LANDTAG MECKLENBURG-VORPOMMERN **Drucksache 6/3173**
6. Wahlperiode **22.07.2014**

UNTERRICHTUNG

durch die Landesregierung

Stellungnahme der Landesregierung zum Elften Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern gemäß § 33 Absatz 1 des Landesdatenschutzgesetzes (DSG M-V) und zum Vierten Tätigkeitsbericht des Landesbeauftragten für die Informationsfreiheit Mecklenburg-Vorpommern gemäß § 14 Satz 2 des Informationsfreiheitsgesetzes (IFG M-V) in Verbindung mit § 33 Absatz 1 DSG M-V

Berichtszeitraum: 1. Januar 2012 bis 31. Dezember 2013

Zugeleitet mit Schreiben des Chefs der Staatskanzlei vom 17. Juli 2014 gemäß § 29 Absatz 1 Satz 2 des Datenschutzgesetzes des Landes Mecklenburg-Vorpommern; federführend ist das Ministerium für Inneres und Sport.

Einleitung

Für den Berichtszeitraum vom 1. Januar 2012 bis zum 31. Dezember 2013 hat der Landesbeauftragte für den Datenschutz (LfD) mit Drucksache 6/2810 seinen Elften Tätigkeitsbericht gemäß § 33 Absatz 1 Satz 1 des Landesdatenschutzgesetzes (DSG M-V) und zugleich - als Landesbeauftragter für die Informationsfreiheit (LfI) - seinen Vierten Tätigkeitsbericht gemäß § 14 Satz 2 des Informationsfreiheitsgesetzes (IFG M-V) in Verbindung mit § 33 Absatz 1 Satz 1 DSG M-V vorgelegt. Gemäß § 33 Absatz 1 Satz 2 DSG M-V nimmt die Landesregierung hierzu Stellung.

Wie auch bei früheren Tätigkeitsberichten verknüpft der LfD seinen Tätigkeitsbericht gemäß § 33 Absatz 1 Satz 1 DSG M-V mit seinem Tätigkeitsbericht gemäß § 38 Absatz 1 des Bundesdatenschutzgesetzes (BDSG). Die Beiträge aufgrund des DSG M-V und die aufgrund des BDSG sind nicht separat aufgeführt; der LfD ist der Auffassung, dass es bei zahlreichen Sachverhalten Überschneidungen zwischen dem öffentlichen und nicht-öffentlichen Bereich gebe, so dass die Themen im Zusammenhang betrachtet werden müssten.

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

Der Vierte Tätigkeitsbericht zum IFG M-V entspricht Abschnitt 9 des Gesamtberichts.

Die Landesregierung sieht nicht bei jedem Thema des Tätigkeitsberichts die Notwendigkeit, Stellung zu nehmen. Sie beschränkt sich darauf, bei Bedarf Erläuterungen zum Fortgang behandelter Angelegenheiten oder, sofern erforderlich, die abweichende Auffassung darzulegen. Wenn 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 einzelne Themen in einer Einleitung an und fasst die Empfehlungen zusammen. Soweit die Landesregierung Stellungnahmen für erforderlich hält, ergehen diese unter den jeweiligen konkreten Themenziffern.

B Im Einzelnen

Zu Ziffer 1.2 Nr. 1 Umsetzung der Empfehlung des Zehnten Tätigkeitsberichtes zu Gliederungspunkt 2.1

Die bisher nebeneinander bestehenden Netzwerke „Medienaktiv M-V“ und das „Medienkompetenz-Netzwerk M-V“ sind endgültig unter dem Namen „Medienaktiv M-V“ zusammengeführt worden. Es wird angestrebt, den Landesbeauftragten für Datenschutz und Informationsfreiheit M-V als Mitunterzeichner der Aktualisierung der Rahmenvereinbarung Anfang 2015 zu gewinnen, um die bestehende Kooperation noch weiter zu vertiefen.

Zu Ziffer 1.2 Nr. 2 Umsetzung der Empfehlung des Zehnten Tätigkeitsberichtes zu Gliederungspunkt 2.2.1

Die Landesregierung hat den Beschluss des IT-Planungsrates, die beabsichtigte Einbindung von Social-Plugins auf den eigenen Homepages vorher durch die behördlichen Datenschutzbeauftragten prüfen zu lassen, an die Landesbehörden Mecklenburg-Vorpommern weitergegeben.

Der Landesregierung ist bewusst, dass Soziale Medien und Netzwerke im Internet immer mehr in den Mittelpunkt der elektronischen Kommunikation rücken. Damit eröffnen sich den Verwaltungsbehörden einerseits neue Einsatzmöglichkeiten, andererseits aber auch neue Risikobereiche. Deshalb wurde ein Leitfaden entwickelt, der Hinweise für Behördenauftritte sowie Regeln zum verantwortungsbewussten Umgang mit Sozialen Medien enthält. Der im Dezember 2013 beschlossene „Leitfaden für die Nutzung von Sozialen Medien in der Landesverwaltung Mecklenburg-Vorpommern“ wurde allen Landesbehörden zugeleitet und im Intranet „LOTSE“ veröffentlicht. Die Hinweise in der Orientierungshilfe „Soziale Netzwerke“ der Datenschutzbeauftragten des Bundes und der Länder sowie die Stellungnahme des LfD wurden bei der Erstellung des Leitfadens berücksichtigt.

Hinsichtlich der Einbindung von Social-Plugins regelt der Leitfaden, dass vor der direkten Einbindung von sozialen Erweiterungsmodulen auf der eigenen Homepage und bei der Nutzung von Fan-Seiten eine sorgfältige Prüfung unter Einbeziehung der behördlichen Datenschutzbeauftragten zu erfolgen hat. Wenn Behördenseiten Verweise (Links) zu Sozialen Medien enthalten sollen, so seien die Nutzer vor einer Übertragung von Daten ausreichend zu informieren. Hierfür sei eine konkrete Information über Art und Umfang der Datenverarbeitung erforderlich. Diese solle durch das Einbinden der „Doppelklicklösung“ erfolgen, bei der die Nutzer im ersten Klick auf die damit verbundene Datenübertragung von IP-Adresse, Identifikationsnummer und Inhaltsdaten hingewiesen werden.

Zu Ziffer 1.2 Nr. 4 Umsetzung der Empfehlung des Zehnten Tätigkeitsberichtes zu Gliederungspunkt 3.1.1

Die Landesregierung ist sowohl über die benannten Bundesratsvertreterinnen und -vertreter in den entsprechenden EU-Gremien (insbesondere der Ratsarbeitsgruppe DAPIX und den agierenden politischen Entscheidungsgremien) als auch über die entsprechenden Stellungnahmen und Beschlüsse der IMK (zuletzt der Umlaufbeschluss der IMK zum Post-Stockholm-Prozess vom 02.05.2014) und des Bundesrates am Diskussionsprozess zum EU-Datenschutzpaket beteiligt.

Zu Ziffer 1.2 Nr. 5 Umsetzung der Empfehlung des Zehnten Tätigkeitsberichtes zu Gliederungspunkt 3.2.6

Der Landesregierung sind die mit dem Einsatz von De-Mails verbundenen Schwächen bekannt. Gleichwohl haben die Bundes- und die Landesregierung De-Mail als zusätzlichen elektronischen Zugang zur Verwaltung im Verwaltungsverfahrensrecht zugelassen. Das Ministerium für Inneres und Sport führt derzeit konzeptionelle Vorarbeiten für den Einsatz von De-Mail in der Landesverwaltung aus, die auch mit dem LfD beraten werden sollen.

Damit beim Versand besonders schutzwürdiger Daten die erforderlichen Sicherheitsmaßnahmen sichergestellt werden können, stellt das Ministerium für Inneres und Sport den Landesbehörden das Elektronische Gerichts- und Verwaltungspostfach (EGVP) bereit, das eine Ende-zu-Ende-Verschlüsselung garantiert und die Möglichkeit der Einbindung der qualifizierten elektronischen Signatur bietet. Kommunalbehörden können das Verfahren ebenfalls nutzen. Weiterhin ist eine kostenlose Office Integration des EGVP-Systems möglich.

Des Weiteren hat das Ministerium für Inneres und Sport die DVZ M-V GmbH beauftragt, auf Anforderung der Behörden Signaturdienste für die qualifizierte elektronische Signatur zur Verfügung zu stellen. Die Entscheidung über die Implementierung obliegt den Behörden, da eine Integration in das jeweilige Fachverfahren notwendig ist. Ein Bezug der Signaturen ist sowohl für die Landes- als auch für die Kommunalverwaltung möglich.

Damit stehen, abhängig vom Schutzbedarf der Daten, abgestufte Verfahren zur sicheren Kommunikation zur bedarfsweisen Nutzung zur Verfügung. Ein pauschales Vorhalten aller technisch möglichen Verfahren auf allen Arbeitsplätzen ist wirtschaftlich nicht vertretbar.

Zu Ziffer 1.2 Nr. 7 Umsetzung der Empfehlung des Zehnten Tätigkeitsberichtes zu Gliederungspunkt 3.3.1

Das Novellierungsvorhaben befindet sich derzeit in der Ressortabstimmung.

Zu Ziffer 1.2 Nr. 8 Umsetzung der Empfehlung des Zehnten Tätigkeitsberichtes zu Gliederungspunkt 4.1.1

Da es hinsichtlich der rechtlichen Ausgestaltung von Cloud-Diensten an vielen Stellen noch Fragen gibt, wurde das Thema von der Landesregierung noch nicht forciert und vorschnell gefördert. Gleichwohl wird mit der DVZ M-V GmbH und den kommunalen Landesverbänden an Konzepten für gemeinsame E-Government-Dienste gearbeitet. Zugleich hat die DVZ M-V GmbH in Zusammenarbeit mit den IT-Dienstleistern der anderen Bundesländer eine Richtlinie „Öffentliche Aufträge in der Cloud“ erarbeitet. Diese soll einen datenschutzgerechten Umgang mit dem Thema sicherstellen und die Nutzung befördern. Die Richtlinie wurde mit dem BSI abgestimmt und dem AK Technik der Landesbeauftragten für Datenschutz vorgestellt.

Zu Ziffer 1.2 Nr. 12 Umsetzung der Empfehlung des Zehnten Tätigkeitsberichtes zu Gliederungspunkt 4.3.6

Der Abschluss des Projektes IT-Grundsystem steht unmittelbar bevor. Der Abschlussbericht befindet sich in der Abstimmung und wird in Kürze dem Kabinett vorgelegt. Das konkrete weitere Vorgehen wird festgelegt, sobald ein entsprechender Beschluss vorliegt.

Zu Ziffer 1.2 Nr. 13 Umsetzung der Empfehlung des Zehnten Tätigkeitsberichtes zu Gliederungspunkt 4.3.4

Zu dem bereits in der Stellungnahme zum 10. Tätigkeitsbericht des LfD ausgeführten Sachstand ist keine Änderung eingetreten. Im Personenstandswesen ist durch den Zweckverband Elektronische Verwaltung in Mecklenburg-Vorpommern (eGo-MV) ein funktionierendes und den Anforderungen des Datenschutzes entsprechendes Signierungsverfahren eingeführt worden. Da die Kommunen (Standesämter) - zum Teil als Mitglieder, zum Teil als Vertragspartner des eGo-MV - abweichende Lösungen nicht eingeführt haben, erscheint eine Fortschreibung der bestehenden Rechtsvorschriften zur Sicherstellung einer einheitlichen Handhabung im Zusammenhang mit Signaturen im Bereich des Personenstandswesen als entbehrlich.

Zu Ziffer 1.2 Nr. 15 Umsetzung der Empfehlung des Zehnten Tätigkeitsberichtes zu Gliederungspunkt 5.4.7

Die Landesregierung verfolgte in Zusammenarbeit mit den kommunalen Landesverbänden und insbesondere mit dem Zweckverband Elektronische Verwaltung in M-V vielmehr einen anderen, weitergehenden Ansatz. Es war ein gemeinsamer eID-Service mit einem Berechtigungszertifikat für alle Kommunen und für mehrere Anwendungen geplant. Dieser konnte letztlich in Abstimmung mit dem Bundesverwaltungsamt und dem LfD umgesetzt werden. Dadurch entstand ein gemeinsamer Dienst, der bei positiver Prüfung des auszulesenden Datenumfangs die Kommunen sowohl hinsichtlich der Zertifikatskosten als auch der Betriebskosten finanziell entlastet.

Zu Ziffer 1.2 Nr. 16 Umsetzung der Empfehlung des Zehnten Tätigkeitsberichtes zu Gliederungspunkt 5.7.3

Die Länder werden weiterhin bestehende Bedenken im Rahmen der Überprüfung des Rundfunkbeitragsstaatsvertrags im Ergebnis der Evaluation mit einbeziehen.

Zu Ziffer 2.2 Projekt „Medienscouts MV“

Die Landesregierung und der LfD arbeiten bei der Umsetzung der Rahmenvereinbarung zur „Förderung von Medienkompetenz“ partnerschaftlich zusammen. Mitarbeiterinnen und Mitarbeiter des LfD und des Instituts für Qualitätsentwicklung Mecklenburg-Vorpommern treten auf Fortbildungsveranstaltungen (Multiplikatorenschulung, Medientango) auf und informieren sich gegenseitig über Aktivitäten in den eigenen Ressorts. Die Landesregierung steht konstruktiven Gesprächen und gemeinsamen Aktivitäten auch künftig offen gegenüber. Sie begrüßt die Initiative des LfD im Rahmen des Projektes „Medienscouts M-V“, Schülerinnen und Schüler zu Expertinnen und Experten in der verantwortungsbewussten Nutzung von Internet und Sozialen Netzwerken auszubilden und dieses Expertenwissen an Gleichaltrige weiterzugeben.

Zu Ziffer 2.9 Projekt „PeerCon“

Im Ergebnis bilateraler Gespräche zwischen dem LfD und der Landesregierung wurde von einer weiteren Verfolgung der Projektidee „PeerCon“ Abstand genommen. Zu begrüßen ist der Ansatz, Schülerinnen und Schüler sowie Lehrkräfte für den selbstbestimmten Umgang mit ihren Daten im Internet zu sensibilisieren und ihnen gleichzeitig inhaltlich und technisch Alternativen anzubieten und diese auszuprobieren. In bewährter Weise soll dieses in Kooperation mit allen relevanten Partnern geschehen. Hier steht die Landesregierung allen Gesprächen offen gegenüber.

Zu Ziffer 2.10 Ausblick

Die Erklärung der Kultusministerkonferenz zur „Medienbildung in der Schule“ vom 08.03.2012 stellt eine zentrale Handlungsgrundlage zur Entwicklung von Medienkompetenz aller am Bildungsprozess Beteiligter dar. Die Landesregierung sieht den Datenschutz und die damit verbundene Sensibilisierung der Schülerinnen und Schüler zum bewussten Umgang mit personenbezogenen Daten als eine wichtige Aufgabe im Rahmen des Bildungsauftrags von Schulen an. Die Zusammenarbeit mit dem LfD in der Fortbildung von Multiplikatorinnen und Multiplikatoren wird fortgesetzt. Eine regelmäßige Abstimmung zu den Bildungsaktivitäten im Bereich „Schule“ erfolgt über die interministerielle Arbeitsgruppe „Förderung von Medienkompetenz“, die die Umsetzung der gleichnamigen Rahmenvereinbarung zwischen Staatskanzlei, Ministerium für Arbeit, Gleichstellung und Soziales, dem Ministerium für Bildung, Wissenschaft und Kultur und der Medienanstalt des Landes begleitet. Die im Bericht geforderte curriculare Verankerung des Themas „Datenschutz“ ist in den Rahmenplänen Informatik bereits erfolgt. Das Thema ist auch prüfungsrelevant. Der Empfehlung, neben dem Datenschutz auch das Urheberrecht und die Medienbildung verstärkt durch Angebote für Kinder und Jugendliche zu untersetzen, wird bereits durch den Schulversuch „Auf dem Weg zur Medienschule“ Rechnung getragen.

Zu Ziffer 3.1 Die EU-Datenschutz-Grundverordnung

Auch die Landesregierung hat großes Interesse an einem starken europäischen Datenschutz. Sie unterstützt allerdings auch die Position der Innenministerkonferenz (IMK), die auf ihrer Sitzung am 23./24. Mai 2013 zentrale Nachbesserungserfordernisse aufgezeigt hat. Die IMK hat sich zuletzt anlässlich der Diskussion um den Post-Stockholm-Prozess umfassend geäußert - auch zu den Problemen, die im Kontext des Datenschutzpakets gesehen werden, wie beispielsweise die Gewährleistung ausreichender Spielräume für nationale Datenschutzregelungen im öffentlichen Bereich, Safe Harbor, das Datenschutz-Rahmenabkommen im Bereich der Strafverfolgung, Datenschutz im Telekommunikationsbereich, Cloud-Computing, die Sicherheit europäischer Kommunikationsnetze oder die Sicherheit vor Cyberangriffen (IMK-Umlaufbeschluss vom 2. Mai 2014). Die Landesregierung ist der Auffassung, dass angesichts des Verordnungs-Charakters und der unmittelbaren Geltung Entscheidungen wohlüberlegt sein müssen.
Außerdem wird auf den Beschluss des Bundesrates (BR-Drs. 123/14) verwiesen.

Zu Ziffer 3.2 Förderung der elektronischen Verwaltung

Die Auffassung des LfD als angehörter Sachverständiger vor dem Deutschen Bundestag ist der Landesregierung bekannt. Sie hat jedoch auch zur Kenntnis genommen, dass diese vom Bundesgesetzgeber nicht aufgegriffen worden ist.

Bund und Länder haben sich bezüglich der Formulierungen in den Verwaltungsverfahrensgesetzen seit langer Zeit auf eine Simultangesetzgebung verständigt. Ziel dieser Simultangesetzgebung ist es, den Bürgerinnen und Bürgern in Deutschland bezüglich des grundlegenden Charakters dieses Gesetzes einheitliche Formulierungen an die Hand zu geben. Zudem ist die letztinstanzliche Zuständigkeit des Bundesverwaltungsgerichts zu ermöglichen (siehe §§ 49, 137 Absatz 1 Nummer 2 Verwaltungsgerichtsordnung). Die Landesregierung unterstützt diesen Ansatz ausdrücklich und hat deshalb davon Abstand genommen, abweichende Formulierungen im § 3a Landesverwaltungsverfahrensgesetz (VwVfG M-V) aufzunehmen. Der Landesgesetzgeber ist dem mit seiner Entscheidung vom 19. Mai 2014 zum vorgelegten Gesetzentwurf gefolgt.

Zu a)

Für den Nachweis der Identität des Absenders (Authentisierung) und der Integrität der übermittelten Nachricht bei De-Mail werden zwei unabhängige Verfahren eingesetzt. Die Sicherung der Übermittlung vom Absender zum Diensteanbieter erfolgt über einen verschlüsselten gegenseitig authentisierten Kanal. Die Nachrichteninhalte (Nachrichtentext und gegebenenfalls vorhandene Anhänge) werden zusätzlich bei der Übertragung separat verschlüsselt. Auf diese Weise kann die Nachricht auf dem Transportweg weder ausgespäht noch spurlos verändert werden. Diese Konzeption sieht eine einfache Handhabbarkeit für den Nutzer vor, da die Verschlüsselung durch die eingesetzten Übertragungsprotokolle transparent für den Nutzer durch die akkreditierten Diensteanbieter erfolgt. Der Nutzer muss hierfür selbst nicht aktiv werden. Der akkreditierte Diensteanbieter hat die Eingangsbestätigung zur Sicherung ihrer Authentizität und Integrität mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz zu versehen. Auf diese Weise kann mithilfe der Eingangsbestätigung der Zugang der in den versendeten Nachrichten enthaltenen Willenserklärungen langfristig nachgewiesen werden.

Zu b)

Auf die Stellungnahme zu Ziffer 3.2 am Anfang zur Simultangesetzgebung und auf den Gesetzesbeschluss zum Zweiten Gesetz zur Änderung des Landesverwaltungsverfahrensgesetzes wird verwiesen.

Der Bundesrat hat empfohlen, die Verwaltungstätigkeit nach der Abgabenordnung aus dem Regelungsbereich des Gesetzes zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften auszunehmen (siehe Beschlussempfehlung des Bundesrats auf Drucksache 557/12). Der Bundesgesetzgeber ist dieser Empfehlung nicht gefolgt.

Zum Thema De-Mail wird auch auf die Stellungnahme zu Ziffer 1.2 Nr. 5 verwiesen.

Zu Ziffer 4.2 Soziale Netze in der Verwaltung

Auf die Stellungnahme zu Ziffer 1.2 Nr. 2 wird verwiesen.

Zu Ziffer 4.3 Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung

Die Landesregierung weist daraufhin, dass die vom LfD ausgesprochene Empfehlung zur Anwendung der Leitlinie für die Kommunen bereits Gegenstand des Beschlusses des IT-Planungsrat war und die Kommunen im Land auch in verschiedenen Veranstaltungen zur Anwendung angehalten wurden. Zudem betont die Landesregierung, dass die Leitlinie in wesentlichen Elementen der Zusammenarbeit mit den Kommunen bereits verbindliche Vorgaben enthält. Dies betrifft sowohl die Regelungen zur Absicherung der Netzinfrastrukturen der öffentlichen Verwaltung als auch die Festlegung von einheitlichen Sicherheitsstandards für ebenen-übergreifende IT-Verfahren. Darüber hinaus werden die Kommunen in den gemäß Leitlinie geforderten Aufbau des Informationssicherheitsmanagements und des Landes-Computer-Emergency-Response-Teams (CERT) mit eingebunden sein.

Zu dem Hinweis der Anwendung der Methodik des Bundesamtes für Sicherheit in der Informationstechnik (BSI) merkt die Landesregierung an, dass sich dies bereits aus der Gesetzesbegründung zu § 22 DSG M-V ergibt.

Die Landesregierung weist ferner darauf hin, dass ungeachtet der Anwendungstiefe der Leitlinie das DSG M-V grundlegende Festlegungen trifft, wie die Schutzbedarfsermittlung von IT-Verfahren und die Erstellung von IT-Sicherheitskonzepten zu erfolgen hat, so dass diesbezüglich kein ungeregelter Rechtsrahmen besteht.

Die Landesregierung schließt sich der Empfehlung des Landesbeauftragten für den Datenschutz an und empfiehlt den Kommunen die Vorgaben der „Leitlinie für die Informationssicherheit in der öffentliche Verwaltung“ in eigener Zuständigkeit umzusetzen.

Zu Ziffer 4.4 Steuerungsprojekt eID-Strategie

Mit der eID-Funktion (Elektronischer Identitätsnachweis) des neuen Personalausweises und des elektronischen Aufenthaltstitels (im Folgenden eID-Funktion des nPA genannt), De-Mail, der qualifizierten elektronischen Signatur und anderen Standards und Technologien gibt es in Deutschland eine gute und solide Basis von Verfahren zu Gewährleistung von Identität, Authentizität, Integrität, Vertraulichkeit und Nachweisbarkeit (im Folgenden Vertrauensdienste). Damit ist die Grundlage vorhanden, um Verwaltungsvorgänge weitgehend medienbruchfrei abzuwickeln. Mit dem E-Government-Gesetz und dem Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten hat der Gesetzgeber den Einsatz der eID-Funktion des nPA in Verbindung mit elektronischen Formularen und von De-Mail zur Ersetzung der Schriftform für verschiedene Bereiche des E-Government sowie von eJustice ermöglicht und eine Öffnungsklausel für Technologien mit gleichwertiger Sicherheit vorgesehen.

Allerdings werden die vorhandenen Vertrauensdienste aus unterschiedlichen Gründen heute von Verwaltungen häufig noch nicht angeboten oder von Unternehmen, Bürgerinnen und Bürgern zu wenig genutzt, da noch zahlreiche Klärungsbedarfe hinsichtlich des Einsatzrahmens bestehen. Daher soll mit dem Steuerungsprojekt „eID-Strategie“ des IT-Planungsrates die Akzeptanz gesteigert werden. Dabei spielt die einfache Handhabbarkeit der Vertrauensdienste eine zentrale Rolle. Die Nutzer sollen mit möglichst wenigen dieser Verfahren möglichst viele für sie relevante Verwaltungsprozesse abwickeln können. Dies kann zum einen durch Reduzierung der Vielfalt der bestehenden Vertrauensdienste (zum Beispiel unterschiedlicher Identifikationsverfahren) und zum anderen - dort wo es technisch möglich ist - durch gegenseitige Anerkennung und Interoperabilität von Vertrauensdiensten im föderalen System unterstützt werden. Darüber hinaus muss auf Grundlage der gesetzlichen Rahmenbedingen Klarheit darüber bestehen, welche dieser Verfahren für welche Verwaltungsprozesse eingesetzt werden können.

Neben der Akzeptanz spielen auch Datenschutz, Sicherheit und Wirtschaftlichkeit der Verfahren eine wesentliche Rolle. Elektronische Verwaltungsprozesse sollen jeweils auf einem Datenschutz- und Sicherheitsniveau abgewickelt werden, das sich aus ihrem Schutzbedarf ergibt. Es wird angestrebt, den Einsatz der Verfahren für alle Kommunikationspartner wirtschaftlich zu gestalten.

Bis zum Jahresende 2014 wird das Steuerungsprojekt „eID-Strategie“ dem IT-Planungsrat weitere Umsetzungsempfehlungen vorlegen.

Zu Ziffer 4.5 Datensicherheit im Verbindungsnetz

Auch im Verbindungsnetz ist die Datensicherheit vornehmlich verfahrensbezogen zu sehen. Insbesondere bei den E-Government-Verfahren werden Verschlüsselungsverfahren, vorwiegend mittels des OSCI-Transportprotokolls und dem „Elektronischen Gerichts- und Verwaltungsportfach“ (EGVP), eingesetzt. Bei diesem Verschlüsselungsverfahren werden Ende-zu-Ende-Verschlüsselungen verwendet. 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.

Zu Ziffer 5.1.4 Cloud-Computing

Die Landesregierung ist sich der Datenschutzanforderungen an Cloud-Computing bewusst. So hat die DVZ M-V GmbH in Zusammenarbeit mit den IT-Dienstleistern der anderen Bundesländer eine Richtlinie „Öffentliche Aufträge in der Cloud“ erarbeitet. Diese soll einen datenschutzgerechten Umgang mit dem Thema sicherstellen und die Nutzung befördern. Die Richtlinie wurde mit dem BSI abgestimmt und dem Arbeitskreis Technik der Landesbeauftragten für Datenschutz vorgestellt. Die Landesregierung wird die Richtlinie in den IT-Planungsrat einbringen.

Zu Ziffer 5.1.6 Elektronische Zeiterfassung in der Landesregierung (ZEUS)

Der LfD vertritt die Ansicht, die im Ministerium für Inneres und Sport praktizierte Vorlage von Saldenauszügen sei - da vom Sinn des Datenschutzes nicht abgedeckt - unzulässig.

Dieser Ansicht schließt sich die Landesregierung nicht an.

Sie ist nicht der Auffassung, dass es für den Dienstherrn zur Wahrnehmung der Personalverantwortung ohne Einschränkung ausreicht, allein aus gegebenen Anlass im Einzelfall Kenntnis von den gespeicherten relevanten Arbeitszeitdaten zu nehmen. Vielmehr sieht sie eine regelmäßige Einsichtnahme in diese Daten zur Erfüllung der Pflichten des Dienstherrn als unverzichtbar an. Eine andere Sichtweise würde die besonderen, von der freien Wirtschaft zu differenzierenden Fürsorge- und Steuerungspflichten des Dienstherrn nicht hinreichend berücksichtigen, die durch die modernen Instrumente des Personalmanagements und gesteigerte Maßnahmen zur Gesundheitsförderung eher noch größere Bedeutung erlangt haben dürften. Insoweit ist die regelmäßige Kenntnis einer Übersicht des Arbeitszeitverhaltens unerlässlich im Sinne der datenschutzrechtlichen Erforderlichkeit. Denn um Instrumente der Personalentwicklung wie Fortbildungen zur Selbstorganisation, Coaching oder Arbeitsplatzerweiterung einsetzen zu können, ist es von entscheidender Bedeutung zu wissen, wie die Leistungsfähigkeit des Beschäftigten im Ist-Zustand ausgeprägt ist. Dabei können über längere Zeit andauernde Arbeitszeitspitzen oder periodisch auftretende Spätarbeitszeiten z. B. auf Selbstorganisationsdefizite oder Überlastung hindeuten, denen mit geeigneten Instrumenten des Personal- beziehungsweise Organisationsmanagements begegnet werden muss, um Motivationslosigkeit und möglicherweise Erkrankungen vorzubeugen. Des Weiteren erfordert die im Rahmen einer modernen Personalentwicklung wichtiger werdende Potentialanalyse, wie sie bereits in den neuen Beurteilungsrichtlinien zum Tragen kommt, auch eine detaillierte Kenntnis des oder der Vorgesetzten über das jeweilige Arbeitszeitverhalten. All dies erfährt vor dem Hintergrund der steigenden Arbeitsverdichtung und des Anwachsens informationstechnisch gesteuerter Arbeitsprozesse bei gleichzeitigem Ansteigen des Lebensalters der Beschäftigten eine zunehmende Bedeutung.

Nach alledem dürfte deutlich werden, dass die nach diesseitiger Ansicht gebotene Kenntnisnahme der Monatsjournale mit dazu beitragen soll, die Erfüllung staatlicher Aufgaben auf einem hohen rechtstaatlichen und professionellen Niveau zu halten, das im Übrigen nicht der bloßen Kontrolle, sondern der Fürsorge und darüber hinaus auch der Förderung von individuellen Entwicklungsmöglichkeiten dient. Die Einsichtnahme in die Monatsjournale trägt nicht nur der besonderen Rechts- und Pflichtenstellung der öffentlich Bediensteten Rechnung, sondern bringt für sie persönliche Vorteile, die ansonsten nicht herbeizuführen wären.

Zu Ziffer 5.1.7 Dokumentenmanagement in der Landesverwaltung (BEATA)

Die Landesregierung begrüßt die positiven Anmerkungen zum Projekt BEATA im Tätigkeitsbericht des LfD und dessen Empfehlung, die Datenschutzaspekte bei der Umsetzung von Projekten von Anfang an zu beachten. Die Projektverantwortlichen im Landesbesoldungsamt Mecklenburg-Vorpommern und im Finanzministerium folgten dieser Empfehlung, einerseits um kompetente Beratung zu erhalten und andererseits um nachträgliche umfängliche Änderungen und zusätzliche Kosten zu verhindern.

Aufgrund der regelmäßigen Beratungen und Vorstellungen des Projektfortschrittes beim LfD sind die Anforderungen des Datenschutzes bereits in der Konzeption des Projektes eingeflossen. Dabei gestaltete sich die Zusammenarbeit sehr gut. Die Projektbeteiligten erhielten immer zeitnah die notwendigen und praxisgerechten Antworten, ohne dass der Projektfortschritt behindert wurde.

Bei der anstehenden Erstellung des Mitarbeiterportals, welches über das Internet allen Bediensteten des Landes angeboten werden soll, sind viele Herausforderungen, gerade aufgrund der aktuellen Entwicklungen (Passwortdiebstahl, Datenausspähung usw.) zu bewältigen. Eine praktikable Lösung kann nur in Zusammenarbeit mit dem LfD gefunden werden. Aufgrund der bisherigen guten Erfahrungen hofft die Landesregierung bei der Entwicklung der noch folgenden Projektbestandteile weiterhin auf eine gute Zusammenarbeit mit dem LfD.

Zu Ziffer 5.1.9 Datentrennung trotz Zentralisierung

Gemäß § 22 DSG M-V ist für IT-Verfahren zur Verarbeitung personenbezogener Daten ein IT-Sicherheitskonzept zu erstellen. Entsprechend der damit einhergehenden Schutzbedarfsfeststellung und der Anwendung des BSI-Grundschutzes ist auch die Erforderlichkeit einer Mandantenfähigkeit des IT-Verfahrens zu prüfen. Dies wurde insbesondere für die übergreifenden E-Government-Infrastruktur und die zentralen E-Government-Verfahren des Landes auch entsprechend umgesetzt. Hier war zudem auch der LfD beteiligt.

Explizit zu nennen ist in diesem Zusammenhang das zentral betriebene IT-Verfahren EPOS, bei dem die Software zwar als mandantenfähig galt, aber Sicherheitsmängel in der Praxis nicht ausgeschlossen werden konnten. Aus diesen Gründen hat das Ministerium für Inneres und Sport für jedes Ressort und die Landespolizei separate Applikationsserver eingesetzt, mit der die Daten- und somit eine sichere Mandantentrennung garantiert werden kann.

Zu Ziffer 5.2.5 Durchfahrtskontrolle per Blitzsäule

Die Landesregierung ist in Anlehnung an die Rechtsprechung des Bundesverfassungsgerichts (Urteil vom 11. März 2008, Az: 1 BvR 2074/05, 1 BvR 1254/07) der Auffassung, dass es für den Datenabgleich mit der „whitelist“, der vor Auslösung des Bildes erfolgt, einer zusätzlichen Rechtsgrundlage bedarf.

Der automatisierte Kennzeichenabgleich ist der Bildaufnahme vorgeschaltet. Das automatisierte Durchfahrtkontrollsystem besteht somit aus zwei Schritten:

Dadurch, dass beim automatischen Kennzeichenabgleich die Kennzeichen vorbeifahrender Fahrzeuge (sowohl der Durchfahrtsberechtigten als auch der -nichtberechtigten) mit einer Kamera optisch erfasst, im Kennzeichenlesegerät für den Zeitraum des Abgleichs gespeichert und mit der „weißen Liste“ der durchfahrberechtigten Fahrzeuge abgeglichen werden und es sich bei den Kennzeichen um personenbezogene Daten im Sinne des § 3 Abs. 1 DSG M-V handelt, erfolgt eine Verarbeitung personenbezogener Daten nach § 3 Abs. 4 DSG M-V, welche gemäß § 7 Abs. 1 DSG M-V nur auf Grundlage der Einwilligung der Betroffenen oder einer Rechtsgrundlage zulässig ist.

Nach § 46 Abs. 1 des Gesetzes über Ordnungswidrigkeiten (OWiG) sind für Bußgeldverfahren die Vorschriften der Strafprozessordnung sinngemäß anzuwenden. § 98c der Strafprozessordnung (StPO) regelt den Datenabgleich zur Aufklärung einer Straftat und kann sinngemäß als Rechtsgrundlage für den Datenabgleich zur Feststellung einer Ordnungswidrigkeit angewendet werden. Der Anwendungsbereich der Vorschrift ist bereits bei Vorliegen eines Anfangsverdachts im Sinne des § 152 Absatz 2 StPO, der hier mit dem Passieren des Verbotsschildes entsteht, eröffnet. Auch erscheint es mit Blick auf den Zweck der Vorschrift, den Strafverfolgungsbehörden zu ermöglichen, bei ihnen „bevorratetes Wissen“ zu nutzen, wohl zumindest vertretbar, die „whitelist“ als eine zur Strafverfolgung oder Strafvollstreckung oder zur Gefahrenabwehr gespeicherte Datei anzusehen. Diese wird zwar bereits im Vorfeld erstellt und gespeichert, aber doch von vornherein für einen Einsatz zu repressiven Zwecken (Herausfiltern der Nichtdurchfahrtsberechtigten zur Verfolgung von Verkehrsordnungswidrigkeiten) angelegt.

Die Frage der Verhältnismäßigkeit einer solchen Maßnahme bedarf einer sehr gründlichen Prüfung. Die Rechtslage wurde noch nicht gerichtlich geklärt.

Zu Ziffer 5.2.6 Videoüberwachung an der Wiecker Klappbrücke

Nachdem es an der Wiecker Klappbrücke in den Vorjahren zahlreiche Unfällen gab, hat die Hansestadt Greifswald am 15.01.2014 eine neue stabile und gut funktionierende Polleranlage in Betrieb genommen. Zudem wurde aufgrund der Anordnung des Oberbürgermeisters eine Bildbeobachtungs- und -aufzeichnungsanlage angebracht. Die Aufzeichnungen wurden ab dem 29.02.2014 vorläufig ausgesetzt.

Auch nach Inbetriebnahme der neuen Polleranlage kam es zu Straftaten.

Zu nennen ist die Abgabenhinterziehung (§ 16 Kommunalabgabengesetz M-V). Seit dem 12.01.2014 wurde die Brücke bis zum 30.04.2014 72-mal gequert, ohne dass die erforderliche Benutzungsgebühr gezahlt wurde. Das entspricht im Schnitt einem Fall pro Tag.

Weiter kam es in diesem Zeitraum zu sechs Sachbeschädigungen (§ 303 StGB) des Pollers. Eine Sachbeschädigung kann auch bedingt vorsätzlich begangen werden. Zumindest die Einheimischen kennen die Situation mit dem Poller genau. Um die Benutzungsgebühr von 0,50 € zu sparen, wird riskant dicht an das vorhergehende Fahrzeug herangefahren. Dabei kann bewusst in Kauf genommen werden, dass der Poller hochfährt und möglicherweise auch beschädigt wird.

Drei der Sachbeschädigungen wurden polizeilich aufgenommen. In den übrigen drei Fällen muss von unerlaubten Entfernen vom Unfallort (§ 142 StGB) ausgegangen werden.

Die Aufzeichnung von Bildern ist nach § 32 Abs. 3 Satz 2 des Sicherheits- und Ordnungsgesetzes M-V (SOG) nur zulässig, wenn an öffentlich zugänglichen Orten „wiederholt Straftaten“ begangen worden sind und Tatsachen die Annahme rechtfertigen, dass dort künftig mit der Begehung von Straftaten zu rechnen ist. Das ist nach der Erfassung der Taten durch die Stadt Greifswald der Fall. Die entsprechende Gefahrenprognose ist gerechtfertigt und vom Wortlaut des Gesetzes abgedeckt. Es trifft zwar zu, dass in der Begründung des Gesetzes (Landtagsdrucksache 4/2116, S. 21) der Begriff „wiederholt Straftaten“ mit den Wörtern „sogenannten Kriminalitätsbrennpunkten“ erläutert wird. Die Begründung enthält aber keine Aussagen dazu, welches Gewicht die Straftaten haben sollten. Vielmehr wird an gleicher Stelle der Begründung ausgeführt, dass die Bildaufzeichnung auch dazu dienen kann, Gefahren bei „Verkehrseinrichtungen“ entgegenzutreten.

Es reicht aus, dass die Lageerkenntnis von der zuständigen Ordnungsbehörde erstellt wird. Eine Feststellung durch die Polizei ist nicht vorgegeben und erforderlich.

Die Hansestadt Greifswald prüft, ob mit einer verbesserten Beschilderung die Warnfunktion erhöht werden kann. Gleiches gilt hinsichtlich der Frage, ob die Aufzeichnung auf die Fälle einer rechtswidrigen Benutzung begrenzt werden kann. Zudem wird eine Verpixelung der Bilder erwogen, die nur im Rahmen der Rechtsverfolgung im Rechtsamt der Stadt und nicht vor Ort aufgelöst werden kann. Die Stadt ist damit bemüht, den Eingriff so gering wie möglich zu halten und so dem Grundsatz der Verhältnismäßigkeit Rechnung zu tragen.

Vor diesen Hintergrund besteht keine Veranlassung zu einem Eingreifen der Aufsichtsbehörde.

Zu Ziffer 6.3.1 Umsetzung des Urteils des Bundesverfassungsgerichts zum Antiterrordateigesetz

In seinem Urteil vom 24. April 2013 hat das Bundesverfassungsgericht festgestellt, dass die Antiterrordatei in ihren Grundstrukturen verfassungsgemäß ist, jedoch hinsichtlich ihrer Ausgestaltung in Einzelpunkten nicht den verfassungsrechtlichen Anforderungen genügt. Es bedürfe einer Ausgestaltung der Datei, die den Informationsaustausch im Einzelnen normenklar regle und hinreichend begrenze. Dies gelte ebenso für die Bestimmung der beteiligten Behörden, die in der Datei zu erfassenden Personen und die über sie zu erfassenden Daten wie für die nähere Regelung der Nutzung dieser Daten. Auch müsse eine effektive Kontrolle gewährleistet sein.

Mit ihrem Entwurf eines Gesetzes zur Änderung des Antiterrordateigesetzes und anderer Gesetze (Drucksache 153/14) hat die Bundesregierung auf diese Rechtsprechung reagiert und entsprechende Änderungen des Antiterrordatei- und des Rechtsextremismusdateigesetzes vorgeschlagen. Am 7. beziehungsweise 8. Mai 2014 berieten der Rechts- und der Innenausschuss des Bundesrates über den Gesetzentwurf. Das Gesetzgebungsverfahren ist gegenwärtig noch nicht beendet.

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

Die Verfassungsschutzbehörden und die Polizeien des Bundes und der Länder konnten in der Vergangenheit zur Erfüllung der ihnen obliegenden Aufgaben Bestandsdatenauskünfte von den Diensteanbietern im sogenannten manuellen Auskunftsverfahren auf der Grundlage des § 113 Abs. 1 des Telekommunikationsgesetzes (TKG, in der bis 01.07.2013 geltenden Fassung) und der allgemeinen Datenerhebungsbefugnisse in den Verfassungsschutzgesetzen bzw. Polizeigesetzen des Bundes und der Länder verlangen. Das Bundesverfassungsgericht entschied am 24. Januar 2012 - Az.: 1 BvR 1299/05 - jedoch, dass

- in § 113 TKG zwar die Befugnis und die Verpflichtung für die Diensteanbieter geregelt werden können, bestimmte Telekommunikationsdaten an die berechtigten Stellen im manuellen Verfahren zu übermitteln. Ergänzend bedürfe es aber in den jeweiligen Fachgesetzen des Bundes und der Länder qualifizierter Vorschriften, die den berechtigten Stellen erlauben, diese Daten überhaupt bei den Diensteanbietern abzufordern (sog. „Doppeltürenmodell“).
- § 113 TKG nicht als Rechtsgrundlage - wie bisher in der Praxis erfolgt - für eine Zuordnung von dynamischen IP-Adressen zu ihren Anschlussinhabern herangezogen werden könne, da für diese Auskunft ein Rückgriff auf Verkehrsdaten notwendig sei und § 113 TKG hierzu erkennbar nicht ermächtige. Insoweit sei auch für die Beauskunftung der Zuordnung dynamischer IP-Adressen eine spezifische Regelungslage zu schaffen.
- die in § 113 Absatz 1 Satz 2 TKG vorgesehene Auskunft über Zugangssicherungscodes zukünftig nur noch dann verlangt werden dürfe, wenn auch die rechtlichen Voraussetzungen für die Nutzung dieser Codes erfüllt sind.

Das Gericht ließ die Anwendung des § 113 TKG für Bestandsdatenbeauskunftungen des Bundes und der Länder nur noch für eine Übergangzeit zu. Um weiterhin Datenauskünfte erhalten zu können, mussten der Bundes- und die Landesgesetzgeber spezielle Rechtsgrundlagen in ihrem jeweiligen Fachrecht zur Erhebung dieser Datenauskünfte bis zum 1. Juli 2013 in Kraft setzen. Vor diesem Hintergrund beschloss der Gesetzgeber des Landes Mecklenburg-Vorpommern das Gesetz zur Änderung des Landesverfassungsschutzgesetzes (LVerfSchG M-V) und des SOG M-V zur Regelung der Bestandsdatenauskunft (GVOBl. M-V 2013, S. 434). Das Gesetz dient mithin der Sicherung des bisherigen Status quo bei der Bestandsdatenbeauskunftung; mit ihm wurden keine neuartigen Datenerhebungsbefugnisse geschaffen.

Das Bundesverfassungsgericht hat weder für die Beauskunftung von Zugangssicherungscodes noch für die Beauskunftung von IP-Adressen ausdrücklich einen Richtervorbehalt gefordert. Demzufolge hat auch der LfD im Rahmen der durchgeführten Ressortanhörung zum Gesetzentwurf weder in Bezug auf § 28a SOG M-V die Einfügung von Richtervorbehalten noch in Bezug auf § 24b LVerfSchG M-V die Aufnahme eines Behördenleitervorbehalts und einer Unterrichtung der G10-Kommission angeregt. Diese Forderungen hat er erst im weiteren Gesetzgebungsverfahren im Landtag erhoben und zwar nachdem der Bundesgesetzgeber seinen ursprünglichen Gesetzentwurf (vgl. Bundesratsdrucksache: 664/12) nachträglich - aus politischen und nicht etwa aus verfassungsrechtlichen Gründen - um verfahrenssichernde Regelungen ergänzte (vgl. Drucksache des Deutschen Bundestages 17/12879, S. 12 zur Erzielung eines politischen Kompromisses).

Zu der im Tätigkeitsbericht wiedergegebenen Stellungnahme des LfD im Rahmen der schriftlichen und mündlichen Anhörung ist insbesondere Folgendes anzumerken:

Soweit der LfD ausführt, im novellierten TKG sei festgeschrieben worden, dass die Beauskunftung von Zugangssicherungscodes und auch für die Auskunft über die Zuordnung von IP-Adressen einem Richtervorbehalt unterliegen, sind diese Ausführungen in zweifacher Hinsicht richtigzustellen:

§ 113 TKG wurde durch den Bundesgesetzgeber unter Beachtung der oben angeführten Bundesverfassungsgerichtsentscheidung durch das Gesetz vom 20. Juni 2013 (BGBl. I S. 1602) geändert. Diese Norm richtet sich an die Diensteanbieter und verpflichtet sie, bei einem entsprechenden Ersuchen der berechtigten Stellen Auskünfte über Bestandsdaten zu erteilen („1. Tür“ des sog. Doppeltürenmodells). Durch die Diensteanbieter sind im Rahmen ihrer Beauskunftungstätigkeit nach § 113 TKG keine Richtervorbehalte zu beachten, so dass die Ausführungen des LfD, das TKG schreibe Richtervorbehalte fest, nicht zutreffen. Vielmehr ist es so, dass die ebenfalls mit dem Gesetz vom 20. Juni 2013 geänderten zahlreichen Fachgesetze des Bundes (z.B. u.a. Strafprozessordnung, Bundespolizeigesetz oder Bundesverfassungsschutzgesetz) jeweils um Rechtsgrundlagen zur Erhebung und Beauskunftung von Bestandsdaten ergänzt wurden, damit die berechtigten Stellen zukünftig überhaupt eine Auskunft nach § 113 TKG verlangen können (sog. „2. Tür“ des sog. Doppeltürenmodells). In diesen bundesfachgesetzlichen Normen sind zur Beauskunftung von Zugangssicherungscodes - wie bereits vorstehend ausgeführt - nachträglich im Zuge des Gesetzgebungsverfahrens aus politischen Gründen u.a. noch Richter- oder auch Behördenleitervorbehalte aufgenommen worden. Hinsichtlich der Beauskunftung von Daten zur Zuordnung von IP-Adressen wurden die bundesfachgesetzlichen Normen - entgegen den Ausführungen des LfD - aber nicht um Richter- oder auch Behördenleitervorbehalte ergänzt. Insofern ist zu konstatieren, dass diese Forderung des LfD noch über die Regelungslage in den Bundesgesetzen hinausgeht.

Soweit der LfD mit Blick auf die Erhebung von Zugangssicherungscodes weiter ausführt, dass in § 28a SOG M-V ein Richtervorbehalt und Benachrichtigungsregelungen bzw. in § 24b LVerfSchG M-V ein Behördenleitervorbehalt und Unterrichtungsregelungen fehlen, so bleibt dabei die bestehende Regelungslage unberücksichtigt. Wie vom Bundesverfassungsgericht gefordert, ist als Voraussetzung in beiden Normen jeweils festgeschrieben worden, dass bereits zum Zeitpunkt der Beauskunftung der Code-Daten die gesetzlichen Voraussetzungen für ihre Nutzung vorliegen müssen.

Damit sind bereits bestehende Regelungen im SOG M-V bzw. im LVerfSchG M-V - also z. B. auch schon bestehende Vorbehalte und Benachrichtigungsregelungen - in Abhängigkeit davon, wofür die Codes im jeweiligen Einzelfall tatsächlich genutzt werden sollen, zu beachten. Zur Erläuterung sei hier kurz folgendes Beispiel dargestellt:

Soll etwa eine Auskunft über Zugangssicherungscodes gem. § 28a SOG M-V eingeholt werden, um eine Überwachung eines noch nicht abgeschlossenen Telekommunikationsvorgangs - und damit einen Eingriff in das Fernmeldegeheimnis - zu gefahrenabwehrrechtlichen Zwecken zu ermöglichen, ist § 34a SOG M-V zu beachten. Dies bedeutet, dass eine Auskunft über Zugangssicherungscodes in diesen Fällen von der Landespolizei nur dann verlangt werden darf, wenn die in § 34a Absatz 1 SOG M-V enthaltenen, strengeren Voraussetzungen zur Telekommunikationsüberwachung erfüllt sind. Damit muss insbesondere die dort geforderte, richterliche Anordnung vorliegen. Sind die beauskunfteten Zugangssicherungscodes durch die Polizei - wie im Beispiel angeführt - tatsächlich zur Überwachung eines noch nicht abgeschlossenen Telekommunikationsvorgangs genutzt worden, dann gelangen auch die Regelungen zur Benachrichtigung in § 34a Absatz 7 SOG M-V zur Anwendung. Insofern hätte die Normierung eines Richtervorbehalts oder auch von Benachrichtigungspflichten in § 28a SOG M-V zu einer Regelungsdoppelung geführt (zur Doppelung des Richtervorbehalts vergleiche auch Innenausschussdrucksache 6/137 des Landtages, dort Stellungnahme zur öffentlichen Anhörung im Innenausschuss des Landtages am 23. Mai 2013 von Prof. Dr. Kyrill-Alexander Schwarz S. 6 unten).

Im Übrigen ist anzumerken, dass die Darstellung des LfD in seinem Bericht (Stand: 19.03.2014), „einige Landespolitiker von BÜNDNIS 90/ DIE GRÜNEN haben daher eine Sammelbeschwerde vor dem Landesverfassungsgericht in Greifswald gestartet“, nach hiesigem Kenntnisstand nicht zutrifft. Denn der Landesregierung ist bis heute (Stand: 26.05.2014) nur die Ankündigung einer Sammelbeschwerde gegen die landesgesetzlichen Regelungen zur Bestandsdatenauskunft bekannt. Die Sammelbeschwerde ist bisher beim Landesverfassungsgericht nicht anhängig.

Zu Ziffer 6.4.4. Übermittlung von Meldedaten an Religionsgemeinschaften und an die GEZ

a) Datenübermittlungen an die Religionsgemeinschaften

Zur Vereinfachung der Datenübermittlung und zur Verbesserung der Qualität der kirchlichen Datenbestände hat der Arbeitskreis I der Innenministerkonferenz (AK I) im Herbst 2012 eine länderoffene Arbeitsgruppe zur Einbindung der Kirchen in den Standard OSCI-XMeld gebildet. Unter Beteiligung von Kirchen, des Bundesministeriums des Inneren, der Länder Brandenburg und Mecklenburg-Vorpommern und der Koordinierungsstelle für IT-Standards wurde diese Einbindung in OSCI-XMeld konzipiert.

Im Jahr 2013 hat der AK I der Erweiterung des Standards OSCI-XMeld zur Datenübermittlung mit öffentlich-rechtlichen Religionsgesellschaften zugestimmt.

Die erforderlichen verfahrensrechtlichen Regelungen für eine Datenübermittlung unter Verwendung des Standards OSCI-XMeld werden im Melderecht geschaffen. Diese Arbeiten an der Erweiterung von OSCI-XMeld sollen bis zum Ende des Jahres 2014 abgeschlossen werden. Der Produktivbetrieb der Erweiterung ist für November 2015 vorgesehen.

b) Datenübermittlungen an den ARD ZDF Deutschlandradio Beitragsservice (ehemals GEZ)

Seit 1. November 2012 stehen die neuen OSCI-XMeld-Nachrichten für die regelmäßige Datenübermittlung an den ARD ZDF Deutschlandradio Beitragsservice (ehemals GEZ) zur Verfügung. Ziel ist es, die heterogenen Landesvorschriften für die regelmäßigen Datenübermittlungen an die öffentlich-rechtlichen Landesrundfunkanstalten zu vereinheitlichen, um bundesweit eine einheitliche Datenübermittlung in OSCI-XMeld und OSCI-Transport zu ermöglichen.

Zu Ziffer 6.4.5 Der neue Personalausweis

Die Landesregierung verkennt vorhandene Risiken nicht. Zur Förderung privater Personen ist derzeit allerdings kein Förderprogramm geplant.

Zu Ziffer 6.4.6 E-Government-Verfahren - sind Kommunen überfordert?

Die Landesregierung verweist auf die Antwort zu Punkt 4.3. Kommunen, die eine angemessene Informationssicherheit und den erforderlichen Datenschutz nicht aus eigener Kraft gewährleisten können, sollten sich der Kompetenz des Zweckverbandes Elektronische Verwaltung in Mecklenburg-Vorpommern bedienen. Zurzeit findet eine Prüfung statt, ob die Notwendigkeit für ein landeseigenes E-Government Gesetz besteht. Hier wird gegebenenfalls eine Abwägung über die Verbindlichkeit der Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung für die Kommunen in Mecklenburg-Vorpommern vorzunehmen sein.

Zu Ziffer 6.5.2 Fragen zum SGB II - Arbeitslosengeld II

Die Landesregierung teilt die Auffassung des LfD, dass im Bereich der Grundsicherung für Arbeitsuchende, in dem sensible und schutzbedürftige Sozialdaten verarbeitet werden, der Beachtung des Datenschutzes eine besondere Bedeutung zukommt.

Neben den speziellen Datenschutzvorschriften der §§ 50 ff. Zweites Buch Sozialgesetzbuch (SGB II) finden die allgemeinen Vorschriften zum Schutz der Sozialdaten nach § 35 Erstes Buch Sozialgesetzbuch (SGB I) und §§ 67 ff. Zehntes Buch Sozialgesetzbuch (SGB X) Anwendung.

Um das Bewusstsein für die Bedeutung des Datenschutzes zu schärfen und den Sozialleistungsträger für die Beachtung der rechtlichen Vorgaben zu sensibilisieren, hat das Ministerium für Inneres und Sport als die nach § 48 Abs. 1 SGB II für vom Landkreis als Optionskommune geführte Jobcenter zuständige Rechtsaufsichtbehörde mit Schreiben vom 28. Februar 2014 die vom Bundesministerium für Arbeit und Soziales am 19. November 2013 an die gemeinsamen Einrichtungen versandten datenschutzrechtlichen Hinweise entsprechend an das kommunale Jobcenter des Landkreis Vorpommern-Rügen weitergegeben.

Hierbei wurden folgende Schwerpunkte benannt:

- Beachtung des Grundsatzes der Erforderlichkeit bei der Erhebung und Speicherung von Sozialdaten,
- sensibler Umgang mit Gesundheitsdaten,
- Wahrung der Grundsätze der Erforderlichkeit und Verhältnismäßigkeit bei der Durchführung von Hausbesuchen,
- grundsätzliches Erfordernis der Beratung von Kundinnen und Kunden in Einzelbüros,
- Beachtung des Erforderlichkeits- und Ersterhebungsgrundsatzes vor der Kontaktierung ehemaliger Arbeitgeber,
- Wahrung der Akteneinsichts-, Berichtigungs- und Löschungsrechte sowie
- Beachtung der Unzulässigkeit der Verwendung von Daten aus sozialen Netzwerken ohne Einwilligung der oder des Betroffenen.

In diesem Zusammenhang wurde darum gebeten, die Beachtung des Datenschutzes regelmäßig durch die behördliche Datenschutzbeauftragte überprüfen zu lassen und die Beschäftigten des Kommunalen Jobcenters Vorpommern-Rügen auf die Einhaltung der datenschutzrechtlicher Vorgaben hinzuweisen.

Die vom LfD benannten, von den Landesbeauftragten für den Datenschutz der Länder Berlin, Brandenburg, Hamburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und Schleswig-Holstein herausgegebenen Hinweise zur datenschutzrechtlichen Ausgestaltung der Anforderungen von Kontoauszügen bei der Beantragung von Sozialleistungen wurden von der Landesregierung an das kommunale Jobcenter Vorpommern-Rügen weitergegeben.

Die Landesregierung weist darauf hin, dass in Mecklenburg-Vorpommern nur noch der Landkreis Vorpommern-Rügen als zugelassener kommunaler Träger das kommunale Jobcenter in alleiniger Trägerschaft betreibt. Das Jobcenter des Landkreises Mecklenburgische Seenplatte ist seit dem 1. Januar 2014 eine gemeinsame Einrichtung nach § 44b SGB II zwischen der Bundesagentur für Arbeit und dem Landkreis Mecklenburgische Seenplatte.

Zu Ziffer 6.6.7 Krankenhausinformationssysteme (KIS)

Zu der Stellungnahme zu Ziffer 6.6.7 hat sich die Landesregierung externen Sachverstands der hierunter namentlich benannten Krankenhausgesellschaft M-V bedient. Die Stellungnahme lautet wie folgt:

Bezug nehmend auf den Abschnitt c) wird ausgeführt, dass die OH KIS allen Krankenhäusern weitgehend bekannt ist, aber unterschiedlich interpretiert wird. Dies ist nach unserem Verständnis vor allem der Tatsache geschuldet, dass die OH KIS bislang auch jede Menge Interpretationsspielraum bot. Dies wurde sowohl von den Datenschutzbeauftragten als auch den Adressaten der OH KIS, den Krankenhäusern und Softwareherstellern, immer wieder betont. Wie anders ist es zu erklären, dass es zwischenzeitlich eine zweite Fassung der OH KIS von März 2014 gibt. Die zweite Fassung wurde nicht nur inhaltlich, sondern auch strukturell unter Beteiligung der DKG und des bvtig überarbeitet. Damit sind Anforderungen, auf die sich die Prüfung bezieht, bereits heute in Teilen obsolet.

Weiter wird die Aussage getroffen, dass die Anforderungen und Empfehlungen der OH KIS insgesamt kaum umgesetzt sind. Dieser Aussage muss entschieden widersprochen werden. In dem vorliegenden Prüfbericht zum Umsetzungsstand der OH KIS in den Krankenhäusern heißt es: „Die konzeptionelle Darstellung von IT-Sicherheit und Datenschutz orientiert sich hauptsächlich an den Maßgaben der Gesetzgebung. Eine genauere Überarbeitung basierend auf der OH KIS ist in vielen Häusern geplant, aber noch nicht umgesetzt.“ Damit bezieht sich diese Aussage auf die Konzeption zum Datenschutz, nicht aber auf den Umsetzungsstand der OH KIS. Im Übrigen wird im Prüfbericht zur Umsetzung der OH KIS aber auch im Tätigkeitsbericht des LfD deutlich, dass die technischen Möglichkeiten zur Umsetzung der OH KIS beschränkt sind. Trotz der beschränkten technischen Möglichkeiten werden in den Krankenhäusern aber organisatorische Maßnahmen zur Umsetzung datenschutzrechtlicher Anforderungen getroffen.

Wir betonen ausdrücklich, dass hier nicht der Eindruck entstehen darf, die KIS sind nicht datenschutzkonform konfiguriert. Bezogen auf einzelne Anforderungskriterien der OH KIS gibt es durchaus Verbesserungsbedarf. Allerdings wird bei der Zuständigkeit zwischen Herstellern und Betreibern von KIS zu wenig differenziert.

Die Umsetzung der OH KIS in Gänze kann jedoch nur gemeinsam gelingen. Hierzu müssen die Verantwortlichen für den Datenschutz, die Krankenhausträger und die Softwarehersteller konstruktiv den Dialog suchen. Hier sei verwiesen auf den Abschnitt i) der Ziffer 6.6.7. In Mecklenburg-Vorpommern wirken der LfD und die Krankenhausgesellschaft gemeinsam an einer verbesserten Umsetzung der OH KIS. Auf der Basis der Errichtung des Arbeitskreises Datenschutz bei der KGMV wurden bereits mehrere Fachtagungen durchgeführt, um die Mitarbeiter in den Krankenhäusern sowohl beim technischen als auch organisatorischen Datenschutz zu schulen. Auf der letzten Tagung am 15.05.2014 in Rostock hatten wir mehr als 40 Teilnehmer zu verzeichnen. Damit hat durchschnittlich jede Mitgliedseinrichtung der KGMV einen Teilnehmer gestellt. Dies spricht für die Sensibilität der Krankenhausleitungen für diese Thematik.

Zu Ziffer 6.7 Zensus 2011

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.

Zu Ziffer 6.8.1 Kartenzahlung per Funk

Für die Zahlstellen des Landes Mecklenburg-Vorpommern wird das Elektronische Zahlstellenverfahren eingesetzt. Mit diesem Verfahren wird die Entgegennahme von Zahlungen mittels elektronischer Karten (ec-Karte und Kreditkarte) und damit die Förderung des unbaren Zahlungsverkehrs realisiert. Mit dem elektronischen Zahlstellenverfahren wird jedoch anders als im Einzelhandel mittels des Kartenterminals auch der gesamte Funktionsumfang des Abrechnungsverkehrs der Zahlstellen mit der Landeszentralkasse abgebildet. Insofern müssen die eingesetzten Terminals diesen Anforderungen genügen. Ein kontaktloses Bezahlen mit der Bezahlart „girogo“ wird nicht praktiziert. Auch für den Bereich der Steuerverwaltung kommt das kontaktlose Bezahlen nicht zur Anwendung.

Zu Ziffer 6.8.3 Einführung der „Bettensteuer“ in Schwerin?

Der LfD sieht datenschutzrechtliche Bedenken mit Blick auf die Einbindung des Beherbergungsbetriebes in das Steuererhebungsverfahren nach § 5 Abs. 2 der „Satzung über die Erhebung einer Kulturförderabgabe in der Landeshauptstadt Schwerin“. Nach den Ausführungen des LfD ist von der Landeshauptstadt Schwerin im Oktober 2012 die Einführung der "Bettensteuer" beschlossen worden.

Die Stadtvertretung der Landeshauptstadt Schwerin hat in ihrer Sitzung am 21.10.2013 eine Satzung über die Erhebung einer Steuer auf Übernachtungen in Beherbergungsbetrieben (Übernachtungssteuer) beschlossen, die nach Genehmigung durch das Ministerium für Inneres und Sport wirksam geworden ist. Diese Satzung enthält keine Regelung, die der vom LfD zitierten Regelung des § 5 Abs. 2 der „Satzung über die Erhebung einer Kulturförderabgabe in der Landeshauptstadt Schwerin“ entspricht. Demnach ist davon auszugehen, dass die vom LfD aufgezeigten Rechtsbedenken ausgeräumt sind.

Ziffer 6.9.2 E-Mail mit unverschlüsselten Personaldaten

Den Empfehlungen des LfD wurde gefolgt. Eine Hausmitteilung zur Verschlüsselung von E-Mails und deren Anhängen wurde veröffentlicht. Allen Mitarbeiterinnen und Mitarbeitern des Ministeriums für Bildung, Wissenschaft und Kultur wird im Laufe des Jahres 2014 eine qualifizierte Signatur bereitgestellt, sodass die vom LfD angeratene Lösung bereits realisiert wird.

Damit beim Versand besonders schutzwürdiger Daten die erforderlichen Sicherheitsmaßnahmen sichergestellt werden können, wird den Landesbehörden das Elektronische Gerichts- und Verwaltungspostfach (EGVP) bereitgestellt, das eine Ende-zu-Ende-Verschlüsselung garantiert und die Möglichkeit der Einbindung der qualifizierten elektronischen Signatur bietet. Kommunalbehörden können das Verfahren ebenfalls nutzen. Weiterhin ist eine kostenlose Office Integration des EGVP-Systems möglich.

Auf die Stellungnahme zu Ziffer 1.2 Nr. 5 wird verwiesen.

Zu Ziffer 6.9.3 Schulinformations- und Planungssystem (SIP)

Die Empfehlungen des LfD wurden bzw. werden vonseiten der Landesregierung umgesetzt. Für die Ausstattung der Schulen mit Hard- und Software sind die Schulträger verantwortlich, die den Ersatz der Computer bzw. die Ausstattung der Computer mit einem moderneren Betriebssystem noch nicht vollständig umgesetzt haben.

Zu Ziffer 6.9.4 Erhebung von personenbezogenen Stellenplandaten von Hochschulen

Mit Schreiben vom 18.04.2014 wurde den Hochschulen des Landes mitgeteilt, dass seitens des Ministeriums für Bildung, Wissenschaft und Kultur personenbezogene Stellenplandaten nicht mehr erhoben werden. Das Bildungsministerium behält sich künftig vor, in begründeten Einzelfällen Stellenplandaten in anonymisierter Form von den Hochschulen zu erheben. Dabei wird es sich um Informationen handeln, die zum Beispiel Auskunft geben zum Umfang der Stellenbesetzung, zum durchschnittlichen Grad der Auslastung der Stellen oder zum Zeitpunkt der Wiederbesetzung frei werdender Stellen.

Zu Ziffer 6.9.6 Nutzen von sozialen Netzwerken im Internet für schulische Zwecke

Eine präventive unterrichtliche Auseinandersetzung mit sozialen Netzwerken und anderen Internet-Plattformen sollte zum Kern der Entwicklung von Medienkompetenz und Medienbildung an den Schulen des Landes gehören, um auf diesem Wege selbstbestimmtes und verantwortungsvolles Handeln von Schülerinnen und Schülern, Lehrkräften und Eltern zu ermöglichen. Die Schulen werden diesbezüglich durch die medienpädagogischen Beraterinnen und Berater des Landes unterstützt, die seit mehreren Jahren Multiplikatorenschulungen, Fortbildungen, Workshops und Elternabende auf dem Gebiet des Jugendmedien- und des Datenschutzes durchführen.

Ziffer 6.10.1 Zweckbindungsprinzip beim Bodenordnungsverfahren

Die Kritik des LfD war berechtigt. Zwar nimmt das Staatliche Amt für Landwirtschaft und Umwelt (StALU) beide Funktionen wahr (Bodenordnungsverfahren und Förderung der privaten Dorferneuerung), doch sind die beiden Funktionen getrennt zu sehen. Die gewährte Förderung im Rahmen der Dorferneuerung hat keine Auswirkungen auf die Höhe der Abfindung im Bodenordnungsverfahren, die dort mit wertgleichen Grundstücken zu erfolgen hat.

Wie der LfD in seinem Bericht schon feststellt, hat das StALU im Beanstandungsverfahren schließlich versichert, dass Informationen über die Förderung der Dorferneuerung künftig nicht mehr im Rahmen von Bodenordnungsverfahren verwendet werden.

Die in der gleichen Ziffer angesprochene Problematik der europaweiten Veröffentlichung der geförderten Vorhaben betrifft ein gesamteuropäisches Problem. Die Europäische Union hatte diese Veröffentlichung in Artikel 44a der Verordnung (EG) Nr. 1290/2005 vom 21. Juni 2005 (ABl. L 209 vom 11.8.2005, S. 1) zwingend vorgeschrieben. Erst der Europäische Gerichtshof hat in seinem Urteil vom 9. November 2010 (Aktenzeichen C-92/09 und C-93-09) festgestellt, dass diese Verpflichtung unwirksam sei, weil sie gegen die Grundsätze des Datenschutzes verstoße.

Von einer Landesbehörde kann nur verlangt werden, dass sie das geltende Recht anwendet. Von ihr kann nicht verlangt werden, dass sie von sich aus die Vereinbarkeit dieser Rechtsvorschriften mit höherrangigem Recht in Frage stellt; diese Feststellung steht ausschließlich dem Europäischen Gerichtshof zu. Es ist daher nicht zu beanstanden, wenn das StALU bis zur Verkündung des genannten Urteils das Einverständnis des Zuwendungsempfängers mit der Veröffentlichung der mit der Förderung verbundenen Angaben verlangt hat. Nach Bekanntwerden des Urteils hat das StALU auf diese Einverständniserklärung verzichtet.

Zu Ziffer 9.1 Rechtliche Entwicklungen

Die Landesregierung sieht, nachdem die Verabschiedung eines Transparenzgesetzes im Landtag Mecklenburg-Vorpommern bereits gescheitert ist, keine Notwendigkeit, eine Novelle des Informationsfreiheitsgesetzes vorzubereiten.

Die Landesregierung steht dem Transparenzgedanken grundsätzlich offen gegenüber. Sie wird deshalb die Erfahrungen, die Hamburg bei der Umsetzung des dortigen Transparenzgesetzes macht, beobachten.

Für die Landesregierung besteht jedoch kein zwingender Zusammenhang zwischen Open Government und der Weiterentwicklung des IFG M-V mit proaktiven Veröffentlichungspflichten.

Zu Ziffer 9.5 Auskunftsrechte der Kommunalverfassung vs. IFG M-V

Der Empfehlung des Berichts, von einer gesetzlichen Klarstellung abzusehen, folgt die Landesregierung schon aus Deregulierungsgründen. Die strittige Normkonkurrenz zwischen der Kommunalverfassung und dem Informationsfreiheitsgesetz ist bisher lediglich in einem einzigen Fall aufgetreten, der auch beim Petitionsausschuss anhängig war.

Zu Ziffer 9.8 Herausgabe von Informationen zu Öko-Eiern?

Entgegen den Feststellungen des LfI begehrte der Antragsteller nicht nur Auskünfte zu einzelnen Verwaltungsverfahren, sondern auch die Offenlegung betriebsinterner Daten. Die Ablehnung der Herausgabe dieser Daten wurde daher nicht nur mit § 5 des IFG M-V begründet, sondern auch mit § 8.

Auf die Beschwerde des Antragstellers beim LfI wurde in Abstimmung mit dem Landesbeauftragten schließlich der Informationszugang gewährt. Auch künftig müssen aber berechtigte Interessen an der Wahrung von Betriebs- und Geschäftsinteressen mit dem Informationsinteresse des Fragestellers abgewogen werden.