

UNTERRICHTUNG

durch die Landesregierung

Stellungnahme der Landesregierung zum Fünfzehnten Tätigkeitsbericht zum Datenschutz und zum Siebenten Bericht über die Umsetzung des Informationsfreiheitsgesetzes des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern

Berichtszeitraum zum Datenschutz: 1. Januar 2019 bis 31. Dezember 2019

Berichtszeitraum zum Informationsfreiheitsgesetz: 1. Januar 2018 bis 31. Dezember 2019

Allgemeines

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern hat als Landesbeauftragter für den Datenschutz für den Berichtszeitraum vom 1. Januar 2019 bis zum 31. Dezember 2019 seinen Fünfzehnten Tätigkeitsbericht gemäß Artikel 59 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), zukünftig Verordnung (EU) 2016/679, und als Landesbeauftragter für Informationsfreiheit für den Berichtszeitraum vom 1. Januar 2018 bis zum 31. Dezember 2019 seinen Siebenten Tätigkeitsbericht nach dem Informationsfreiheitsgesetz Mecklenburg-Vorpommern vorgelegt (siehe Drucksache 7/5046).

Die Pflicht der Landesregierung, dem Landtag zu den jeweiligen Berichten innerhalb von sechs Monaten nach Vorlage der Berichte ihre Stellungnahme zuzuleiten, ergibt sich zum einen aus § 21 des Landesdatenschutzgesetzes, zum anderen aus § 14 Absatz 8 des Informationsfreiheitsgesetzes.

Wie auch bei früheren Tätigkeitsberichten verknüpft der Tätigkeitsbericht gemäß Verordnung (EU) 2016/679 den Bereich des öffentlichen und des nicht-öffentlichen Datenschutzes. Die Landesregierung geht, wie 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 Tätigkeitsbericht zum Informationsfreiheitsgesetz ist als Abschnitt Neun 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.

In der Folge wird der Landesbeauftragte für Datenschutz und Informationsfreiheit bei den Datenschutz-Themen als Landesbeauftragter für den Datenschutz, bei den Informationsfreiheits-Themen als Landesbeauftragter für Informationsfreiheit bezeichnet.

Einleitung

Der Berichtszeitraum des Fünfzehnten Tätigkeitsberichtes des Landesbeauftragten für den Datenschutz zum Datenschutz umfasst das erste vollständige Kalenderjahr nach Geltung des neuen europäischen Datenschutzrechts.

Er bestätigt die Auffassung der Landesregierung, dass weit überwiegend eine große Übereinstimmung zwischen dem Landesbeauftragten für den Datenschutz und der Landesregierung zu datenschutzrechtlichen Fragestellungen besteht.

Zu 1 Empfehlungen

Zu 1.1 Zusammenfassung aller Empfehlungen

Zu Nummer 1

Die Problematik ist der Landesregierung bekannt. Die Landesregierung ist - wie der Landesbeauftragte für den Datenschutz - der Auffassung, dass der Bundesrat schnellstmöglich einen Stellvertreter für den deutschen Vertreter im Europäischen Datenschutzausschuss wählen sollte. Auf die Stellungnahme der Landesregierung zum Vierzehnten Tätigkeitsbericht (Drucksache 7/4327) wird verwiesen.

Zu Nummer 2

Die Landesregierung wird sich für eine verfassungskonforme Regelung zum Einsatz eines Identifikationsmerkmals einsetzen, das bei der Registermodernisierung eine wichtige Rolle spielen wird. Dabei wird die Landesregierung die entsprechenden Bundesregelungen daraufhin zu prüfen haben, ob nur bereichsspezifische Identifikationsmerkmale verfassungskonform sein können oder ob auch ein einheitliches Identifikationsmerkmal verfassungsrechtlich möglich sein kann. Die Position der Datenschutzkonferenz ist der Landesregierung dabei bekannt.

Die Landesregierung weiß aber auch, dass sich ein Gesetzentwurf des Bundes zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz - RegMoG) im parlamentarischen Verfahren befindet, der sich auch mit der Frage der Nutzung einer einheitlichen Identifikationsnummer oder bereichsspezifischer Identifikationsnummern auseinandersetzt. Nach jetzigem Stand kommt der Bund zu dem Ergebnis, dass in der vornehmlich dezentral organisierten deutschen Verwaltung bereichsspezifische Identifikationsnummern wegen der rechtlichen, technischen und organisatorischen Komplexität, wo Aufwand und Nutzen in keinem vertretbaren Verhältnis zueinanderstehen würden, nicht zu befürworten seien. Der Bund hat deshalb ein neues Stammgesetz zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung (Identifikationsnummerngesetz - IDNrG) vorgelegt, welches vorsieht, die Identifikationsnummer nach § 139b der Abgabenordnung (Steuer-Identifikationsnummer) als registerübergreifendes Ordnungsmerkmal in alle für die Umsetzung des Onlinezugangsgesetzes relevanten Register von Bund und Ländern einzuführen und dieses durch rechtliche und technisch-organisatorische Maßnahmen abzusichern.

Es enthält auch Regelungen zu einem Datencockpit, das eine einfache, transparente und zeitnahe Wahrnehmung der Betroffenenrechte nach der Verordnung (EU) 2016/679 ermöglicht. Die Inhalte des Gesetzentwurfes entsprechen den Beschlüssen des IT-Planungsrates vom 12. März 2019 zum registerübergreifenden Identitätsmanagement sowie des Koalitionsausschusses des Bundes vom 3. Juni 2020 und basieren auf dem Beschluss der 212. Sitzung der Innenministerkonferenz vom 17. bis 19. Juni 2020.

Zu Nummer 3

Die Landesregierung nimmt die Empfehlungen bezüglich des datenschutzkonformen Einsatzes von Verfahren zur Verarbeitung biometrischer Daten zu Kenntnis.

Vor der Einführung von Prozessen unter Verwendung von biometrischen Daten werden die Anforderungen der nach der Verordnung (EU) 2016/679 aufgeführten Anforderungen in einem Datenschutz- und Sicherheitskonzept verpflichtend mit aufgenommen.

Zu Nummer 4

Die Landesregierung nimmt die Empfehlungen bezüglich der Risiken beim Einsatz von Windows 10 und den entsprechenden Office-Anwendungen zur Kenntnis.

Sie verweist hierbei auf das Prüfschema zur Einhaltung des Datenschutzes bei Windows 10 der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz). Unter Anwendung dieses Prüfschemas sowie mit Hilfe der vorhandenen technischen und organisatorischen Möglichkeiten, der Umsetzung der Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und einer eigenverantwortlichen Risikoabschätzung, konnte der Einsatz von Windows 10 ermöglicht werden. Alle notwendigen Maßnahmen wurden durch die Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH (DVZ) in einem Handlungsleitfaden dokumentiert. Der Handlungsleitfaden wurde am 17. Juni 2020 vom Lenkungsausschuss Digitalisierung zur Kenntnis genommen. Im Vorfeld fanden hierzu auch intensive Abstimmungen mit dem Landesbeauftragten für den Datenschutz statt.

Zu Nummer 5

KI- bzw. KI-gestützte Systeme befinden sich innerhalb der Landesregierung derzeit nicht im Einsatz oder in der Planung. Sollten diese in Betracht gezogen werden, werden frühzeitig datenschutzrechtliche Anforderungen berücksichtigt.

Zu Nummer 6

Für die Überprüfung der Kompatibilität zu Produkten aus dem Open Source Bereich, sind umfangreiche Recherchen erforderlich. Die Landesregierung prüft hierzu, inwieweit Lösungen implementiert werden können, die eine gemeinsame Datenhaltung möglich machen.

Zu Nummer 7

Das Standard-Datenschutzmodell wird in Abstimmung mit dem Landesbeauftragten für den Datenschutz in den Prozessen der Landesregierung berücksichtigt.

Zu Nummer 8

Die Landesregierung nimmt die Empfehlung des Landesbeauftragten für den Datenschutz zur Kenntnis. Die Zweite Lesung zum Entwurf eines Zweiten Gesetzes zur Änderung des E-Government-Gesetzes Mecklenburg-Vorpommern ist im Oktober 2020 erfolgt. Nach dem Inkrafttreten des Gesetzes ist vorgesehen, von der Ermächtigungsgrundlage in § 15 Absatz 4 des E-Government-Gesetzes Mecklenburg-Vorpommern Gebrauch zu machen und eine Landesverordnung über die Bereitstellung, Ausgestaltung und Nutzung von E-Government-Basisdiensten im Land Mecklenburg-Vorpommern zu erlassen. Hierzu wurde ein Referentenentwurf erarbeitet, zu welchem derzeit die Ressorts angehört werden. Mit der Landesverordnung wird dann die Rechtsgrundlage für den Einsatz eines Nutzerkontos nach dem Onlinezugangsgesetz (OZG) geschaffen.

Das MV-Serviceportal wird wegen der im Bericht dargelegten Punkte nach wie vor nicht im Portalverbund und ohne ein identifizierendes Nutzerkonto betrieben.

Zu Nummer 9

Die Landesregierung nimmt interne Sicherheitsmaßnahmen sehr ernst und wird die Einführung beziehungsweise Betreuung eines geeigneten Passwortmanagementsystems prüfen. Zudem werden die Beschäftigten hinsichtlich der IT-Sicherheitsthemen regelmäßig sensibilisiert und Schulungen angeboten.

Zu Nummer 10

Die Landesregierung nimmt die Empfehlung, sich mit Zertifizierungen vertraut zu machen, zur Kenntnis. Sie beschäftigt sich bereits mit dem Potenzial von Zertifizierungen hinsichtlich Auftragsverarbeitung und Cloudstrukturen sowie deren Implementation.

Zu Nummer 11

Die Landesregierung hat diesen Bericht einschließlich des Whitepapers an die Krankenhausesellschaft Mecklenburg-Vorpommern weitergeleitet, verbunden mit der Anregung, ihrerseits die Mitglieder zu informieren, da sich die Empfehlungen zu Messenger-Diensten an die Verantwortlichen in Krankenhäusern richten.

Zu Nummer 12

Die Landesregierung nimmt die Empfehlung zur Kenntnis und wird erneut prüfen, ob weiterer Handlungsbedarf für die von der Landesregierung betriebenen Internetseiten besteht.

Zu Nummer 13

Die Landesregierung hat Organisationsmaßnahmen in den Ressorts getroffen, Schulungsangebote bestehen.

Zu Nummer 14

Die Bedenken des Landesbeauftragten für den Datenschutz werden nicht geteilt. Hierzu wird auf die zu den in der Vergangenheit singular durchgeführten Meldedatenabgleichen ergangenen Rechtsprechungen, hier insbesondere des Bayerischen Verfassungsgerichtshofes, verwiesen. Diese haben ausdrücklich bestätigt, dass der Meldedatenabgleich einen legitimen Zweck (Sicherung der Aktualität des Datenbestandes zur Herstellung größtmöglicher Beitragsgerechtigkeit) verfolgt sowie geeignet und erforderlich ist, insbesondere das mildeste wirksame Mittel darstellt, die gesetzgeberische Zielstellung zu erreichen, also den Eingriff in das Recht auf informationelle Selbstbestimmung rechtfertigt. Zudem unterliegt der nunmehr periodisch durchzuführende Meldedatenabgleich einem Korrektiv, das auch dem Grundsatz der Datenminimierung Rechnung trägt, indem der Abgleich dann nicht vorgenommen wird, wenn der Datenbestand nach Prüfung durch die Kommission zur Ermittlung des Finanzbedarfs der Rundfunkanstalten (KEF) noch hinreichend aktuell ist. Ergänzend ist darauf hinzuweisen, dass die Länder zur Einschätzung der durch den Meldedatenabgleich betroffenen datenschutzrechtlichen Belange am 29. April 2019 eine Anhörung durchgeführt hatten, bei der die öffentlich-rechtlichen Rundfunkanstalten, deren betriebliche Datenschutzbeauftragte, die Rundfunkdatenschutzbeauftragten und die Datenschutzbeauftragten der Länder vertreten waren. Die vorgebrachten Positionen wurden bei der Ausgestaltung der Vorschrift zum Meldedatenabgleich einbezogen. Die Länder sehen insoweit die Vorgaben der Verordnung (EU) 2016/679 als hinreichend gewürdigt und im 23. Rundfunkänderungsstaatsvertrag als europarechtskonform umgesetzt an. Dem Vorhalt, dass mit der Neuregelung zum Meldedatenabgleich mehr, vor allem nicht notwendige personenbezogene Daten abgerufen würden, als die Beitragszahlerinnen und -zahler bei der Anmeldung mitteilen müssen, wird entgegengehalten, dass die Neuregelung nicht über die Datenarten hinausgeht, die bereits im Rahmen des letzten singularen Datenabgleichs erhoben worden sind. Die mit dem 23. Rundfunkänderungsstaatsvertrag beabsichtigte Neuregelung in § 11 Absatz 5 Satz 1 des Rundfunkbeitragsstaatsvertrages entspricht in Umfang und Art der zu erhebenden Daten der aus dem 19. Rundfunkänderungsstaatsvertrag resultierenden Vorgängerregelung in § 14 Absatz 9 Satz 1 des Rundfunkbeitragsstaatsvertrages. Auch hierzu hatte der Bayerische Verfassungsgerichtshof (Entscheidung vom 15. Mai 2014) die Erforderlichkeit der dort aufgeführten Datenarten bestätigt. So decken sie sich im Wesentlichen mit denjenigen Daten, die von den Betroffenen bereits bei der Anmeldung eines Beitragskontos anzuzeigen sind. Die zusätzliche Übermittlung von Doktorgrad und Familienstand im Rahmen des Meldedatenabgleichs dienen der eindeutigen Identifikation einer Person und können die Zuordnung der Mitbewohnerinnen und Mitbewohner in einer Wohnung maßgeblich erleichtern.

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 Vermietersauskunft oder durch Ermittlungen vor Ort wären nicht erfolgversprechend. Hinzukommen würde der deutlich stärkere Eingriff in die Privatsphäre der Betroffenen.

Zu Nummer 15

Das Ministerium für Bildung, Wissenschaft und Kultur begrüßt den regen Austausch mit dem Landesbeauftragten für den Datenschutz außerordentlich und profitiert von der Expertise und der damit einhergehenden Rechtsicherheit für die Vorhaben der Landesregierung in den zuständigen Bereichen.

Derzeit findet dieser Austausch insbesondere in Zusammenhang mit der Einführung einer zentralen Schulverwaltungssoftware und der Einführung von Möglichkeiten der digitalen Unterrichtsgestaltung statt. Für die gute Zusammenarbeit an der Schuldatenschutzverordnung dankt die Hausleitung dem Landesbeauftragten für den Datenschutz und seiner Behörde ausdrücklich.

Auch in der Zukunft wird das Ministerium für Bildung, Wissenschaft und Kultur am regen Austausch mit dem Landesbeauftragten für den Datenschutz festhalten und steht diesem aufgeschlossen gegenüber.

Zu Nummer 16

Die Landesregierung beabsichtigt derzeit auch unter Berücksichtigung der Ausführungen des Landesbeauftragten für Informationsfreiheit nicht, das Informationsfreiheitsgesetz zu novellieren.

1.2 Umsetzungen der Empfehlungen des Vierzehnten Tätigkeitsberichtes**Zu Nummer 1**

Es wird auf die Stellungnahme der Landesregierung unter Punkt 1.1 Nummer 1 verwiesen.

Zu Nummer 2

Die Landesregierung unterstützt die Vernetzung aller medienpädagogischen Akteure und hat sich im Koalitionsvertrag unter Punkt 215 zur „Kooperationsvereinbarung zur Förderung von Medienkompetenz“ bekannt. Mit Kabinettsbeschluss vom 19. Februar 2019 hat die Staatskanzlei die Federführung zur Erarbeitung der vierten Kooperationsvereinbarung übernommen.

Der Landesbeauftragte für den Datenschutz ist Mitunterzeichner der Vereinbarung. Das Engagement des Landesbeauftragten für den Datenschutz im Bereich der Medienbildung sowie auf dem Gebiet der Fortbildungen zur Vermittlung von Datenschutzbewusstsein für alle Bürgerinnen und Bürger wird seitens der Landesregierung begrüßt.

Neben anderen Akteuren wird auch die Fachhochschule für öffentliche Verwaltung, Polizei und Rechtspflege des Landes Mecklenburg-Vorpommern (FHöVPR M-V) an der Erarbeitung der neuen Kooperationsvereinbarung zur Förderung von Medienkompetenz in Mecklenburg-Vorpommern mitwirken, um die medienpädagogisch Arbeitenden in Mecklenburg-Vorpommern weiter zu vernetzen.

Zu Nummer 3

Es wird auf die Stellungnahme der Landesregierung unter Punkt 1.1 Nummer 8 verwiesen.

Zu Nummer 4

Es wird auf die Stellungnahme der Landesregierung unter Punkt 1.1 Nummer 7 verwiesen.

Zu Nummer 5

Der Landesbeauftragte für den Datenschutz hat in seinem Vierzehnten Tätigkeitsbericht die Erwartungshaltung dargestellt, dass das Ministerium die Erfahrungen des Einsatzes von Bodycams ergebnisoffen auswertet und vor allem auf Grundlage dieser Erfahrungen dann über das weitere „Ob“ und „Wie“ von Bodycams entscheidet.

Der Landesbeauftragte für den Datenschutz stellt in seinem Fünfzehnten Tätigkeitsbericht nunmehr heraus, dass mit der Besprechung vom 15. Oktober 2019 im Ministerium für Inneres und Europa Einvernehmen im Sinne der Evaluation zum Pilotprojekt hergestellt wurde und die Auswertung des Pilotprojektes ergeben hat, dass in Mecklenburg-Vorpommern der Einsatzwert zum Schutz der Polizeivollzugsbeamtinnen und -beamten gegeben ist und mit Einführung der Bodycam in der Landespolizei alle erforderlichen Aspekte des Datenschutzes eingehalten werden.

Zu 3 Entwicklung der Behörde

Mit Schreiben vom 5. Juni 2019 stellte die Landtagspräsidentin nach Herstellung des Benehmens in der Sitzung des Ältestenrates am 5. Juni 2019 gemäß Artikel 29 Absatz 6 der Verfassung des Landes Mecklenburg-Vorpommern den Haushaltsplan-Entwurf 2020/2021 für den Einzelplan 01 mit Ausnahme des Kapitels 0102 - Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern - fest und übersandte diesen an das Finanzministerium. Hinsichtlich der unterschiedlichen Übersendungen der Kapitel 0101, 0103, 0104 und des Kapitels 0102 war seitens des Finanzministeriums eine Auslegung der Aufnahme in den Haushaltsplan-Entwurf vorzunehmen. Nach dem übersandten Protokollauszug der Sitzung des Ältestenrates ging das Finanzministerium davon aus, dass die Entscheidung über die übersandte Anmeldung des Kapitels 0102 im parlamentarischen Verfahren durch die Ausschüsse und abschließend im Landtag erfolgt. Insofern hat das Finanzministerium im Rahmen der Haushaltsplanaufstellung das Kapitel 0102 zunächst mit den Ansätzen und Stellen der Anmeldung in den (Gesamt-)Haushaltsplan-Entwurf aufgenommen. Die über die vom Haushaltsgesetzgeber zuletzt genehmigten Ansätze und Stellen (Haushaltsplan 2018/2019) hinausgehenden Anmeldungen und Stellenmehrbedarfe des Kapitels 0102 wurden allerdings mit einer Sperre versehen. Sie bedurften der abschließenden Prüfung durch den Haushaltsgesetzgeber im parlamentarischen Verfahren. Ihm oblag dann die Zustimmung/Entsperrung hinsichtlich der angemeldeten Mehrbedarfe oder deren Ablehnung.

Der Einfachheit halber wurden die gesamten Mehranmeldungen bei den Sachkosten in einem Titel gesperrt. Dies betrifft den Titel 0102 517.01 „Bewirtschaftung der Grundstücke, Gebäude und Räume“ und diente lediglich der Verwaltungserleichterung bei Aufnahme des Sperrvermerkes in den Haushaltsplan. Ansonsten hätte bei vielen Titeln für geringe Summen derselbe Vermerk aufgenommen werden müssen.

Die Sperrung der Mittel führt jedoch nicht, wie vom Landesbeauftragten für den Datenschutz ausgeführt, zur völligen Handlungsunfähigkeit dieser Behörde. Es besteht innerhalb der 5er Titel Deckungsfähigkeit (§ 7 Absatz 1 Nummer 3 des Haushaltsgesetzes 2018/2019), sodass die benötigten Mittel (außer die Mehranmeldungen) für die Bewirtschaftungskosten der Büroräume bei Inanspruchnahme dieser Deckungsmöglichkeiten zur Verfügung stehen. Im Rahmen des parlamentarischen Verfahrens wurde die Sperrung auf die Sachmittel der neu beantragten Stellen reduziert.

Zum Stellenbedarf des Landesbeauftragten für den Datenschutz äußert sich die Landesregierung nicht. Dies ist eine Angelegenheit, über die der Landtag zu entscheiden hat.

Zu 4 Zusammenarbeit auf Europäischer Ebene

4.1 Europäischer Datenschutzausschuss (EDSA)

Es wird auf die Stellungnahme der Landesregierung unter Punkt 1.1 Nummer 1 verwiesen.

Zu 5 Zusammenarbeit auf deutscher Ebene

5.3 IT-Planungsrat

5.3.2 Registermodernisierung

Es wird auf die Stellungnahme der Landesregierung unter 1.1 Nummer 2 verwiesen.

Zu 6 Datenschutz und Bildung

6.1 Medienbildung

Medienkompetenz bedeutet, sich in der von digitalen Medien durchdrungenen Lebens- und Arbeitswelt kompetent orientieren und verantwortungsbewusst handeln zu können. Das betrifft sowohl die vielfältigen Nutzungsmöglichkeiten digitaler Medien als auch insgesamt den Umgang mit Informationen, Kommunikations- und Interaktionsmöglichkeiten und die eigene Gestaltung medialer Produkte. Die kritische Reflektion der medialen Welten ist eine Grundvoraussetzung zur Teilhabe und Mitgestaltung der gegenwärtigen und zukünftigen realen Welt.

Die Landesregierung begrüßt, dass der Landesbeauftragte für den Datenschutz der Medienbildung für alle Bürgerinnen und Bürger eine hohe Bedeutung beimisst, denn Medienkompetenz ist Lebenskompetenz (siehe Landtags-Drucksache 7/5046 Seite 23 Absatz 3).

Die Landesregierung ist sich mit dem Landesbeauftragten für den Datenschutz einig, dass der Grad der Medienkompetenz seiner Bürgerinnen und Bürger über den Grad seiner Teilhabe und seiner Selbstbestimmtheit in der digitalisierten Welt entscheidet. Sie sieht daher, ebenso wie der Landesbeauftragte für den Datenschutz, die diesbezügliche lebenslange Bildung als eine Kernaufgabe an. Der Vielschichtigkeit der Aufgabe entsprechend müssen und werden in diesem Prozess möglichst alle an der Bildung beteiligten Personen und Institutionen in möglichst allen Phasen involviert.

Die Landesregierung sieht die politischen Rahmenbedingungen mit dem Kabinettsbeschluss vom 19. Februar 2019 zur Erarbeitung einer vierten Kooperationsvereinbarung als gegeben an.

Auch an der FHöVPR M-V werden Medienkompetenzen sowie Kenntnisse im Datenschutzrecht im Studium und in der Fortbildung vermittelt.

6.1.1 Datenschutz als Bildungsaufgabe

Der Erwerb von Medienkompetenz, insbesondere unter dem Blickwinkel der zunehmenden Digitalisierung unserer Gesellschaft, erweitert den Bildungsauftrag unserer Schulen wie auch der Kindertageseinrichtungen und der Kindertagespflege. Die Bundesländer haben sich mit der Strategie der Kultusministerkonferenz zur Bildung in der digitalen Welt zu diesem erweiterten Bildungsauftrag bekannt und sich verpflichtet, den dort beschriebenen Kompetenzrahmen so umzusetzen, dass jede Schülerin und jeder Schüler, der im Schuljahr 2018/19 in eine weiterführende Schule versetzt wird, bis zum Ende seiner Schullaufbahn diese Kompetenzen erwerben kann. Mit der landesrechtlichen Einführung des eigenständigen Bildungs- und Erziehungsbereichs „Medien und digitale Bildung“ in § 3 Absatz 1 Nummer 5 des Kindertagesförderungsgesetzes zum 1. Januar 2020 hat sich das Land Mecklenburg-Vorpommern zu diesem Bildungsauftrag auch in der frühkindlichen Bildung bekannt. Die Vermittlung von Medienkompetenz und Grundlagen des Datenschutzes ist zudem eine zentrale Aufgabe der außerschulischen Bildung und damit Bestandteil des Aufgaben- und Angebotspektrums in den Einrichtungen der Kinder- und Jugendhilfe, insbesondere im Bereich der (offenen) Jugendarbeit.

6.1.2 Projekte „Medienscouts MV“ und „TEO - Tage ethischer Orientierung“

Die Landesregierung begrüßt die Initiative des Landesbeauftragten für den Datenschutz, im Rahmen des Projektes „Medienscouts M-V“ Schülerinnen und Schüler zu Experten für sicheres jugendliches Medienhandeln auszubilden. Aus Sicht der Landesregierung sollte dieses bundesweit beachtete Kooperationsprojekt des Landesbeauftragten für den Datenschutz mit den außerschulischen Bildungspartnern des Netzwerkes „Medienaktiv M-V“ auch weiterhin fortbestehen.

Der Landesbeauftragte für den Datenschutz als Projektträger bemüht sich um den Aufbau einer Kommunikationsplattform „MedienScout-App“ zur Projektbegleitung.

Da das Ministerium für Bildung, Wissenschaft und Kultur ab 2020 ein landesweites Lernmanagementsystem einführt, bei dem die Kommunikation zwischen Schülerinnen und Schülern sowie Lehrkräften ein Leistungsmerkmal ist, könnte die Kommunikation und der Austausch über das Projekt „Medienscout M-V“ ergänzend zur oben genannten App mittelfristig auch über diese Plattform laufen.

6.1.3 Netzwerk Medienaktiv M-V

Die Landesregierung begrüßt das Engagement des Landesbeauftragten für den Datenschutz bei der Koordinierung der Aktivitäten des Netzwerkes „Medienaktiv M-V“ und dankt allen beteiligten Institutionen für ihre Mitarbeit.

Ein wesentlicher Schwerpunkt der Arbeit ist die außerschulische Medienbildung sowie das Vorhalten von Angeboten zum lebenslangen Lernen. Daher müssen sich schon jetzt Projekte, die in diesem Bereich durch das Ministerium für Soziales, Integration und Gleichstellung gefördert werden, daran messen lassen, wie sie auch den Umgang junger Menschen mit den neuen digitalen Möglichkeiten im Blick haben. Mit dem neuen Landesjugendplan sollen zudem die eigenständigen Förderschwerpunkte „Jugendbeteiligung“ und „Stärkung von Medienkompetenz und Mediensicherheit“ eingeführt werden. Die digitale Teilhabe von Kindern und Jugendlichen und angesichts fortschreitender Mediatisierung die Stärkung von Medienkompetenz und -sicherheit sollen so zukünftig stärker berücksichtigt werden. Durch den neuen Förderschwerpunkt „Stärkung von Medienkompetenz und Mediensicherheit“ sollen perspektivisch Projekte initiiert werden, die die Fähigkeiten und Fertigkeiten von Kindern und Jugendlichen, Medien und ihre Inhalte den eigenen Zielen und Bedürfnissen entsprechend sachkundig, verantwortungsvoll, sicher, selbstbestimmt und kreativ zu nutzen, stärken.

Das Medienpädagogische Zentrum (MPZ) ist Partner des Netzwerkes und arbeitet mit zahlreichen Mitgliedern des Netzwerkes über viele Jahre zusammen. Die Unterstützung der Schulen durch außerschulische Partner und die Durchführung von schulspezifischen Veranstaltungen durch das Netzwerk wird ausdrücklich begrüßt.

Zur Unterstützung der schulischen Medienbildung wurde mit Beginn des Schuljahres 2018/2019 wurde in Abhängigkeit von der Anzahl der Schulen in den Landkreisen und kreisfreien Städten eine flächendeckende Multiplikatorenstruktur aufgebaut. Dazu wurden 39 Multiplikatoren im Umfang von 5 Anrechnungstunden an das MPZ teilabgeordnet. 13 der Multiplikatoren übernehmen koordinierenden Aufgaben für die verschiedenen Schularten sowie die Regionen.

Im MPZ werden alle regionalen Aktivitäten über die Regionalbeauftragten für Medienbildung koordiniert. Auch hier erfolgt eine verbesserte Regionalisierung durch die Abordnung von drei weiteren Regionalbeauftragten. Damit stehen je Landkreis ein Ansprechpartner sowie Multiplikatoren zur Verfügung. Jede Schule besitzt ein Zeitkontingent für den Einsatz der Multiplikatoren im Rahmen der schulinternen Fortbildungen.

6.1.4 klickern, spielen, zappen“ - Modulare Fortbildungsreihe für Erzieherinnen und Erzieher

Die Landesregierung bewertet die Zusammenarbeit in der Arbeitsgemeinschaft „Frühkindliche Medienbildung“ des Ministeriums für Soziales, Integration und Gleichstellung, die mit Unterstützung von Herrn Prof. Dr. Roland Rosenstock, dem Lehrstuhlinhaber für Praktische Theologie und Religionspädagogik/Medienpädagogik erfolgte, als gelungen.

Zu 7 Technik und Organisation**7.1 Neue Technologien****7.1.1 Positionspapier „Biometrische Analyse“**

Die Landesregierung teilt die Rechtsauffassung zum Begriff der Biometrie. Nach dieser ist nicht schon allein ein einzelnes Sample, etwa ein Gesichtsbild oder Ähnliches, als biometrisches Datum zu verstehen. Es bedarf darüber hinaus auch eines Abgleiches mit einem entsprechenden Datenbestand, welcher aus der Kombination des bereits vorhandenen Datenbestandes und des beispielweise erfassten Gesichtsbildes eine eindeutige Identifizierung herstellen kann. Bei der bloßen Aufnahme eines Gesichtes durch eine Videokamera etwa kann es sich daher aus Sicht der Landesregierung nicht schon um ein biometrisches Datum handeln, da es zu diesem Zeitpunkt noch zu keiner Identifikation mittels Abgleich mit einem Referenzdatenbestand kam.

7.1.2 Windows 10

Es wird auf die Stellungnahme der Landesregierung unter Punkt 1.1 Nummer 4 verwiesen.

7.1.3 Datenschutzaspekte Künstlicher Intelligenz

Es wird auf die Stellungnahme der Landesregierung unter Punkt 1.1 Nummer 5 verwiesen.

7.1.4 Microsoft Office 365

Es wird auf die Stellungnahme der Landesregierung unter Punkt 1.1 Nummer 6 verwiesen.

7.1.5 Standard-Datenschutzmodell (SDM)

Es wird auf die Stellungnahme der Landesregierung unter Punkt 1.1 Nummer 7 verwiesen.

7.1.6 MV-Serviceportal - das Tor zu digitalen Verwaltung

Es wird auf die Stellungnahme der Landesregierung unter Punkt 1.1 Nummer 8 verwiesen.

7.1.7 Elektronische Akte (eAkte)

Ende 2019 wurde der Anforderungskatalog finalisiert, sodass Anfang Februar 2020 die Beschaffung einer neuen E-Akten-Software auf einer entsprechenden Vergabeplattform europaweit veröffentlicht werden konnte. Mittlerweile ist die erste Phase der Ausschreibung abgeschlossen. Nach Prüfung der Angebote schließt sich eine Teststellung der Anbieterprodukte sowie die Verhandlungsphase an.

Im Anforderungskatalog wurde darauf geachtet, sowohl den Anforderungen der Verordnung (EU) 2016/679 und landesseitiger Datenschutzregelungen als auch den Anforderungen der Barrierefreiheit nach der Richtlinie (EU) 2016/2102 zu entsprechen. Zusätzlich wurde die Neufassung des Sicherheitskonzeptes für den Betrieb des DMS/VBS-DOMEA® gemäß den genannten Anforderungen einschließlich der dazu nötigen technischen und organisatorischen Maßnahmen begonnen. Dieses wird voraussichtlich im Herbst 2020 fertig gestellt werden.

Es ist davon auszugehen, dass voraussichtlich im Frühjahr 2021 der Zuschlag erteilt wird, dem sich eine Pilotierungsphase anschließt. Danach kann der Rollout zunächst in den nachgeordneten Behörden beginnen.

Die Landespolizei beabsichtigt im kommenden Jahr zunächst die Einführung von DOMEA® im Bereich der Verwaltung der Polizei. Eingesetzt werden soll dabei der Landesstandard DOMEA®, sodass unter den Aspekten des Datenschutzes auf die dortige Weiterentwicklung abgestellt wird. Innerhalb der Projektstruktur ist der Landesbeauftragte für den Datenschutz als Berater im Lenkungsausschuss vertreten.

Im Bereich des Polizeivollzuges werden zunächst die notwendigen Anpassungsbedarfe im Rahmen von Prozessuntersuchungen und ersten Gesprächen zur möglichen technischen Umsetzung durchgeführt. Zu gegebener Zeit erfolgt die Einbeziehung des Landesbeauftragten für den Datenschutz, damit bei den Anpassungen die Belange des Datenschutzes in notwendiger Form berücksichtigt werden können. Parallel dazu gibt es im Bereich der Polizei der Länder und des Bundes Bestrebungen zu gemeinsamen IT-Projekten, die auch die „elektronische Akte in Strafsachen“ (EAS) betreffen. In diesem Bereich werden aktuell Überlegungen zu gemeinsamen Projekten auf abstrakter Ebene angestellt, sodass eine Einbeziehung des Landesbeauftragten für den Datenschutz derzeit noch nicht erfolgt ist.

7.1.8 Wenn kein sicheres Passwort verwendet wird

Es wird auf die Stellungnahme der Landesregierung unter Punkt 1.1 Nummer 9 verwiesen.

7.2 Zertifizierung nach der DS-GVO

Es wird auf die Stellungnahme der Landesregierung unter Punkt 1.1 Nummer 10 verwiesen.

7.3 Kommunikation/Neue Medien

7.3.1 Messenger-Dienste im Krankenhaus

Es wird auf die Stellungnahme der Landesregierung unter Punkt 1.1 Nummer 11 verwiesen.

7.3.2 Neue Regeln für Webseitenanbieter

Es wird auf die Stellungnahme der Landesregierung unter Punkt 1.1 Nummer 12 verwiesen.

8 Datenschutz in verschiedenen Rechtsgebieten

8.1 Rechtswesen

8.1.1 Informationsportal „Neutrale Schule“ - AfD stellt Lehrer an den Pranger

Nach dem Verbot des AfD-Portals "Neutrale Schule" durch den Landesbeauftragten für den Datenschutz wurden die Staatlichen Schulämter in geeigneter Weise informiert. Da nicht auszuschließen war, dass - trotz des Verbotes dieses ungeeigneten Instrumentes - personenbezogene Daten verarbeitet wurden, waren die Staatlichen Schulämter aufgefordert, die Lehrkräfte auf ihre Rechte diesbezüglich hinzuweisen.

8.1.4 Betroffenenrechte nach der Datenschutz-Grundverordnung - Eine Herausforderung für Unternehmen und Behörden

Es wird zunächst auf die Stellungnahme der Landesregierung unter Punkt 1.1 Nummer 13 verwiesen.

Darüber hinaus ist die Landesregierung der Auffassung, dass Artikel 15 der Verordnung (EU) 2016/679 nicht den Anspruch auf Kopien der in den Akten eines Verantwortlichen befindlichen Dokumente normiert. Artikel 15 Verordnung (EU) 2016/679 enthält lediglich das Recht auf Erhalt einer Kopie der personenbezogenen Daten des Antragstellers an sich, nicht der Schriftstücke. Die Regelungsrichtung dieser Vorschrift zielt darauf ab, dass der Antragsteller die Möglichkeit auf Kontrolle der über ihn gespeicherten personenbezogenen Daten hat und nicht etwa auf die Möglichkeit amtliche Dokumente oder Zweitschriften zu beschaffen. Anders würde der 15 Verordnung (EU) 2016/679 dazu führen, dass zum Beispiel Ehekunden oder Abschriften aus Geburtenregistern, bestehende Regelungen völlig unterlaufend, kostenfrei über Artikel 15 Verordnung (EU) 2016/679 erwirkt werden könnten. Genauso verhält es sich auch mit Akteneinsichtsrechten sowie dem Recht auf Informationen nach dem Informationsfreiheitsgesetz. Auch insoweit würde die Auffassung des Landesbeauftragten für den Datenschutz dazu führen, dass die gesonderten Rechtsvorschriften gegenstandslos würden, einschließlich entsprechender Gebührentatbestände.

8.1.6 Stetiger Meldedatenabgleich für den Rundfunkbeitrag

Es wird auf die Stellungnahme der Landesregierung unter Punkt 1.1 Nummer 14 verwiesen.

8.2 Polizei/Ordnungswesen

8.2.1 Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommern (SOG M-V)

Die Landesregierung teilt die geäußerte Kritik an der Verständlichkeit und Vollziehbarkeit der Vorschriften im neuen Sicherheits- und Ordnungsgesetz in dieser Form nicht.

Die Komplexität des Sicherheits- und Ordnungsgesetzes ist maßgeblich begründet durch die aufgrund der europäischen Datenschutzvorschriften sowie der aktuellen Rechtsprechung des Bundesverfassungsgerichts vorzunehmenden Anpassungen und Umsetzungen. Abgesehen von dem als Auffangnorm fungierenden § 3 des Landesdatenschutzgesetzes wurden vom Landesgesetzgeber bewusst - und damit anders als beim Bund und in anderen Bundesländern (siehe etwa Bundesdatenschutzgesetz, Bayerisches Polizeiaufgabengesetz/Bayerisches Datenschutzgesetz, Hessisches Gesetz über die öffentliche Sicherheit und Ordnung/Hessisches Datenschutzgesetz) - keine Vorschriften im Landesdatenschutzgesetz zur Umsetzung der Richtlinie (EU) 2016/680 geschaffen. Deren konkrete Umsetzung im Land Mecklenburg-Vorpommern sollte im jeweiligen (Landes-)Fachrecht mit einem entsprechend größeren Regelungsaufwand vorgenommen werden. Demzufolge sind im Gefahrenabwehrrecht des Landes und damit im Sicherheits- und Ordnungsgesetz spezielle Regelungen aufzunehmen, die die Datenverarbeitung im Anwendungsbereich der Richtlinie (EU) 2016/680 erfassen und damit den Willen des EU-Richtliniengabers in nationales Recht umsetzen. Dies ist mit dem vorgelegten Entwurf zur Neufassung des Sicherheits- und Ordnungsgesetzes geschehen.

Die Landesregierung befürwortet grundsätzlich klare und verständliche gesetzliche Regelungen. Im Gesetzgebungsprozess müssen aber auch die Anforderungen des Bundesverfassungsgerichts an die Bestimmtheit einer gesetzlichen Regelung beachtet werden. Im Sicherheits- und Ordnungsgesetz wird eine hochkomplexe Rechtsmaterie in abstrakt genereller Weise für eine Vielzahl von unterschiedlichen Lebenssachverhalten geregelt. Zu deren Verständnis ist selbstverständlich auch die Gesetzesbegründung heranzuziehen. Auch der plakativ kritisierte § 25 des Sicherheits- und Ordnungsgesetzes ist bei einem hinreichenden Verständnis der Regelungssystematik des neuen Sicherheits- und Ordnungsgesetzes ohne Weiteres zu verstehen.

Im Übrigen erfordert die gesamte Rechtsmaterie schon immer eine umfangreiche Schulung der Beamtinnen und Beamten, die von der FHÖVPR M-V bereits geleistet wird.

Die Landesregierung teilt auch nicht die Kritik an den Regelungen zu den Befugnissen der Aufsichtsbehörde im Anwendungsbereich der Richtlinie (EU) 2016/680. Anders als die Verordnung (EU) 2016/679 enthält die vorgenannte Richtlinie ausdrücklich „nur“ beispielhaft genannte, mögliche Abhilfebefugnisse. Abgestellt wird vielmehr auf die Regelung wirksamer Abhilfebefugnisse, wobei auch zu beachten ist, dass die Sicherheitsbehörden ausnahmslos an Recht und Gesetz gebunden sind. Damit ist es nicht zwingend geboten, alle Befugnisse aus der Verordnung (EU) 2016/679 in den Anwendungsbereich der Richtlinie zu übernehmen. Auch andere Bundesländer, wie zum Beispiel Thüringen (siehe § 7 des Thüringer Datenschutzgesetzes) oder auch Bayern (siehe Artikel 34 Absatz 1 des Bayerischen Datenschutzgesetzes), sehen eingeschränkte Abhilfebefugnisse vor. Die Regelung des § 48b des Sicherheits- und Ordnungsgesetzes schließt weder eine Beratung noch eine Verwarnung aus.

Ebenso sind Anordnungen möglich, denn Absatz 2 spricht ausdrücklich von weitergehenden Maßnahmen in Bezugnahme auf die in Absatz 1 ausdrücklich genannten Befugnisse. Ausdrücklich ausgeschlossen wird letztlich „nur“ die Anordnung einer Löschung von Daten der Sicherheitsbehörden, um die Aufgabe der Gefahrenabwehr im Einzelfall nicht zu gefährden. Auch hierzu wird eine umfassende Begründung im Entwurf gegeben.

Der Regelung zur sogenannten Onlinedurchsuchung in § 33c des Sicherheits- und Ordnungsgesetzes fehlt es auch nicht an verfassungsrechtlich hinreichenden Vorkehrungen auf der Ebene des nachgelagerten Kernbereichsschutzes. Übersehen wird hier seitens des Landesbeauftragten für den Datenschutz, dass § 26a Absatz 5 des Sicherheits- und Ordnungsgesetzes („Soweit in diesem Gesetz nichts Besonderes geregelt ist [...]“) nicht einschlägig ist, weil § 33c Absatz 9 des Sicherheits- und Ordnungsgesetzes eine spezielle Regelung für den nachgelagerten Schutz enthält. Dort heißt es: „Das anordnende Gericht ist über den Verlauf und die Ergebnisse zu unterrichten; es entscheidet unverzüglich über die Rechtmäßigkeit der Datenverarbeitung. Sofern die Voraussetzungen der Anordnung nicht mehr vorliegen, ordnet es die Beendigung der Maßnahme an, soweit diese nicht bereits durch die Leitung der zuständigen Polizeibehörde veranlasst wurde.“

Entsprechende Protokollierungsvorschriften enthalten die §§ 46e und 46f des Sicherheits- und Ordnungsgesetzes.

Auch die Kritik des Landesbeauftragten für den Datenschutz an der Regelung zur automatischen Kennzeichenerfassung teilt die Landesregierung nicht. § 43a des Sicherheits- und Ordnungsgesetzes normiert für Kennzeichenkontrollen zur vorbeugenden Bekämpfung der grenzüberschreitenden Kriminalität oder zur Unterbindung des unerlaubten Aufenthalts eindeutig das Gebiet „von der Bundesgrenze bis einschließlich der Bundesautobahn A 20“. Die Norm legt damit ein Gebiet mit einem ausdrücklichen und eindeutigen örtlichen Bezug zur Grenze fest, womit den spezifischen geografischen Gegebenheiten des Landes Mecklenburg-Vorpommern und der Bedeutung der Autobahn 20 für den grenzüberschreitenden Verkehr Rechnung getragen wird. Die Festlegung einer kilometermäßigen Begrenzung hat das Bundesverfassungsgericht nicht gefordert. Kfz-Kennzeichenkontrollen zur vorbeugenden Bekämpfung der grenzüberschreitenden Kriminalität oder zur Unterbindung des unerlaubten Aufenthalts auf Durchgangsstraßen außerhalb dieses konkret festgelegten, grenzbezogenen Gebietes sind somit nicht zulässig. Die Orte für gefahrenabwehrrechtliche Kfz-Kennzeichenkontrollen im Land sind also in einer den Bestimmtheitsanforderungen genügenden Weise bestimmt, da ein konsequenter und klar bestimmbarer Grenzbezug sichergestellt wird, sodass die vom Bundesverfassungsgericht bei den Ländern Bayern, Hessen und Baden-Württemberg gerügte Möglichkeit von Kontrollen innerhalb des gesamten Landes hier gerade nicht besteht. Hinzu kommt, dass der flächendeckende Einsatz (in diesem Gebiet) nach § 43a Absatz 1 Satz 5 des Sicherheits- und Ordnungsgesetzes nicht erlaubt ist.

8.2.2 Videoüberwachung Marienplatz

In seinem Fünfzehnten Tätigkeitsbericht nimmt der Landesbeauftragte für den Datenschutz Stellung zu den rechtlichen Aspekten der Verordnung (EU) 2016/679 und stellt die Genese des Aufbaus der Bildüberwachung Marienplatz bis hin zur gerichtlichen Güteverhandlung dar, in dessen Ergebnis keine Veranlassung mehr für ein förmliches Gerichtsverfahren gesehen wurde. Es wird herausgestellt, dass sich das Ministerium für Inneres und Europa an die bei Gericht geschlossene Vereinbarung bezogen auf die notwendige Verschlüsselung gehalten hat.

Der Bericht nimmt Bezug auf einen Erfahrungsbericht der Polizeiinspektion Schwerin, wonach sich die Erwartungen nicht bestätigt hätten, dass durch die Bildüberwachung Personen von der Begehung strafbarer Handlungen abgehalten würden. Daneben wird aber auch auf die erhöhte Aufklärungsquote bei Straftaten im Bereich des Marienplatzes abgestellt.

Der Landesbeauftragte für den Datenschutz kündigt an, auch zukünftig die Auswirkungen der Bildüberwachung auf dem Marienplatz auf das Straftatenaufkommen und die Aufklärungsquote im Blick zu haben.

Aus einsatztaktischer Sicht hat sich der Einsatz der Bildüberwachung Marienplatz, wie vom Landesbeauftragten für den Datenschutz dargestellt, bewährt. Es ist festzustellen, dass insbesondere seit der Installation der Bildüberwachung und der Umsetzung der bisherigen Präsenzkonzepte eine deutliche Beruhigung der Lage 2018 gegenüber der Lage 2015 bis 2017 eingetreten ist. Die Straftaten am Marienplatz sind bis 2018 deutlich zurückgegangen.

8.2.3 Einsatz von Bodycams bei der Polizei

Es wird auf die Stellungnahme der Landesregierung unter Punkt 1.2 Nummer 5 verwiesen.

8.2.4 Bußgeldverfahren gegen Polizisten

Wie bereits in der Stellungnahme der Landesregierung zum Vierzehnten Tätigkeitsbericht des Landesbeauftragten für den Datenschutz gemäß Artikel 59 der Verordnung (EU) 2016/679 mitgeteilt, ist die Sicherstellung der datenschutzrechtlichen Vorgaben und der Umgang mit den Daten der Bürgerinnen und Bürger in der Landespolizei durch organisatorische, technische und dienstaufsichtliche Maßnahmen gewährleistet und findet als wesentlicher Teil in der Aus- und Fortbildung der Beschäftigten der Landespolizei Beachtung. Jeder Zugriff auf polizeiliche Informationssysteme wird durchgehend protokolliert. Sollte dennoch unberechtigt Zugriff genommen werden, lässt sich dies durch die Protokollierung nachweisen und die Beschuldigten können festgestellt werden.

Die Anzahl der benannten geführten Verfahren beim Landesbeauftragten für den Datenschutz kann im Detail nicht nachvollzogen werden. So ist die Rede von insgesamt 16 Verfahren, die geführt wurden und werden, sodass offenbar auch Altfälle erfasst wurden. Wie bereits in der Stellungnahme im Vorjahr mitgeteilt, ist eine konsequente dienstrechtliche Ahndung etwaiger Datenschutzverstöße durch Bedienstete unter Ausnutzung ihrer dienstlichen Stellung nur möglich, wenn die jeweiligen Aufsichtsbehörden Kenntnis von den Sachverhalten haben. Dies ist jedoch dann nicht der Fall, wenn sich eine betroffene Person nur an den Landesbeauftragten für den Datenschutz wendet. Es ist hier zu keiner Änderung in der Verwaltungspraxis gekommen, sodass weiterhin die Landesregierung den Landesbeauftragten für den Datenschutz in der Pflicht sieht, den Dienstherrn über den Sachverhalt auf Grundlage der vorhandenen Mitteilungsmöglichkeiten im Rahmen eines Ordnungswidrigkeitenverfahrens zu informieren.

Nicht nachvollzogen werden kann die Aussage, dass die geführten 16 Verfahren „als Spitze des Eisberges“ betrachtet werden. Mit keiner nachvollziehbaren Begründung oder einem Beweis für diese Aussage werden damit alle Bediensteten der Landespolizei Mecklenburg-Vorpommern pauschal diskreditiert und das Ansehen der Landespolizei in der Bevölkerung herabgesetzt.

In einem Presseartikel der Ostsee-Zeitung vom 22. Juli 2020 wird der Landesbeauftragte für den Datenschutz wie folgt zitiert: „Ein Missbrauch von personenbezogenen Daten durch die Polizei geht gar nicht“, so Heinz Müller. „Hier beschädigt eine verhältnismäßig kleine Anzahl von Missetätern den Ruf einer ganzen Institution. Darauf sind viele Polizisten zu Recht sauer.“ Er persönlich habe das Gefühl, dass das Interesse der Polizeiführung groß sei, diese „schwarzen Schafe“ ausfindig zu machen, „einen Großteil der Hinweise auf mögliche Datenschutzverstöße bekomme ich übrigens aus der Polizei selbst“, sagt er.“

Hier trifft der Landesbeauftragte für den Datenschutz selbst eine reflektierte Aussage zur Thematik und würdigt auch die Kontrollmechanismen innerhalb der Landespolizei. Eine ebenso differenzierte Aussage lässt der Fünfzehnte Tätigkeitsbericht vermissen.

8.3 Justiz

8.3.1 Justizvollzugsdatenschutzgesetz

Die Kritik an den Regelungen zu den Befugnissen des Landesbeauftragten für den Datenschutz im Entwurf des Justizvollzugsdatenschutzgesetzes Mecklenburg-Vorpommern (E-JVollzDSG M-V) wird nicht geteilt. Anders als die unmittelbar geltende Verordnung (EU) 2016/679 gesteht die Richtlinie (EU) 2016/680 den Mitgliedstaaten insbesondere bei der Ausgestaltung der Abhilfebefugnisse der Datenschutzaufsichtsbehörde einen Gestaltungsspielraum zu, indem in Artikel 47 der Richtlinie (EU) 2016/680 lediglich exemplarisch bestimmte Abhilfebefugnisse genannt werden, ohne hiermit einen zwingenden Umsetzungsbefehl zu verknüpfen.

Die Regelungsaufträge der Artikel 46, 47 der Richtlinie (EU) 2016/680, wonach die unabhängige Aufsichtsbehörde bestimmte Aufgaben wahrzunehmen hat und ihr wirksame Untersuchungs-, Abhilfe- und Beratungsbefugnisse zustehen müssen, werden im Entwurf des Justizvollzugsdatenschutzgesetzes Mecklenburg-Vorpommern mit § 58 umgesetzt. Diese Vorschrift gibt der oder dem Landesbeauftragten für den Datenschutz zunächst die Möglichkeit des Ausspruchs der Warnung und Verwarnung. Darüber hinaus bestehen Untersuchungs-, Beratungs- und Beanstandungsbefugnisse. Nach § 58 Absatz 3 des Entwurfs des Justizvollzugsdatenschutzgesetzes Mecklenburg-Vorpommern kann der oder die Landesbeauftragte für den Datenschutz die Behebung datenschutzrechtlicher Verstöße binnen angemessener Frist einfordern. Bei Nichtbehebung können vom Justizministerium Mecklenburg-Vorpommern als Aufsichtsbehörde geeignete Maßnahmen gefordert werden. Kommt es auch hier nicht zur gewünschten Abhilfe, kann die Landesregierung verständigt werden. § 58 Absatz 2 des Entwurfs des Justizvollzugsdatenschutzgesetzes Mecklenburg-Vorpommern eröffnet sodann die Möglichkeit, weitergehende Anordnungen zu treffen.

Unter Berücksichtigung der vorgenannten Befugnisse gibt § 58 des Entwurfs des Justizvollzugsdatenschutzgesetzes Mecklenburg-Vorpommern der oder dem Landesbeauftragten für den Datenschutz damit einen hinreichend wirkungsvollen Abhilfemechanismus an die Hand. Insoweit orientiert sich der Gesetzentwurf im Interesse einer im Bundesland einheitlichen Umsetzung der Richtlinie (EU) 2016/680 an der Ausgestaltung der Befugnisse der oder des Landesbeauftragten für den Datenschutz des im Juni 2020 in Kraft getretenen Sicherheits- und Ordnungsgesetzes.

8.3.2 Kopie der Prüfungsakte des Landesjustizprüfungsamtes

Die Rechtsfrage, ob die Prüfungsämter nach Maßgabe der Verordnung (EU) 2016/679 verpflichtet sind, den Prüflingen über das nach den einschlägigen landesrechtlichen Vorschriften (hier: §§ 33 Absatz 3 sowie 53 Absatz 2 und 3 Juristenausbildungs- und Prüfungsordnung) vorgesehene Akteneinsichtsrecht hinaus auf Antrag eine kostenfreie Erstkopie der Prüfungsakte zur Verfügung zu stellen, wurde und wird von den zuständigen Behörden der Bundesländer unterschiedlich beantwortet und ist in der Rechtsprechung der Verwaltungsgerichte auch weiterhin nicht abschließend geklärt. Das Landesjustizprüfungsamt Mecklenburg-Vorpommern hat gleichwohl von einer gerichtlichen Überprüfung der Anordnung des Landesbeauftragten für den Datenschutz abgesehen. Den Prüflingen werden seitdem trotz des damit verbundenen erheblichen Verwaltungsaufwands kostenlose Erstkopien ihrer Prüfungsakten zur Verfügung gestellt.

8.4 Gesundheitswesen

8.4.1 Digitale Anwendungen und datenschutzrechtliche Verantwortlichkeiten

und

8.4.2 Projekt „Umgang mit Patientendaten in den Krankenhäusern Mecklenburg-Vorpommerns

Die Landesregierung nimmt die Informationen und Empfehlungen zur Kenntnis. Der Abschlussbericht zum Umgang mit den Patientendaten in den Krankenhäusern wurde der Krankenhausgesellschaft Mecklenburg-Vorpommern zur Verfügung gestellt.

8.7 Schule/Bildung

8.7.1 Integriertes-Schulmanagement-System (ISY)

Das Ministerium für Bildung, Wissenschaft und Kultur begrüßt die konstruktive Zusammenarbeit und beratende Unterstützung des Landesbeauftragten für den Datenschutz. Dadurch können wesentliche Grundlagen für die Umsetzung der datenschutzrechtlichen Anforderungen bereits bei der Planung der verschiedenen Softwaremodule des Integrierten Schulmanagementsystems Mecklenburg-Vorpommern berücksichtigt und erarbeitet werden.

Aufgrund des ISY-Projektfortschritts ergibt sich ein erhöhter Abstimmungsbedarf zum Datenschutz. Diesem wird seit Anfang 2020 durch monatliche Gespräche Rechnung getragen.

8.7.2 Bring Your Own Device (BYOD) im Schulbereich

Im Themenpunkt „Bring Your Own Device (BYOD) im Schulbereich“ geht es vor allem darum, dass Lehrkräfte ihre privaten Datenverarbeitungsanlagen der Schule für deren Aufgabenerfüllung zur Verfügung stellen.

Hierzu ist ein Hinweisschreiben zur Thematik „Handreichung zum Umgang mit den datenschutzrechtlichen Regelungen nach §§ 70 - 72 Schulgesetz“ an die Schulleiterinnen und Schulleiter entsandt worden. Hierin werden ausführliche Aussagen zur Problematik „Benutzung von privaten Datenverarbeitungsanlagen“ getroffen.

Darüber hinaus gab es notwendige Hinweise im Rahmen der „Corona-Krise“.

8.9 Kommunales

8.9.2 Verweigerung von Auskunftsansprüchen

Der im Tätigkeitsbericht geschilderte Vorfall ist hier nicht bekannt. Jedoch gab es in der Vergangenheit im Rahmen des Petitionsrechtes Eingaben an das Ministerium für Inneres und Europa mit der Bitte um Unterstützung im Rahmen eines Auskunftsersuchens gegenüber einer Landkreisverwaltung. In diesen Fällen, die sich alle auf die Verordnung (EU) 2016/679 stützten und bei denen ein Verstoß seitens der Kommune erkannt wurde, wurde diese durch die oberste Rechtsaufsicht zur Einhaltung ihrer rechtlichen Verpflichtungen aufgefordert. Sollte einer solchen Aufforderung nicht Folge geleistet werden, besteht die Möglichkeit, den Einsatz weiterer rechtsaufsichtlicher Mittel zu prüfen und diese gegebenenfalls anzuwenden.

8.9.3 Nutzung von Drohnen zu behördlichen Zwecken

Das Ministerium für Inneres und Europa hat im August 2014 ein umfangreiches Rechtsgutachten für den Einsatz von Drohnen durch die Landespolizei erstellt. Auf dieses wird hinsichtlich aller Fragen zum Sicherheits- und Ordnungsgesetz, zur Strafprozessordnung und zum Versammlungsrecht verwiesen. Auch in Bezug auf das Luftfahrtrecht gelten die dort enthaltenen Grundaussagen.

8.9.5 Vertraulichkeit bei Übermittlungen von E-Mails

Die Hinweise sind nachvollziehbar. Grundsätzlich ist zu unterscheiden zwischen der Authentifizierung und Autorisierung. Eine konsequente Authentifizierung mittels öffentlich signierter Zertifikate ist maßgeblich für die Wahrung der Integrität von Daten und Absender und sollte insbesondere konsequent im Austausch mit dem Bürger erfolgen. Als Beispiel sind Einstellungsverfahren zu nennen. Die Kommunikation mit dem Bewerber sollte möglichst immer mit zertifizierten Absende-Adressen des Mitarbeiters einer öffentlichen Verwaltung erfolgen.

Im weiteren Schritt ist die Gewährleistung der Autorisierung zu gewährleisten. Dies ist implizit die Betrachtung der Vertraulichkeit. Hat derjenige das Recht die Nachricht zu lesen ist dabei die Grundfrage. Diese Lösung geht derzeit immer noch mit Mehraufwänden bei den Bürgern einher. Diese müssen ihre E-Mail-Clients entsprechend eingerichtet haben, damit eine Verschlüsselung der Nachricht erfolgen kann. Dies ist in den meisten Fällen nicht gegeben. Alternativ wird als Mindeststandard vorausgesetzt, dass die Verschlüsselung zwar nicht Ende-zu-Ende erfolgt, aber zumindest zwischen den E-Mail-Servern. Für die Server der öffentlichen Einrichtungen kann dies in der Regel zugesichert werden. Nutzt der Bürger aber kostenlose E-Mail-Dienste von frei verfügbaren Providern, ist dies meist nicht mehr der Fall.

Eine weitere Variante ist es sensible Daten (unter anderem personenbezogene Daten) verschlüsselt per komprimierter Datei (zum Beispiel ZIP) zu versenden. Jedoch stellt dies ein Interessenskonflikt mit der IT-Sicherheit da, da die Inhalte vorab nicht mehr durch Antiviren-Software geprüft werden kann.

Es bleibt daher nur die Möglichkeit, gegebenenfalls vorab die Zustimmung des unverschlüsselten Versandes von Daten beim Bürger einzuholen, falls dieser einen „unsicheren“ E-Mail-Provider nutzt.

Eine perspektivische möglichst landesweite zentrale Lösung wäre es ein hybrides System aufzusetzen, welches neben einer Digitalen Signierung auch die Verschlüsselung zum Bürger übernimmt. Der Bürger kann dann per eigenem Zugang den Inhalt verschlüsselt herunterladen und erhält per E-Mail nur Informationen, dass neue Daten vorliegen. Dies wäre jedoch auch mit einem zusätzlichen Aufwand auf Seiten des Bürgers verbunden, da er einen Account anlegen müsste, jedoch könnten über diesen Zugang mehrere Services (auch im Sinne des Onlinezugangsgesetzes) angeboten werden, sodass hier eine deutliche Steigerung der Motivation erfolgen würde.

Zur Sensibilisierung und zur sicheren Kommunikation mit den Kommunen wurden Anfang des Jahres 2020 zwei Runderlasse herausgegeben. Diese richten sich an die Landkreise, die kreisfreien und großen kreisangehörigen Städte, sowie die unteren Rechtsaufsichtsbehörden und geben Hinweise zur Verordnung (EU) 2016/679, zu sicheren Kommunikationswegen und weitere Empfehlungen.

Zu 9 Informationsfreiheitsgesetz Mecklenburg-Vorpommern - IFG M-V

9.1 Informationsfreiheit in Mecklenburg-Vorpommern - Bedeutung, Zahlen, Fakten

Es wird auf die Stellungnahme der Landesregierung unter Punkt 1.1 Nummer 16 verwiesen.

9.6 Keine Zuständigkeit des Landesbeauftragten für Informationsfreiheit bei Informationen nach dem Verbraucherinformationsgesetz

Die Zuständigkeit für die Umsetzung des Verbraucherinformationsgesetzes liegt im Ministerium für Landwirtschaft und Umwelt. Die Mehrzahl der Anfragen nach dem Verbraucherinformationsgesetz zielen auf Kontrollberichte der Lebens- und Futtermittelüberwachung durch die Veterinär- und Lebensmittelüberwachungsämter bei den Landkreisen und kreisfreien Städten (= auskunftspflichtige Stellen) ab.

9.10 Herausgabe von Abituraufgaben der vergangenen Jahrgänge über das Portal FragDenStaat

Die Darstellung des Landesbeauftragten für Informationsfreiheit hinsichtlich der zeitlichen Abläufe treffen so zu. Als Wikimedia sich in diesen Vorgang eingeschaltet und auch angekündigt hatte, dass eine große Anzahl von Aufgabenabforderungen auf das Ministerium für Bildung, Wissenschaft und Kultur zukommen werde, stieg die Zahl der Anfragen erheblich an.

Gemeinsam mit dem Institut für Qualitätsentwicklung Mecklenburg-Vorpommern (IQ M-V) wurde seinerzeit an einer Strategie gearbeitet, die (Abitur-) Prüfungsaufgaben den Schülerinnen und Schülern des Landes über die Lehrkräfte in den jeweils einschlägigen Schularten zur Verfügung zu stellen ohne den teilweise für diesen kostenpflichtigen Umweg über Veröffentlichungen auf dem freien Markt, die sich aus den Zusendungen auch der an uns gerichteten Anfragen speisen konnten.

Letztlich wurde der Weg gewählt, den Anfragenden die Prüfungsaufgaben zur Verfügung zu stellen. Sie erhielten (und erhalten auch aktuell) einen Bescheid, der allerdings mit der Auflage verbunden ist, diese weder gewerblich zu nutzen noch die Aufgaben zu veröffentlichen.

Mit dieser Vorgehensweise wurde somit ein Weg gewählt, das Begehren der Anfragenden zu erfüllen, aber gleichzeitig den von Seiten des IQ M-V erwünschten Effekt der kostenfreien Zurverfügungstellung zu erreichen.

Parallel dazu wurde beim für die Länder der Bundesrepublik zuständigen Verhandlungsführer mit den Verwertungsgesellschaften nachgefragt, inwieweit dieser eine Verfahrensweise, wie sie vom Ministerium für Bildung, Wissenschaft und Kultur intendiert ist, für vereinbar mit den Vereinbarungen des Gesamtvertrags über die Abgeltung urheberrechtlicher Ansprüche hält. Diese Antwort erhielt das IQ M-V aufgrund eines Verwaltungsversehens (im Bayerischen Ministerium für Unterricht und Kultus) erst jetzt. Von dort aus wurde die hier intendierte Vorgehensweise voll umfänglich für rechtmäßig gehalten.

All diese Verfahren, die parallel durchgeführt worden sind, kosteten Zeit. Zeit, die nun als Verzögerungen im Bericht des Landesbeauftragten für Informationsfreiheit moniert worden sind. Diese Zeit war aber notwendig, da nur ein rechtmäßiger Bescheid die vorliegenden Interessen der Anfragenden, aber auch der Verwaltung wahren konnte.

9.12 Bereitstellung von Informationen durch reine Addition gleichartiger Informationen ist kein Ausschlusskriterium

Das Verwaltungsgerichtsurteil wurde allen Finanzämtern des Landes zur Kenntnis gegeben.