LANDTAG MECKLENBURG-VORPOMMERN **Drucksache 6/5916**
6. Wahlperiode **24.08.2016**

UNTERRICHTUNG

durch die Landesregierung

Stellungnahme der Landesregierung zum Zwölften Tätigkeitsbericht des Landesbeauftragten für den Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern gemäß § 33 Absatz 1 des Landesdatenschutzgesetzes Mecklenburg-Vorpommern (DSG M-V), zum Fünften Tätigkeitsbericht nach dem Informationsfreiheitsgesetz Mecklenburg-Vorpommern (IFG M-V) und zum Siebenten Tätigkeitsbericht gemäß § 38 Absatz 1 des Bundesdatenschutzgesetzes (BDSG)

Berichtszeitraum: 1. Januar 2014 bis 31. Dezember 2015

Zugeleitet mit Schreiben des Chefs der Staatskanzlei vom 23. August 2016 gemäß § 29 Absatz 1 Satz 2 des Datenschutzgesetzes des Landes Mecklenburg-Vorpommern; federführend ist das Ministerium für Inneres und Sport.

Einleitung

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (LfDI) hat mit Drucksache 6/5356 seinen Zwölften Tätigkeitsbericht gemäß § 33 Absatz 1 des Landesdatenschutzgesetzes Mecklenburg-Vorpommern (DSG M-V), den Fünften Tätigkeitsbericht nach dem Informationsfreiheitsgesetz Mecklenburg-Vorpommern (IFG M-V) und den Siebenten Tätigkeitsbericht gemäß § 38 Absatz 1 des Bundesdatenschutzgesetzes (BDSG) für den Berichtszeitraum vom 1. Januar 2014 bis zum 31. Dezember 2015 vorgelegt. Gemäß § 33 Absatz 1 Satz 2 DSG M-V nimmt die Landesregierung hierzu Stellung.

Wie auch bei früheren Tätigkeitsberichten verknüpft der LfDI in seinem Tätigkeitsbericht den Bereich des öffentlichen und des nicht-öffentlichen Datenschutzes. Der LfDI ist der Auffassung, dass es bei etlichen Sachverhalten fachliche Überschneidungen gibt, die im Zusammenhang betrachtet werden müssen, sodass die Beiträge nach dem DSG M-V und dem BDSG nicht separat aufgeführt werden.

Die Landesregierung geht, wie auch bei ihren Stellungnahmen zu den vorhergehenden Tätigkeitsberichten, auf die den privaten Datenschutz betreffenden Beiträge nicht ein, da für den nicht-öffentlichen Bereich keine kompetenzrechtliche Zuständigkeit von Landesbehörden besteht.

Der Fünfte Tätigkeitsbericht zum IFG M-V ist als Abschnitt 8 des Gesamtberichts enthalten.

Die Landesregierung sieht nicht bei jedem Thema des Tätigkeitsberichts die Notwendigkeit zur Stellungnahme. Sie beschränkt sich darauf, bei Bedarf Erläuterungen zum Fortgang behandelter Angelegenheiten oder, sofern erforderlich, eine abweichende Auffassung darzulegen. Wenn und soweit die Landesregierung auf eine Stellungnahme verzichtet, bedeutet dies jedoch nicht, dass sie sich den Wertungen und Auffassungen, die im Tätigkeitsbericht ihren Niederschlag finden, in jedem Fall anschließt.

A Allgemeines

Der Bericht spricht in der Einleitung die Entwicklung des Datenschutzrechts auf europäischer Ebene sowie weitere Tätigkeitsschwerpunkte aus Sicht des LfDI an und fasst die hieraus und aus dem Elften Tätigkeitsbericht resultierenden Empfehlungen zusammen. Soweit die Landesregierung den Bedarf einer Stellungnahme sieht, wird darauf unter Nennung der konkreten Ziffer, die diese Themen bearbeiten, eingegangen.

B Im Einzelnen

0 Zur Einleitung

Entwicklung des Datenschutzrechts

Die Landesregierung begrüßt die Verabschiedung des Gesetzgebungspakets für eine europaweite Neuregelung des Datenschutzrechts. Das Regelungspaket umfasst zwei Rechtsakte:

1. die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) und
2. die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates.

EU-Datenschutzgrundverordnung (EU-DSGVO)

Die EU-DSGVO ist nunmehr seit dem 04.05.2016 im Amtsblatt der Europäischen Union [L 119/(EU) 2016/679] veröffentlicht. Sie ist gemäß ihrem Artikel 99 am 25.05.2016 in Kraft getreten und wird ab dem 25.05.2018 unmittelbar anwendbares Recht sein. Bund und Länder haben damit bis zum 24.05.2018 Zeit, ihre allgemeinen und bereichsspezifischen Datenschutzvorschriften an die EU-DSGVO anzupassen.

Die Landesregierung begrüßt, dass die langjährigen Verhandlungen zur EU-DSGVO zu einer Einigung geführt haben. Sie ist ein wichtiger Schritt hin zu einem europaweit einheitlichen Datenschutzrecht. Das deutsche Datenschutzniveau bleibt gewahrt. Datenschutzrechtliche Grundsätze wie etwa die Zweckbindung und die Datensicherheit bleiben ebenso erhalten wie die Einwilligung als Voraussetzung für die rechtmäßige Datenverarbeitung. Die bekannten Betroffenenrechte werden gestärkt und um das Recht auf Datenportabilität erweitert. Durch das Marktortprinzip wird sichergestellt, dass das europäische Recht für alle Datenverarbeiter gilt, die in der EU Dienstleistungen und Waren anbieten.

Während im Bereich der Datenverarbeitung durch private Stellen auf europäischer Ebene eine sehr weitgehende Harmonisierung erreicht werden konnte, eröffnet die EU-DSGVO dem Bundes- und Landesgesetzgeber im Bereich der Datenverarbeitung durch öffentliche Stellen notwendige Spielräume (sogenannte Öffnungsklauseln) für die Aufrechterhaltung von Rechtsgrundlagen inklusive präzisierender Regelungen zu den Einzelheiten der Verarbeitung.

Hinzuweisen ist besonders darauf, dass durch die EU-DSGVO der Sprung von einer bislang durch die Mitgliedstaaten umzusetzende Datenschutz-Richtlinie (95/46/EG) zu einer unmittelbar geltenden EU-Verordnung vollzogen wurde. Dies stellt einen Systemwechsel im Bereich der Rechtsinstrumente dar, der die Landesregierung in dem zur Anpassung des Landesrechts zur Verfügung stehenden Zeitrahmens stark fordern wird.

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

Auch die JI-Richtlinie ist am 04.05.2016 im selben Amtsblatt der Europäischen Union veröffentlicht worden wie die EU-DSGVO.

Die Landesregierung sieht in dieser Richtlinie eine gute Basis für die Arbeit der Strafverfolgungs- und Vollstreckungsbehörden. Die Landesregierung wird in dem für die Umsetzung in Bundes- und Landesrecht zur Verfügung stehenden Zeitrahmen intensiv an den zu entwickelnden Umsetzungsschritten und gesetzlichen Lösungen (mit-) arbeiten.

Für den Bereich der Polizei weist die Landesregierung darauf hin, dass sie es günstiger gefunden hätte, wenn die Aufgabenbewältigung durch die Polizei auch im Bereich der polizeilichen Gefahrenabwehr gänzlich der JI-Richtlinie unterstellt worden wäre.

Weiterer Verlauf

Im Rahmen der zweijährigen Anpassungsfrist für die EU-DSGVO muss

- entgegenstehendes nationales Recht aufgehoben werden,
- gleichlautendes nationales Recht aufgehoben werden, sofern nicht Öffnungsklauseln ein Beibehalten allgemeiner oder bereichsspezifischer Datenschutzregelungen erlauben und diese auch beibehalten werden sollen,
- ergänzendes Recht an den Stellen, an denen die Datenschutz-Grundverordnung dies erlaubt, erlassen werden und
- ergänzendes Recht an den Stellen, an denen die Datenschutz-Grundverordnung dies fordert, erlassen werden.

Eine vergleichbare Prüfung muss im Bereich der JI-Richtlinie erfolgen. Denn im Rahmen der zweijährigen Umsetzungsfrist müssen die Mitgliedstaaten die Rechts- und Verwaltungsvorschriften erlassen, die erforderlich sind, um der JI-Richtlinie nachzukommen.

Die Landesregierung teilt die Auffassung des LfDI, dass jedes Ministerium das geltende Recht in seinem Zuständigkeitsbereich auf die Vereinbarkeit mit dem europäischen Datenschutzrecht überprüfen muss. Der Staatssekretär des Ministeriums für Inneres und Sport (IM) hat am 13. April 2016 in der St-Runde zu Anpassungsaufgaben nach Verabschiedung der EU-DSGVO informiert und der Staatskanzlei und den Ressorts eine Liste möglicher betroffener Vorschriften ausgehändigt, die bereits knapp 100 Gesetze und Verordnungen umfasste. Diese Liste ist nach kursorischer Durchsicht im für Grundsatzfragen des Datenschutzes zuständigen Referat erstellt und ausdrücklich als nicht abschließend gekennzeichnet worden.

Die Fachebenen von Bund und Ländern arbeiten bereits an den erforderlichen Analysen und an der bis Mitte 2018 abzuschließenden Anpassungsgesetzgebung.

Weitere Tätigkeitsschwerpunkte im Berichtszeitraum

Die Landesregierung begrüßt das breit gefächerte Engagement des LfDI zum Thema „Datenschutz und Bildung“. Begleitend zu dem im Bericht benannten Projekt „Datenschutz an Schulen in Mecklenburg-Vorpommern“ ist eine AG „Digitale Schule“ durch das IM initiiert worden. Der Schwerpunkt der Arbeit der Arbeitsgruppe umfasst die Erarbeitung von „Kriterien der IT-Ausstattung“ an Schulen. Grundlage ist die Kooperationsvereinbarung zur Förderung der Medienkompetenz in Mecklenburg-Vorpommern zwischen der Staatskanzlei (Stk), dem IM, dem Ministerium für Bildung, Wissenschaft und Kultur (BM), dem Ministerium für Arbeit, Gleichstellung und Soziales (SM), dem LfDI und der Medienanstalt vom 21.04.2015.

Im Kontext Datenschutz an Schulen arbeitet die Landesregierung, federführend das BM, an einem Projekt für die Entwicklung des Schulmanagementsystems in Mecklenburg-Vorpommern. Damit soll die Umsetzung des Datenschutzes an den Schulen unterstützt und mit einheitlichen Regeln anhand der europäischen, nationalen und länderspezifischen Datenschutzrichtlinien verbessert werden.

Ergänzend ist ein „Kooperationsprojekt Schul-IT“ durch das IM initiiert worden. Hier soll besonders der Schutz sensibler Schuldaten für Lehrende und Lernende anhand von vereinheitlichenden Prozessanalysen und deren exemplarischen Lösungsevaluierungen betrachtet werden. Aktuell wird die zentralisierte, kommunale Eigenmittelfinanzierungsmöglichkeit über den Beirat für den kommunalen Finanzausgleich (FAG-Beirat) geprüft, welche die 75-prozentige Förderung über die E-Government-Richtlinie des Landes (EGovRL M-V) ergänzen soll.

Auch wenn die Aktivitäten teilweise erst an den Berichtszeitraum anschließen, liegen deren Vorbereitungen innerhalb des Berichtszeitraumes des Tätigkeitsberichtes.

1 Empfehlungen

1.1 Zusammenfassung aller Empfehlungen

Stellungnahmen finden ihren Niederschlag unter den einzelnen Punkten des Tätigkeitsberichtes, auf welche sich die Empfehlungen im Einzelnen beziehen. Eine Stellungnahme zu Punkt 1.1.1 findet sich z. B. unter Punkt. 3.3 usw.

1.2 Umsetzungen des Elften Tätigkeitsberichtes

Zu Nummer 1

Die Vermittlung von Datenschutzbewusstsein und die Förderung von Medienkompetenz für die Schülerinnen und Schüler des Landes ist der Landesregierung ein hohes Anliegen. Die Landesregierung unterstützt daher die curriculare Verankerung des Datenschutzes und die qualifizierte Medienbildung. Im Rahmen eines Modellvorhabens wird zum Schuljahresbeginn 2017/2018 die Installation eines durchgängigen Faches „Informatik und Medienkunde“ erprobt. Der in diesem Zusammenhang zu entwickelnde neue Rahmenplan für dieses Fach nimmt sich des Themas Datenschutz in Form eines Spiralcurriculums an.

Zu Nummer 2

Die Kommunen sind im aktuellen Berichtszeitraum auf dem Partner- und Mitgliedertag des Zweckverbandes „elektronische Verwaltung in Mecklenburg-Vorpommern“ (eGo-MV), aber auch durch frühzeitige Beteiligungsverfahren von der Ausrichtung der zu erwartenden gesetzlichen Vorgaben unter anderem für die „Leitlinien für Informationssicherheit in der öffentlichen Verwaltung“ oder die BSI-Grundschutzmethodik in Kenntnis gesetzt worden, um Ihrer Eigenverantwortlichkeit vorsorglich und rechtzeitig nachkommen zu können.

Das Land erarbeitet zudem in Zusammenarbeit mit kommunalen Vertretern einen Handlungsleitfaden zur Umsetzung des neuen E-Government-Gesetzes Mecklenburg-Vorpommerns (EGovG M-V) vom 20.04.2016. In diesem Leitfaden kann nur entsprechend des Standes des derzeitigen § 15 des EGovG M-V auf eine freiwillige Nutzung der Basisdienste und Berücksichtigung der vom Land gegebenenfalls festzulegenden IT-Interoperabilititäts- oder IT-Sicherheitsstandards gesetzt werden. Entschließen sich Kommunen zur Mitnutzung der E-Government-Basisdienste, dann haben sie auch die für diese Basisdienste geltenden IT-Sicherheitsstandards zu beachten und die Mehrkosten der Nutzung der Einhaltung des entsprechenden Sicherheitsniveaus zu finanzieren. Im selben Fall haben die Kommunen auch die für diese Basisdienste anzuwendenden IT-Planungsratsbeschlüssen der IT-Interoperabilitäts- und IT-Sicherheitsstandards anzuwenden, sofern es den länderübergreifenden Datenaustausch betrifft.

Darüber hinaus kann der Lenkungsausschuss E-Government (§ 17 EGovG M-V) Empfehlungen für eine ebenenübergreifende Kooperation auch für landesspezifische Interoperabilitäts- und Informationssicherheitsstandards geben, sofern sie nicht bereits vom IT-Planungsrat als verbindlich erklärt wurden.

Die meisten eGo-MV-Mitgliedskommunen (Stand Juni 2016 insgesamt 99 Mitglieder) haben allein durch die Nutzung der standardisierenden Leistungen des Verbandes, der permanent intern und extern für die Anwendung der BSI-Grundschutzmethodik wirbt, diese implizit durch organisatorische und technische Maßnahmen umgesetzt. Das betrifft sowohl die Verfahrens- und Vorhabenleistungen (Paketleistungen inklusive der notwendigen BSI-Grundschutzeinzelleistungen) als auch die separat „buchbaren“ Verbandsleistungen der „fliegenden Datenschutz-/IT-Sicherheitsbeauftragten“. In welchem Umfang diese dann als operative Maßnahmen in der einzelnen Kommune umgesetzt werden, unterliegt der jeweiligen Behördenleitungsentscheidung.

Zu Nummer 3

Die Landesregierung unterstützt den datenschutzgerechten Einsatz elektronischer Identifizierungs- und Signaturverfahren.

Zu Nummer 4

Bei den E-Government-Verfahren der Landesregierung wird grundsätzlich das OSCI-Transportprotokoll eingesetzt. Dieses bietet die Möglichkeit einer Ende-zu-Ende-Verschlüsselung. Eine Entscheidung zur Nutzung des sicheren OSCI-Transportprotokolls trifft der jeweilige Fachverfahrensverantwortliche entsprechend dem ermittelten Schutzbedarf der Daten. Dieses Vorgehen ist unter anderem in der IT-Sicherheitsleitlinie des IT-Planungsrates für gemeinsame Verfahren explizit festgelegt worden. Im Rahmen der Zusammenarbeit wird seitens des zuständigen Referates für E-Government regelmäßig auf den Einsatz von Verschlüsselungstechniken hingewirkt.

Um die Nutzung einer, auch Ende-zu-Ende-, Verschlüsselung für die Fachverantwortlichen und Nutzer in der Landesregierung zu erleichtern, wird aktuell das „Elektronischen Gerichts- und Verwaltungspostfach“ (EGVP) in allen Landesbehörden eingerichtet. Dies wird flankiert von kooperativen Vereinbarungen, die z. B. zu einer zentral finanzierten Einrichtung des EGVP in den Ämtern des Landes geführt haben und von weiteren Maßnahmen, wie der Konsolidierung einer einfacher pfleg- und nutzbaren Adressbasis im Umfeld des Instruments „SAFE“ und den „Infodiensten M-V“. Durch diese Erleichterungen soll insbesondere auch die Verschlüsselung auf dem Stand der Technik in der Landesregierung umgesetzt werden.

Zu Nummer 5

Die Landesregierung wird die Methoden und Unterlagen des Trusted-Cloud-Projekts bei der Erstellung der künftigen IT-Landesstandards als Anlage zu den IT-Richtlinien gemäß des E-Government-Gesetzes berücksichtigen.

Zu Nummer 6

Hinsichtlich der in der Landesverwaltung zentral eingesetzten Personal-, Organisations- und Stellenmanagement-Software EPOS 2.0 sind die Hinweise aus der Orientierungshilfe der Datenschutzbeauftragten des Bundes und der Länder vom 11.10.2012 berücksichtigt worden. Auch bei der Planung einer neuen Serverarchitektur wurden die technischen und organisatorischen Anforderungen zur Trennung von automatisierten Verfahren bei der Nutzung einer gemeinsamen IT-Infrastruktur beachtet worden. Für jeden Mandanten werden künftig parallele Middlewarekomponenten (JBoss Instanzen) eingerichtet. Die Trennung der EPOS-Anwendungen bleibt somit bestehen, es werden lediglich die Serverressourcen CPU und RAM von mehreren Middlewarekomponenten (JBoss Instanzen) gemeinsam genutzt. Es ist beabsichtigt, den LfDI nach der Serverarchitekturumstellung davon zu unterrichten.

Zu Nummer 7

Diese Empfehlung ist bereits in der Praxis umgesetzt.

Zu Nummer 8

Bisher richteten sich alle Förderwerkzeuge des IM nur an behördliche Zuwendungsempfänger, wie Gemeinden, Ämter, Landkreise, kreisfreie Städte, einschlägige aktive Zweckverbände und die kommunalen Landesverbände.

Eine direkte Förderung der bevorzugten Nutzung von Ausweiskartenlesegeräten mit eigener Tatstatur für Bürgerinnen und Bürger und/oder Unternehmen ist insofern durch das IM im Rahmen der bestehenden Fördermechanismen/-normen nicht möglich. Für die verwaltungsinterne Authentifizierung und Signierung ist sie durchgesetzter Standard.

Eine Eingrenzung der vom Land geförderten Online-Verwaltungsdienste nur auf die Benutzung von Tastatur-Kartenlesegeräte durch Bürgerinnen und Bürger und Unternehmen würde die deutschlandweit eher spärliche Akzeptanz des neuen Personalausweises und andere elektronischer Authentifizierungs- und Signaturkarten weiter lähmen. Eine indirekte Begünstigung der schwächer gesicherten eID-Dienste wäre die Folge.

Zu Nummer 9

Zu jeder datenschutz-/sicherheitstechnischen Risikoanalyse eines IT-Vorhabens als Basis für ein geordnet ablaufendes Förderprojekt gehört auch die Prüfung der Zulässigkeit der Nutzung eines (oder wie hier gefordert des eGo-MV) Berechtigungszertifikates und insbesondere die Prüfung des Umfangs der Berechtigungstiefe des Zertifikates. Insofern hat das IM im Bereich der E-Government-Förderung auch bisher die korrekte Nutzung von Berechtigungszertifikaten bereits eingefordert und in allen Förderfällen im Zuge der Verwendungsnachweisprüfungen als Fachaufsicht auch in Augenschein genommen. Dennoch bleibt die jeweilige Kommune in der eigenen Generalverantwortung.

Zu Nummer 10

Die Landesregierung verweist auf die Eigenverantwortung der Kommunen sowie auf den eGo-MV. Im Rahmen des Aufbaus eines Informationssicherheitsmanagements bietet die Landesregierung den Kommunen einfach ausgeprägte Unterstützung bei der Sensibilisierung ihrer Mitarbeiter sowie in partiellen Umfang organisatorische Hilfen an.

Um den „Wunsch“ dieser Empfehlung zu erfüllen müsste der § 15 und/oder der § 17 des EGovG M-V mit dem Ziel einer Bindung der Kommunen geändert werden. Solange dieses nicht der Fall ist, wird auf die unter Punkt 1.2.2 beschriebenen Verbindlichkeitsmechanismen verwiesen.

Zu Nummer 11

Wie der LfDI in Ziffer 1.2 lfd. Nr. 11 ausgeführt hat, wird die Landesregierung eine datenschutzgerechte Ausgestaltung beim Zensus 2021 beachten und bei der Erarbeitung der landesrechtlichen Vorschriften für den Zensus 2021 berücksichtigen. Derzeit werden die bundesrechtlichen Vorschriften zum Zensus 2021 von der Bundesregierung vorbereitet. Erst nach deren Erlass kann mit der Erarbeitung der landesrechtlichen Vorschriften begonnen werden.

Zu Nummer 14

Bereits im September 2013 hat die Fraktion BÜNDNIS 90/DIE GRÜNEN einen Gesetzentwurf eines Transparenz- und Informationsfreiheitsgesetzes für das Land vorgelegt. Im Plenum hat der Innenminister für die Landesregierung Stellung genommen.

Der Landtag hat den Gesetzesentwurf, insbesondere wegen rechtlicher, und technischer Probleme, abgelehnt.

2 Projekte

2.1 Datenschutz und Bildung

Die Landesregierung bekennt sich zu der im Koalitionsvertrag verankerten Aufgabe hinsichtlich des Datenschutzes als Bildungsaufgabe und setzt sie in seiner Zuständigkeit in vielfältiger Weise unter dem Primat der Zielgruppenadäquatheit und der Nachhaltigkeit um. Diesem Ziel dienen die durch das Medienpädagogische Zentrum im Institut für Qualitätsentwicklung Mecklenburg-Vorpommern (MPZ) angebotenen Lehrerfortbildungen und Multiplikatorenschulungen, die modulare Ausbildung von Referendaren zur schulischen Medienbildung sowie die Begleitung von Schulentwicklungsprozessen mit dem „Audit - Auf dem Weg zur Medienschule“. Letzteres enthält seit seiner neu überarbeiteten 2. Auflage (Januar 2015) auch dem Qualitätsbereich „Prävention“. Und schließlich wird dieser Aufgabe auch weiterhin durch die Kooperation mit allen Partnern der Medienbildung im Land Rechnung getragen.

Das BM und der LfDI arbeiten bei der Umsetzung der Rahmenvereinbarung zur „Förderung von Medienkompetenz“ partnerschaftlich zusammen.

Insbesondere hat sich die langjährige Kooperation im Rahmen des Netzwerkes „Medienaktiv M-V“ bewährt: Die Mitarbeiter des LfDI und des BM informieren sich gegenseitig über eigene Aktivitäten und treten gemeinsam auf Fortbildungsveranstaltungen auf.

Begrüßenswert ist die berichtete neuerdings stärkere Zuwendung des LfDI zur Zielgruppe der Eltern, der Familien und der Erzieherinnen und Erzieher, wodurch das Bestreben des BM, an jeder Schule mindestens eine qualifizierte Lehrkraft zu allen Fragen des Jugendmedienschutzes zu haben, komplementär ergänzt wird. Dem gleichen Ziel dienen auch die Angebote des LfDI zur Schulung von Kindern und Jugendlichen.

2.1.1 Vermittlung von Medienkompetenz und Datenschutzbewusstsein an den Schulen

Eine Stellungnahme zu den hier unter 2.1.1 angeschnittenen Themen ergibt sich aus der Gesamtheit der Darstellungen zu den nachfolgenden Punkten 2.1.2 bis 2.1.5.

2.1.2 Kooperationsvereinbarung zur Medienkompetenzförderung

Die Landesregierung begrüßt den LfDI als neuen Partner der Kooperationsvereinbarung zur Förderung der Medienkompetenz in Mecklenburg-Vorpommern, die im April 2015 unterzeichnet wurde. Durch die erweiterte und aktualisierte Rahmenvereinbarung können die Potenziale der Vertragspartner bedarfsgerecht und zielgruppenorientiert zur Förderung der Medienkompetenz ausgerichtet werden.

Sowohl der LfDI als auch das BM arbeiten im Rahmen der seit dem 21. April 2015 gültigen Kooperationsvereinbarung in der Arbeitsgruppe „KITA“ und der Arbeitsgruppe „Digitale Schule“ mit.

Die Arbeitsgruppe „KITA“ hat seither zwei Mal getagt. Alle Beteiligten sind sich einig, dass ein steigender Bedarf für Schulungs- und Informationsmaßnahmen für Eltern, Erzieherinnen und Erzieher sowie für Ausbilderinnen und Ausbilder besteht. Der entsprechende Bedarf bei Kindern im Vorschulalter wird vom federführenden BM durchaus differenziert gesehen. Der Abstimmungsprozess zu Zielsetzungen und daraus resultierenden Empfehlungen befindet sich derzeit in einem frühen Entwicklungsstadium.

Die Mitwirkung des LfDI in der Arbeitsgruppe „Digitale Schule“ und in ihren drei Unter-Arbeitsgruppen ist bei der Schaffung zukunfts- und rechtssicherer Grundlagen, Strukturen und Angebote zielführend und eine wichtige Ergänzung zur Arbeit der anderen teilnehmenden Institutionen.

2.1.3 Netzwerk „Medienaktiv M-V“

Eine wichtige Aufgabe der Kooperationsvereinbarung ist die Stärkung und der Ausbau des Netzwerkes „Medienaktiv“. Mit seinen Angeboten leistet das Netzwerk einen unverzichtbaren Beitrag zur Medienbildung. Hervorzuheben ist die Zusammenarbeit von Partnern unterschiedlicher Ressorts und Zuständigkeitsgebieten, wie Datenschutz, Suchthilfe, Jugendhilfe, Medienpädagogik, Polizei und Schule. Die Landesregierung begrüßt daher in besonderer Weise, dass sich die langjährige, bewährte Kooperation mit dem LfDI im Rahmen der Initiative „Medienaktiv M-V“ weiter vertieft hat.

2.1.4 „Medienscouts MV“ und TEO „Protect Privacy“

Die Landesregierung begrüßt die Initiative des LfDI im Rahmen des Projektes „Medienscouts M-V“ Schülerinnen und Schüler zu Experten in der verantwortungsbewussten Nutzung von Internet und sozialen Netzwerken auszubilden und dieses Expertenwissen an Gleichaltrige weiterzugeben. Damit wird das Bestreben, an jeder Schule mindestens eine qualifizierte Lehrkraft zu allen Fragen des Jugendmedienschutzes zu haben, um präventiv mit Schülerinnen und Schülern zu arbeiten, durch jugendliche Experten unterstützt. Dieses Konzept ist ein gelungenes Projekt des Datenschutzes im Zusammenwirken mit verschiedenen Partnern, die an sogenannten „Medienscouts-Wochenenden“ Jugendliche befähigen, kritisch und achtsam mit digitalen Medien umzugehen und ihr neu erworbenes Wissen an ihre Mitschüler, Lehrer und Eltern weiterzugeben.

Das Modell TEO „Tage der ethischen Orientierung“ der Evangelisch-Lutherischen Kirche in Norddeutschland ist ein schulkooperatives Gemeinschaftsprojekt des Datenschutzes und weiterer Partner. Das darin enthaltene Modul „protect privacy - mein Klick, meine Verantwortung!?“, welches den Schutz der Privatsphäre in den Blick nimmt, ist speziell für die 5. und 6. Klassen konzipiert. Hierbei handelt es sich um ein Angebot, welches sich dem Thema des verantwortungsvollen und reflektierten Handelns im Internet zuwendet und dieses einem breiteren Kreis von Schülerinnen und Schülern im sensiblen Alter von 11 oder 12 Jahren eröffnet.

2.1.5 Datenschutz an den Schulen in Mecklenburg-Vorpommern

Um den datenschutzrechtlichen Ist-Zustand an den Schulen im Land zu erfassen, hat der LfDI zusammen mit dem BM eine Online-Befragung aller 593 Schulen vorgenommen und im Anschluss an 18 ausgewählten Schulen im Land die Einhaltung des Datenschutzes überprüft. Im Ergebnis sind laut LfDI diverse Datenschutzverstöße festgestellt worden. Der LfDI geht davon aus, dass die Umsetzung des Datenschutzes an der überwiegenden Zahl der Schulen des Landes ebenfalls als kritisch einzuschätzen ist. Die Ergebnisse vorgenannter Untersuchung sind in dem Projektbericht „Datenschutz an den Schulen in Mecklenburg-Vorpommern“ zusammengefasst. Es werden Handlungsbedarfe bei allen Beteiligten im gesamten Schulbereich ausgemacht.

So wird beispielsweise unter der dortigen Ziffer 4.3.2 an das IM die Empfehlung ausgesprochen, Rahmenbedingungen zu schaffen, die die Schulträger motivieren und in die Lage versetzen, mit den Schulen vertragliche Beziehungen einzugehen, etwa im Zusammenhang mit der Verarbeitung personenbezogener Daten im Auftrag gemäß § 4 DSG M-V. Insbesondere möchte der LfDI finanzielle Mittel bereitgestellt wissen, damit die Anforderungen des DSG M-V, des SchulG M-V und der SchulDSVO M-V, speziell in Bezug auf den technischen Datenschutz an den Schulen, umgesetzt werden können.

Die Landesregierung stimmt mit dem LfDI überein, dass die Beseitigung der datenschutzrechtlichen Defizite ein gemeinsames Handeln aller Beteiligten erfordert, um rechtliche Klarstellungen vorzunehmen und geeignete technische und organisatorische Maßnahmen umzusetzen. Insofern wird auch von der Landesregierung ausdrücklich das in der gemeinsamen Pressemitteilung des LfDI, des BM, des Städte- und Gemeindetages (StGT) und des Landkreistages (LKT M-V) vom 26.04.2016 benannte Projekt begrüßt, an dem auch der eGo-MV mitwirkt.

An Musterschulen sollen die technischen und organisatorischen Erfordernisse des Datenschutzes erarbeitet werden. Danach kann entschieden werden, wer welche Aufgaben künftig zu verantworten hat, welche Rechtsänderungen erforderlich sein werden und wie dies künftig finanziert werden soll. Die Landesregierung rechnet damit, dass praktikable Modelle in ca. fünf Jahren vorliegen. Mit dem neuen Schulrechtsportal steht Schulleitern aber schon jetzt eine Plattform auch in datenschutzrechtlichen Fragestellungen zur Verfügung. Die Schuldatenschutzverordnung wird zudem bereits vom fachlich zuständigen BM überarbeitet.

Von dem Modellprojekt an einer Musterschule oder mehreren Musterschulen verspricht sich auch das IM, Hinweise zu erhalten, wie der Datenschutz an den hiesigen Schulen verbessert werden kann. Von daher sollte - vor Schaffung etwaiger Rahmenbedingungen durch das IM - zunächst der Ausgang dieses Pilotprojektes abgewartet werden.

2.2 Kommunales/Personenstandswesen

Die Kommunen sind wegen der ebenen- und infrastrukturübergreifenden Architektur der IT-Systeme daran interessiert, ein gemeinsam mit dem Land finanziertes und „gelebtes“ einheitliches Informationssicherheits- und Datenschutz-Management-System aufzubauen. Dazu ist es unter anderem notwendig, ein gemeinsames Management-Werkzeug im Ersatz für das vom Bund als auslaufend angekündigte GS-Tool effizient und effektiv zu nutzen. Die landesweit beabsichtigte Einführung des für die Landesbehörden beschafften Werkzeuges (ISMS „Verinice“) wird durch fehlerbehaftete GS-Tool-Altdatenübernahmen ausgebremst. Damit wird die Nachnutzbarkeit der im Berichtszeitraum erstellten Datenbasis infrage gestellt.

Erst wenn eine Datenübernahme auch für kommunale Altdatenbestände fehlerfrei funktioniert, kann Doppelarbeit mit dem bereits jetzt frei verfügbaren Produkt vermieden werden. Die Kommunen stehen derzeit vor dem Problem, entscheiden zu müssen, ob sie ein eigenes importfähigeres Managementsystem einführen oder ob sie die Freigabe des Verinice-Werkzeuges nach Fehlerbereinigung abwarten.

3 IT-Planungsrat

3.2 Cloud-Richtlinie der Datenzentralen

Die Landesregierung ist sich der Datenschutzanforderungen an Cloud-Computing bewusst. So hat die Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH (DVZ M-V GmbH) in Zusammenarbeit mit den IT-Dienstleistern der anderen Bundesländer die Richtlinie „Öffentliche Aufträge in der Cloud“ im Auftrag des IT-Planungsrats erarbeitet. Diese soll einen datenschutzgerechten Umgang mit dem Thema sicherstellen und die Nutzung befördern. Die Richtlinie wurde mit dem BSI und dem AK Technik des LfDI abgestimmt. Auf der 16. Sitzung des IT-Planungsrats wurde die Richtlinie zur Kenntnis genommen sowie empfohlen, bei der Inanspruchnahme von Cloud-Dienstleistungen und Cloud Service Providern die Verwendung der Handlungsempfehlung einschließlich der Kriterientabelle anzuwenden. Diese Vorgehensweise soll in die IT-Richtlinie als zukünftiger Landesstandard aufgenommen werden.

3.3 Informationssicherheit in den Kommunen

Die Empfehlung ist zuletzt auf dem Partner- und Mitgliedertag des eGo-MV durch Workshop-Vorträge der kommunalen Datenschützer eGo-MV und des Beauftragten der Landesverwaltung für Informationssicherheit (BeLVIS) bekräftigt worden, um die Leitungen der kommunalen Verwaltungen wiederholt auf unterschiedlichsten Verantwortungsebenen zu sensibilisieren.

Die Landesregierung weist daher erneut darauf hin, dass die wiederholt vom LfDI ausgesprochene Empfehlung an die Kommunen zur Anwendung der „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ im Landtag, in den Arbeitsgremien sowie in mehreren gemeinsamen Veranstaltungen umfassend thematisiert wurde. Über diese Leitlinie hinaus, insbesondere bei den ebenenübergreifenden IT-Verfahren sowie bei der Absicherung der gemeinsam genutzten Kommunikationsinfrastruktur (CN LAVINE) soll die Grundschutzmethodik des BSI verbindlich angewendet werden. Flankierend hierzu strebt das IM den landeseinheitlichen Einsatz eines ISMS-Werkzeuges an. Darüber hinaus werden die Kommunen auch in den gemäß Leitlinie geforderten Aufbau des Informationssicherheitsmanagements und des Landes-CERT eingebunden werden.

3.5. Die Umsetzung der eID-Strategie - Schwerpunkt Bürgerkonten

Die Konzeption zukünftiger Servicekonten (vormals Bürgerkonten) im IT-Planungsrat berücksichtigt die rechtlichen Rahmenbedingungen. Dazu gehören auch Aspekte des Datenschutzes. Das IM wird die Empfehlungen des LfDI in die Überlegungen zur Ausgestaltung von Servicekonten einbeziehen.

4 Technik und Organisation

4.1 Neue Technologien

4.1.1 Das Standard-Datenschutzmodell

Die Empfehlung des LfDI, bei der Planung, der Einrichtung und dem Betrieb von Verfahren zur Verarbeitung personenbezogener Daten die im Standard-Datenschutzmodell (SDM) beschriebene Verfahrensweise evaluierend anzuwenden, ist zu begrüßen. Es ist zu erwarten, dass den datenverarbeitenden Stellen ein Werkzeug an die Hand gegeben wird, personenbezogene Verfahren nicht nur sicher, sondern auch datenschutzgerecht einzurichten und zu betreiben.

Die Landesregierung beabsichtigt bei der Planung, Einrichtung und dem Betrieb von IT-Verfahren zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten neben der Vorgehensweise und den Maßnahmen aus dem BSI IT-Grundschutz insbesondere auch auf den Einsatz des SDM hinzuwirken.

4.1.2 Das Technologieprogramm Trusted Cloud

Die Landesregierung wird die Methoden und Unterlagen des Trusted-Cloud-Projekts bei der Erstellung der künftigen IT-Landesstandards als Anlage zu den IT-Richtlinien gemäß des E-Government-Gesetzes M-V berücksichtigen.

4.1.3 Digitale Selbstvermessung

Zum Thema Gesundheits-Apps ist vom Bundesministerium für Gesundheit eine Studie in Auftrag gegeben worden, die erstmals einen Überblick über Datenschutzaspekte, Transparenz und die medizinische Qualität der Angebote auf dem Markt gibt. Die im April 2016 veröffentlichte Studie soll danach eine wichtige Grundlage für den weiteren Fachdialog mit den Verantwortlichen im Gesundheitswesen, Datenschützern, App-Herstellern und Experten sein, um daraus konkrete Maßnahmen und Selbstverpflichtungen abzuleiten.

Da bei den zahlreichen frei zugänglichen Gesundheits- oder Fitness-Apps zum Teil sensible Gesundheitsdaten erfasst und verarbeitet werden, erscheint die Aufklärung der Nutzer über die Risiken der Preisgabe persönlicher Gesundheitsdaten im privaten Bereich besonders wichtig (Orientierungshilfen, Vertrauenswürdigkeit).

4.1.4 Risiken der Fernwartung

Die Hinweise zur Anwendbarkeit von Fernwartungen werden aufgegriffen und in allen neuen Projekten beachtet (Auflagen-Textbaustein im jeweiligen Förderbescheid). Für bereits laufende Entwicklungen neuer Informationssysteme im Bereich der E-Government-Förderung werden die Projektleitungen über das Förderreferat auf die Handlungsnotwendigkeiten hingewiesen. Für ebenenübergreifende Kooperationsprojekte werden über das Büro Kooperatives E-Government als operative Koordinierungsinstanz entsprechende Informationen an alle Verantwortlichen der projektbeteiligten Kommunen versendet. Die kommunalen Landesverbände werden um Verteilung der Informationen über die einschlägigen Informationskanäle [z. B. „Rundschreiben“ (LKT M-V), „Der Überblick“ (StGT M-V)] gebeten.

4.1.5 XTA - sicherer Datentransport in der öffentlichen Verwaltung

Die Landesregierung war gemeinsam mit den Datenschutzbehörden an der Entwicklung des Standards zum sicheren Datentransport beteiligt. Die Vorteile des Standards werden ebenso gesehen. Es ist vom IM geplant, diesen Standard auch in Mecklenburg-Vorpommern zu etablieren. So soll das Verfahren XTA bei der laufenden Migration des Dienstleistungsportals zur datenschutzgerechten Übergabe von Antragsdaten an die angeschlossenen Verfahren zum Einsatz kommen.

4.1.6 Neue Norm zur Datenträgervernichtung

Die Landesregierung begrüßt die Orientierungshilfe des LfDI zur „Ermittlung des Schutzbedarfs personenbezogener Daten für den Prozess der Datenträgervernichtung“ und wird sie weiterhin entsprechend berücksichtigen. Relevante Datenträger werden nach der DIN 66399 seit deren Gültigkeit vernichtet.

4.1.9 Gewährleistung der Menschenrechte bei der elektronischen Kommunikation

Im Kontext mit der Gewährleistung der Vertraulichkeit, der Integrität und der Authentizität der Kommunikationsinfrastruktur der Landesverwaltung wird das IM die empfohlenen Maßnahmen berücksichtigen. Hierbei wird insbesondere der Fokus auf die Förderung der Vertraulichkeit informationstechnischer Systeme durch BSI-Zertifizierungen bzw. vergleichbare Zertifizierungen und „Made in Germany“ liegen. Das IM wird im Rahmen seiner Kompetenz darauf hinwirken, dass der betriebliche Einsatz von Verschlüsselungstechnologien und -produkten in Abhängigkeit von den wirtschaftlichen Sicherheitskosten dem „Stand der Technik“ sowie den Empfehlungen des BSI entsprechen.

4.1.10 Verschlüsselung ohne Einschränkungen

Die Landesregierung setzt auf den Einsatz von Transportprotokollen und Verfahren, die eine möglichst einfache Anwendung von Verschlüsselungstechniken erlauben.

In einer gesamtheitlichen Sicht wird bei den laufenden Planungen auch die Kommunikation zu den Bürgern und der Wirtschaft mit betrachtet. Gängige Verschlüsselungstechniken sollen hier unterstützt, durchgehend implementiert und die Nutzung durch flankierende Maßnahmen, wie z. B. dem leichten Zugang zu benötigten Verschlüsselungszertifikaten, erleichtert werden.

Ebenso wird bei der Beteiligung an entsprechenden Entwicklungen auf die Umsetzung der genannten Ziele hingewirkt.

4.1.11 Cloud-Nutzung - oft ohne Wissen der Nutzenden

In der Landesverwaltung ist eine Nutzung von Cloud-Diensten in der Software Microsoft Office bezüglich der IT-Arbeitsplätze per Gruppenrichtlinie unterbunden. Eine Nutzung in den mobilen Geräten der Mobile-Device-Management-Lösung der Landesverwaltung ist standardmäßig deaktiviert. Zusätzlich beschreibt die Richtlinie zum Umgang mit dienstlichen mobilen Geräten vom 07.11.2012 die Vorgaben beim Betrieb von dienstlichen mobilen Geräten, um die bestehenden Sicherheits- und Datenschutzanforderungen zu gewährleisten. In dieser ist hinsichtlich der Cloud-Nutzung Folgendes geregelt: *„Eine Speicherung von Daten bei Dritten, z. B. in einem sogenannten Cloud-Service im Internet, ist nicht gestattet.“*

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

Wie zutreffend wiedergegeben, enthält die Gemeinsame Geschäftsordnung I der Ministerien und der Staatskanzlei des Landes Mecklenburg-Vorpommern (GGO I) in ihrer aktuellen Fassung keine Ausführungen mehr zum E-Mail-Versand von Dokumenten. Das EGovG M-V enthält dafür in seinem § 15 Abs. 2 die Ermächtigung, eine verbindliche IT-Richtlinie erlassen zu können, in der als Landesstandard vergleichbare Forderungen zum sicheren Datenaustausch aufgenommen werden. Damit wird der Forderung ein erheblich stärkeres Gewicht verliehen, als dies die GGO I bislang vermochte.

Diese IT-Richtlinie wird bereits im „Rat der IT-Verantwortlichen der Ressorts“ abgestimmt, in welchem auch der LfDI vertreten ist.

Die beschriebenen Verunsicherungen bei Mitarbeiterinnen und Mitarbeitern sind der Landesregierung nicht bekannt.

5 Datenschutz in verschiedenen Rechtsgebieten

5.1 Rechtswesen

5.1.1 Bundesnotarordnung - Gesetz zur Neuordnung der Aufbewahrung von Notariatsunterlagen

Im Auftrag der Justizministerkonferenz erarbeitete eine länderoffene Arbeitsgruppe einen Gesetzentwurf zur Neuordnung der Aufbewahrung von Notariatsunterlagen, mit welchem ein elektronisches Urkundenarchiv für die Aufbewahrung von Notariatsunterlagen errichtet werden soll. Der LfDI wurde von einem Länderkollegen von der Tätigkeit dieser Arbeitsgruppe in Kenntnis gesetzt und erbat im Justizministerium (JM) nähere Informationen zum Gesetzgebungsvorhaben. Der seinerzeit aktuelle Arbeitsentwurf der Arbeitsgruppe wurde dem LfDI daraufhin übersandt. Die daraufhin erhobenen datenschutzrechtlichen Bedenken des LfDI wurden an die Arbeitsgruppenmitglieder weitergeleitet. Auch Datenschutzbeauftragte anderer Länder erhoben Bedenken. Die Arbeitsgruppe hatte sich mit den datenschutzrechtlichen Bedenken eingehend auseinander gesetzt und entsprechende Änderungen des Gesetzentwurfs vorgenommen.

Nach Kenntnisnahme des Berichtes der Arbeitsgruppe und Billigung des erarbeiteten Gesetzentwurfs durch die Justizministerkonferenz im Juni 2016 in Nauen haben die Justizministerinnen und -minister die Bereitschaft des Bundesministeriums der Justiz und für Verbraucherschutz begrüßt, auf Grundlage des Gesetzentwurfes eine Gesetzgebungsinitiative der Bundesregierung vorzubereiten. Die ursprünglich eingesetzte Arbeitsgruppe beabsichtigt nun, an den notwendigen Verordnungsentwürfen weiter zu arbeiten.

In den Beratungen wurde seitens des Bundesministeriums der Justiz und für Verbraucherschutz zugesichert, dass die notwendig zu beteiligenden Stellen im Gesetzgebungsverfahren eingeschaltet werden. Datenschutzrechtliche Belange werden dort abschließend behandelt.

Ein landesinternes Beteiligungsverfahren ist wegen der Initiative der Bundesregierung für den Gesetzesentwurf nicht vorgesehen.

5.1.2 Forschungsprojekt zum Warnschussarrest

Das Forschungsinstitut hatte sich an die Landesjustizverwaltungen gewandt, um das Einverständnis zur Durchführung des Projektes einholen.

In Mecklenburg-Vorpommern war kein Landgerichtsbezirk hinsichtlich der Auswertung von Verfahrensakten bzw. der Praktikerbefragung betroffen, sondern lediglich die Jugendarrestanstalt Neustrelitz im Rahmen der Befragung sämtlicher Vollzugsleiterinnen und -leiter. Unter der Voraussetzung, dass den seitens des LfDI geäußerten Bedenken Rechnung getragen wird, wurde dem Forschungsvorhaben zugestimmt.

5.1.3 Öffentlichkeitsfahndung in sozialen Netzwerken im Internet

Die Änderung der Anlage B der Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) wurde in Mecklenburg-Vorpommern durch die Gemeinsame Verwaltungsvorschrift des IM und des JM vom 9. Mai 2016, wie bereits in den meisten anderen Bundesländern, mit Wirkung vom 1. März 2016 in Kraft gesetzt (Erste Änderung der Verwaltungsvorschrift über die Inanspruchnahme von Publikationsorganen und Nutzung des Internets sowie anderer elektronischer Kommunikationsmittel zur Öffentlichkeitsfahndung nach Personen im Rahmen von Strafverfahren, AmtsBl. S. 329). Die Neufassung berücksichtigt die in der Entschließung der 87. Konferenz der Datenschutzbeauftragten angemerkte Kritik.

Das Bundesministerium der Justiz und für Verbraucherschutz hat darüber hinaus in einem Schreiben an die Bundesbeauftrage für den Datenschutz und die Informationsfreiheit vom 27. April 2016 betont, dass die im Schreiben der Bundesdatenschutzbeauftragen vom November 2015 geäußerten datenschutzrechtlichen Bedenken gegen die Änderung der Anlage B der RiStBV bei der Neufassung berücksichtigt wurden.

5.2 Polizei

5.2.1 Gemeinsame Telekommunikationsüberwachung der norddeutschen Küstenländer

Der Landtag hat am 08.06.2016 dem Staatsvertrag über die Einrichtung und den Betrieb eines Rechen- und Dienstleistungszentrums zur Telekommunikationsüberwachung (RDZ) der Polizei im Verbund der norddeutschen Küstenländer zugestimmt.

Die LfDI der Vertragspartner begleiten den Aufbau und den Betrieb des RDZ fachlich und haben eine gemeinsame Stellungnahme zum Vertrag abgegeben. Den Anregungen wurde durch Änderungen im Vertragstext Rechnung getragen.

5.2.2 Neue Richtlinien für die erkennungsdienstliche Behandlung

Die Bearbeitung der Richtlinie für die erkennungsdienstliche Behandlung ist fast abgeschlossen. Derzeit wird seitens des Landesamtes für Zentrale Aufgaben und Technik der Polizei, Brand- und Katastrophenschutz (LPBK) noch an der technischen Umsetzung der Vordrucke gearbeitet, die den Polizeibeamten zentral zur Verfügung gestellt werden. Sofern dies beendet ist, soll die Richtlinie in Kraft treten.

Die seitens des LfDI im Rahmen des Entwicklungsprozesses der Richtlinie und nunmehr im Tätigkeitsbericht geäußerten Bedenken wurden geprüft und das Ergebnis der Prüfung dem LfDI mit Schreiben vom 23.06.2016 mitgeteilt. Die Bedenken konnten dabei entweder entkräftet werden oder ihnen wurde in der Richtlinie Rechnung getragen.

5.2.3 Neue Richtlinie zur Funkzellenabfrage

Dem LfDI wurde mehrfach - letztmalig im April 2016 - zum Richtlinienentwurf Gelegenheit zur Stellungnahme gegeben. Die hierzu eingegangenen Anmerkungen und Änderungsvorschläge des LfDI wurden dabei aufgegriffen und in die Richtlinie eingearbeitet. Im weiteren Verlauf der Abstimmung ist ein Gespräch zwischen dem Landeskriminalamt und LfDI vorgesehen. Insofern erfolgt die Erarbeitung der Richtlinie zur Funkzellenabfrage in Zusammenarbeit mit dem LfDI.

5.2.4 Verschlüsselung bei Anfragen der Polizei nach dem Telekommunikationsgesetz

Bei dem im Bericht geschilderten Vorfall handelt es sich um einen Einzelsachverhalt. Hinweise auf vergleichbare Sachverhalte liegen nicht vor. Die Polizeivollzugsbeamten werden regelmäßig zum richtigen Umgang mit personenbezogenen Daten sensibilisiert.

5.3 Verfassungsschutz

5.3.1 Änderung des Landesverfassungsschutzgesetzes

Der Hinblick auf den zu Nummer 5.3.1 nur auszugsweise zitierte BVerfG-Urteilstext zeigt in seiner Gesamtwiedergabe klar und deutlich die Verfassungsrechtslage zur Internetkommunikation auf.

Der Regelung des § 10 Absatz 1 Ziffer 12 des Landesverfassungsschutzgesetzes (LVerfSchG) wird durch den LfDI ein Eingriffscharakter zugesprochen, den sie nicht hat, sodass es insbesondere keiner ausdrücklichen Regelung zum Schutz des Kernbereichs privater Lebensgestaltung bedarf. Der LfDI wirft die Frage auf, „wann ein Vertrauen in einen Gesprächspartner schutzwürdig ist“ und meint, dass die Ausführungen des Bundesverfassungsgericht (BVerfG) in seinem Urteil vom 28. Februar 2008 (E 120, 274 ff. - Online-Durchsuchung) zum Eingriff in das Recht auf informationelle Selbstbestimmung durch Ermittlungstätigkeiten der Polizei „entsprechend heranzuziehen“ sind.

Das BVerfG selbst zeigt demgegenüber in der bezogenen Entscheidung, welche Befugnisse der Verfassungsschutzbehörde im Rahmen der Aufklärung von Internetkommunikation zustehen, ohne dass ein Eingriff in Artikel 10 bzw. Artikel 2 des Grundgesetzes (GG) vorliegt. Das BVerfG führt aus (Zitat nach Juris-Fassung Rn 291 - 293, 310/311):

> „[...] Steht im Vordergrund einer staatlichen Ermittlungsmaßnahme nicht der unautorisierte Zugriff auf die Telekommunikation, sondern die Enttäuschung des personengebundenen Vertrauens in den Kommunikationspartner, so liegt darin kein Eingriff in Art. 10 Abs. 1 GG (vgl. BVerfGE 106, 28 <37 f.>). Die staatliche Wahrnehmung von Inhalten der Telekommunikation ist daher nur dann am Telekommunikationsgeheimnis zu messen, wenn eine staatliche Stelle eine Telekommunikationsbeziehung von außen überwacht, ohne selbst Kommunikationsadressat zu sein. **Das Grundrecht schützt dagegen nicht davor, dass eine staatliche Stelle selbst eine Telekommunikationsbeziehung zu einem Grundrechtsträger aufnimmt.** Erlangt eine staatliche Stelle Kenntnis von den Inhalten einer über die Kommunikationsdienste des Internet geführten Fernkommunikation auf dem dafür technisch vorgesehenen Weg, so liegt darin nur dann ein Eingriff in Art. 10 Abs. 1 GG, wenn die staatliche Stelle hierzu nicht durch Kommunikationsbeteiligte autorisiert ist. **Da das Telekommunikationsgeheimnis das personengebundene Vertrauen der Kommunikationsbeteiligten zueinander nicht schützt, erfasst die staatliche Stelle die Kommunikationsinhalte bereits dann autorisiert, wenn nur einer von mehreren Beteiligten ihr diesen Zugriff freiwillig ermöglicht hat.**
>
> Das heimliche Aufklären des Internet greift danach dann in Art. 10 Abs. 1 GG ein, wenn die Verfassungsschutzbehörde zugangsgesicherte Kommunikationsinhalte überwacht, indem sie Zugangsschlüssel nutzt, die sie ohne oder gegen den Willen der Kommunikationsbeteiligten erhoben hat. So liegt es etwa, wenn ein mittels Keylogging erhobenes Passwort eingesetzt wird, um Zugang zu einem E-Mail-Postfach oder zu einem geschlossenen Chat zu erlangen.
>
> Dagegen ist ein Eingriff in Art. 10 Abs. 1 GG zu verneinen, wenn etwa ein Teilnehmer eines geschlossenen Chats der für die Verfassungsschutzbehörde handelnden Person seinen Zugang freiwillig zur Verfügung gestellt hat und die Behörde in der Folge diesen Zugang nutzt. Erst recht scheidet ein Eingriff in das Telekommunikationsgeheimnis aus, wenn die Behörde allgemein zugängliche Inhalte erhebt, etwa indem sie offene Diskussionsforen oder nicht zugangsgesicherte Webseiten einsieht.
>
> [...]
>
> **Ein Eingriff in das Recht auf informationelle Selbstbestimmung liegt nicht schon dann vor, wenn eine staatliche Stelle sich unter einer Legende in eine Kommunikationsbeziehung zu einem Grundrechtsträger begibt**, wohl aber, wenn sie dabei ein schutzwürdiges Vertrauen des Betroffenen in die Identität und die Motivation seines Kommunikationspartners ausnutzt, um persönliche Daten zu erheben, die sie ansonsten nicht erhalten würde.
>
> [...]

> **Danach wird die reine Internetaufklärung in aller Regel keinen Grundrechtseingriff bewirken.** Die Kommunikationsdienste des Internet ermöglichen in weitem Umfang den Aufbau von Kommunikationsbeziehungen, in deren Rahmen das Vertrauen eines Kommunikationsteilnehmers in die Identität und Wahrhaftigkeit seiner Kommunikationspartner nicht schutzwürdig ist, da hierfür keinerlei Überprüfungsmechanismen bereitstehen. Dies gilt selbst dann, wenn bestimmte Personen - etwa im Rahmen eines Diskussionsforums - über einen längeren Zeitraum an der Kommunikation teilnehmen und sich auf diese Weise eine Art „elektronische Gemeinschaft“ gebildet hat. **Auch im Rahmen einer solchen Kommunikationsbeziehung ist jedem Teilnehmer bewusst, dass er die Identität seiner Partner nicht kennt oder deren Angaben über sich jedenfalls nicht überprüfen kann. Sein Vertrauen darauf, dass er nicht mit einer staatlichen Stelle kommuniziert, ist in der Folge nicht schutzwürdig**. [...]“
> (textliche Hervorhebungen durch die Landesregierung).

Im Sinne dieser klaren Aussagen des BVerfG ist die Regelung des § 10 Absatz 1 Ziffer 12 LVerfSchG zu verstehen. Ausdrücklich ist ein Eingriff in den von Artikel 10 GG geschützten Bereich durch die vorgesehene Regelung ausgeschlossen. Im Übrigen sind die Regelungen des § 10 Absatz 2 und 3 LVerfSchG anzuwenden. Soweit vom LfDI Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung gefordert werden, wären diese laut BVerfG nur dann erforderlich, „soweit eine staatliche Stelle zur Erhebung von Inhalten der Telekommunikation unter Eingriff in Art. 10 Abs. 1 GG ermächtigt wird (vgl. BVerfGE 113, 348 <390 ff.>)“ (zitiert nach BVerfGE 120, 274 ff. - Online-Durchsuchung, Rn 299 in Juris-Fassung).

Weiterhin meint der LfDI im Hinblick auf den neu gefassten § 20 Absatz 4 LVerfSchG, dass „die Übermittlungsbefugnisse durch die Verfassungsschutzbehörde an Polizei und Staatsanwaltschaften insgesamt etwas konkreter gefasst“ werden sollten.

Hierzu ist anzumerken, dass das Bundesministerium des Innern (BMI) zur Neufassung der parallelen Vorschrift des Bundesverfassungsschutzgesetzes (BVerfSchG) eine Bund-Länder-Arbeitsgruppe eingerichtet hatte. Der dort erarbeitete neue § 19 Absatz 1 BVerfSchG wurde in § 20 Absatz 4 wortgleich übernommen. Die Erarbeitung erfolgt auf der Grundlage des ATD-Urteils des BVerfG vom 24.04.2013, wonach der „Austausch von Daten zwischen den Nachrichtendiensten und Polizeibehörden für ein mögliches operatives Tätigwerden […] grundsätzlich einem herausragenden öffentlichen Interesse dienen“ muss, „das den Zugriff auf Informationen unter den erleichterten Bedingungen, wie sie den Nachrichtendiensten zu Gebot stehen, rechtfertigt.“ Dementsprechend wurden die Normen des Bundes und des Landes - jeweils insbesondere die Nummern 2 bis 4 der eingefügten Absätze - gestaltet.

5.4 Kommunales Meldewesen

5.4.1 Das E-Government-Gesetz des Landes

Die Landesregierung beabsichtigt, die Frage des Geltungsbereiches des EGovG M-V im Zusammenhang mit der Weiterentwicklung der Schulverwaltungssoftware und dem Projekt „Digitale Schule“ erneut aufzugreifen.

5.4.3 Lücke in Personenstandssoftware wird zu langsam geschlossen

Die Landesregierung weist darauf hin, dass es nach ihrem Informationsstand bislang keinen Sicherheitsvorfall gegeben hat. Die vom LfDI konstruierte Sicherheitslücke hätte die Manipulation von drei Anwendungen (Citrix/Austista/SecSigner) erfordert, um überhaupt erfolgreich eine Urkunde zu ändern. Selbst wenn dies gelungen wäre, wäre diese dann wiederum vom Registerverfahren abgewiesen worden. Die Formulierung im 1. Absatz zu Punkt 5.4.3, dass es durch diesen Mangel zu besonders schwerwiegenden Auswirkungen gekommen sei, ist derzeit daher nicht nachvollziehbar.

Für die Erstellung der Notfallpläne zur unverzüglichen Bewältigung akuter IT-Sicherheitsprobleme sind die Kommunen selbst zuständig. Bisher ist es nicht flächendeckend gelungen, in Ergänzung des landesseitigen zentralen Managementsystems für Informationssicherheit (ISMS) und des BeLVIS auch eine konzentrierend kommunale Instanziierung zu finanzieren, aufzubauen und in Arbeitsbereitschaft zu versetzen. Einzelinitiativen von verantwortungsbewussten Kommunen sind zu verzeichnen. Die Kernfrage einer lückenlosen Finanzierung muss vor der konkreten organisatorischen und technischen Umsetzung des ISMS im kommunalen Raum gelöst werden. Der eGo-MV hat 2015 nach einer Schätzung die kommunalseitigen Kosten mit bis zu ca. 2 Mio. Euro beziffert und eine zwischen Land und Kommunen aufgeteilte Finanzierung vorgeschlagen. Der vorgeschlagene Lösungsansatz wird weiterhin zu erörtern sein.

5.4.4 Kontrollserie Personenstandswesen

Das IM prüft seit der Errichtung des zentralen Sicherungsregisters die durch § 1 Absatz 1 Satz 3 Sicherungsregisterverordnung eröffnete Möglichkeit, den Betrieb des Sicherungsregisters durch eine Körperschaft des öffentlichen Rechts wahrnehmen zu lassen. Derzeit existiert für den Betrieb des Sicherungsregisters des Personenstandswesens ein Vertrag des Landes mit dem technischen Betreiber der DVZ-GmbH in dem auf die Belange des Datenschutzes eingegangen wird.

Daneben befindet sich auch die Änderung der Verordnung noch im laufenden Abstimmungsprozess. Der LfDI ist in beiden Prozessen frühzeitig eingebunden worden. Es wird darauf hingewiesen, dass das IM durch die Sicherungsregisterverordnung bisher nicht verpflichtet ist, den Betrieb des Sicherungsregisters an den Zweckverband zu übertragen. Es besteht, wie dargestellt, lediglich die Möglichkeit der Übertragung. Der vorletzte Absatz unter 5.4.4 enthält daher eine Aussage, die nach Auffassung der Landesregierung nicht zutreffend ist.

5.4.5 Datenpanne bei der Erstellung eines Adressbuches

Es handelte sich hierbei um einen Einzelfall aus dem Bereich des Melderechts. Dieser ist aber, nachdem das Problem offenbar wurde, korrekt behandelt worden und vollständig abgeschlossen.

5.4.6 Sparsamer Umgang mit Angaben von Antragstellern bei Beschlussvorlagen

Aus Sicht der Landesregierung bedarf es beim Thema „Beschlussvorlagen“ einer strikten Differenzierung zwischen der Behandlung in der Gemeindevertretung und in der Öffentlichkeit. Es gibt entgegen der Auffassung des LfDI keine Grundlage, der Gemeindevertretung als oberstem Willensbildungsorgan der Gemeinde persönliche Daten Dritter im Zusammenhang mit von der Gemeindevertretung zu treffenden Entscheidungen vorzuenthalten. Die Gemeindevertretung ist in der Gemeinde Organ der Kommunalen Selbstverwaltung und damit der Exekutive. Sie steht im eigenen Wirkungskreis an der Spitze des Entscheidungsprozesses und insofern an einer Stelle, wie sie im übertragenen Wirkungskreis der jeweilige Behördenleiter einnimmt, bei dem niemand fordern würde, persönliche Daten aus Entscheidungsvorlagen zu entfernen, weil sie für seine abschließende Entscheidung vermeintlich „nicht erforderlich“ wären. Abgesehen davon liegt die Erforderlichkeit der Kenntnis im vorliegenden Fall vor: Zum einen könnte kein Gemeindevertreter seiner Verpflichtung nachkommen, eigene Mitwirkungsverbote (§ 24 KV M-V), die aus verwandtschaftlichen Beziehungen zu Antragstellern resultieren, zu erkennen und anzuzeigen, wenn Beschlussvorlagen anonymisiert würden. Zum anderen wäre auch die der Gemeindevertretung obliegende Kontrolle der Verwaltung (§ 34 KV M-V) beeinträchtigt, wenn die Gemeindevertretung aufgrund einer Anonymisierung der Vorlagen nicht beurteilen könnte, ob verwaltungsseitig Entscheidungen aus unter Umständen illegitimen Gründen (verwandtschaftliche Beziehungen pp.) initiiert wurden. Dass Beschlussvorlagen, die persönliche Daten enthalten, dagegen nicht der Öffentlichkeit zugänglich gemacht werden dürfen, steht außer Frage. Sie sind auch nur für nicht-öffentliche Sitzungen vorzusehen.

5.4.7 Internetveröffentlichung einer Vorschlagsliste ehrenamtlicher Richter

In seinem Tätigkeitsbericht führt der LfDI aus, dass IM und JM sich mit dem LfDI in dieser Angelegenheit abstimmen will. Ein Ergebnis dazu läge noch nicht vor. Dies war lediglich bis Redaktionsschluss des Tätigkeitsberichts der Fall. Unterdessen hat IM dem LfDI geantwortet. Die Antwort lautete wie folgt:

> „Hinsichtlich der Behandlung der persönlichen Daten der Bewerber vor und während der Sitzung der Vertretungskörperschaft gibt es zwischen uns m. E. keine divergierenden Auffassungen mehr. Im Hinblick auf eine Veröffentlichung von Bewerberdaten im Zuge der Veröffentlichung der Niederschrift nach der Sitzung sehe ich §§ 29 Abs. 8 Satz 2, 107 Abs. 8 Satz 2 KV M-V als hinreichende Rechtsgrundlage für die jeweilige Kommune an, alles, was in der öffentlichen Sitzung Erwähnung gefunden hat und protokolliert wurde (also auch persönliche Daten der Bewerber) auf eine eigenverantwortlich festgelegte Art (also auch im Internet) der Öffentlichkeit zugänglich zu machen. Für ein rechtsaufsichtliches Einschreiten gegen derartige Vorgehensweisen fehlt es insofern an der verfassungsrechtlichen und einfachgesetzlichen Voraussetzung der Rechtswidrigkeit des kommunalen Handelns.“

Das JM wurde beteiligt.

5.4.8 Landesgesetz zur Ausführung des Bundesmeldegesetzes

Der LfDI hat bereits im Zuge der Ressort- und Verbandsanhörung zum Entwurf des Gesetzes zur Ausführung des Bundesmeldegesetzes im Land eine entsprechende Stellungnahme abgegeben. Die Prüfung seiner Vorschläge wird im Rahmen des Gesetzgebungsverfahrens erfolgen.

5.4.10 Erneuter Meldedatenabgleich für den Beitragsservice der Rundfunkanstalten

Die Durchführung eines wiederholten vollständigen Meldedatenabgleichs ist geeignet, die von den Ländern verfolgten Zwecke der Beitragsgerechtigkeit und der Vermeidung eines Vollzugsdefizits zu erreichen. Durch einen wiederholten vollständigen Meldedatenabgleich können in einfacher Weise Personen ermittelt werden, die einer beitragspflichtigen Wohnung zugeordnet werden können, mangels Erfüllung ihrer Anzeigepflicht aber nicht als Beitragsschuldnerin oder Beitragsschuldner erfasst sind. Durch den vollständigen Meldedatenabgleich erhalten die Landesrundfunkanstalten qualitativ hochwertige Daten bei zugleich geringer Eingriffsintensität für die Betroffenen.

Der Bayerische Verfassungsgerichtshof (Urteil vom 15. Mai 2014, Aktenzeichen 8-VII-12) führt hierzu aus, dass der Gesetzgeber den Gemeinwohlbelang, die Beitragsehrlichkeit durch Kontrollmöglichkeiten zu ergänzen, höher gewichten dürfe als die Schwere des Eingriffs in das Recht auf informationelle Selbstbestimmung. Die Daten seien zudem durch eine strikte Zweckbindung und strenge Löschungspflichten hinreichend abgesichert.

Eine vergleichsweise vollständige Erfassung von Personen im Wege alternativer Instrumente, wie der vollständigen dauerhaften Speicherung der Daten von Nicht-Beitragszahlerinnen und Nicht-Beitragszahlern, dem Adressankauf, der anlassbezogenen Meldedatenübermittlung, der Vermieterauskunft oder durch Ermittlungen vor Ort, ist nicht erfolgsversprechend. Hinzu kommt der deutlich stärkere Eingriff in die Privatsphäre der Betroffenen.

5.5 Soziales/Arbeitnehmerdatenschutz

5.5.1 Datenschutz bei der Förderung des Europäischen Sozialfonds

Die Initiative des LfDI, gemeinsam mit dem europäischen Datenschutzbeauftragten datenschutzrechtliche Fragen, die für die Verarbeitung von personenbezogenen Daten zum Zwecke der Förderung mit Mitteln des Europäischen Sozialfonds wesentlich sind, zu klären, wird von der Landesregierung begrüßt.

Im Ergebnis dieser Bemühungen wird zu prüfen sein, ob und inwieweit die bisherige Praxis der Datenerhebung, der Datenverarbeitung und der Datenübermittlung weiter optimiert werden kann. Das betrifft insbesondere auch den Umfang der eingesetzten Fragebögen. Insoweit wird zu prüfen sein, in welchem Umfang die Verarbeitung von personenbezogenen Daten unerlässlich ist, um einerseits die Förderung mit Mitteln des Europäischen Sozialfonds erfolgreich durchführen zu können und andererseits dem Grundsatz der größtmöglichen Datenvermeidung zu entsprechen (§ 5 Absatz 1 Satz 1 DSG M-V).

Eine Nichtbeachtung der einschlägigen europarechtlichen Vorgaben könnte allerdings dazu führen, dass für den weiteren Aufbau des Landes wichtige Aufgabenbereiche nicht von der Förderung mit Mitteln des Europäischen Sozialfonds profitieren könnten und das Land sich der Gefahr von Rückforderungen der Europäischen Kommission aussetzt, mit den damit verbundenen Risiken für den Landeshaushalt.

5.5.2 Datenerhebung durch den Träger einer Kindertagesstätte

In dem zugrunde liegenden Fall hat sich der LfDI dafür eingesetzt, dass der Träger einer Kindertagesstätte nicht bereits bei Abschluss des Betreuungsvertrages bestimmte personenbezogene Daten (Geburtsort, Geburtsname) der Eltern „auf Vorrat“ erhebt, sondern erst, wenn dies erforderlich ist (z. B. zur Einleitung eines Mahnverfahrens). Diese Empfehlung des LfDI findet die Zustimmung der Landesregierung.

5.6 Gesundheitswesen

5.6.2 Datenübermittlung von Ärzteversorgung an Gutachter

Laut dem Tätigkeitsbericht des LfDI hat die Ärzteversorgung ihr Fehlverhalten bei einer Datenübermittlung an einen Gutachter eingeräumt und zugesichert, die datenschutzrechtlichen Vorgaben in Zukunft zu beachten. Ein aufsichtsrechtliches Tätigwerden von Seiten des SM erscheint nicht notwendig.

5.6.3 Sichere Übermittlung von Krebsregisterdaten

Gegen die Auffassung des LfDI bestehen seitens der Landesregierung keine Bedenken.

5.7 Personal

5.7.1 Dokumentenmanagement in der Landesverwaltung (BEATA)

Auch im weiteren Verlauf des Projektes BEATA konnten die Projektverantwortlichen im Landesbesoldungsamt (LBesA) und im Finanzministerium (FM) von der sehr guten Zusammenarbeit mit dem LfDI profitieren. Unter anderem ist das LBesA im Zuge der Konzipierung des Dienststellenportals der Empfehlung des LfDI, die Daten der zugrunde gelegten Datenbank mit einem kryptografischen Verfahren zu verschlüsseln, gefolgt und hat diese entsprechend umgesetzt. Das Dienststellenportal konnte erfolgreich pilotiert und die Einführung des Portals in den personalführenden Dienststellen des Landes Anfang Juni des Jahres 2016 begonnen werden.

Im aktuellen Teilprojekt Mitarbeiterportal, welches den Landesbediensteten die Möglichkeit bietet, mit dem LBesA zu kommunizieren, bereitgestellte Formulare zu nutzen und Anträge elektronisch zu stellen, wurde auch hier der LfDI bereits bei der Erstellung des Pflichtenhefts aktiv mit einbezogen. Dessen Anmerkungen und Empfehlungen sind ein wichtiger Bestandteil für die Entwicklung einer praktikablen Lösung. Die Landesregierung hofft auch weiterhin auf eine gute Zusammenarbeit mit dem LfDI bei der Entwicklung und des Abschlusses des Gesamtprojektes BEATA.

5.7.4 Umgang mit amtsärztlichen Gutachten

Den Ausführungen des LfDI in diesem Abschnitt wird zugestimmt.

5.10 Bildung

Die Empfehlung des LfDI an die „Verantwortlichen“, auf den Einsatz bestimmter internetbasierter Lernsoftware zu verzichten, ist nicht in Gänze zielführend.

Der Einsatz von Informations- und Kommunikationstechnologien in den Schulen des Landes hat aus datenschutzrechtlicher Sicht mindestens drei grundlegende Aspekte, die getrennt betrachtet werden müssen.

1. Datenschutz und Datensicherheit in der Schulverwaltung bei der Erfassung und Verarbeitung personenbezogener Daten,
2. Datenschutz bei der Nutzung digitaler Medien im Unterricht und
3. Datenschutz als Bildungsaufgabe.

Beim Blick auf die Lernsoftware ist vor allem der zweite Aspekt relevant sowie die „Kooperationsvereinbarung zur Förderung von Medienkompetenz in Mecklenburg-Vorpommern“ entsprechend derer die „Medienbildung eine Zukunftsaufgabe unseres Landes, Medienkompetenz eine notwendige Schlüsselkompetenz für alle Menschen in unserer Gesellschaft“ ist sowie schließlich die Forderungen des Bundestages (zuletzt Drucksache 18/6203 vom 30. September 2015) nach fächerintegrativer und standardbasierter Medienbildung mit dem Ziel, allen Kindern und Jugendlichen digitale Teilhabe und Chancengleichheit zu ermöglichen.

Gemäß § 4 DSG M-V müssen Schulen bei der Nutzung von Lernsoftwareprodukten insbesondere derer mit Cloud-Lösungen einen Vertrag zur Auftragsdatenverarbeitung mit der datenverarbeitenden Stelle oder Person abschließen. Hilfreich ist hier das Unterstützungsangebot des LfDI, unabhängige Prüfer überprüfen derartige Produkte auf ihre Datenschutzkonformität hin und bescheinigen das Ergebnis mit einem Datenschutz-Gütesiegel.

Die Empfehlung des LfDI „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“, kann nicht die Lösung vor dem Hintergrund sein, dass sich das digitalisierte und internetbasierte Lernen und Lehren rasch ausweiten wird.

Es ist aus Sicht der Landesregierung zur Erlangung von Rechtssicherheit und zur Entlastung der Schulleiter notwendig, hier generalisierter vorzugehen.

In enger Zusammenarbeit aller diesbezüglich relevanten und beteiligten Institutionen des Landes, insbesondere unter Beteiligung des BM, sollten zeitnah Listen bereits datenschutzrechtlich geprüfter Produkte zusammengestellt und zentral veröffentlicht werden. Zudem sollten von einem zu bildenden Gremium standardisierte Musterverträge mit Anbietern sowie Verfahrensverzeichnisse gemäß § 18, Sicherheitskonzepte gemäß § 22 Absatz 5 und Vorgaben zur förmlichen Freigabe gemäß § 19 DSG M-V für die Schulen erarbeitet und anschließend zum Download bereitgestellt werden. Dieses Vorhaben und seine Konzipierung könnten im Rahmen der Arbeitsgruppe „Digitale Schule“ und hier im Besonderen in der Unter-Arbeitsgruppe „Datenschutz und Organisation“ angesiedelt sein.

8 Informationsfreiheitsgesetz Mecklenburg-Vorpommern - IFG M-V

8.2 Vergütungstransparenzgesetz Mecklenburg-Vorpommern

Im Ergebnis der Ressort- und Verbandsanhörung des Referentenentwurfs für ein Vergütungstransparenzgesetz des Landes ist die - unter anderem vom LfDI geäußerte - Empfehlung zur individualisierten Veröffentlichung der Bezüge jedes einzelnen Mitglieds der Geschäftsleitung aufgegriffen und der Gesetzentwurf der Landesregierung mit entsprechenden Offenlegungsvorgaben ausgestaltet worden.

Die vom LfDI für erstrebenswert gehaltene direkte Verpflichtung aller öffentlichen Unternehmen zur Offenlegung hingegen ist, wie in der Gesetzesbegründung detailliert ausgeführt, aufgrund der bestehenden bundesrechtlichen Regelungen im Handelsgesetzbuch aus Rechtsgründen ausgeschlossen. Ausweislich seiner Stellungnahme im parlamentarischen Verfahren zum Vergütungstransparenzgesetz M-V geht auch der LfDI davon aus, dass das Transparenzziel mit dem Gesetzentwurf in ausreichendem Maße realisiert worden ist und es dem Land verwehrt sein dürfte, für alle öffentlich-rechtlichen Unternehmen eine direkte Veröffentlichungspflicht zu normieren.

8.4 Informationen über Ausgaben der Verfassungsschutzbehörde

Hiesige Dokumente, die sich auf den finanziellen und personellen Aufwand des Verfassungsschutzes in Mecklenburg-Vorpommern beziehen, sind zu Recht in die Geheimhaltungsstufe VS-vertraulich eingestuft, da aus ihnen die Arbeitsweise des Verfassungsschutzes entnommen und damit der Aufgabenvollzug gefährdet werden kann. Soweit auf der Internetpräsenz des Verfassungsschutzes Zahlen veröffentlicht wurden, die wegen ihres Abstraktionsgrades dem Schutzzweck der Geheimhaltungsstufe und dem § 5 Nummer 1 IFG M-V nicht entgegenstehen, widerspricht dies nicht der grundsätzlichen Verweigerung der gewünschten vollständigen Auflistung der genannten Dokumente. Dementsprechend konnte auch für allgemeine Informationen auf die Internetpräsenz (www.verfassungschutz-mv.de) hingewiesen werden.

8.5 Zu hohe Gebühren für Verbraucherinformationen

Die Landesregierung teilt die Auffassung des LfDI, dass bei Verbraucherinformationen die Bestimmungen der Verbraucherinformationsgesetzes (VIG) und der dazugehörigen Kostenverordnung hätten geprüft werden müssen.

8.6 Auskunft über vertrauliches Gutachten einer Wirtschaftsprüfungsgesellschaft

Der Sachverhalt wird vom LfDI im Wesentlichen zutreffend wiedergegeben. Nach wie vor bestehen jedoch unterschiedliche Rechtsauffassungen zu der Frage der Rechtmäßigkeit der Einstufung des Gutachtens als „VS-Nur für den Dienstgebrauch“.

Der LfDI führt dazu selbst aus, dass eine VS-Einstufung grundsätzlich nur bei Informationen in Betracht kommt, die die äußere Sicherheit, auswärtige Beziehungen oder die innere Sicherheit betreffen. Dies schließt weitere Fallkonstellationen wie die Vorliegende nicht aus.

Die Entscheidung über die Rechtmäßigkeit der VS-Einstufung und damit zusammenhängend auch die Ablehnung des Informationszugangs zu dem begehrten Gutachten wird auf dem Verwaltungsgerichtsweg geklärt.

8.7 Herausgabeanspruch von Haushaltsdaten gegenüber Kammern

Die Landesregierung wird darauf hinwirken, dass entsprechend § 14 Satz 2 IFG M-V i. V. m. § 32 Absatz 1 und 3 DSG M-V in geeigneter Weise Stellung zu den im Tätigkeitsbericht angesprochenen Beanstandungen des LfDI Stellung genommen wird.