen konnte, dass unberechtigte Dritte mit einfachsten Mitteln und offenbar ohne technische Absicherung auf diese Datenbanken zugreifen können. Des Weiteren hatten wir um Mitteilung gebeten, welche technischen und organisatorischen Maßnahmen gemäß § 21 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) zum Schutz der zum Teil sehr sensiblen Daten ergriffen werden. Zudem sollte der Vorfall mit den Mitarbeiterinnen und Mitarbeitern ausgewertet werden, um sie für diese datenschutzrechtliche Frage weiter zu sensibilisieren.

Die öffentliche Stelle teilte mit, dass es sich hier um ein Pilotprojekt zur Bearbeitung von Gutachteraufträgen handelte. Hierfür wurde der entsprechende Auftrag mit den für diesen Einzelfall erforderlichen Patientendaten auf einem externen Portal-Server, der keinen Zugriff auf das Netzwerk der öffentlichen Stelle hatte, bereitgestellt. Der Auftragnehmer konnte diese Daten dann dort abrufen. Der Link war vertraulich und nur den Personen bekannt, die mit dem Projekt betraut waren.

Nachdem die öffentliche Stelle unseren Hinweis erhalten hatte, wurden die Daten auf dem externen Server umgehend gelöscht. Außerdem wird dieser Übertragungsweg nicht weiter genutzt. Der Vorgang wurde intern ausgewertet. Man war zu dem Ergebnis gekommen, dass diese praktizierte Übermittlung von Patientendaten nicht den erforderlichen Sicherheitsstandards entsprach. Die Ablage nicht verschlüsselter Daten widersprach den internen Anweisungen zum Umgang mit vertraulichen Daten. Des Weiteren wurde der Vorfall durch die Datenschutzbeauftragte und den Leiter des Sachgebietes EDV aufgearbeitet. Es wurden weitere Maßnahmen entwickelt, um künftig einen Datenmissbrauch auszuschließen. Bei der elektronischen Übermittlung von Daten werden somit künftig erforderliche technische und organisatorische Maßnahmen realisiert, die es nur berechtigten Empfängern ermöglicht, die Daten wieder zu entschlüsseln.

5.7 Personal

5.7.1 Dokumentenmanagement in der Landesverwaltung (BEATA)

Im Elften Tätigkeitsbericht haben wir unter Punkt 5.1.7 bereits über die Einführung des elektronischen Aktenablage- und Verwaltungssystem für Bezügeakten BEATA (**B**ezügedaten **e**lektronisch **a**nweisen, **t**ransportieren und **a**rchivieren) berichtet. Das Verfahren dient dem behördenübergreifenden, elektronischen Austausch von bezügerelevanten Daten und ermöglicht allen Landesbediensteten, in elektronischer Form mit dem Landesbesoldungsamt (LBesA) zu kommunizieren.

Bereits vor zwei Jahren konnten wir bestätigen, dass dem Thema Datenschutz ausreichend Beachtung geschenkt wurde. Frühzeitig wurde das BEATA-Projekt am „Privacy by Design"-Gestaltungsprinzip ausgerichtet. So sind datenschutzrechtliche Vorgaben schon in der Projektplanung und -entwicklung berücksichtigt worden, wodurch Zeit und Geld für gegebenenfalls später notwendige Korrekturmaßnahmen gespart werden konnten.

Im Berichtszeitraum haben wir uns mit der Umsetzung des Dienststellenportals befasst, mit dessen Hilfe Formulare auf elektronischem Wege zwischen den einzelnen Dienststellen und dem LBesA ausgetauscht werden sollen. Wir haben dabei sowohl an der Umsetzungskonzeption als auch an der notwendigen Dienstvereinbarung über den Einsatz des BEATA-Dienststellenportals mitgewirkt. Im Zusammenhang mit der Konzipierung des Dienststellenportals haben wir empfohlen, die Daten in der zu Grunde liegenden Datenbank mit einem kryptographischen Verfahren nach dem Stand der Technik zu verschlüsseln. Da in diesem Verfahren auch hoch schutzbedürftige Daten verarbeitet werden, ist diese Maßnahme zur Gewährleistung der Vertraulichkeit (§ 21 Abs. 2 Nr. 2 Landesdatenschutzgesetz Mecklenburg-Vorpommern - DSG M-V) unumgänglich. Das LBesA ist unserer Empfehlung gefolgt und hat uns eine entsprechende Umsetzung zugesagt.

5.7.2 Travel-Management-System (TMS)

Zu Beginn des Jahres 2014 hat uns das Finanzministerium unseres Landes über die Planungen zur Neugestaltung des Travel-Management-Systems (TMS) unterrichtet, siehe Achter Tätigkeitsbericht, Punkt 2.10.1. Das TMS ermöglicht den Bediensteten der Landesregierung, ihre Dienstreisen auf elektronischem Wege zu organisieren, zu beantragen und abzurechnen.

Das überarbeitete TMS besteht aus zwei Komponenten: einem elektronischen Antrags-, Genehmigungs- und Abrechnungsverfahren und einer Anbindung an ein Reisedienstleistungsportal für die Buchung von Flug, Bahn, Hotel und Mietwagen.

Zur datenschutzrechtlichen Bewertung des Verfahrens erhielten wir unter anderem das Sicherheitskonzept, die Verfahrensdokumentation, die Dienstvereinbarung sowie das Betriebshandbuch. So war es uns möglich, einen umfassenden Eindruck vom TMS zu gewinnen und entsprechende Empfehlungen für eine datenschutzgerechte Ausgestaltung des Verfahrens zu geben.

Das Finanzministerium hat einen Großteil unserer Empfehlungen umgesetzt. So wurde die Anmeldeprozedur entsprechend unserer Empfehlungen ausgestaltet. Um einen Missbrauch durch gefälschte Registrierungen zu verhindern, soll der Nutzer durch die Eingabe persönlicher Daten eindeutig identifiziert werden. Bei der ersten Anmeldung soll er dazu selbst Daten wie Personalnummer, Name und IBAN eingeben, die in verschlüsselter Form in das System übertragen werden. Aus unserer Sicht handelt es sich insbesondere bei der IBAN um ein sensibles Datum, welches nicht ohne Weiteres Dritten bekannt ist und auch nicht im Rahmen einer stellvertretenden Anmeldung an Dritte weitergegeben werden sollte. Deshalb haben wir empfohlen, dass die erstmalige Registrierung nur durch den Anwender selbst und nicht durch seinen Vertreter oder durch das Sekretariat durchgeführt werden kann. Im Ergebnis unserer Empfehlungen wurde die Möglichkeit, sich von einem Vertreter im Verfahren anmelden zu lassen, gestrichen. Mit dem neu konzipierten Anmeldeverfahren wird - auch unter dem Gesichtspunkt der Datensparsamkeit - verhindert, dass nicht einfach auf Verdacht Accounts für Bedienstete angelegt werden können, sondern nur dann, wenn diese auch wirklich im Rahmen einer Dienstreise benötigt werden. Auch wird die Möglichkeit, Accounts widerrechtlich anzulegen, etwa um „gefälschte“ Reisen zu beantragen, zu buchen und abzurechen, deutlich erschwert.

Es wurden jedoch nicht alle Empfehlungen umgesetzt. Nach wie vor wird die vom Gesetz angeordnete Schriftform im TMS nicht ordnungsgemäß elektronisch umgesetzt. Die qualifizierte elektronische Signatur (QES) wird immer noch nicht im erforderlichen Umfang eingesetzt. Bereits bei den Beratungen zur vorhergehenden TMS-Version im Jahr 2006 hatten wir darauf hingewiesen, dass die QES der Dienstreisenden bzw. Vorgesetzten insbesondere bei der Genehmigung und Abrechnung der Dienstreise notwendig ist. Ohne die qualifizierte elektronische Signatur hat der Antragsteller im Zweifelsfall keine Möglichkeit, die Echtheit der Dienstreisegenehmigung oder der Abrechnung beweisen zu können. Die sich daraus ergebenden Nachteile bedürfen keiner weiteren Erläuterung.

Bis zum Ende des Berichtszeitraumes sind die Diskussionen um den Einsatz der QES, welche durch das Signaturgesetz bereits im Jahr 2001 geregelt wurde, nicht beendet. Nach wie vor sind die Arbeitsplätze der Landesbediensteten nicht in ausreichender Zahl mit Kartenlesern und qualifizierten Zertifikaten ausgestattet. Der Gesetzgeber hat inzwischen darauf reagiert und mit einer Änderung des § 3a Abs. 2 des Verwaltungsverfahrensgesetzes Mecklenburg-Vorpommern (VwVfg M-V) die Möglichkeit eröffnet, dass auch andere sichere Verfahren das Schriftformerfordernis abbilden können, beispielsweise der Einsatz von De-Mail oder die Nutzung elektronischer Formulare im Zusammenhang mit der eID-Funktion des neuen Personalausweises, siehe Elfter Tätigkeitsbericht, Punkt 3.2.

Trotz der bestehenden Mängel haben wir dem Betrieb der neuen Version des TMS unter folgenden Voraussetzungen zugestimmt: TMS-Nutzer, die schon jetzt über eine Signaturkarte zur Erstellung der QES verfügen, müssen diese im TMS verwenden können. Das Finanzministerium muss zudem zusichern, sich intensiv mit der Problematik der fehlenden QES oder eines geeigneten Ersatzverfahrens zu befassen, und kurzfristig Lösungen anbieten. Als Ersatzlösung für die persönliche QES akzeptieren wir für eine kurze Übergangszeit eine Stapelsignaturlösung. Bei der Stapelsignatur handelt es sich um eine besondere Form der QES, bei der automatisch eine größere Anzahl von Dokumenten unter Nutzung einer einzigen Signaturkarte qualifiziert signiert wird. Der Einsatz der Stapelsignatur bedeutet jedoch, dass nicht jedes einzelne Dokument vor seiner Signatur der visuellen Kontrolle des Signierenden unterliegt und demzufolge auch keinen vergleichbaren Beweiswert hat.

Wir empfehlen der Landesregierung, die flächendeckende Verfügbarkeit von Kartenlesern und Signaturkarten für die qualifizierte elektronische Signatur voranzutreiben und gleichzeitig zu prüfen, welche anderen der in § 3a Abs. 2 VwVfg M-V genannten sicheren Verfahren eingesetzt werden können.

5.7.3 Interessenkollisionen eines behördlichen Datenschutzbeauftragten

Ein Petent hat uns darüber informiert, dass bei seinem Arbeitgeber die Funktion des behördlichen Datenschutzbeauftragten und die Leitung der Personalabteilung von ein und derselben Person wahrgenommen werden. Er wollte von uns wissen, wie dies zu werten sei.

Bei der Beurteilung dieses Sachverhaltes waren die Regelungen des § 20 Abs. 1 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) zu berücksichtigen. Danach darf zum behördlichen Datenschutzbeauftragten nur bestellt werden, wer dadurch keinem Interessenkonflikt mit sonstigen dienstlichen Aufgaben unterliegt und die zur Erfüllung seiner Aufgabe erforderliche Sachkunde und Zuverlässigkeit besitzt.

Die Tätigkeit des behördlichen Datenschutzbeauftragten darf zu keiner Interessenkollision mit seinen anderen dienstlichen Aufgaben führen. Damit scheidet zum Beispiel die Bestellung des Leiters der IT-Abteilung grundsätzlich aus. Entsprechendes gilt für den Leiter der datenverarbeitenden Stelle sowie den Leiter der personalaktenführenden Stelle, da hier Entscheidungs- und Kontrollfunktion in einer Hand lägen. Besteht bei der datenverarbeitenden Stelle eine Organisationseinheit, die für die Rechnungsprüfung zuständig ist, so hat es sich bewährt, einem Mitarbeiter dieser Stelle die Aufgabe des behördlichen Datenschutzbeauftragten zu übertragen. Ebenso kommt die Übernahme dieser Aufgabe durch einen Mitarbeiter der Rechtsabteilung in Betracht. Auch die Bündelung mit anderen Aufgaben bietet sich gegebenenfalls an. Dies ist im Einzelfall genau zu prüfen.

Bei der vorliegenden Konstellation lagen jedoch Entscheidungs- und Kontrollfunktionen in einer Hand und deshalb waren Interessenkollisionen, auch bei Sachkunde und Zuverlässigkeit, strukturell naheliegend. Die Daten der Beschäftigten zählen zu den am häufigsten verarbeiteten Angaben. Ihre Verwendung ist zudem nicht nur mit einem hohen Risiko für die Betroffenen, sondern auch mit einer Vielzahl von Streitfragen belastet. Jeder Versuch, jemanden zum behördlichen Datenschutzbeauftragten zu bestellen, der in die Verarbeitung von Beschäftigtendaten einbezogen ist und dabei vor allem die bisweilen gegenläufigen Interessen der verantwortlichen Stelle wahren muss, löst deshalb mit höchster Wahrscheinlichkeit Konfliktlagen aus, die sich negativ auf die Zuverlässigkeit des behördlichen Datenschutzbeauftragten auswirken werden. Aus diesem Grund darf der behördliche Datenschutzbeauftragte nicht gleichzeitig auch eine leitende Funktion in der Personalabteilung innehaben.

Unsere Hinweise zu diesem Sachverhalt wurden berücksichtigt.

5.7.4 Umgang mit amtsärztlichen Gutachten

Ein Mitarbeiter eines Klinikums, der dort als Krankenpfleger tätig ist, hat sich an uns gewandt. In den letzten drei Jahren sei er innerhalb des Klinikums mit einer anderen Tätigkeit betraut gewesen, die aus Drittmitteln finanziert worden sei. Da die Förderung der Stelle nicht verlängert worden sei, solle er wieder in einen Bereich des Klinikums wechseln, in dem im Drei-Schicht-System gearbeitet wird. Aufgrund gesundheitlicher Einschränkungen sähe er sich jedoch nicht in der Lage, diese Stelle anzunehmen. Er habe daher mit dem Personaldezernat vereinbart, diese gesundheitlichen Einschränkungen durch ein amtsärztliches Gutachten bestätigen zu lassen. Über das Ergebnis des Gutachtens sei das Personaldezernat durch das Gesundheitsamt informiert worden. In diesem Schreiben seien dem Personaldezernat auch Daten zur fachärztlichen Diagnose, Angaben über eine stationäre Behandlung in einem Fachkrankenhaus für Psychiatrie und Psychotherapie sowie auch darüber, dass er gegenwärtig Psychopharmaka einnimmt, übermittelt worden. Der Petent bat uns zu prüfen, ob dieses Vorgehen mit den datenschutzrechtlichen Bestimmungen vereinbar war.

Auf unsere Anfrage hin begründete der Amtsarzt die Übermittlung der oben genannten Gesundheitsdaten damit, dass der Arbeitgeber nur anhand dieser Angaben die vom Gesundheitsamt ausgesprochene Empfehlung nachvollziehen kann.

Wegen der Schwere und Besonderheiten der Erkrankung sowie der ungewöhnlichen umfangreichen und notwendigen Erleichterungen und im Interesse der Gesundheit des Petenten wurde dem Arbeitgeber auch die fachliche Diagnose übermittelt. Der Amtsarzt bedauert, dass er es versäumt hat, vom Petenten eine Schweigepflichtentbindungserklärung einzuholen.

Durch die medizinische Begutachtung soll in der Regel festgestellt werden, ob der Arbeitnehmer körperlich und seelisch in der Lage ist, eine bestimmte Tätigkeit unter den üblichen Bedingungen der jeweils in Betracht kommenden Arbeitssituation auszuüben. Dabei sind die besonderen Anforderungen hinsichtlich der Arbeitsschwere, des Arbeitsablaufs, der Einflüsse des Arbeitsumfeldes, der Arbeitszeit und der Arbeitsdauer individuell zu berücksichtigen.

Medizinische Erkenntnisse, die der Arzt im Rahmen einer Begutachtung über einen Arbeitnehmer gewonnen hat, unterliegen in vollem Umfang der ärztlichen Schweigepflicht. Unterzieht sich der Arbeitnehmer der ärztlichen Begutachtung, so kann der Arzt in der Regel davon ausgehen, dass der Betroffene mit der Weitergabe des Ergebnisses der Untersuchung an den Arbeitgeber einverstanden ist (konkludentes Handeln des Arbeitnehmers).

Der Umfang der ärztlichen Mitteilung an den Arbeitgeber hat sich jedoch grundsätzlich auf das Ergebnis der Untersuchung zu beschränken, also in dem geschilderten Fall auf die Feststellung, ob der Mitarbeiter geeignet ist, die Anforderungen des Schichtdienstes zu erfüllen. Diagnosen und Befunde gehören in der Regel nicht zu den Daten, die für den Arbeitgeber relevant sind. Sofern ein Arzt im Einzelfall feststellt, dass aus ärztlicher Sicht weitergehende Mitteilungen für den Arbeitgeber unbedingt erforderlich sind, weil diese Daten geeignet sind, Art, Schwere und den voraussichtlichen Verlauf der Gesundheitsstörung plausibel zu machen, ist das Einverständnis (Entbindung von der ärztlichen Schweigepflicht) des Betroffenen unbedingte Voraussetzung. Die Schweigepflichtentbindung muss konkret genug formuliert sein, damit der Betroffene, wie gesetzlich vorgeschrieben, abschätzen kann, welche Daten warum an wen übermittelt werden. Sie muss auf der freien Entscheidung des Betroffenen beruhen, der auf die Folgen einer Verweigerung einer Einwilligung hinzuweisen ist. Entbindungen von der Schweigepflicht sind zweckmäßigerweise schriftlich einzuholen, um zum Beispiel bei Streitigkeiten nachweisen zu können, dass diese erteilt worden ist. Selbst wenn der Amtsarzt aus fachlicher Sicht entscheidet, dem Arbeitgeber auch Gesundheitsdaten zu übermitteln, hat er auch den datenschutzrechtlichen Grundsatz der Erforderlichkeit zu berücksichtigen. Der Begriff der Erforderlichkeit ist dabei eng auszulegen. Erforderlich sind personenbezogene Daten nur dann, wenn die Aufgabe sonst nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllt werden kann.

Für den geschilderten Sachverhalt bedeutet dies, dass zunächst hätte geprüft werden müssen, ob die Übermittlung des Ergebnisses des Gutachtens ausreichend gewesen wäre. Sofern man zu dem Ergebnis gekommen wäre, dass weitere medizinische Daten an den Arbeitgeber zu übermitteln wären, hätte der Petent darüber informiert und um eine Entbindung von der ärztlichen Schweigepflicht gebeten werden müssen. Anderenfalls verletzt der Arzt die ärztliche Schweigepflicht und macht sich möglicherweise gemäß § 203 Strafgesetzbuch (StGB) der Verletzung von Privatgeheimnissen strafbar. Wir haben daher empfohlen, jede einzelne medizinische Angabe dahingehend zu prüfen, ob diese für die Plausibilitätsprüfung des Arbeitgebers erforderlich ist.

Der Amtsarzt hat unsere Ausführungen zum Anlass genommen, um das amtsärztliche Gutachten vom Personaldezernat zurückzufordern und in Abstimmung (ärztliche Schweigepflichtentbindungserklärung) mit dem Petenten abzuändern.

5.8 Statistik

5.8.1 Verdienststrukturerhebung benötigt Rentenversicherungsnummer

Im Jahr 2015 haben uns sehr viele Anfragen von öffentlichen Einrichtungen und Firmen erreicht, weil sie vom Statistischen Amt Mecklenburg-Vorpommern einen Heranziehungsbescheid zur Verdienststrukturerhebung 2014 erhalten haben. Einigen war die Verpflichtung zur Erhebung der Angaben im Rahmen der Verdienststrukturerhebungen aus den vergangenen Jahren schon bekannt. Allerdings sollte für das Jahr 2014 erstmals auch die Rentenversicherungsnummer für jede Arbeitnehmerin und jeden Arbeitnehmer angegeben werden. Dies ist bei den Anfragenden auf großes Unverständnis gestoßen.

Gegen die Erhebung der Rentenversicherungsnummer ist aus datenschutzrechtlicher Sicht nichts einzuwenden, da sich eine entsprechende Rechtsgrundlage für diese Datenübermittlung im Gesetz über die Statistik der Verdienste und Arbeitskosten (Verdienststatistikgesetz - VerdStatG) befindet. Neben den in §§ 3, 4 VerdStatG genannten Erhebungsmerkmalen sind auch die Hilfsmerkmale nach § 7 VerdStatG zu übermitteln. Nach dem ausdrücklichen Wortlaut der Nr. 3 VerdStatG gehört hierzu auch die Versicherungsnummer der gesetzlichen Rentenversicherung oder, wenn keine Versicherung in der gesetzlichen Rentenversicherung vorliegt, die Namen der Beschäftigten.

Die Erhebung dieses Hilfsmerkmals ist allerdings relativ neu in das Gesetz mit aufgenommen worden und hängt mit dem neu gefassten § 6 VerdStatG (Erprobung der Verwendung von Verwaltungsdaten) zusammen. Dort ist vorgesehen, dass beginnend mit der Verdienststrukturerhebung für das Kalenderjahr 2014 überprüft wird, inwieweit durch eine Verwendung von Daten der Sozialversicherung unter Nutzung des Hilfsmerkmals der Versicherungsnummer der gesetzlichen Rentenversicherung zukünftig auf die Erhebung gleichartiger Daten im Rahmen der Verdienststrukturerhebung verzichtet und die Auskunftspflicht entlastet werden kann.

Darüber hinaus haben wir den Anfragenden auch erläutert, dass im Statistikrecht ganz bestimmte strenge Vorschriften und Instrumentarien, die der Geheimhaltung dienen, bestehen bzw. einzuhalten sind. Letztere müssen hohen organisatorischen und technischen Anforderungen genügen, um eine Re-Identifizierung auszuschließen. So gelten für Hilfsmerkmale die Trennungs- und Löschvorschriften des Bundesstatistikgesetzes. Das heißt, auch die Rentenversicherungsnummer wird von den Erhebungsmerkmalen zum frühestmöglichen Zeitpunkt getrennt und bis zu ihrer Löschung gesondert aufbewahrt.

Zunächst dienen diese Merkmale der technischen Durchführung der Statistik und sind, soweit nicht etwas anderes bestimmt ist, zu löschen, sobald die Überprüfung der Erhebungs- und Hilfsmerkmale auf ihre Schlüssigkeit und Vollständigkeit abgeschlossen ist. So können zum Beispiel bei Unstimmigkeiten Nachfragen des Statistischen Amtes erforderlich sein und hierbei Verwechslungen vermieden werden.

Wenn keine Rückfragen mehr notwendig sind, wird die Versicherungsnummer zu einem anonymisierten Schlüssel umgewandelt und danach sofort gelöscht. Da das Verschlüsselungsverfahren nicht umkehrbar ist, kann von dem anonymisierten Schlüssel nicht auf die Versicherungsnummer geschlossen werden. Der in § 6 VerdStatG festgelegte Prüfungszweck erfolgt dann anhand der anonymisierten Schlüssel.

5.8.2 Modifizierung des Mikrozensus

Im Elften Tätigkeitsbericht hatten wir unter Punkt 6.7 bereits über die Volks- und Wohnungszählung (Zensus 2011) berichtet. Insbesondere ging es hierbei um den Einsatz der Erhebungsbeauftragten und um die Verschlüsselung der elektronischen Datenübermittlungen.

Mit Blick auf § 33 Abs. 5 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) informierte uns das Statistische Amt Mecklenburg-Vorpommern im Januar 2014 über ein modifiziertes automatisiertes Verfahren des unterjährigen Mikrozensus. Die Regelung im Landesdatenschutzgesetz soll sicherstellen, dass der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern rechtzeitig über neue Verfahrensentwicklungen im Zusammenhang mit der automatisierten Verarbeitung personenbezogener Daten informiert wird. So können bei der Planung von neuen oder veränderten Anwendungen unsere Hinweise zur datenschutzgerechten Ausgestaltung schon rechtzeitig berücksichtigt und somit das von uns immer wieder geforderte Datenschutzprinzip „Privacy by Design“ umgesetzt werden.

Das Statistische Amt Mecklenburg-Vorpommern beauftragt sogenannte Erhebungsbeauftragte, die statistische Daten direkt bei den zu Befragenden erheben. Dazu nutzen sie Laptops mit einem speziellen Mikrozensus-Clientprogramm, das die Daten über das Internet an den Mikrozensus-Server im Statistischen Amt überträgt. Bei der Prüfung dieses Verfahrens haben wir festgestellt, dass für den Verbindungsaufbau des Mikrozensus-Clientprogramms zum Mikrozensus-Server noch das veraltete TLS 1.0 und SSL 2 Protokoll verwendet wird *(siehe Kasten)*. Beide Varianten entsprechen nicht mehr dem aktuellen Stand der Technik, seit bei beiden mehrere Sicherheitslücken bekanntgeworden sind. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat daher empfohlen, bei der Übertragung von Daten in unsicheren Netzen TLS 1.2 in Verbindung mit Perfect Forward Secrecy *(siehe Kasten)* zu verwenden, um die Vertraulichkeit, Authentizität und Integrität der übermittelten Daten zu gewährleisten.

Wir haben das Statistische Amt Mecklenburg-Vorpommern über diese Empfehlung informiert und die Umstellung auf die aktuellen Protokolle empfohlen. Das Statistische Amt hat unsere Empfehlung akzeptiert und kurzfristig das Übermittlungsverfahren entsprechend geändert.

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.

TLS 1.2 wird mittlerweile häufig in Verbindung mit Perfect Forward Secrecy (*PFS*) oder zu Deutsch mit einer perfekt vorwärts gerichteten Geheimhaltung verwendet. PFS stellt hierbei sicher, dass ein in der Vergangenheit aufgezeichneter verschlüsselter Kommunikationsinhalt auch dann nicht bekannt wird, wenn der verwendete geheime Schlüssel kompromittiert wurde. Um dies zu erreichen, einigen sich beide Kommunikationspartner durch den Austausch mehrerer Nachrichten auf einen gemeinsamen, temporären Sitzungsschlüssel, der nicht über die „unsichere Leitung“ übertragen und nach Beendigung der Kommunikation zerstört wird.
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.

5.9 Werbung

5.9.1 Ungewollte E-Mail-Werbung und Newsletter

Immer wieder erhalten wir Petitionen, in welchen sich die Betroffenen darüber beschweren, dass sie ungewollt E-Mail-Werbung und Newsletter erhalten. Den Versendern von E-Mail-Werbung und Newslettern ist zum Teil nicht bekannt, dass dies eine unzumutbare Belästigung nach dem Gesetz gegen unlauteren Wettbewerb darstellt.

Um zulässig E-Mail-Werbung und Newsletter versenden zu können, muss grundsätzlich die Einwilligung des privaten Empfängers vorliegen. Dass eine Einwilligung vorliegt, muss der Versender im Zweifel nachweisen können.

Sofern die Einwilligung auf elektronischem Wege erfolgt, sollte hierfür das sogenannte Double-Opt-In-Verfahren verwendet werden. Meldet sich jemand für E-Mail-Werbung oder Newsletter mit seiner E-Mail-Adresse an, wird bei diesem Verfahren an die eingetragene Adresse ein Freischaltungslink versandt.

Wird dieser durch den E-Mail-Adresseninhaber aktiviert, bestätigt er dadurch, dass die Anmeldung durch ihn erfolgte und er in die Verwendung seiner E-Mail-Adresse für E-Mail-Werbung oder den Newsletter eingewilligt hat. Ferner muss der Versender jede individuell einzelne Eintragung in seinen E-Mail-Verteiler protokollieren, sodass in Zweifelsfällen die Einwilligung später individuell belegbar nachvollzogen werden kann, denn dem Versender obliegt die Darlegungs- und Beweislast.

Die E-Mail-Werbung und Newsletter müssen weiterhin den Hinweis enthalten, dass die erteilte Einwilligung jederzeit für die Zukunft widerrufen werden kann. Auch empfiehlt es sich, einen Link zu installieren, der es dem Betroffenen ermöglicht, sich ohne Weiteres aus dem E-Mail-Verteiler wieder austragen zu können.

Die von uns angeschriebenen Unternehmen haben in den überwiegenden Fällen sofort reagiert und die personenbezogenen Daten der Betroffenen gelöscht oder auf eine Sperrliste gesetzt, sodass die Betroffenen keine ungewollte E-Mail-Werbung oder Newsletter mehr erhalten.

5.9.2 Biometrische Gesichtserkennung für Werbezwecke

Gesichtserkennungssysteme werden zunehmend auch zu Werbezwecken genutzt, etwa um das Interesse von potentiellen Kundinnen und Kunden an einer bestimmten Werbung erfassen und auswerten zu können.

Ein Softwareprodukt, zu dessen datenschutzrechtlicher Bewertung wir aufgefordert wurden, sollte zu diesem Zweck in Ladengeschäften, Einkaufspassagen etc. in Verbindung mit Videokameras fortlaufend die Gesichter aller Personen erfassen, die sich im Erfassungsbereich der Kamera befanden. Ein Algorithmus wertet diese Gesichter sodann anhand biometrischer Merkmale aus (Behaarung, stark ausgeprägter Adamsapfel, Falten etc.), um das Geschlecht und das geschätzte Alter der abgebildeten Personen zu bestimmen. Ferner bewertet der Algorithmus anhand der Blickrichtung (Bewegung der Augenpupillen) und der Entfernung zum Werbemonitor und ihrer Verweildauer, ob die Person „stark interessiert“, „interessiert“ oder nur „aufmerksam geworden“ ist. Die genannten biometrischen Merkmale werden im Arbeitsspeicher des Rechners verarbeitet. Nachdem die aufgenommenen Personen das Kamerafeld verlassen hatten, sollten sechs abstrakte Informationen (Alter, Geschlecht, Zeit, Entfernung zum Produkt und Interesse) gespeichert bleiben. Die im Arbeitsspeicher gespeicherten Bildinformationen sollten automatisch gelöscht werden.

Nach unserer Auffassung war das Bundesdatenschutzgesetz (BDSG) anwendbar, weil (wenn auch nur kurzzeitig) personenbeziehbare Daten erhoben werden sollten. Nach § 6 b Abs. 1 BDSG war zu berücksichtigen, dass ein berechtigtes Interesse an einer solchen Datenerhebung und -verarbeitung in Bezug auf wirtschaftliche Interessen grundsätzlich restriktiv auszulegen ist. Ein berechtigtes Interesse ist daher zu verneinen für eine als Hauptzweck der Geschäftstätigkeit durchgeführte Beobachtung, wie es zum Beispiel bei einer Nutzung von Videoüberwachungsbildern zu reinen Werbezwecken der Fall wäre. Auch die nötige Erforderlichkeit sahen wir - insbesondere in Hinblick auf personelle Alternativlösungen (z. B. Kundenzufriedenheitsbeobachtungen und Nachfragen durch eigenes Personal) nicht als gegeben an. Insbesondere sahen wir ein überwiegendes schutzwürdiges Interesse der betroffenen Personen.

Auch wenn nach den technischen Angaben des Herstellers das Bild der jeweiligen Person später gelöscht wird und lediglich die genannten Merkmale verbleiben, die auf eine Vielzahl von Personen zutreffen, bestehen unseres Erachtens überwiegende schutzwürdige Interessen der betroffenen Passanten bereits darin, mit ihren biometrischen Merkmalen von vornherein im Alltag nicht erfasst zu werden. Schutzwürdige Interessen überwiegen regelmäßig, wenn automatisierte Verfahren beispielsweise zum Herausfiltern einzelner Personen, zur biometrischen Gesichtserkennung oder zum Bildabgleich mit anderen bereits gespeicherten Daten eingesetzt werden. Dies war hier - wenn auch kurzfristig - sowohl während der Erhebung der Bilddaten nach § 6 b Abs. 1 BDSG als auch während der Nutzung (§ 6 b Abs. 3 BDSG) dieser erhobenen Daten zum Zweck der Auswertung biometrischer Merkmale der Fall.

Unabhängig von der rechtlichen Bewertung sehen wir im Fall der Einführung solcher Systeme die Gefahr, dass eine Infrastruktur entsteht, die mit nur geringfügigen technischen Änderungen zu einer sehr großflächigen Überwachung führen kann. In Anbetracht des starken Trends zur personalisierten Werbung und im Hinblick auf die allgegenwärtigen Werbeflächen im Alltag wäre mit einer großen Verbreitung zu rechnen, sodass sich die ohnehin schon große Zahl von Videokameras im öffentlichen Raum noch erheblich erhöhen würde. Wir sahen hier ein hohes Missbrauchspotential, weil damit faktisch in weiten Bereichen der Öffentlichkeit eine Infrastruktur aufgebaut werden würde, die technisch dazu in der Lage ist, biometrische Daten von Personen erfassen und auswerten zu können.

5.10 Bildung

5.10.1 Schulverwaltungssoftware und Lernsoftware

Im Laufe des Berichtzeitraums erreichten uns mehrere Anfragen zum Einsatz von Schulverwaltungs- und Lernsoftware. Die beiden Softwarevarianten unterscheiden sich wesentlich, da sie unterschiedliche datenschutzrechtliche Anforderungen erfüllen müssen.

Mit Hilfe der Schulverwaltungssoftware werden klassische Verwaltungsaufgaben bearbeitet, wie die Pflege von Schüler- und Lehrerstammdaten, die Lernmittelverwaltung oder Statistikaufgaben. Lernsoftware hingegen soll die Digitalisierung des Unterrichtes unterstützen. Sie soll Wissen während und außerhalb des Unterrichts digital vermitteln und gegebenenfalls die Kommunikation zwischen Schülern und Lehrern unterstützen.

In der Praxis erleben wir regelmäßig, dass Schulverwaltungs- und Lernsoftware einen sehr breiten Funktionsumfang haben. Dieser breite Funktionsumfang ist vielfach nur schwer mit dem deutschen Datenschutzrecht vereinbar, weil mitunter weit mehr personenbezogene Daten verarbeitet werden können als erforderlich oder gesetzlich zulässig ist.

Bei der Planung und beim Einsatz von Schulverwaltungs- und Lernsoftware muss berücksichtigt werden, dass Daten mit unterschiedlichem Schutzbedarf verarbeitet werden. So haben sensible Daten wie beispielsweise Noten, Ergebnisse aus schulärztlichen Untersuchungen oder aber besondere Vorkommnisse im Unterricht einen höheren Schutzbedarf als das einfache Einschulungs- oder Geburtsdatum eines Schülers. Um aber Daten mit einem höheren Schutzbedarf insbesondere im Hinblick auf ihre Vertraulichkeit und Integrität sicher verarbeiten zu können, sind höhere Anforderungen an die dafür notwendigen technischen und organisatorischen Maßnahmen zu stellen.

Diese Maßnahmen ergeben sich aus § 21 Abs. 1 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V). Um die Vertraulichkeit zu gewährleisten, sei an dieser Stelle beispielsweise die Zwei-Faktor-Authentifizierung genannt. Hierbei wird die Anmeldung am IT-System mit Hilfe von zwei unterschiedlichen Komponenten realisiert, zum Beispiel durch die Verwendung eines starken Passwortes in Verbindung mit einem Besitz, wie einer Chipkarte oder einem Hardware-Token. Zur Gewährleistung der Integrität und der Authentizität, also der Unversehrtheit und der Echtheit der elektronisch gespeicherten Daten, ist beispielsweise eine qualifizierte elektronische Signatur geeignet.

Die uns bekannten Softwareprodukte verfügen jedoch über keine Vorkehrungen, die eine Verarbeitung von Daten mit höherem Schutzbedarf datenschutzrechtlich legitimieren.

In diesem Zusammenhang ist auch zu beachten, dass insbesondere Lernsoftwareprodukte oftmals als Cloud-Lösungen konzipiert sind. Die zu verarbeitenden Daten werden in diesem Fall nicht auf einem Server in der Schule gespeichert sondern in der Regel beim Hersteller der Lernsoftware. Ob die Server des Herstellers in Deutschland, in Europa oder anderswo auf der Welt stehen, ist für den Kunden oftmals nicht ersichtlich. Damit kann der Kunde nicht beurteilen, ob es überhaupt möglich ist, die Vorgaben des deutschen Datenschutzrechts einzuhalten.

Neben den bisher genannten technischen Rahmenbedingungen sind jedoch auch noch einige organisatorische zu beachten. Wenn etwa die Schule die Daten nicht selbst verarbeitet, sondern damit andere Personen oder Stellen („Dritte“) beauftragt, muss die Schule einen Vertrag zur Verarbeitung von Daten im Auftrag gemäß § 4 DSG M-V abschließen. Die Schule ist dabei verpflichtet, den Auftragnehmer unter besonderer Berücksichtigung seiner Eignung auszuwählen. Dieser muss also in der Lage sein, die notwendigen technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten zu gewährleisten.

Jedoch kann nach unserer Erfahrung kaum eine Schule alleine das notwendige Know-How aufbringen, um eine solche Beurteilung rechtssicher treffen zu können. Das Landesdatenschutzgesetz Mecklenburg-Vorpommern bietet aber auch in solchen Fällen Unterstützung, indem es ermöglicht, dass unabhängige Prüfer derartige Produkte auf ihre Datenschutzkonformität hin überprüfen und das Ergebnis mit einem Datenschutz-Gütesiegel bescheinigen. Jeder Hersteller hat die Möglichkeit, auf freiwilliger Basis seine Software auf die Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit in einem solchen Prüfverfahren feststellen zu lassen. Das Landesdatenschutzgesetz legt fest, dass eine so zertifizierte Software durch die öffentlichen Stellen sogar vorrangig einzusetzen ist. Die Schule muss dann nur noch prüfen, ob die Funktionen der Software geprüft wurden, die sie verwenden möchten, und kann dann ohne weitere Detailprüfungen das entsprechende Produkt verwenden.

Der Vollständigkeit halber sei hier noch erwähnt, dass zu den organisatorischen Anforderungen natürlich auch das Verfahrensverzeichnisses gemäß § 18, ein Sicherheitskonzept gemäß § 22 Abs. 5 und die förmliche Freigabe gemäß § 19 DSG M-V zählen. Dass die Erstellung dieser Unterlagen sowohl technisches Verständnis als auch ein angemessenes Zeitbudget erfordert, sollte von vornherein berücksichtigt werden.

Wir empfehlen den Verantwortlichen im Bereich Schule, auf die automatisierte Verarbeitung von Daten mit höherem Schutzbedarf mit Hilfe von Verwaltungs- und Lernsoftware zu verzichten, solange dafür keine datenschutzkonforme Software am Markt verfügbar ist. Schon bei der Konzipierung derartiger Softwareprodukte ist in jedem Falle das Gebot der Datensparsamkeit zu berücksichtigen.

5.10.2 Das Portal „Young Data“

Die Webseite „Young Data“ (https://www.youngdata.de/) wird seit 2014 als gemeinsames Portal der Datenschutzbeauftragten des Bundes und der Länder betrieben. Mit „Young Data“ wird jungen Leuten ein jugendgerecht aufbereitetes Angebot zur Verfügung gestellt, das Informationen zum Datenschutz, Datenschutztipps für ein sorgsames Verhalten im Internet sowie Berichte über die digitale Zukunft unserer Gesellschaft beinhaltet.

Um mit den technologischen Entwicklungen sowie den fortschreitenden Angeboten im Internet Schritt zu halten, ist eine kontinuierliche Entwicklung der Webseite notwendig. Da uns das Thema „Datenschutz als Bildungsaufgabe“ (siehe auch Punkt 2.1) besonders wichtig erscheint, stand für unsere Behörde außer Frage, dass wir uns auch an der Entwicklung beteiligen. Wir haben daher die Patenschaft für die Hauptmenüpunkte „Facebook“ und „WhatsApp, Skype & Co.“ übernommen.

Zurzeit entwickeln wir mit mehreren Kollegen aus anderen Bundesländern einen neuen Menüpunkt, der praktische Tipps geben soll, um den „Selbstdatenschutz“ im Internet zu verbessern.

6 Arbeitskreis „Technische und organisatorische Datenschutzfragen“

6.1 Turnusmäßige Sitzungen des AK Technik

Im Zeitalter des E-Government und der ständig steigenden Zahl der länderübergreifenden elektronischen Verwaltungsverfahren einerseits sowie der komplexen elektronischen Verfahren im Bereich der Wirtschaft andererseits spielt die bundesweite Koordinierung der technischen und organisatorischen Datenschutzaspekte eine immer größere Rolle. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz) hat uns auch im vergangenen Berichtszeitraum das Vertrauen ausgesprochen, den zu diesem Zweck gegründeten Arbeitskreis „Technische und organisatorische Datenschutzfragen (AK Technik) zu leiten. Zudem hat sich gezeigt, dass der AK Technik als Bindeglied zwischen dem IT-Planungsrat, siehe Punkt 3, und der Datenschutzkonferenz eine wichtige Rolle spielt.

Auch in diesem Berichtszeitraum haben wir die bewährte Tagungsfrequenz beibehalten: Wir haben in den Jahren 2014 und 2015 jeweils zwei Sitzungen des AK Technik organisiert und durchgeführt.

Zur **62. Sitzung** hatten uns die Kollegen aus Rheinland-Pfalz im Februar 2014 nach Mainz eingeladen. Anlass für diese Einladung war das Projekt „Cloud-Richtlinien der Datenzentralen“. Der Arbeitskreis der Leiter der Datenzentralen der Bundesländer hatte eine Richtlinienempfehlung für die Ausschreibung, die Vergabe und den Betrieb von öffentlichen Aufträgen in der Cloud erarbeitet, siehe Punkt 3.2, die der Landesbetrieb Daten und Information Rheinland-Pfalz dem AK Technik vorstellen wollte. Der AK Technik befürwortete die Richtlinien und begrüßte den Ansatz, personenbezogene Daten nur in solchen Cloud-Strukturen zu verarbeiten, die in nationalen, zertifizierten Hochsicherheitsrechenzentren betrieben werden und somit den Datenschutzregeln in der Europäischen Union unterliegen. Während dieser Sitzung befasste sich der Arbeitskreis auch mit der neuen DIN 66399 (Vernichtung von Datenträgern - siehe Punkt 4.1.6) und mit ersten Umsetzungsempfehlungen, die die Gesellschaft für Datenschutz und Datensicherung in ihrer Broschüre „Datenschutzgerechte Datenträgervernichtung“ veröffentlicht hat. Darüber hinaus beschloss der AK Technik einen Stufenplan zur Sicherung der elektronischen Kommunikation zwischen den Aufsichtsbehörden. Schließlich erarbeiteten die Mitglieder den Entwurf der Entschließung zur Gewährleistung der Grundrechte bei der elektronischen Kommunikation, den die Datenschutzkonferenz auf ihrer Sitzung im Frühjahr 2014 verabschiedete, siehe Punkt 4.1.9.

Die **63. Sitzung** im September 2014 fand in Schwerin statt. Angesichts der zahlreichen Anfragen bei den Datenschutzbehörden zu Microsoft-Office-Produkten, insbesondere zu Office 365 und zu verschiedenen Cloud-Angeboten, war der Vertriebsleiter Cloud-Computing für öffentliche Auftraggeber der Firma Microsoft eingeladen worden, um die für Cloud-Dienstleistungen verwendete Rechenzentrumslandschaft von Microsoft, die Nutzung von MS-Cloud-Dienstleistungen im eigenen Hause sowie Details zu Administration und Anwendersupport bei MS Office 365 vorzustellen. Der Arbeitskreis beschloss in dieser Sitzung auch, den Entwurf des Standard-Datenschutzmodells, siehe Punkt 4.1.1, der Datenschutzkonferenz vorzulegen, um das Mandat zur weiteren Bearbeitung und die Zustimmung zur Einbeziehung der Fachöffentlichkeit einzuholen. Darüber hinaus beschloss der AK Technik in dieser Sitzung, einen Anforderungskatalog zur sicheren Übermittlung von Krebsregisterdaten auszuarbeiten und der Datenschutzkonferenz zu empfehlen, auf diese Anforderungen mit einer Entschließung hinzuweisen, siehe Punkt 5.6.3.

Die **64. Sitzung** fand auf Einladung des Thüringer Landesdatenschutzbeauftragten im Februar 2015 in Erfurt statt. Unser Thüringer Kollege leitet den Arbeitskreis „Datenschutz und Bildung“ und wollte die Gelegenheit nutzen, Fragen des datenschutzgerechten Einsatzes von Informationstechnik an Schulen mit den Mitgliedern des AK Technik zu beraten. Wir berieten gemeinsam über den Einsatz von Apps auf privaten IT-Systemen von Lehrkräften und diskutierten über den Entwurf einer Orientierungshilfe „Online-Lernplattformen im Schulunterricht“. Auch in dieser Sitzung wurde wieder ein Entschließungsentwurf für die Datenschutzkonferenz vorbereitet, der unter anderem die uneingeschränkte Nutzung von Verschlüsselungstechnik fordert, siehe Punkt 4.1.10.

Als Schwerpunktthema für die **65. Sitzung**, diesmal wieder in Schwerin, hatten wir das Thema „Schutz personenbezogener Daten durch Verschlüsselung“ gewählt und dazu mehrere Experten eingeladen. Herr Dr. Wegener von der Ruhr-Universität Bochum/Fakultät für Elektrotechnik und Informationstechnik beschrieb Angriffsmöglichkeiten auf kryptographischen Verfahren und erläuterte deren Langzeitsicherheit.

Wir erörterten gemeinsam, welche Schutzwirkungen von kryptographischen Verfahren für personenbezogene Daten realistisch zu erwarten sind. Anhand von zwei bereits realisierten Verschlüsselungslösungen erläuterten Experten aus dem Bereich der Wirtschaft die Möglichkeiten der Verschlüsselung in der Cloud und Szenarien für sichere mobile Unternehmenskommunikation mit Hilfe einer speziellen Verschlüsselungs-App für mobile Geräte. Zudem beschlossen die Mitglieder eine fortgeschriebene Version des Standard-Datenschutzmodells mit dem Ziel der uneingeschränkten Veröffentlichung durch die Datenschutzkonferenz. Der Arbeitskreis befasste sich in dieser Sitzung erneut mit Produkten der Firma Microsoft und beriet über die erforderlichen Prüfstrategien bei neuen Cloud-basierten Betriebssystemen wie Windows 10 oder Office-Produkten wie Office 365, siehe dazu auch Punkt 4.1.11.

6.2 Workshop des AK Technik

Den inzwischen etablierten gemeinsamen Workshop von Juristen und Technikern der Dienststellen der Datenschutzbehörden von Bund und Ländern haben wir in diesem Berichtszeitraum genutzt, um unsere Kolleginnen und Kollegen mit dem Standard-Datenschutzmodell vertraut zu machen, siehe Punkt 4.1.1. Bis zum Zeitpunkt des Workshops im April 2015 hatte sich vorwiegend eine kleine Arbeitsgruppe aus Juristen und Technikern unter Federführung Schleswig-Holsteins mit dem Modell befasst. Deshalb war es an der Zeit, die inzwischen schon weit fortgeschrittenen Entwürfe des Modells einem möglichst großen Kollegenkreis vorzustellen.

Dank der Unterstützung unserer Kolleginnen und Kollegen aus Niedersachsen konnten wir den Workshop in Hannover durchführen. Wir konnten zahlreiche Teilnehmerinnen und Teilnehmer aus allen Datenschutzdienststellen von Bund und Ländern begrüßen. Die Mitglieder der Arbeitsgruppe gingen in ihren Vorträgen auf die Entstehungsgeschichte des Modells ein, erläuterten den Bezug der Gewährleistungsziele zu den bestehenden rechtlichen Regelungen und zu der kommenden Europäischen Datenschutz-Grundverordnung (EU-DSGVO) und beschrieben das Zusammenspiel von Recht und Technik bei der Nutzung des Modells. Anhand konkreter Fallbeispiele erläuterten sie die Anwendung des Modells sowohl im öffentlichen als auch im nicht-öffentlichen Bereich. In der anschließenden Diskussion wurde intensiv über verschiedene Details des Modells beraten und es wurden zahlreiche Vorschläge für Verbesserungen und Konkretisierungen des Modells unterbreitet. Dabei wurde aber auch deutlich, dass auch weiterhin intensiv für die Akzeptanz des Standard-Datenschutzmodells geworben und dass das Modell mit Blick auf die Europäische Datenschutz-Grundverordnung im internationalen Umfeld etabliert werden muss.

Die Materialien des Workshops haben wir insbesondere mit Hilfe unserer sächsischen Kollegen in einem Tagungsband zusammengefasst und in unserem Internetangebot zusammen mit dem Standard-Datenschutzmodell veröffentlicht (https://www.datenschutz-mv.de/datenschutz/sdm/sdm.html). Wir verweisen an dieser Stelle noch einmal auf unsere Empfehlung an die Landesregierung in Punkt 4.1.1, das Modell evaluierend anzuwenden und uns über die Erfahrungen beim Umgang mit diesem Werkzeug zu berichten.

6.3 Technology Subgroup – Zusammenarbeit auf europäischer Ebene

Die Artikel-29-Gruppe wurde als zentrales Koordinierungsgremium für die datenschutzrechtliche Aufsicht innerhalb der Europäischen Union eingerichtet. Ähnlich dem AK Technik, siehe Punkt 6, 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 der regelmäßige Meinungsaustausch und die gemeinsame Meinungsbildung zwischen den Mitgliedsstaaten. Dazu gehören auch gemeinsame Untersuchungen bei international agierenden Unternehmen wie Facebook und Google sowie 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 Meldepflicht bei Datenlecks (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf), Anonymisierungstechniken (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf), Internet der Dinge (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf), Fingerprinting (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp224_en.pdf), Einsatz von Drohnen (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf) sowie die Selbstverpflichtung von Cloud-Computing-Anbietern (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf) ausführlich bewertet. Weiterhin wurde in einer gemeinsamen Aktion eine Untersuchung zum Einsatz von Cookies auf europäischen Webseiten (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp229_en.pdf) durchgeführt.

7 Öffentlichkeitsarbeit

7.1 Datenschutz-Fachtagungen

7.1.1 E-Government in den Kommunen – sicher und datenschutzkonform?

Die Datenschutz-Fachtagung 2014 zum Thema „E-Government in den Kommunen – sicher und datenschutzkonform“ fand am 7. Mai 2014 im Bürgersaal in Waren (Müritz) statt. Sowohl Bürgerinnen und Bürger als auch Unternehmen, Vereine und viele andere fordern von der kommunalen Verwaltung die Möglichkeit der elektronischen Kommunikation. Sie erwarten einen schnellen, einfachen und sicheren Zugang zur Verwaltung zu jeder Zeit und von jedem Ort und eine rasche Erledigung ihrer Anliegen. E-Government-Verfahren können die Voraussetzungen für zeit- und ortsunabhängige Verwaltungsdienste schaffen. Die Erfahrung zeigt jedoch immer wieder, dass viele Kommunen erhebliche Schwierigkeiten haben, die Anforderungen an die Informationssicherheit und an den Datenschutz umzusetzen. Die Datenschutz-Fachtagung hat aus diesem Grunde die Rahmenbedingungen für kommunales E-Government analysiert und Lösungsansätze aufgezeigt.

Norbert Möller, Bürgermeister der Stadt Waren (Müritz), teilte in seinem Grußwort mit, dass das Thema Datenschutz überall präsent sei. Überall wird mit großen Datenmengen gearbeitet und der Schutz insbesondere von personenbezogenen Daten und der entsprechende sachgerechte und verantwortungsbewusste Umgang mit diesen Daten ist eine der wichtigsten täglichen Aufgaben. Eine Kommunalverwaltung kann ihre Aufgaben nicht ohne die Einbeziehung persönlicher Daten der Bürgerinnen und Bürger erfüllen. Eine weitere Herausforderung zum Thema Datenschutz innerhalb der Verwaltung bestehe darin, dass nicht immer alles, was technisch möglich ist, auch aus datenschutzrechtlicher Sicht umgesetzt werden kann. Er wünschte der Datenschutz-Fachtagung eine interessante und vielschichtige Diskussion und jede Menge Input für den künftig richtigen Umgang mit dem komplexen Thema Datenschutz in den Kommunen.

Dr. Thomas Darsow, Abteilungsleiter im Ministerium für Inneres und Sport Mecklenburg-Vorpommern, ging in seinem Grußwort auf die sich durch die technische Entwicklung verändernden Bedingungen ein. Er stellte Unterschiede der Erwartungen der Bürgerinnen und Bürger im elektronischen Handeln im privaten Bereich einerseits und im Kontakt mit der öffentlichen Verwaltung andererseits heraus. Dies und das deutsche Verständnis des Schutzes personenbezogener Daten berücksichtigend beschrieb er die Anforderungen, denen sich die Kommunalverwaltungen in Bezug auf die erforderlichen technischen Systeme stellen müssen, und zeigte anhand von Beispielen, wie diese Anforderungen in der Vergangenheit bereits bewältigt wurden und welche Schlussfolgerungen daraus gezogen werden können.

Dr. Stefan Grosse, Referatsleiter im Bundesministerium des Innern, sprach zu den Vorgaben des IT-Planungsrates. Die „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ wurde im März 2013 durch den IT-Planungsrat verabschiedet. Damit wurde zwischen Bund und Ländern ein verbindliches Mindestsicherheitsniveau in der Verwaltungs-IT vereinbart. Der Vortrag gab einen Überblick über die hieraus resultierenden Vorgaben des IT-Planungsrates. Dr. Grosse stellte die Sicht des Bundes auf die Rolle der Kommunen in der Informationssicherheit vor und betonte die Notwendigkeit der Ebenen übergreifenden Zusammenarbeit und weiteren Professionalisierung in der Verwaltungs-IT.

Franz-Reinhard Habbel, Direktor für politische Grundsatzfragen beim Deutschen Städte- und Gemeindebund, sprach zum Thema „Die Leitlinie für die Informationssicherheit - Pflicht für die Kommunen?“. In seinem Vortrag ging er darauf ein, dass die fortschreitende Digitalisierung neue Anforderungen an Datensicherheit und Datenschutz in Politik und Verwaltung stellt. Er warnte vor der Illusion einer „100-Prozent-Sicherheit“ und forderte dennoch höchstmögliche Sicherheit und ein ständiges Auseinandersetzen und Nachbessern mit dem Thema IT-Sicherheit. IT-Experten der Verwaltung und IT-Experten der Wirtschaft müssten hier Hand in Hand zusammenarbeiten.

Bernd Anders, Verbandsvorsteher des Zweckverbandes „Elektronische Verwaltung in Mecklenburg-Vorpommern“ (eGo M-V), ging in seinem Vortrag „IT-Sicherheit und Datenschutz in den Kommunen - eine Bestandsaufnahme“ auf die Themenbereiche IT-Sicherheit und Datenschutz in den Kommunen Mecklenburg-Vorpommerns ein. Dabei stellte er für beide Bereiche den aktuellen Stand in den Kommunalverwaltungen vor. Er erläuterte, welche Maßnahmen in den Verwaltungen in Bezug auf IT-Sicherheit und Datenschutz bereits umgesetzt sind und beschrieb, warum es zwischen den Verwaltungen doch erhebliche qualitative Unterschiede gibt.

Matthias Bitterlich, Sachgebietsleiter EDV - Allgemeine Verwaltung in der Stadtverwaltung der Stadt Waren (Müritz), gab in seinem Vortrag „Sicheres E-Government in der Kommune – geht das eigentlich?“ einen Einblick in die tägliche Praxis eines Administrators vor Ort. Auch er wies darauf hin, dass es sicheres E-Government in der Kommune nie zu 100 % geben kann - aber die Risiken können durch entsprechende technische und organisatorische Maßnahmen minimiert werden.

Hubert Ludwig, Geschäftsführer der DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH (DVZ M-V GmbH), ging in seinem Vortrag „DVZ M-V GmbH - IT-Dienstleister auch für die Kommunen?“ schwerpunktmäßig auf die Entwicklung der DVZ M-V GmbH, auf deren Rolle im Verbund der Datenzentralen in Deutschland, auf Entwicklungstendenzen des Bundes sowie die Nationale E-Government-Strategie und auf die Ausrichtung der DVZ M-V GmbH aus Kompetenzcluster des Landes Mecklenburg-Vorpommern ein. Darüber hinaus erläuterte er Möglichkeiten der Nutzung gemeinsamer Landesressourcen und informierte über Service- und Leistungsangebote der DVZ M-V GmbH in gemeinsamer Abstimmung mit dem Zweckverband M-V.

Rolf Christiansen, Landrat des Landkreises Ludwigslust-Parchim, informierte in seinem Vortrag „Interkommunale Zusammenarbeit - der Ausweg?“ über neue Wege, die der Landkreis Ludwigslust-Parchim und die Landeshauptstadt Schwerin im Rahmen der interkommunalen Zusammenarbeit mit der Errichtung eines gemeinsamen Kommunalunternehmens für den Betrieb ihrer Informationstechnik beschreiten. Ein gemeinsames Kommunalunternehmen in der Rechtsform einer kommunalen Anstalt des öffentlichen Rechts gab es bisher im Land Mecklenburg-Vorpommern noch nicht, diese Möglichkeit der interkommunalen Zusammenarbeit wurde erst mit Änderung der Kommunalverfassung Ende 2011 geschaffen. Der Landkreis Ludwigslust-Parchim und die Landeshauptstadt Schwerin kooperieren bereits seit mehreren Jahren auf verschiedenen Gebieten der Verwaltung. Beispiele sind die Leitstelle Westmecklenburg sowie die gemeinsam von Landkreis und Stadt betriebene Kfz-Zulassung, der Fachdienst Vermessung und Geoinformation sowie der Fachdienst Veterinär- und Lebensmittelüberwachung.

Gerd Czyborra, Referatsleiter im Ministerium für Inneres und Sport Mecklenburg-Vorpommern, ging in seinem Vortrag „Kooperatives E-Government in Mecklenburg-Vorpommern“ auf die Möglichkeiten des Verwaltungsebenen übergreifenden E-Governments ein. In der Landesverwaltung Mecklenburg-Vorpommern bezeichnet man die Zusammenarbeit Land – Bund sowie Land – Land als föderatives E-Government. Die Zusammenarbeit zwischen Land und Kommunen wird als kooperatives E-Government definiert.

Um die Zusammenarbeit zwischen Land und Kommunen abzustimmen und weiterzuentwickeln, wurde im Jahr 2003 eine gemeinsame E-Government-Initiative gestartet. Wichtige strategische Ausrichtungen, Meilensteine und Standards fanden in Folge im Masterplan (2004) sowie in der Roadmap (2007) ihren Eingang. Zur Steuerung der Umsetzung wurde ein Lenkungsausschuss gebildet, in dem das Land, der Landkreistag und der Städte- und Gemeindetag in paritätischer Besetzung vertreten sind. Zwischen den Ausschusstagungen leitet das „Büro kooperatives E-Government“ die Geschäfte. Zu den aktuellen Arbeitsschwerpunkten gehören insbesondere die gemeinsame Nutzung und Entwicklung von Infrastrukturen und Basiskomponenten, die Umsetzung des E-Government-Gesetzes, Standardisierung von Leistungen, Datenschutz- und Datensicherheit, einheitliche Grundlagen für das Wissens- und Prozessmanagement, Bürgerpartizipation (etwa D115, DeMail, „Klarschiff“). Die Ausgangssituation sowie die Rahmenbedingungen und das Umfeld für ein kooperatives E-Government sind gut. Um eine weitere Voraussetzung - die Einigkeit der Akteure - gilt es ständig zu ringen.

Die Beiträge der Datenschutz-Fachtagung können im Internetangebot unserer Behörde nachgelesen werden (https://www.datenschutz-mv.de/datenschutz/veranstaltungen/egov.html).

7.1.2 Schöne neue Schule? - Im Spannungsfeld von Datenschutz, informationstechnischer Entwicklung und schulischer Wirklichkeit

Die Datenschutz-Fachtagung 2015 zum Thema „Schöne neue Schule - Im Spannungsfeld von Datenschutz, informationstechnischer Entwicklung und schulischer Wirklichkeit“ fand am 25. Juni 2015 im Bürgersaal in Waren (Müritz) statt. Die Erwartungen an Schulverwaltungs- und Lernsoftware sowie die Berücksichtigung datenschutzrechtlicher Aspekte beim Einsatz dieser Software standen im Mittelpunkt der Fachtagung. Diese Thematik wirft viele Fragen auf: Wie kann Schulverwaltungs- und Lernsoftware multifunktional sein und gleichzeitig auch datenschutzrechtliche Forderungen umsetzen? Wie kann diese Software den Informations- und Kommunikationsprozess optimieren und dabei datenschutzrechtliche Aspekte zuverlässig berücksichtigen? Wie kann der Einsatz von Lernsoftware zur Entwicklung von Medienkompetenz beitragen und dabei auch stets den Datenschutz garantieren? Denn Schulverwaltungs- und Lernsoftware sind geeignet, den Arbeitsalltag zu erleichtern und Information und Kommunikation zu optimieren, sie müssen dabei jedoch stets einen zuverlässigen und sicheren Umgang mit allen Daten gewährleisten.

Mathias Brodkorb, Minister für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern, stellte in seinem Vortrag zum Thema „Informations- und Kommunikationstechnik in den Schulen des Landes Mecklenburg-Vorpommern - Ausstattung der Schulen mit Schulverwaltungs- und Lernsoftware“ seine Erwartungen an Schulverwaltungs- und Lernsoftware vor.

Zusammengefasst favorisierte er eine einheitliche, serverbasierte Lösung in Mecklenburg-Vorpommern, die alle Schulen im Land nutzen und über das Corporate Network des Landes (CN LAVINE) erreichen könnten. Die Standards sollen dabei in enger Abstimmung mit dem Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern erarbeitet werden.

Jan Krienke, freiberuflicher Medienpädagoge, legte in seinem Vortrag „Digital oder eher nicht? Erwartungen und Wünsche an schulische Medienbildung“ dar, dass die wichtigen und richtigen Vorgaben für Medienbildung in der Schule seit längerem gemacht worden seien. Um diesen Vorgaben und auch den Wünschen der Schülerinnen und Schüler gerecht werden zu können, bestünde jedoch weiterhin Handlungsbedarf. Als unverzichtbare Grundlage für schulische Medienbildung sieht er eine entsprechende technische Ausstattung sowie ein sicheres Netzwerk und einen schnelleren Internetzugang an Schulen, damit an die Lebenswelt der Kinder und Jugendlichen angeknüpft werden kann und Medienerfahrungen auch in Schulen gemacht werden könnten. Wichtig sei aber auch, dass Medienbildung nicht beim reinen Nutzen von Medien ende, sondern auch einen kritischen Umgang und kreativen Gebrauch von Medien umfasse. Wie das funktionieren kann, sei den Lehrenden besonders in der Lehramtsausbildung sowie der Lehrerfort- und -weiterbildung zu vermitteln. Für solche Fortbildungen wie auch für die Anwendung des Erlernten muss den Lehrenden ausreichend Zeit und ggf. Begleitung eingeräumt werden. Am wichtigsten sei in der Arbeit an Schulen sowie mit Eltern ein offenes, aufgeschlossenes Klima, welches ein weitgehend angstfreies Ausprobieren, eine die Medienkompetenz fördernde Auseinandersetzung und eine kreative Entfaltung mit und über Medien erst ermögliche.

Dr. Stephan Pfisterer, Bereichsleiter Bildungspolitik und Arbeitsmarkt bei BITKOM, stellte die BITKOM-Studie zum Einsatz digitaler Medien im Schulunterricht „Digitale Schule - vernetztes Lernen - Kompetenzen für eine sichere IT- und Mediennutzung“ vor. Demnach erteilen Schülerinnen und Schülern der IT-Ausstattung ihrer Schulen von Jahr zu Jahr schlechtere Noten. Sie wünschen sich einen stärkeren Einsatz von digitalen Medien im Unterricht. Wenn die Ausstattung bestimmten Mindeststandards nicht entspricht, seien die Bemühungen zum Einsatz digitaler Medien im Unterricht zum Scheitern verurteilt. Die Studie zeigt zudem, dass sich die Schere zwischen der privaten IT-Ausstattung und dem Gerätepark der Schulen immer weiter öffne. Notwendig sei eine „Digitale Agenda“ für die Schulen. Nur auf den ersten Blick gehörten inzwischen PC, Notebook und Beamer im Unterricht zum Standard. Ein regelmäßiger Nutzen diese Geräte im Rahmen der Unterrichtsarbeit erfolge jedoch kaum. Überwiegend werden der Studie zufolge digitale Geräte für die Präsentation von Lerninhalten sowie zur Internetrecherche genutzt.

Dr. Imke Sommer, Landesbeauftragte für Datenschutz und Informationsfreiheit Bremen, sprach zum Thema „Informationelle Selbstbestimmung beim Einsatz von Lernplattformen - Bremer Erfahrungen“. Aus der Sicht des Grundrechts auf informationelle Selbstbestimmung gehörten der Einsatz von Lernplattformen und die Bewertung von Big-Data, Cloud-Computing und vermeintlich „smarten“ Anwendungen zusammen. Die bei dem Einsatz von Lernplattformen entstehenden Daten der Schüler/innen, Lehrer/innen und der Eltern wären ein gefundenes Fressen für Profilbildungen und „smarte“ Anwendungen. Vor solchen Missbräuchen könnte vor allem die Beachtung des Grundrechtes auf informationelle Selbstbestimmung wirksam schützen.

Die bremische Landesbeauftragte für Datenschutz und Informationsfreiheit referierte über die datenschutzrechtlichen Aspekte der bremischen Diskussion über den Einsatz von Lernplattformen. Dabei ging es laut Sommer auch um die gesetzlich geforderte Transparenz für die Betroffenen und um die Umsetzung der rechtlichen Rahmenbedingungen im Vergabeverfahren und in einer geplanten Dienstvereinbarung.

Frank Hunger, Pädagogischer Leiter/Teamkoordinator des Medienpädagogischen Zentrums Meißen, sprach zum Thema „Schulisches Cloud-Computing und Online-Mediendistribution in Sachsen“. Mit „MeSax/LernSax“ wird sächsischen Bildungseinrichtungen ein komplexes Unterstützungswerkzeug zur Arbeit mit elektronischen Medien zur Verfügung gestellt. Hunger stellte heraus, dass für den Erfolg entscheidend gewesen sei, die Projektleitung in die Hände einer kompakten, mit weitreichenden Entscheidungskompetenzen ausgestatteten Projektgruppe aus Schulpraktikern mit Spezialkenntnissen im Medienbereich zu legen. Diese wiederum koordiniere alle Entwicklungen nicht nur mit den vorgesetzten Dienststellen, sondern auch mit dem Datenschutzbeauftragten. In Sachsen besteht diese Gruppe aus Referenten der Sächsischen Bildungsagentur und Teamkoordinatoren von Medienpädagogischen Zentren.

Prof. Dr. Wilfried Hendricks, Institut für Bildung in der Informationsgesellschaft Berlin, fasste die Ergebnisse der Fachtagung unter Berücksichtigung der datenschutzrechtlichen Aspekte zusammen. Seine Schlussfolgerungen waren unter anderem, dass Datenschutz und Informationsfreiheit wesentliche Inhaltskomponenten einer zukunftsfähigen Medienkompetenz seien, dass der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern den Schulen beratend und unterstützend zur Seite stehe und dass alle Schulen grundsätzlich als wichtige Partner zu einem landesweiten schon jetzt in bemerkenswert effektiver Weise arbeitenden Medienkompetenz-Netzwerk gehören.

Die Beiträge der Datenschutz-Fachtagung können im Internetangebot unserer Behörde nachgelesen werden (https://www.datenschutz-mv.de/datenschutz/veranstaltungen/Schule.html).

7.2 Datenschutz-Beirat

Mit der Novellierung des Landesdatenschutzgesetzes Mecklenburg-Vorpommern (DSG M-V) im Jahr 2011 wurde in § 33b 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.

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.

Im Berichtszeitraum tagte der Datenschutz-Beirat dreimal.

Am 17. Februar 2014 befassten sich die Mitglieder des Beirates auf ihrer Sitzung mit den Themen Videoüberwachung sowie dem kontinuierlichen Informationsaustausch zwischen dem Beirat und dem im Rahmen der gemeinsamen E-Government-Initiative des Landes und der Kommunen eingerichteten Lenkungsausschuss. Die Referenten stellten Rechtsfragen sowie Fälle aus der Praxis vor und beantworteten im Anschluss die Fragen der Teilnehmerinnen und Teilnehmer.

Am 12. Januar 2015 wurde eine neue Vorsitzende des Datenschutz-Beirates gewählt, weil die bisherige Vorsitzende andere Aufgaben übernommen hatte und somit nicht mehr die Funktion der Beirats-Vorsitzenden wahrnehmen konnte. Der Schwerpunkt dieser Sitzung lag im Bereich E-Government. Den Mitgliedern wurde das E-Government-Gesetz des Bundes vorgestellt und die Auswirkungen auf die Kommunen in Mecklenburg-Vorpommern wurden beraten.

Am 7. September 2015 befassten sich die Mitglieder des Datenschutz-Beirates schwerpunktmäßig mit den Themen EU-Datenschutz-Grundverordnung und Datenschutz im Fördermittelbereich.

8 Informationsfreiheitsgesetz Mecklenburg-Vorpommern - IFG M-V

8.1 Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK)

Im Jahr 2015 hatte Mecklenburg-Vorpommern den Vorsitz der Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK). Die Konferenz dient dem Austausch über aktuelle Fragen der Informationsfreiheit und der Fortentwicklung einer modernen Informationsfreiheitsgesetzgebung. Sie ist ein Zusammenschluss der Informationsfreiheitsbeauftragten des Bundes und der Länder Berlin, Brandenburg, Bremen, Hamburg, Mecklenburg-Vorpommern, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland, Sachsen-Anhalt, Schleswig-Holstein und Thüringen. Niedersachsen, Baden-Württemberg und Sachsen sind zwar zurzeit noch nicht dabei, jedoch liegen dort bereits Gesetzentwürfe vor. Lediglich in Bayern und Hessen gibt es noch keine Bestrebungen, Informationsfreiheitsgesetze zu schaffen.

Die Konferenz tagte am 30. Juni 2015 im Schweriner Schloss. Die Sitzungen der Konferenzen und der diesen zuarbeitenden Arbeitskreisen (AKIF) sind öffentlich. Jeder Interessierte kann nach Anmeldung teilnehmen. Ebenso werden die Tagesordnung und das Protokoll der Konferenzen und Arbeitskreise auf unserer Homepage veröffentlicht.

Die Konferenz hat auf ihrer Frühjahrssitzung zwei Entschließungen verabschiedet zu den Themen „Mehr Transparenz bei den Verhandlungen über das Transatlantische Freihandelsabkommen (TTIP)!“ und „Auch Kammern sind zur Transparenz verpflichtet!“.

Noch im Jahr 2015 sollte das geplante Transatlantische Freihandelsabkommen (TTIP) zwischen der EU und den Vereinigten Staaten von Amerika verabschiedet werden. Die Konferenz der Informationsfreiheitsbeauftragten fordert von der EU und der Bundesregierung, der Öffentlichkeit neben zusammenfassenden und erläuternden Informationen vermehrt Originaldokumente zur Verfügung zu stellen, um es den Bürgerinnen und Bürgern zu ermöglichen, sich eine eigene Meinung vom Inhalt und Ablauf der Verhandlungen zu bilden. Hierzu gehören auch Informationen über die Positionen und Forderungen der USA sowie von Lobbyisten. Zudem setzen sich die Informationsfreiheitsbeauftragten dafür ein, dass zur Beilegung von Streitigkeiten zwischen den Handelspartnern öffentlich tagende hoheitliche Gerichte geschaffen werden.

Informationen, die im Rahmen der Tätigkeit von Kammern anfallen, unterfallen den Informationszugangsgesetzen des Bundes und der Länder, da die Kammern hoheitliche Aufgaben wahrnehmen. In der Vergangenheit kam es des Öfteren vor, dass Kammern der Auffassung waren, dass sie beispielsweise Informationen zu Jahresabschlüssen und Angaben zu Einnahmen, Ausgaben und Rückstellungen nicht herausgeben müssten, da es sich hierbei um „interne Informationen“ handele. Die IFK fordert daher die Kammern auf, ihren Transparenzverpflichtungen nachzukommen.

Im Herbst gab es wegen anderer vordringlicher datenschutzrechtlicher Themen wie der EU-Datenschutz-Grundverordnung (EU-DSGVO) keine Konferenz, sondern lediglich eine Arbeitskreissitzung (AKIF). Dort wurde eine Entschließung zum Thema: „Informationsfreiheit 2.0 - endlich gleiches Recht in Bund und Ländern!“ vorbereitet und dann von der Konferenz im Umlaufverfahren verabschiedet. Nach Auffassung der Informationsfreiheitsbeauftragten sollten moderne Regelungen über den Informationszugang in Form effektiver Transparenzgesetze

- der herkömmlichen Informationserteilung auf Antrag eine Pflicht der Verwaltung zur proaktiven Veröffentlichung von Informationen in Open-Data-Portalen zur Seite stellen,
- Ausnahmen vom freien Zugang zu Informationen nur in einem unbedingt erforderlichen Maß enthalten,
- Neben klassischen Verwaltungen und Unternehmen der öffentlichen Hand einbeziehen und
- der vorhandenen Rechtszersplitterung auf dem Gebiet der Informationsfreiheit entgegenwirken und das Umweltinformationsrecht mit dem Informationsfreiheitsrecht zusammenführen.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) fordert die Gesetzgeber in Bund und Ländern daher auf, die positiven Erfahrungen mit der Informationsfreiheit in Deutschland anzuerkennen und die Einheitlichkeit der Lebensbedingungen auch im Bereich der Verwaltungstransparenz herzustellen.

8.2 Vergütungstransparenzgesetz Mecklenburg-Vorpommern

Durch das hiesige Finanzministerium wurden wir im Sommer 2015 um Stellungnahme zu dem Entwurf eines Gesetzes der Transparenz bei der Vergütung der Geschäftsleitung öffentlicher Unternehmen im Land Mecklenburg-Vorpommern (VergütungsTG M-V) gebeten. Grundlage für die Erarbeitung des Gesetzentwurfes war ein Kabinettsbeschluss vom 21. April 2015, die Offenlegung der Vergütung der Geschäftsleitung privatrechtlicher Unternehmen mit Beteiligung des Landes, landesunmittelbarer Unternehmen in der Rechtsform des öffentlichen Rechts sowie bei den Sparkassen in Mecklenburg-Vorpommern gesetzlich zu regeln. Diese Regelungen betreffen sowohl die Schaffung einer neuen gesetzlichen Grundlage zur Offenlegung der Bezüge der Geschäftsleitung (BezügeOG M-V) als auch die Änderung der Landeshaushaltsordnung und des Sparkassengesetzes.

Der vorliegende Gesetzentwurf wurde durch uns aus den in der Gesetzesbegründung ausgedrückten Zielen zur Stärkung der Transparenz ausdrücklich begrüßt. Leider wurde im Gesetzentwurf aber darauf verzichtet, verpflichtend festzulegen, dass die Bezüge jedes einzelnen Mitglieds eines Geschäftsführungsorgans veröffentlicht werden sollen. Dieses betrifft sowohl die geplanten Änderungen der Landeshaushaltsordnung als auch den Entwurf zum BezügeOG M-V. Den Darstellungen in der Gesetzesbegründung entnehmend soll die Geschäftsleitung öffentlicher Unternehmen in Mecklenburg-Vorpommern in den weit überwiegenden Fällen nur aus einem Mitglied bestehen, sodass mit der Veröffentlichung der Gesamtbezüge regelmäßig auch die Offenlegung der individuellen Bezüge verbunden ist. Auf eine Offenlegungsregelung mit zwingend individualisierter Veröffentlichung der Bezüge sei daher verzichtet worden.

Um dem Transparenzgedanken stärker Rechnung tragen zu können und aufgrund des oben genannten Umstandes, dass sich in den meisten Fällen aller Wahrscheinlichkeit nach sowieso eine Personenbeziehbarkeit herstellen lässt, halten wir es für angebracht, an dieser Stelle auch eine individualisierte Veröffentlichung der Bezüge vorzusehen. Diese würde im Übrigen auch im Einklang mit den hierzu bereits bestehenden gesetzlichen Regelungen, die beispielsweise in Schleswig-Holstein und Berlin getroffen wurden, stehen. Daher haben wir die Empfehlung abgegeben, die betreffenden Bestimmungen entsprechend zu erweitern.

In dem überarbeiteten Gesetzentwurf der Landesregierung, der als Drucksache 6/4845 am 2. Dezember 2015 im Landtag eingebracht wurde, ist nunmehr eine individualisierte Offenlegung der Bezüge der Mitglieder der Geschäftsleitung vorgesehen. Unserer ausgesprochenen Empfehlung ist somit Rechnung getragen worden.

Im Gesetzentwurf ist bezogen auf die Offenlegung der Gesamtbezüge häufig nur eine Hinwirkungspflicht des Landes vorgesehen. Bezüglich einer erstrebenswerten unmittelbaren Verpflichtung zur Offenlegung wird auch seitens des Finanzministeriums dargestellt, dass dies sehr wohl als effektivere Möglichkeit zum Erreichen des Ziels (Offenlegung der Gesamtvergütung) angesehen wird, dem Land bei privat-rechtlichen Unternehmen und bestimmten öffentlich-rechtlichen Unternehmen (z. B. Sparkassen) jedoch die hierfür erforderliche Gesetzgebungskompetenz fehlen würde.

Der Gesetzentwurf wurde an den Finanzausschuss des Landtages Mecklenburg-Vorpommern zur Beratung verwiesen.

8.3 Zugang zu Protokollen nicht-öffentlicher Sitzungen

Ein Bürger informierte uns darüber, dass er bei einer Amtsverwaltung einen Antrag auf Übersendung eines Auszugs aus einem Protokoll einer nichtöffentlichen Sitzung gestellt hat. Die betreffende Amtsverwaltung lehnte diesen jedoch Antrag ab. Dem Antragsteller wurde lediglich die Möglichkeit zugestanden, Einsicht in die betreffenden Unterlagen zu nehmen.

Die Amtsverwaltung teilte uns mit, dass üblicherweise Protokolle von nichtöffentlichen Sitzungen, auch wenn es sich nur um Ergebnisprotokolle handelt, dann nicht herausgegeben werden, wenn sich in der Antragstellung nicht explizit auf das Informationsfreiheitsgesetz Mecklenburg-Vorpommern (IFG M-V) bezogen wird. Eine Übermittlung einer Protokollkopie würde demnach nur dann erfolgen, wenn ein entsprechender Antrag nach dem IFG M-V gestellt wird.

Gemäß § 10 Abs. 1 IFG M-V wird der Zugang zu Informationen auf Antrag (schriftlich oder zur Niederschrift) gewährt. Diese Formerfordernisse waren im vorliegenden Fall gegeben. Auch wurde die erwünschte Information, wie durch § 10 Abs. 2 IFG M-V gefordert, näher beschrieben. Was allein gefehlt hat, war die Bezugnahme auf das IFG M-V.

Bei ihrer ablehnenden Haltung hat die Verwaltung unbeachtet gelassen, dass unter Berücksichtigung des § 133 Bürgerliches Gesetzbuch (BGB) dieses Begehren als ein Antrag auf Informationszugang nach dem IFG M-V hätte ausgelegt werden können. Gemäß § 133 BGB ist bei der Auslegung einer Willenserklärung der wirkliche Wille zu erforschen und nicht an dem buchstäblichen Sinne des Ausdrucks zu haften.

Es kann von einem Antragsteller nicht verpflichtend verlangt werden, dass dieser die gesetzlichen Bestimmungen des IFG M-V kennt. Aus Transparenzgründen und unter Berücksichtigung des § 133 BGB hätte seine Willenserklärung vielmehr als ein Antrag nach dem IFG M-V ausgelegt werden müssen. Schlussfolgernd hätte der Antragsteller bereits nach erstmaliger Antragstellung einen Anspruch auf Übersendung von Kopien, wie es gesetzlich auch in § 4 Abs. 3 Satz 3 IFG M-V vorgesehen ist.

Aus oben genannten Gründen haben wir deshalb die Empfehlung ausgesprochen, zukünftig Anträge, die sich nicht ausdrücklich auf das IFG M-V beziehen aber durch die ein Informationszugang begehrt wird, als Anträge nach dem IFG M-V auszulegen und als solche zu behandeln.

Die Amtsverwaltung teilte diese Einschätzung und sagte zu, alle künftigen Informationsanträge nach dem IFG M-V abzuprüfen.

8.4 Informationen über Ausgaben der Verfassungsschutzbehörde

Über das Informationsfreiheitsportal „frag den staat“ erhielt die hiesige Verfassungsschutzbehörde eine Anfrage, bei der eine vollständige Auflistung von Dokumenten, die sich auf den finanziellen und personellen Aufwand der Landesbehörde für Verfassungsschutz in Mecklenburg-Vorpommern in den Jahren 2012 und 2013 bezog, erbeten wurde. Der Antrag wurde insbesondere unter Hinweis auf § 5 Nr. 1 Informationsfreiheitsgesetz Mecklenburg-Vorpommern (IFG M-V) abgelehnt und damit begründet, dass die Haushaltsakte bei der Landesbehörde für Verfassungsschutz in Mecklenburg-Vorpommern mit den Dokumenten der Haushaltsplanung, Haushaltsführung und Haushaltsrechnung in die Geheimhaltungsstufe VS-vertraulich eingestuft seien. Gleiches würde für den personellen Aufwand der Landesbehörde gelten. Zu aktuellen Meldungen und Informationen wurde der Antragsteller lediglich auf die Internetpräsenz (www.verfassungsschutz-mv.de) verwiesen.

Nach § 5 Nr. 1 IFG M-V ist ein Antrag auf Zugang zu Informationen abzulehnen, soweit und solange das Bekanntwerden der Informationen dem Wohl des Landes, den inter- und supranationalen Beziehungen, den Beziehungen zum Bund oder zu einem Land schwerwiegende Nachteile bereiten oder die Landesverteidigung oder die innere Sicherheit schädigen würde.

Vorausgesetzt, die Einstufung der Dokumente als VS-vertraulich erfolgte rechtmäßig, wäre gegen die von der Landesbehörde für Verfassungsschutz aufgeführte Argumentation nichts einzuwenden. Verwundert hat uns in diesem Zusammenhang aber, dass es dem Antragsteller um Dokumente und damit um Informationen ging, die zumindest teilweise aus verschiedenen öffentlich zugänglichen Quellen hätten entnommen werden können. Dieses war Ergebnis einer von uns hierzu durchgeführten Internetrecherche.

Unter anderem konnte der oben genannten Internetpräsentation der Verfassungsschutzbehörde unter der Rubrik „Daten und Fakten für M-V“ einige organisatorische Angaben und Informationen zu den Gesamtanzahlen der Stellen entnommen werden. Außerdem waren auch Informationen über die Haushaltsansätze der Jahre 2012 und 2013 verfügbar.

Darüber hinaus waren der Internetseite des hiesigen Finanzministeriums konkrete Informationen zu veranschlagten Sachkosten entnehmbar.

Auch wenn einige der erbetenen Informationen als VS-vertraulich eingestuft und damit nach § 5 Nr. 1 IFG M-V vom Informationszugangsanspruch ausgenommen sind, hätte seitens der Verfassungsschutzbehörde doch mindestens der aus öffentlichen Quellen entnehmbare Teilzugang gewährt werden müssen. Insoweit hätte der Antragsteller entsprechend den Bestimmungen zu § 4 Abs. 4 IFG M-V auf die Fundstellen hingewiesen werden müssen.

Wir haben gegenüber der Verfassungsschutzbehörde in diesem Zusammenhang auch darauf hingewiesen, dass eine Verweisungsmitteilung nicht in Abhängigkeit davon steht, ob die Informationen eigenen Ursprungs sind oder nicht. Entscheidendes Kriterium ist vielmehr, dass es sich um jeweils vorhandene amtliche Informationen handelt.

8.5 Zu hohe Gebühren für Verbraucherinformationen

Mitunter gibt es bei Behörden Fragen im Zusammenhang mit der Anwendung des Informationsfreiheitsgesetzes Mecklenburg-Vorpommern (IFG M-V) oder anderer gesetzlicher Ermächtigungsgrundlagen. Dies ist vor allem dem Umstand geschuldet, dass nach § 1 Abs. 3 IFG M-V besondere Rechtsvorschriften über den Zugang zu amtlichen Informationen, die Auskunftserteilung oder die Gewährung von Akteneinsicht unberührt bleiben (Unberührtheitsklausel). Diese Regelung bezieht sich dabei nicht nur auf den Umfang des Informationszugangs.

Uns lag ein Fall vor, bei dem es in einer Reihe von Anfragen um den Zugang von Informationen aus dem Bereich der ökologischen Tierhaltung ging. Für einige dieser Anträge wurde dem Antragsteller die Erhebung von Gebühren angekündigt. Die Gesamtsumme belief sich dabei auf rund 3.000,00 Euro. Eine der dabei angekündigten Gebühren überstieg (wenn auch nur geringfügig) sogar den in der Informationskostenverordnung (IFGKostVO M-V) festgelegten Höchstsatz von 500,00 Euro. Gestützt wurde die hohe Summe auf durchzuführende Amtshandlungen, die nach § 13 IFG M-V in Verbindung mit den Bestimmungen zur IFG KostVO M-V kostenpflichtig sind. Dem Antragsteller wurde dabei die Möglichkeit eingeräumt zu entscheiden, ob er seinen Antrag weiter aufrecht halten will oder nicht.

Unberücksichtigt blieb dabei allerdings, dass nach der in § 1 Abs. 3 IFG M-V verankerten Unberührtheitsklausel zu prüfen gewesen wäre, ob (unabhängig von einer auf das IFG M-V bezogenen Antragstellung) der Antragsteller durch die Bestimmungen des Verbraucher-Informationsgesetzes (VIG) und der dazugehörigen Kostenverordnung (VIGKostVO M-V) besser gestellt gewesen wäre. Voraussetzung hierfür ist, dass es sich bei den vom Antragsteller begehrten Informationen auch um Verbraucherinformationen im Sinne des §1 VIG handelt. Sollte dies ganz oder zum Teil der Fall sein, käme nach § 1 Abs. 3 IFG M-V auch das VIG als Anspruchsgrundlage in Betracht. Dies hätte zur Folge, dass auch die VIGKostVO M-V anzuwenden wäre. Hierdurch wiederum wäre es höchstwahrscheinlich auch zu einer entsprechenden Kostenreduzierung gekommen, da nach § 7 VIG in Verbindung mit der VIGKostVO M-V einige Amtshandlungen gebührenfrei sind.

Im vorliegenden Fall sind wir zu der Entscheidung gekommen, dass es sich bei den begehrten Informationen sehr wohl um Verbraucherinformationen handeln dürfte, sodass die betreffende Behörde nach § 1 Abs. 3 IFG M-V auch die Bestimmungen des VIG und der dazugehörigen Kostenverordnung hätte prüfen/beachten müssen.

Da der Antragsteller im Laufe des Verfahrens seine kostenpflichtigen Anträge zurückgezogen hat, konnten wir mit der betreffenden Behörde zumindest für zukünftige Anträge auf Informationszugang nach dem IFG M-V (bei denen es um den Zugang zu Verbraucherinformationen geht) abstimmen, dass § 1 Abs. 3 IFG M-V und damit auch das VIG berücksichtigt wird. Dies betrifft sowohl den inhaltlichen Informationszugang als auch die Frage nach der Gebührenhöhe.

8.6 Auskunft über vertrauliches Gutachten einer Wirtschaftsprüfungsgesellschaft

Über eine Rechtsanwaltsgesellschaft begehrte die Hegemann Verwaltungs- und Beteiligungs GmbH als ehemalige Hauptgesellschafterin der P + S Werften und damit eine nach § 1 Abs. 2 IFG M-V anspruchsberechtigte juristische Person des Privatrechts Zugang zu einem Gutachten zum Sanierungskonzept von KPMG für die Hegemann Werftengruppe. Dieser Antrag wurde vom Ministerium für Wirtschaft, Bau und Tourismus Mecklenburg-Vorpommern abgelehnt, da das Gutachten als Verschlusssache-Nur für den Dienstgebrauch (VS-NfD) eingestuft ist. Begründet wurde die VS-NfD-Einstufung damit, dass die Kenntnisnahme der begehrten Informationen durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein könnte. Diese möglichen Nachteile wurden im Zusammenhang mit diversen Klageverfahren, die im Nachgang zur Insolvenz der Hegemann Werftengruppe gegen das Land geführt werden, gesehen. Insbesondere betrifft dies eine möglicherweise anstehende zivilrechtliche Schadensersatzklage, bei der das vorgenannte Ministerium vermutete, dass über das IFG M-V hierfür weitere Informationen ausgeforscht werden sollen.

Unsere Prüfung richtete sich bei diesem Sachverhalt vor allem auf die Frage, ob die VS-NfD Einstufung rechtmäßig ist. Hierbei stellten wir fest, dass eine derartige Einstufung durch die Verschlusssachen-Anweisung Mecklenburg-Vorpommern (VSA M-V) so nicht vorgesehen ist. Nach § 7 Nr. 4 VSA M-V ist eine Sache gemäß § 2 Abs. 2 Sicherheitsüberprüfungsgesetz Mecklenburg-Vorpommern (SÜG M-V) als VS-NfD einzustufen, wenn die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder schädlich sein kann. Nach den Hinweisen zu VS-Einstufungen muss dabei allerdings schlüssig dargestellt werden, welche Gefährdung, Schäden oder Nachteile für die Bundesrepublik Deutschland oder eines ihrer Länder konkret entstehen können, wenn Unbefugte von den Informationen Kenntnis erhalten. Dabei kommt eine VS-Einstufung grundsätzlich nur bei Informationen in Betracht, die die äußere Sicherheit, auswärtige Beziehungen oder innere Sicherheit betreffen. Für andere schutzwürdige Informationen sind die hierfür bestehenden Regelungen - zum Beispiel Pflicht zur Wahrung von Dienst- oder Steuergeheimnissen, Schutz personenbezogener Daten nach dem Bundesdatenschutzgesetz, Bundesarchivgesetz oder internen Geschäftsordnungen - anzuwenden. Unseres Erachtens lagen derartige Voraussetzungen im vorliegenden Fall nicht vor, sodass wir die vorgenommene VS-Einstufung als unberechtigt angesehen haben.

Da kein weiterer Ablehnungstatbestand im Sinne der §§ 5 bis 8 IFG M-V ersichtlich war beziehungsweise in der mit dem betreffenden Ministerium geführten Korrespondenz aus unserer Sicht nicht schlüssig vorgetragen wurde, hätte das Gutachten herausgegeben werden müssen.

Da dieses jedoch nicht erfolgt ist, ist durch den Antragsteller nach Beendigung des Vorverfahrens Klage erhoben worden. Eine Entscheidung ist durch das zuständige Verwaltungsgericht hierzu jedoch noch nicht ergangen.

8.7 Herausgabeanspruch von Haushaltsdaten gegenüber Kammern

Der Bundesverband für freie Kammern e. V. (BffK) stellte in 2014 flächendeckend an Kammern in Deutschland Auskunftsanträge nach dem Informationsfreiheitsgesetz - so auch in Mecklenburg-Vorpommern.

Der BffK stellte Anträge zur Übersendung folgender Informationen:

- Gesamteinnahmen 2012
- Gesamtausgaben 2012
- Zuführungen zu den Rücklagen oder Entnahmen aus den Rücklagen 2012
- Höhe der gesamten Rücklagen zum 31.12.2012
- Gesamtes Kapitalvermögen zum 31.12.2012

Unterschiedliche Kammern aus Mecklenburg-Vorpommern haben den Antrag entweder abgelehnt oder gar nicht erst beschieden. Daher bat der BffK den Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern um Unterstützung nach § 14 Informationsfreiheitsgesetz Mecklenburg-Vorpommern (IFG M-V).

Bis zum Schluss weigerten sich lediglich die Landestierärztekammer Mecklenburg-Vorpommern und die Ärztekammer Mecklenburg-Vorpommern, die begehrten Informationen herauszugeben.

Die Landestierärztekammer vertritt die Auffassung, dass es sich bei den begehrten Informationen nicht um amtliche Informationen handele und damit das IFG M-V keine Anwendung fände.

Bei den Kammern handelt es sich um Körperschaften des öffentlichen Rechts, denen hoheitliche Aufgaben durch das Land Mecklenburg-Vorpommern übertragen wurden. Daher findet das IFG M-V auf Kammern eindeutig Anwendung (§ 3 Abs. 1 IFG M-V). Demnach liegen auch amtliche Informationen vor, soweit die Informationen im Zusammenhang mit einer amtlichen Tätigkeit angefallen sind. Aufgrund des Gesetzeszwecks unterliegt der Begriff der Amtlichkeit einem weiten Begriffsverständnis - nur Informationen, die ausschließlich und eindeutig privaten Zwecken dienen, sind vom Begriff „amtliche Information“ ausgeschlossen. Auch wenn die Informationen nicht im Zusammenhang mit einem konkreten Verwaltungsakt stehen, handelt es sich trotzdem um amtliche Informationen.

Die Einnahmen, Ausgaben und Rückstellungen können nur durch ihre vom Gesetzgeber übertragene, amtliche Tätigkeit generiert werden. Demnach handelt es sich bei den begehrten Informationen um amtliche Informationen.

Die Ärztekammer Mecklenburg-Vorpommern lehnte den IFG-Antrag des BffK dagegen ab, weil sie die Auffassung vertritt, dass die Kammer lediglich selbstverwaltend tätig sei und dass nur Kammermitgliedern das Recht nach dem IFG M-V zustehe. Im Weiteren erklärte die Ärztekammer, dass es sich bei den Informationen um Betriebs- und Geschäftsgeheimnisse handele.

Obwohl sich die Kammer aus Beiträgen und Gebühren ihrer Mitglieder finanziert und organisatorisch aus der staatlichen Verwaltungshierarchie ausgegliedert ist, nimmt die Kammer staatliche Aufgaben wahr und ist demnach Teil der öffentlichen Gewalt. Betriebs- und Geschäftsgeheimnisse kommen auch nicht in Betracht, da die Kammer keine Mitanbieter am Markt hat und damit auch keine Schäden bei einer möglichen Veröffentlichung der Haushaltsdaten zu erwarten sind.

Da weder die Landestierärztekammer Mecklenburg-Vorpommern noch die Ärztekammer Mecklenburg-Vorpommern die beantragten Auskünfte geben wollten, haben wir eine Beanstandung gegenüber diesen Kammern ausgesprochen und die zuständigen Aufsichtsbehörden darüber informiert. Die Landestierärztekammer Mecklenburg-Vorpommern erwiderte auf die Beanstandung, dass der BffK gegen den ablehnenden Bescheid kein Rechtsmittel eingelegt hätte. Die Beanstandung des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern erfolgt jedoch unabhängig davon, ob der BffK Rechtsmittel gegen den ablehnenden Bescheid eingelegt hat und ist damit als Stellungnahme auf die Beanstandung nicht geeignet.

Die Ärztekammer Mecklenburg-Vorpommern hat bisher zu der Beanstandung keine Stellung genommen. Die begehrten Informationen wurden dem Bundesverband für freie Kammern e. V. in beiden Fällen bis heute nicht gewährt.

9 Organigramm

<table>
<tr><td>Stand:
19.02.2015</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

Anne Anderson
0385 59494-33</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

Maik Sarunski
0385 59494-38

Adam Kipka
0385 59494-44</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

Anne Anderson
0385 59494-33</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
IuK
E-Government
Internet/Netzwerke
Betriebssysteme
Standardsoftware
Verschlüsselung, Signatur
Biometrie
baulicher Datenschutz
Sicherheitskonzepte
Verfahrensverzeichnis
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>

10 Abkürzungsverzeichnis

95/46/EG	Europäische Datenschutzrichtlinie (Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr)
AGB	Allgemeine Geschäftsbedingungen
AK Technik	Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder
AKIF	Arbeitskreis Informationsfreiheit
AO	Abgabenordnung
AStV	Ausschuss der Ständigen Vertreter
AWO	Arbeiterwohlfahrt
BffK	Bundesverband für freie Kammern e. V.
BDSG	Bundesdatenschutzgesetz
BEATA	Bezügedaten elektronisch anweisen, transportieren und archivieren
BetrVG	Betriebsverfassungsgesetz
BezügeOG M-V	Gesetz zur Offenlegung der Bezüge der Geschäftsleitung bei Unternehmen in der Rechtsform einer landesunmittelbaren juristischen Person des öffentlichen Rechts im Land Mecklenburg-Vorpommern
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BMeldDÜV	Bundesmeldedatenübermittlungsverordnung
BMG	Bundesmeldegesetz
BMI	Bundesministerium des Innern
BMWi	Bundesministerium für Wirtschaft
BOÄ M-V	Berufsordnung für die Ärztinnen und Ärzte in Mecklenburg-Vorpommern
BSI	Bundesamt für Sicherheit in der Informationstechnik
BTM	Betäubungsmittel
BVerfG	Bundesverfassungsgericht
BVA	Bundesverwaltungsamt
CDU	Christlich Demokratische Union
CSG	ComputerSpielSchule Greifswald
CN-LAVINE	Corporate Network der Landesverwaltung
DIN	Deutsches Institut für Normung
DPAG	Deutsche Post AG
DRK	Deutsches Rotes Kreuz
DSG M-V	Landesdatenschutzgesetz Mecklenburg-Vorpommern
DSK	Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder
DVZ M-V GmbH	Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH
E-LMG	Neufassung Landesmeldegesetz
ED-Richtlinien	Erkennungsdienstliche Richtlinien
EDV	elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
eGo-MV	Zweckverband „Elektronische Verwaltung in Mecklenburg-Vorpommern“
EGVP	Elektronisches Gerichts- und Verwaltungspostfach
eID	elektronischer Identitätsnachweis

ESF	Europäischer Sozialfonds
EU	Europäische Union
EU-DSGVO	Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutzgrundverordnung)
EVA	Elektronischer Vorgangsassistent
GEZ	Gebühreneinzugszentrale
GG	Grundgesetz
GGO	Gemeinsame Geschäftsordnung
GPS	Global Positioning System
HGB	Handelsgesetzbuch
HTTP	Hypertext Transport Protocol
HTTPS	Hypertext Transport Protocol Secure
ICILS 2013	International Computer and Information Literacy Study 2013
ICD-Schlüssel	Internationale Klassifizierung von Krankheiten
ID	Identifikationsnummer
IFG M-V	Informationsfreiheitsgesetz Mecklenburg-Vorpommern
IFGKostVO M-V	Informationskostenverordnung Mecklenburg-Vorpommern
IFK	Konferenz der Informationsfreiheitsbeauftragten in Deutschland
IP	Internet Protocol
IQMV	Institut für Qualitätsmanagement Mecklenburg-Vorpommern
ISMS	Informationssicherheits-Management-Systeme
ISO	Internationale Organisation für Standardisierung
ISO 27001	internationale Norm für Informationssicherheits-Managementsysteme
JI-Richtlinie	Europäische Datenschutzrichtlinie für Polizei und Justiz
KAG M-V	Kommunalabgabengesetz Mecklenburg-Vorpommern
Kfz	Kraftfahrzeug
KPG M-V	Kommunalprüfungsgesetz Mecklenburg-Vorpommern
KIS	Krankenhausinformationssysteme
KITA	Kindertagesstätte
KunstUrhG	Kunsturheberrechtsgesetz
KV M-V	Kommunalverfassung für das Land Mecklenburg-Vorpommern
LAKOST M-V	Landeskoordinierungsstelle für Suchtvorbeugung Mecklenburg-Vorpommern
LBesA M-V	Landesbesoldungsamt Mecklenburg-Vorpommern
LIBE	Ausschuss für bürgerliche Freiheiten, Justiz und Inneres
LJR M-V	Landesjugendring Mecklenburg-Vorpommern
LKA M-V	Landeskriminalamt Mecklenburg-Vorpommern
LKHG M-V	Landeskrankenhausgesetz Mecklenburg-Vorpommern
LMG M-V	Landesmeldegesetz Mecklenburg-Vorpommern
LPBK M-V	Landesamt für zentrale Aufgaben und Technik der Polizei, Brand- und Katastrophenschutz Mecklenburg-Vorpommern
LT-Drs.	Landtags-Drucksache
MMV	Medienanstalt Mecklenburg-Vorpommern
NADA	National Anti Doping Agentur
NEGS	Nationale E-Government-Strategie
nPA	neuer Personalausweis
OSCI	Online Services Computer Interface
OWiG	Gesetz über Ordnungswidrigkeiten

PAYD	Pay as you drive
PDF	Portable Document Format (plattformunabhängiges Dateiformat für Dokumente)
PFS	Perfect Forward Secrecy
QES	qualifizierte elektronische Signatur
RiStBV	Richtlinien für das Strafverfahren und das Bußgeldverfahren
RStV	Rundfunkstaatsvertrag
SchulDSVO M-V	Schuldatenschutzverordnung Mecklenburg-Vorpommern
SchulG M-V	Schulgesetz Mecklenburg-Vorpommern
SDM	Standard-Datenschutzmodell
SGB	Sozialgesetzbuch
SiRegVO M-V	Sicherungsregisterverordnung Mecklenburg-Vorpommern
SOG M-V	Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommern
SPD	Sozialdemokratische Partei Deutschlands
SRP	Secure Remote Password Protocol
SSL	Secure Sockets Layer
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
SÜG M-V	Sicherheitsüberprüfungsgesetz Mecklenburg-Vorpommern
TCDP	Trusted-Cloud-Datenschutzprofil
TEO	Tage ethischer Orientierung
TKG	Telekommunikationsgesetz
TLBS	Täterlichtbildsystem
TLS	Transport Layer Security
TMG	Telemediengesetz
TMS	Travel-Management-System
TR	Technische Richtlinie
TTIP	Transatlantisches Freihandelsabkommen
URL	Uniform Resource Locator
USA	United States of America
VIG	Verbraucher-Informationsgesetz
VIGKostVO	Kostenverordnung des Verbraucher-Informationsgesetzes
VPN	Virtual Private Network
VSA M-V	Verschlusssachenanweisung Mecklenburg-Vorpommern
VwGo	Verwaltungsgerichtsordnung
VwVfG M-V	Verwaltungsverfahrensgesetz Mecklenburg-Vorpommern
VerdStatG	Verdienststatistikgesetz
VergütungsTG M-V	Gesetz zur Erhöhung der Transparenz bei der Vergütung der Geschäftsleitung öffentlicher Unternehmen im Land Mecklenburg-Vorpommern
WADA	World Anti-Doping Agency
WLAN	Wireless Local Area Network (drahtloses lokales Netzwerk)
WLV	Wahllichtbildvorlage
WWW	World Wide Web
XTA	Standard für den einheitlichen Zugang zu Transportverfahren im E-Government
ZensG 2011	Zensusgesetz 2011
ZLD	zentrale Lichtbilddatei

11 Stichwortverzeichnis