

UNTERRICHTUNG

durch die Landesregierung

Stellungnahme der Landesregierung zum Sechzehnten Tätigkeitsbericht des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern

Berichtszeitraum zum Datenschutz: 1. Januar 2020 bis 31. Dezember 2020

Allgemeines

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern hat als Landesbeauftragter für den Datenschutz für den Berichtszeitraum vom 1. Januar 2020 bis zum 31. Dezember 2020 seinen Sechzehnten 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, vorgelegt (siehe Drucksache 7/6311).

Die Pflicht der Landesregierung, dem Landtag innerhalb von sechs Monaten nach Vorlage des Berichts ihre Stellungnahme zuzuleiten, ergibt sich aus § 21 des Landesdatenschutzgesetzes.

Wie auch bei früheren Tätigkeitsberichten verknüpft der Tätigkeitsbericht gemäß Artikel 59 der 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.

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 als Landesbeauftragter für den Datenschutz bezeichnet.

Einleitung

Der Berichtszeitraum des Sechzehnten Tätigkeitsberichtes des Landesbeauftragten für den Datenschutz umfasst das gesamte Kalenderjahr 2020 und damit das zweite vollständige Jahr nach Geltung des neuen europäischen Datenschutzrechts.

Auch aus Sicht der Landesregierung war das zentrale Ereignis des Berichtszeitraumes die Corona-Pandemie. Bei der Bewältigung der damit verbundenen Herausforderungen, wie zum Beispiel die Handlungsfähigkeit der Verwaltung sicherzustellen, lag das Handlungsfeld „Datenschutzrecht“ stets im Blickfeld der Landesregierung.

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

Zu 0 Empfehlungen

Zu 0.1 Zusammenfassung aller Empfehlungen

Stellungnahmen der Landesregierung finden sich bei den laufenden Nummern, auf die sie sich beziehen. Insoweit wird die Gliederung des Berichts des Landesbeauftragten für den Datenschutz zugrunde gelegt.

Zu 0.2 Umsetzung der Empfehlungen des Fünfzehnten Tätigkeitsberichtes

Zu Nummer 1

Die Stellungnahme der Landesregierung findet sich unter 3.1.

Zu Nummer 2

Die Stellungnahme der Landesregierung findet sich unter 4.3.2.

Zu Nummer 5

Die im Bericht ausgewiesene Einlassung der Landesregierung zum 15. Tätigkeitsbericht zur Nutzung von KI-Systemen ist weiterhin gültig. Derzeit befinden sich also nach wie vor keine KI- bzw. KI-gestützten Systeme innerhalb der Landesregierung im Einsatz oder in der Planung.

Zu Nummer 6

Eine Überprüfung möglicher Open Source Möglichkeiten ist im MV-PC-Projekt der Landesregierung integriert (siehe auch 7.2 und 7.3).

Zu Nummer 8

Die notwendige Rechtsgrundlage für die Einrichtung und Registrierung von Nutzerkonten ist die Landesverordnung über die Bereitstellung, Ausgestaltung und Nutzung von E-Government-Basisdiensten im Land Mecklenburg-Vorpommern (BasDi LVO M-V), welche ein aufeinander abgestimmtes, kompatibles Dienstangebot zur Erbringung digitaler Verwaltungsleistungen für Bürgerinnen und Bürger und für die Wirtschaft beinhaltet. Diese Landesverordnung ist veröffentlicht im GVOBl. M-V 2021, S. 1356 ff.

Zu Nummer 12

Die Internetpräsenz der Landesregierung befindet sich aus Sicht der Landesregierung auf einem Stand, der die aktuellen datenschutzrechtlichen Vorgaben berücksichtigt. Nichtsdestotrotz verfolgt die Landesregierung hierzu die Entwicklungen und Erkenntnisse, um sich weiterhin stetig am Stand der Technik zu orientieren.

Zu Nummer 13

Auf die Gewährleistung und Beachtung der Betroffenenrechte wurde in Hausverfügungen und ergänzenden Informationen und Belehrungen gegenüber den Beschäftigten bereits seit dem Jahre 2018 nachdrücklich und fortlaufend hingewiesen. Der Umgang mit den Betroffenenrechten erfolgt daher entsprechend verordnungskonform.

Zu 1 Zahlen und Fakten

Auch aus Sicht der Landesregierung war das zentrale Ereignis des Berichtszeitraumes die Corona-Pandemie. Bei der Bewältigung der damit verbundenen Herausforderungen, wie zum Beispiel die Handlungsfähigkeit der Verwaltung sicherzustellen, lag das Handlungsfeld „Datenschutzrecht“ stets im Blickfeld der Landesregierung. Vor diesem Hintergrund bedauert die Landesregierung ebenfalls, dass zahlreiche Veranstaltungen mit Datenschutzbezug ausfallen mussten.

Zu 2 Entwicklung der Behörde

Soweit der Landesbeauftragte für den Datenschutz darauf hinweist, dass die Staatsanwaltschaften ihre Akten zur Prüfung in Papier einreichen, entspricht dies unter Berücksichtigung der gesetzlichen Vorgaben dem Stand der Digitalisierung im Ministerium für Justiz, Gleichstellung und Verbraucherschutz. Bezüglich der Akten für die Justizverwaltung wird die elektronische Übersendung mit der Einführung der eGov-Suite von Fabasoft mittelfristig möglich sein, in Strafsachen ist die Einführung der elektronischen Akte für das Jahr 2024 geplant. Grundsätzlich ist in Einzelfällen die elektronische Bereitstellung von Papierakten nach Einscannen über einen sicheren Übermittlungsweg aber auch jetzt bereits möglich.

Zu 3 Zusammenarbeit auf Europäischer Ebene

Zu 3.1 Europäischer Datenschutzausschuss

Der Bundesrat hat am 25. Juni 2021 Herrn Prof. Dr. Thomas Petri (bayerischer Beauftragter für den Datenschutz) als Stellvertreter für den gemeinsamen Vertreter im Europäischen Datenschutzausschuss gewählt.

Zu 3.3 Technology Subgroup

Soweit der Landesbeauftragte für den Datenschutz moniert, dass die Landesregierung nach wie vor dem gesteigerten Arbeitsaufwand nicht ausreichend Rechnung trage, weist die Landesregierung auf die alleine Verantwortung des Landtages für die Stellen- und Sachmittelausstattung des Landesbeauftragten für den Datenschutz hin. Darüber hinaus verweist die Landesregierung auf ihre Stellungnahme zu Nummer 3 zum 15. Tätigkeitsbericht (Drucksache 7/5665).

Zu 3.5 Erarbeitung von Leitlinien

Die Landesregierung ist der Auffassung, dass das Recht auf Auskunft nach Artikel 15 der Verordnung (EU) 2016/679 nicht grundsätzlich das physische Erstellen einer Kopie des konkreten Aktenblattes umfasst. Vielmehr kann das Auskunftsbegehren eines Antragstellers auch dadurch erfüllt werden, dass eine Kopie einer Datenauflistung gemäß dem Katalog des Artikel 15 Absatz 1 beziehungsweise Absatz 2 der Verordnung (EU) 2016/679 zur Verfügung gestellt wird. Ziel des Rechts auf Auskunft ist es nämlich, einer betroffenen Person zu ermöglichen, grundsätzlich über die Verwendung ihrer Daten selbst zu bestimmen. Dieses Recht umfasst daher auch die Kontrollmöglichkeit einer betroffenen Person gegenüber einem Verantwortlichen. Die beschriebene Verfahrensweise garantiert aus Sicht der Landesregierung einer betroffenen Person in einem ersten Schritt, dieses Kontrollrecht effektiv wahrzunehmen und sorgt einerseits gleichzeitig dafür, dass der Schutz der Persönlichkeitsrechte Dritter, deren personenbezogene Daten mit den Daten einer betroffenen Person verbunden sein können, gewahrt bleibt und andererseits dafür, dass Auskunftsrechte nicht rechtsmissbräuchlich angewendet werden, indem versucht wird, Zweitschriften von Dokumenten zu erlangen, die normalerweise Gebührentatbeständen unterlägen. Das Auskunftsrecht wird insgesamt dabei nicht in seinem Wesensgehalt angetastet.

Die Rechtsprechung und auch die Aufsichtsbehörden der Länder, sind sich in ihrer Sichtweise ebenfalls uneinig. Gerichte befürworten nach derzeitigem Stand lediglich in wenigen Einzelfallentscheidungen, dass eine physische Kopie des konkreten Aktenblattes zur Erfüllung des Auskunftsrechts erforderlich war; sie unterlassen es bei all diesen Entscheidungen aber zu klären, was grundsätzlich unter dem Begriff der „Kopie“ im Sinne des Artikel 15 der Verordnung (EU) 2016/679 verstanden werden soll.

Nach Auffassung der Landesregierung sollte diese Frage wegen der großen Uneinigkeit vom Normengeber selbst geklärt werden. Hierfür sieht die Landesregierung es als erforderlich an, dass der Europäische Datenschutzausschuss diese Frage thematisiert und die Regelung anwendungsfehlerfrei auslegt. Die Landesregierung würde es auch begrüßen, wenn Gerichte diese Thematik in einem geeigneten Fall dem Europäischen Gerichtshof zur Klärung vorlegen würde.

Zu 3.6 Das Schrems-II-Urteil des EuGH

Als Reaktion auf die Vorgaben aus dem Urteil des Europäischen Gerichtshofs in der Rechtsache C-311/18 „Schrems II“ hat die Landesregierung im Hinblick auf die zum Einsatz gebrachten Betriebssysteme, Büro-Anwendungen und Videokonferenzen eventuelle Datentransfers in Drittländer einer Überprüfung unterzogen. Im Ergebnis kann festgestellt werden, dass diese Anwendungen und Systeme in einem kontinuierlichen Prozess sicherheitstechnischen Analysen und Prüfungen unterzogen werden. Bei diesen Prüfungen werden die Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) sowie die Entschlüsse der Datenschutzkonferenz berücksichtigt.

Der Lenkungsausschuss für die Digitalisierung der Landesverwaltung hat auf seiner 8. Sitzung vom 17. Juni 2020 beschlossen, dass die Ressorts anhand der Empfehlungen des Handlungsleitfadens zum sicheren Betrieb von Windows 10 und Office 2016 vom 28. Februar 2020, unter Berücksichtigung der tatsächlichen individuellen Gegebenheiten, zwischenzeitlich veränderten Rahmenbedingungen und der eigenverantwortlichen Risikoabschätzung, Windows 10 und Office 2016 einsetzen können.

Zu 4 Zusammenarbeit auf deutscher Ebene

Zu 4.1 Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz)

Der Bundesgesetzgeber hat seine Regelungslagen zu den manuellen Bestandsdatenauskunftsverfahren aufgrund der genannten Entscheidung des Bundesverfassungsgerichts nunmehr angepasst. Damit sind auch die Landesgesetzgeber - unter Berücksichtigung des sogenannten Doppeltürenmodells - gefordert, ihre diesbezüglichen Regelungslagen auf der Grundlage der neuen bundesgesetzlichen Regelungen zu überprüfen und gegebenenfalls anzupassen. In Mecklenburg-Vorpommern sind Befugnisse zur Beauskunftung von Bestandsdaten im § 33h SOG M-V und im § 24b LVerfSchG M-V enthalten. Das Landesverfassungsgericht M-V hat die Anwendung beider Normen unter bestimmten Maßgaben bis zu einer Neuregelung, längstens jedoch bis 31. Oktober 2022, für weiter anwendbar erklärt (Az.: LVerfG 3/14).

Zu 4.3 IT-Planungsrat

Zu 4.3.2 Registermodernisierung

Abgesehen davon, dass das angesprochene Registermodernisierungsgesetz bereits am 6. April 2021 verkündet wurde, ist der bereits aus dem 15. Tätigkeitsbericht bekannten und im 16. Tätigkeitsbericht zum Datenschutz des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern erneut ausgesprochenen Empfehlung in Sachen Registermodernisierung aus den folgenden Gründen nicht gefolgt worden:

Im Gegensatz zu den meisten anderen europäischen Staaten verfügt Deutschland über kein konsistentes System zur eindeutigen Identifizierung natürlicher Personen in Registern und anderen strukturierten Datenbeständen der öffentlichen Hand. Während andernorts jeder Person eine allgemeine und einheitliche Identifikationsnummer zugeordnet ist, verwendet die deutsche Verwaltung einerseits bereichsspezifische Personenkennezeichen, wie z. B. die Sozialversicherungsnummer oder die Steueridentifikationsnummer.

Andererseits wird in Bereichen, in denen keine solche Nummer existiert sowie auch für die Datenübermittlung zwischen einzelnen Verwaltungsbereichen in der Regel ein Bündel sprechender Basisdaten verwendet (z. B. Name, Geburtsdatum, Wohnort), um weitere Fachdaten einer bestimmten Person zweifelsfrei zuordnen zu können. Da dieses Bündel sprechender Basisdaten veränderlich ist oder durch Schreibfehler Verwechslungen oder Nichtzuordnungen auftreten können, ist das bestehende System nicht geeignet, um insbesondere im digitalen Verwaltungsverkehr, schnelle, medienbruchfreie und nutzerfreundliche Datenaustausche zu organisieren.

Über die Qualitätssicherung der Register hinaus ist die Schaffung eines Ordnungskriteriums zugleich Voraussetzung, um nutzerfreundliche und medienbruchfreie Verwaltungsverfahren anzubieten. Denn nutzerfreundlich und medienbruchfrei sind Verwaltungsverfahren erst dann, wenn Bürgerinnen und Bürger weitestgehend von Nachweispflichten entlastet sind. Dafür muss die Verwaltung ertüchtigt werden, diese Nachweise (etwa Geburtsurkunden) selbst auf digitalem Wege zu beschaffen. Dieser behördenübergreifende Datenaustausch kann effizient nur umgesetzt werden, wenn die Register der Verwaltungen anhand eines Ordnungskriteriums synchronisiert werden. Ohne ein solches kann der Grundsatz „once only“ nicht umgesetzt werden, da die nur einmalige Abgabe von Nachweisen durch Bürgerinnen und Bürger denotwendig die zweifelsfreie Identifikation im späteren Prozess erfordert.

Die Identifikationsnummer wird in die für die Umsetzung des Onlinezugangsgesetzes relevanten Verwaltungsregister von Bund und Länder eingeführt. Dadurch wird gewährleistet, dass Basisdaten natürlicher Personen von einer dafür verantwortlichen Stelle auf Inkonsistenzen geprüft, verlässlich gepflegt, aktualisiert und bereitgestellt werden. Hierzu wird auf die vorhandenen Strukturen der Identifikationsnummer nach § 139b der Abgabenordnung (Steuer-Identifikationsnummer) aufgesetzt, und diese werden durch die für ein registerübergreifendes Identitätsmanagement notwendigen Elemente ergänzt. Das Identifikationsmerkmal wird in den für die Umsetzung des Onlinezugangsgesetzes relevanten Fachregistern der geführten Verwaltungsverfahren gespeichert.

Die zur Identifikation erforderlichen personenbezogenen Daten in diesen Registern werden öffentlichen Stellen, die diese zur Erbringung von Verwaltungsleistungen nach dem Onlinezugangsgesetz benötigen, aktuell und in hoher Qualität bereitgestellt. Zusätzlich werden Qualitätssicherungsprozesse eingerichtet, die die Aktualität, Konsistenz und Validität der personenidentifizierenden Basisdaten sicherstellen.

Für die Transparenz gegenüber den Bürgerinnen und Bürgern wird ein Datencockpit aufgebaut, das eine einfache, transparente und zeitnahe Übersicht über zwischen Behörden vorgenommenen Datenübermittlungen ermöglicht.

Die eindeutige Identifikation und die Bereitstellung von qualitätsgesicherten personenbezogenen Daten leisten einen wichtigen Beitrag zur Erreichung der Ziele des Onlinezugangsgesetzes. In der Interaktion mit der Verwaltung müssen Bürgerinnen und Bürger regelmäßig grundlegende Daten wie Adresse oder Familienstand immer wieder angeben oder bestimmte Dokumente, wie zum Beispiel die Geburtsurkunde, vorlegen. Diese Aufwände lassen sich minimieren, wenn die jeweilige Behörde die Basisdaten zu einer natürlichen Person über die neu geschaffene Registermodernisierungsbehörde direkt abrufen kann.

Statt die grundlegenden Daten zu einer Person an vielen dezentralen Stellen permanent aktuell halten zu müssen, würden die Basisdaten einer natürlichen Person zentral durch die Registermodernisierungsbehörde qualitätsgesichert. Im Übrigen wird auf die Ausführungen zur Rechts- und Verwaltungsvereinfachung verwiesen.

Die Einführung eines Systems bereichsspezifischer Identifikationsnummern nach dem Vorbild der Republik Österreich wäre in der vornehmlich dezentral organisierten deutschen Verwaltung von größerer rechtlicher, technischer und organisatorischer Komplexität. Aufwand und Nutzen eines solchen Modells stünden in einem ungünstigeren Verhältnis zueinander. Die Systeme in Österreich und Deutschland lassen sich wegen Unterschieden in der Registerstruktur nicht ohne Weiteres vergleichen. Eine komplette Harmonisierung der Grunddatensätze ohne Nutzung einer Identifikationsnummer wäre ebenfalls außerordentlich zeit- und kostenaufwändig, hätte eine aus datenschutzrechtlicher Sicht abzulehnende Ausdehnung der Datensätze in den (größtenteils dezentralen) Fachverfahren zur Folge und wäre sehr pflegeintensiv und fehleranfällig.

Die Landesregierung stuft die Verwendung der Steueridentifikationsnummer überdies nicht als verfassungswidrig ein, da die Verwendung dieses einheitlichen Personenkennzeichens nicht zur Erstellung von Persönlichkeitsprofilen von Bürgerinnen und Bürgern genutzt wird. Hierfür ist durch technisch-organisatorische Maßnahmen, die Einbindung einer zentralen Registerbehörde, über die Abfragen und die Antworten zu laufen haben sowie die Regelungen zum Datenschutzcockpit Vorsorge getroffen worden.

Zu 4.3.3 Umsetzung des Onlinezugangsgesetzes (OZG)

Die Vorstellung des Bundesgesetzgebers beim Onlinezugangsgesetz (OZG) ist es, dass Bürgerinnen und Bürger sowie Unternehmen ihre Verwaltungsangelegenheiten bis Ende des Jahres 2022 (auch) online erledigen können. Diese Vorstellung kann für das Flächenland M-V uneingeschränkt übernommen werden und ihre Umsetzung stellt im Jahr 2021 letztlich eine Selbstverständlichkeit dar. Die Umsetzung des OZG in Mecklenburg-Vorpommern erfolgt über eine zentrale Steuerung im Ministerium für Inneres, Bau und Digitalisierung (ehemals Ministerium für Energie, Infrastruktur und Digitalisierung). Neben den Themenfeldern Bauen & Wohnen werden im OZG-Programm Mecklenburg-Vorpommern über das zentrale Programmmanagement die Verwaltungsleistungen 13 weiterer Themenfelder im Reifegrad 3 umgesetzt sowie die technische Infrastruktur bereitgestellt. Das OZG-Programm Mecklenburg-Vorpommern arbeitet in der Umsetzung eng mit dem Bund, den Bundesländern und der kommunalen Ebene zusammen. Es startete am 1. Juli 2021 und geht derzeit von einer Umsetzung in acht Umsetzungswellen aus.

Damit Bürgerinnen und Bürger sowie Unternehmen ihre Anträge und Angelegenheiten auch wirklich vollständig online abwickeln können, müssen die digital bereitgestellten Verwaltungsleistungen nicht nur rechtssicher, sondern auch nutzerfreundlich sein. Datenschutzfragen spielen in diesem Spannungsfeld eine wichtige Rolle, weshalb die Landesregierung in verschiedenen Arbeitsgruppen vertreten ist und die Prozesse dort zusammen mit den anderen Bundesländern sowie dem Bund gestaltet, um zentrale und übergeordnete Fragen in diesem Themenfeld gemeinsam zu klären. Außerdem steht die Landesregierung sowohl im Kontext der OZG-Umsetzung als auch im Bereich der technischen Infrastruktur im engen Austausch mit den behördlichen Datenschutzbeauftragten der Ressorts sowie dem Landesbeauftragten für den Datenschutz.

Dies zeigt, dass die Landesregierung der Empfehlung des Landesbeauftragten für den Datenschutz, insbesondere frühzeitig die datenschutzrechtlichen Rahmenbedingungen zu berücksichtigen und ihn frühzeitig in die Entwicklung der digitalen Angebote einzubeziehen, bereits seit jeher folgt.

Im Themenfeld Bauen & Wohnen sind fünf OZG-Leistungen (Bauvorbescheid und Baugenehmigung, Verkehrswertgutachten und Auskünfte aus der Kaufpreissammlung, Einsicht in das und Auszüge aus dem Liegenschaftskataster, Hoheitliche Vermessung im Liegenschaftskataster, Genehmigung zur Leitungsverlegung nach § 68 Abs. 3 TKG) online verfügbar und können durch andere Vollzugsbehörden (teilweise) nachgenutzt werden.

Das Go-Live der Leistung „Genehmigungsfreistellungsverfahren“ erfolgte Ende März 2021 und auch die Go-Lives der Leistungen „Denkmalförderung“ und „denkmalrechtliche Genehmigung“ sollen bis Ende 2021 erfolgen.

Für die OZG-Leistung „Baugenehmigung und Bauvorbescheid“ wird das sogenannte Nutzungsmodell „EfA“ (Einer für Alle) angestrebt. Bisher ist eine Nachnutzung in anderen Bundesländern noch nicht erfolgt, aber derzeit in Planung und Vorbereitung. Es besteht gegenwärtig ein Nachnutzungsinteresse aus den Ländern Sachsen-Anhalt, Rheinland-Pfalz, Saarland und Schleswig-Holstein. Weitere Länder beteiligen sich an regelmäßigen Austauschterminen und prüfen die Möglichkeiten einer Nachnutzung.

Der vielfach kommunizierte Wunsch der öffentlichen Verwaltung, gute und nutzbare Online Angebote zur Verfügung zu stellen, kann mit der Umsetzung des OZG einen ersten Anstoß bekommen.

Zu 4.3.4 Digitale Souveränität

Die Landesregierung begrüßt ausdrücklich die Aktivitäten, die im Rahmen des IT-Planungsrates zur „digitalen Souveränität“ unternommen werden. Darüber hinaus wird auf die Stellungnahme der Landesregierung zu 0.2 Nummer 6 verwiesen.

Zu 5 Corona

Zu 5.1 Videokonferenzsysteme

Sowohl die „Orientierungshilfe Videokonferenzsysteme“ der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder als auch die Untersuchung von Videokonferenzsystemen der Berliner Beauftragten für den Datenschutz sind der Landesregierung bekannt. Derzeit werden in der gesamten Landesverwaltung Cisco Webex Meetings und Cisco Live HD als Grundverfahren eingesetzt. Die Ablösung durch ein anderes Videokonferenzsystem wird geprüft.

Die nach der ad-hoc-Einführung des derzeit in der Landesverwaltung genutzten Videokonferenzsystems gemachten Erfahrungen fließen in die Auswahl eines Nachfolgesystems ein. Die Konzeption des neuen Videokonferenzsystems für die Landesverwaltung priorisiert eine Lösung, die bei einem IT-Dienstleister der Landesverwaltung gehostet und betrieben werden kann. Quelloffene Lösungen stehen hierbei ganz besonders im Fokus.

Die Empfehlungen der „Orientierungshilfe Videokonferenzsysteme“ werden bei der Auswahl, der Inbetriebnahme und des Betriebes des Videokonferenznachfolgesystems berücksichtigt werden. Die für einen Betrieb erforderlichen Maßnahmen, um die geltenden Regeln des Datenschutzes und der Informationssicherheit zu gewährleisten, werden dabei mit der notwendigen Sorgfalt, Sensibilität und Konsequenz ermittelt und umgesetzt werden.

Der Landesbeauftragte für den Datenschutz ist intensiv in das Procedere zum Videokonferenznachfolgesystem eingebunden.

Zu 5.2 Corona-Fragebogen vor Gerichtszutritt im Amtsgericht Greifswald

Die Gerichte und Staatsanwaltschaften wurden von Seiten des damaligen Justizministeriums informiert und sensibilisiert.

Der in Rede stehende Fragebogen wurde dergestalt abgeändert, dass auf Gesundheitsfragen verzichtet wird.

Zu 5.4/5.5 Corona-Listen/bzw. Unsicherheiten der Sportvereine beim Umsetzen der Auflagen der Corona-Landesverordnung Mecklenburg-Vorpommern

Zu diesen Punkten nimmt die Landesregierung im Zusammenhang Stellung:

Um Infektionsketten und Ausbrüche von SARS-CoV-2 (Covid-19) schnellstmöglich zu erkennen und einzugrenzen, wurden in Abstimmung mit dem Landesbeauftragten für den Datenschutz in den Corona-Verordnungen des Landes Dokumentationspflichten zur Kontaktnachverfolgung unter anderem für Betriebe des Einzelhandels, der körpernahen Dienstleistungen, der Gastronomie oder auch für Veranstaltungen von Sportvereinen geregelt. Gleiches galt auch für Angebote und Einrichtungen der Jugendarbeit, Jugendverbandsarbeit und Jugendsozialarbeit. Hierbei wurden rechtliche Vorgaben dahingehend gemacht, welche konkreten Daten zu Kontaktdatennachverfolgung erhoben werden sollen und wie diese Erhebung unter Beachtung von datenschutzrechtlichen Gesichtspunkten zu erfolgen hat. Es wurden seitens der Landesregierung jedoch keine konkreten Formulare, Vorlagen oder Ähnliches erstellt.

Vielmehr wurde infolge ebenfalls geregelt, dass die verpflichtende Dokumentation zur Kontaktnachverfolgung auch in elektronischer Form, zum Beispiel mittels einer speziellen Anwendungssoftware (App) erfolgen kann. Dazu war es erforderlich, sicherzustellen, dass die Daten datenschutzkonform erfasst, die Erreichbarkeit der Kontaktpersonen hinreichend präzise dokumentiert und die Daten im Falle des Infektionsgeschehens unmittelbar dem zuständigen Gesundheitsamt in einer geeigneten Art und Weise zur Verfügung gestellt werden. Zentrales Ziel der Einführung eines elektronischen Systems war die Verbesserung der Kontaktdatennachverfolgung durch eine korrekte Nachverfolgung bei einfacher Handhabung und gleichzeitiger datenschutzkonformer Speicherung der Daten, welche nur im Infektionsfall vom zuständigen Gesundheitsamt eingesehen werden können.

Die Landesregierung hatte sich in einem Vergabeverfahren entschieden, dass die elektronische Kontaktdatennachverfolgung in Mecklenburg-Vorpommern landeseinheitlich mittels der Luca-App erfolgen soll. Mit dem Luca-App-System können die Gesundheitsämter Kontaktpersonen von Infizierten ermitteln: Wird ein Anwender der Luca-App positiv auf SARS-CoV-2 getestet, kann er seine Historie (Kontaktdatenbuch) dem Gesundheitsamt mittels einer zwölfstelligen Transaktionsnummer (TAN) freigeben. Dadurch sendet die Luca-App des Getesteten - mit Ausnahme von privaten Treffen - alle Veranstaltungsorte der letzten 14 Tage an das Luca-System. Das Gesundheitsamt fordert dann über das Luca-System die entsprechenden Veranstalter auf, die Kontaktdaten aller Gäste, die zur selben Zeit wie der Meldende am jeweiligen Veranstaltungsort waren, an das Gesundheitsamt zu übertragen. Die Veranstalter können dieser Aufforderung über das Webinterface des Luca-App-Systems folgen. Anschließend stehen die Kontaktdaten dem Gesundheitsamt über ein Webinterface zur Verfügung und können entweder in dieser Webanwendung verwendet oder in dessen System zur Kontaktnachverfolgung übernommen werden. Damit erhält das Gesundheitsamt die Kontaktdaten aller Gäste, die in den letzten 14 Tagen zur selben Zeit am selben Ort wie der Meldende angemeldet („checked in“) waren. Das Befragen des Infizierten, eventuelle Erinnerungslücken sowie das aufwendige und zeitintensive Beschaffen, Entziffern und Abgleichen handschriftlicher Gästelisten mit teilweise falschen Angaben sollte hierdurch entfallen.

Nichtdestotrotz wird die Landesregierung die Empfehlung des Landesbeauftragten für den Datenschutz bei der Gestaltung künftiger Regelungen zur Bewältigung der Corona-Pandemie, die bisherigen Erfahrungen und Probleme bei der Umsetzung datenschutzrechtlicher Belange in den Blick zu nehmen, angemessen berücksichtigen.

Zu 5.6 Corona-Montagsspaziergang

Die Landesregierung hat die Ausführungen des Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern geprüft und teilt die Auffassung, dass zukünftig durch die Polizei grundsätzlich keine Fotos von Personalausweisen gefertigt werden dürfen. Dies ergibt sich aus Sicht der Landesregierung aus § 20 Abs. 2 Personalausweisgesetz. Dort heißt es: „Der Ausweis darf nur vom Ausweisinhaber oder von anderen Personen mit Zustimmung des Ausweisinhabers in der Weise abgelichtet werden, dass die Ablichtung eindeutig und dauerhaft als Kopie erkennbar ist. Andere Personen als der Ausweisinhaber dürfen die Kopie nicht an Dritte weitergeben. Werden durch Ablichtung personenbezogene Daten aus dem Personalausweis erhoben oder verarbeitet, so darf die datenerhebende oder -verarbeitende Stelle dies nur mit Einwilligung des Ausweisinhabers tun.“ Diese Regelung wurde im Jahr 2017 geschaffen. Nach der Gesetzesbegründung (Drucksache 787/16) fällt auch das Fotografieren unter den Begriff des Ablichtens. Aus Sicht der Landesregierung wäre das Abfotografieren von Personalausweisen zur Identitätsfeststellung nur auf Grundlage einer Einwilligung der betroffenen Person möglich, soweit es keine anderweitige Rechtsgrundlage gibt, die das Ablichten ohne Einwilligung zulässt (wie im § 8 Abs. 2 GwG, § 95 Abs. 4 TKG oder § 64 Abs. 1 FeV - so auch das BMI unter <https://www.bmi.bund.de/Webs/PA/DE/buergerinnen-und-buerger/der-personalausweis/ausweiskopien/ausweiskopien-node.html>). Eine solche hinreichend bestimmte Rechtsgrundlage für das Anfertigen von Personalausweisfotos zu strafverfolgungs- oder gefahrenabwehrrechtlichen Zwecken durch die Polizei ist jedoch nicht ersichtlich.

Zu 6 Datenschutz und Bildung**Zu 6.1 Datenschutz und die Förderung von digitalen Kompetenzen**

Die Landesregierung begrüßt das Engagement des Landesbeauftragten für den Datenschutz, die Förderung von Medienkompetenz in allen Bevölkerungsschichten zu unterstützen und teilt dessen Auffassung, dass „die Vermittlung von Datenschutzbewusstsein und Medienkompetenz/Digitaler Kompetenz weiterhin eine notwendige Zukunftsaufgabe unseres Landes“ ist.

Die Landesregierung ist sich ebenfalls 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 teilt die Auffassung des Landesbeauftragten für den Datenschutz zur generellen Bedeutung des Umgangs junger Menschen mit Medien und zur damit einhergehenden Notwendigkeit der Förderung von Medienkompetenz und Mediensicherheit einschließlich des Datenschutzes vollumfänglich. Die Vermittlung von Medienkompetenz und Grundlagen des Datenschutzes ist eine zentrale Aufgabe der außerschulischen Bildung und damit Bestandteil des Aufgaben- und Angebotspektrums in den Einrichtungen der Kinder- und Jugendhilfe, insbesondere in den Bereichen der (offenen) Jugendarbeit, der Jugendverbands- und Jugendsozialarbeit im Sinne der §§ 11ff. Achstes Buch Sozialgesetzbuch (SGB VIII). Schon nach der Zielrichtung des SGB VIII sind auch im Bereich der digitalen Medien Kinder und Jugendliche in ihrer individuellen und sozialen Entwicklung zu fördern, vor Gefahren für ihr Wohl zu schützen sowie etwaige Benachteiligungen zu vermeiden oder abzubauen. Dabei ist maßgeblich, die Fähigkeiten und Fertigkeiten von Kindern und Jugendlichen, Medien und ihre Inhalte den eigenen Zielen und Bedürfnissen entsprechend sachkundig, bewusst, verantwortungsvoll, sicher, selbstbestimmt und kreativ zu nutzen, zu stärken sowie digitale Teilhabe zu ermöglichen. Die Befähigung junger Menschen zu einer sozial verantwortlichen und reflektierten Handlungspraxis im Umgang mit der Internetnutzung und speziell der Nutzung sozialer Netzwerke ist dabei essentiell.

Aus Sicht der Landesregierung ist Medienkompetenz aber auch eine notwendige Grundvoraussetzung für Mediensicherheit und somit wesentlicher Bestandteil der Kriminalitätsvorbeugung sowie Bestandteil der Extremismusprävention, mithin wesentlicher Baustein für eine gelingende demokratische Kultur in Deutschland, und sollte daher prioritär behandelt werden.

Zu 6.2 Medienscouts MV und TEO - Tage ethischer Orientierung - protect privacy

Die Landesregierung begrüßt die Bestrebungen der in Rede stehenden Projekte des Landesbeauftragten für den Datenschutz ausdrücklich und unterstützt diese.

In diesem Zusammenhang ist die Landesregierung bestrebt, mit den eigenständigen Förderschwerpunkten „Jugendbeteiligung“ und „Stärkung von Medienkompetenz und Mediensicherheit“ des neuen Landesjugendplans die digitale Teilhabe von Kindern und Jugendlichen und angesichts fortschreitender Mediatisierung, die Stärkung von Medienkompetenz und -sicherheit zukünftig bei der Umsetzung eigener Projekte im Bereich der Jugend-, Jugendverbands- und Jugendsozialarbeit stärker zu berücksichtigen.

Durch den neuen Förderschwerpunkt „Stärkung von Medienkompetenz und Mediensicherheit“ sollen perspektivisch medienpädagogische Projekte initiiert werden, welche Fragen der pädagogischen Bedeutung von Medien in den Nutzungsbereichen Freizeit, Bildung oder Beruf beinhalten und dort ansetzen, wo Medien als Mittel der Information, Beeinflussung, Unterhaltung, Unterrichtung und Alltagsorganisation Relevanz für die Sozialisation junger Menschen haben. Insbesondere sollen hier Projekte in den Blick genommen werden,

- die Kindern und Jugendlichen Medienkompetenz und/oder Mediensicherheit sowie Möglichkeiten digitaler Teilhabe direkt vermitteln,
- die über Medienkompetenz und/oder Mediensicherheit sowie digitale Teilhabe informieren sowie
- die Aus-, Fort- und Weiterbildungen von Fachkräften der Jugendhilfe, insbesondere im Bezug zur Medienpädagogik zum Gegenstand haben.

Darüber hinaus hat sich die Landesregierung - insbesondere mit Blick auf die Auswirkungen der Corona-Pandemie auf Kinder und Jugendliche in ländlichen Räumen des Flächenbundeslandes Mecklenburg-Vorpommern und der damit einhergehenden Einschränkungen der sozialen Teilhabe junger Menschen - zum Ziel gesetzt, mit dem Aktionsprogramm „Aufholen nach Corona für Kinder und Jugendliche“ verstärkt die Medienkompetenzbildung und -förderung sowie die (digitale) Jugendbeteiligung in den Fokus zu rücken.

Die Landesregierung unterstützt ebenfalls seit Jahren aus Mitteln des Europäischen Sozialfonds das schulkooperative Modellprojekt TEO (Tage ethischer Orientierung) der Nordkirche.

Die Landesregierung begrüßt auch, dass es in enger Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz gelungen ist, mit dem Modul „protect privacy - mein Klick, meine Verantwortung“ einen Beitrag dazu zu leisten, den kritischen, verantwortungsvollen Umgang mit digitalen Medien von Heranwachsenden zu fördern.

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. Obwohl das Projekt nicht wie geplant die notwendigen Ausbildungswochenenden im Jahr 2020 umsetzen konnte, sollte dieses bundesweit beachtete Kooperationsprojekt des Landesbeauftragten für den Datenschutz mit den außerschulischen Bildungspartnern des Netzwerkes „Medienaktiv M-V“ auch weiterhin fortbestehen.

6.3 Medienaktiv MV

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, insbesondere für die Bereitschaft ihre Expertise bei der Ausgestaltung der ersten Medienbildungstage des damaligen Bildungsministeriums mit einzubringen und als Referenten zur Verfügung zu stehen. Obwohl in 2020 keine Fachtagungen durchgeführt werden konnten, zählt die Arbeit des Netzwerkes zu einem wichtigen Bestandteil der Medienlandschaft in Mecklenburg-Vorpommern. Im Übrigen wird auf die Stellungnahme der Landesregierung zu 6.2 verwiesen.

Zu 6.4 Kooperationsvereinbarung zur Förderung von Medienkompetenz in Mecklenburg-Vorpommern

Die Ressortanhörung zur vierten Kooperationsvereinbarung liegt derzeit still, da Einigkeit in der Arbeitsgruppe darüber bestand, dass zunächst weitere Gespräche zur Errichtung eines Landesmedienkompetenzzentrums erforderlich sind. Übereinstimmend sollten in die vierte Kooperationsvereinbarung die Errichtung des Landesmedienkompetenzzentrums, die Ausgestaltung und die zukünftigen Aufgaben eines solchen mit aufgenommen werden. In Abstimmung mit allen Akteuren hat die Staatskanzlei im Oktober 2020 eine Arbeitsgruppe Medienkompetenz unter Leitung von Herrn Prof. Rosenstock von der Universität Greifswald berufen, die ein Gutachten zur Errichtung eines Landesmedienkompetenzzentrums zu erarbeiten hatte.

Der Arbeitsgruppe gehörten die folgenden Akteure an: die Staatskanzlei, das damalige Ministerium für Soziales, Gleichstellung und Integration, die Landesmedienanstalt (MMV), die Landesarbeitsgemeinschaft (LAG) Medien und der Landesbeauftragte für den Datenschutz. Daraus hervorgegangen ist die Kabinettsvorlage 86-21, Konzept und Gutachten zur Errichtung eines Landesmedienkompetenzzentrums. Das Landesmedienkompetenzzentrum Mecklenburg-Vorpommern wird als Fachbereich bei der Medienanstalt Mecklenburg-Vorpommern angesiedelt. Es besteht aus einer zentralen Geschäftsstelle und vier dezentralen, regionalen Medienkompetenzzentren, die ein dezentralisiertes Landesmedienkompetenzzentrum entsprechend der Vorgaben des Landtages beinhaltet. Es ist vorgesehen, zum 1. Januar 2022 die Arbeitsfähigkeit des Landesmedienkompetenzzentrums herzustellen. Gleichzeitig wurde die Weiterarbeit an der 4. Kooperationsvereinbarung auf die Zeit nach Errichtung des Landesmedienkompetenzzentrums verschoben, um die Neuentwicklung der Strukturen bereits berücksichtigen zu können. Insgesamt wird durch die neue Struktur die Medienkompetenzförderung deutlich getrennt von der Filmförderung. Parallelstrukturen werden dadurch vermieden.

Zu 6.5 Medien und Familie

Aus familienpolitischer Sicht gewinnt der Datenschutz in der Medienbildung und Medien-erziehung in den Familien einen immer größer werdenden Stellenwert. Kinder und Jugendliche und deren Familien auf einen nachhaltigen positiven Umgang mit digitalen Medien vorzubereiten, wird in den Einrichtungen für Familien seit einigen Jahren verstärkt in den Fokus genommen und ist ein fester Bestandteil ihrer Informations- und Bildungsarbeit. Vor diesem Hintergrund wurde die Stärkung der Medienkompetenz auch als ein Fördergegenstand in der „Richtlinie zur Gewährung von Zuwendungen für Leistungen der allgemeinen Förderung der Erziehung in der Familie“ von 2017 festgeschrieben.

Diverse Angebote, Maßnahmen und Projekte wurden und werden in den Familienzentren, Mehrgenerationenhäusern und Familienbildungsstätten regelmäßig Familien angeboten und erfolgreich umgesetzt.

Beispiele hierfür sind:

- „Warum Hate Speech und Fake News schon früh Bildungsthemen sein müssen?! Hass begegnen durch Wissen, Empathie und eigene Haltung.“ Hier arbeiteten die Fachkräfte mit dem Landeskriminalamt im Projekt „Helden statt Trolle“ zusammen,
- „Kinder & Neue Medien - Cyber-Mobbing, Recht am eigenen Bild, Urheberrecht, Kinder nutzen Technik für Erwachsene - Welche Informationen brauchen Sie, Eltern, Lehrer und Erzieher?“ Hier erhielten die Fachkräfte interessante Informationen von einer Rechtsanwältin, um Konzepte und Formate für Familienbildungsangebote zu erarbeiten.

Zudem stehen Themen der Medienbildung in den Netzwerkkonferenzen der „FamilienInfo M-V“ regelmäßig auf der Agenda, wie zum Beispiel auf der Netzwerkkonferenz 2019 zum Thema „Demokratie. Bildung. Digitalisierung. - Herausforderungen für die Familienarbeit“.

Insbesondere vor dem Hintergrund der Corona-Pandemie sehen es die Fachkräfte der Familienbildung als wichtiges Schwerpunktthema in ihrer Arbeit, Kinder, Jugendliche und Familien im Umgang mit digitalen Medien zu unterstützen und damit ein Fundament der Medienkompetenzbildung zu legen.

Zu 6.5.1 Medienguides Mecklenburg-Vorpommern

Die Landesregierung begrüßt das Vorhaben des Landesbeauftragten für den Datenschutz, seine Erfahrungen aus dem Projekt „MedienScout - Jugend klärt auf“ auf die Zielgruppe der Eltern auszuweiten und ein Projekt „Medienguides M-V“ zu initiieren. Für die Nachhaltigkeit der Medienkompetenzentwicklung bei Kindern und Jugendlichen ist ein entsprechendes Grundverständnis bei Eltern unumgänglich.

Seitens der Landesregierung wird angeregt, dass die Angebote der ausgebildeten Medienguides auch auf die Einrichtungen für Familien ausgeweitet und diese in das Netzwerk der Medienakteure integriert werden.

Zu 6.5.2 Neues Kapitel Bildungskonzeption der 0- bis 10-Jährigen in Mecklenburg-Vorpommern

Die intensive Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz ist mit Fertigstellung des neuen Kapitels „Medien und digitale Bildung“ in der Bildungskonzeption für 0- bis 10-jährige Kinder im Jahr 2020 zu einem erfolgreichen Ende gekommen. Innerhalb der Landesregierung hat das damalige Ministerium für Soziales, Integration und Gleichstellung gemeinsam mit den Akteuren der AG Medienbildung im Bereich der frühkindlichen Bildung intensiv an der aktuellen inhaltlichen Ausrichtung gearbeitet. Das positive Ergebnis wird begrüßt. Damit ist das Thema „Medien und digitale Bildung“ fester Bestandteil des Bildungsplans für die Kindertageseinrichtungen des Landes sowie der Fort- und Weiterbildung der Fachkräfte.

Zu 6.5.3 Fortbildungsreihe „klicken, spielen, zappen“

Die Landesregierung wertschätzt die Plakatkampagne „Heute schon mit deinem Kind gesprochen“ und begrüßt das modulare Fortbildungsangebot für die Erzieherinnen und Erzieher im Land. Durch Angebote dieser Art werden die Fachkräfte für die Herausforderungen der Digitalisierung sensibilisiert, im Umgang mit dem Thema gestärkt und zugleich mit den relevanten Inhalten der Medienbildung auf der Grundlage des Kindertagesförderungsgesetzes vertraut gemacht.

Soweit der Landesbeauftragte für den Datenschutz eine Verstärkung der Mittel durch die Landesregierung über die LAKOST M-V fordert, weist die Landesregierung darauf hin, dass die Fortführung von Kampagnen und Projekten stets von der Haushaltslage des Landes abhängig ist.

Zu 7 Technik und Organisation**Zu 7.1 Das Standard-Datenschutz-Modell (SDM)**

Die im Standard-Datenschutzmodell (SDM) beschriebene Vorgehensweise bei der Planung, der Einrichtung und dem Betrieb von Verfahren zur Verarbeitung personenbezogener oder personenbeziehbarer Daten wird in verschiedenen Bereichen der Landesverwaltung neben dem BSI IT-Grundschutz angewendet. So erfolgten kontinuierliche Anpassungen vorhandener Sicherheitskonzepte unter Nutzung des SDM mit Unterstützung der Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH. Auch die Schutzbedarfsfeststellung und Risikoanalyse mit Schwellwertanalyse zur Datenschutzfolgenabschätzung für das Servicekonto des M-V-Serviceportals sowie der E-Government Basisdienste wurden mit der SDM-Methodik durchgeführt. Die Landesregierung wird auch weiterhin über die Erfahrungen beim Umgang mit diesem Werkzeug berichten, um dadurch die Weiterentwicklung zu unterstützen.

Zu 7.2 Microsoft Office 365

Die Landesregierung teilt die Empfehlung des Landesbeauftragten für den Datenschutz und wird den möglichen Einsatz von alternativen Produkten, insbesondere Open-Source, im Rahmen des Programms MV-PC prüfen.

Zu 7.3 Microsoft Windows 10

Die Landesregierung teilt auch hier die Empfehlung des Landesbeauftragten für den Datenschutz und wird den Einsatz geeigneter Betriebssysteme im Rahmen des Programms MV-PC prüfen. Bestehende PC-Arbeitsplätze werden dann künftig auf den MV-PC migriert bzw. gewährleisten den Datenschutz bis dahin durch die Anwendung des „Handlungsleitfadens zum sicheren Betrieb von Windows 10 und Office 2016 vom 28. Februar 2020“.

Zu 7.4 Akkreditierung und Zertifizierung nach der DS-GVO

Die Landesverwaltung wird die Entwicklung im Bereich der Akkreditierung und Zertifizierung nach der Verordnung (EU) 2016/679 weiter beobachten und bei der Auswahl seiner IT-Dienstleister berücksichtigen.

Zu 8 Datenschutz in verschiedenen Rechtsgebieten

Zu 8.1 Parlament

Zu 8.1.1 Urteil EuGH: DS-GVO und Parlamente

Der Landesbeauftragte für den Datenschutz bejaht verallgemeinernd die Geltung der Verordnung (EU) 2016/679 für das „Parlament als Ganzes, seine Ausschüsse, die Fraktionen und auch die einzelnen Abgeordneten in ihrer parlamentarischen Tätigkeit“. Der Tätigkeitsbericht lässt jedoch unerwähnt, dass in der Literatur durchaus abweichende Auffassungen vertreten werden. In einigen einschlägigen Beiträgen wird die Verallgemeinerungsfähigkeit des Urteils mit Vorsicht betrachtet (vergleiche etwa die Anmerkung von Engelbrecht, ZD 2020, 577, 579) beziehungsweise gar verneint (vergleiche den - allerdings bei Abfassung des Tätigkeitsberichts noch nicht veröffentlichten - Beitrag von Hilbert, NVwZ 2021, 1173, 1175, 1177).

Zu 8.1.2 Verschlüsselung - gut oder gar nicht

Am 14. Dezember 2020 hat der Rat der Europäischen Union die Entschließung zur Verschlüsselung - Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung angenommen. Begründet wurde dies damit, dass die Digitalisierung moderner Gesellschaften gewisse Schwachstellen und das Potenzial einer Ausbeutung für kriminelle Zwecke mit sich bringe. So könnten Kriminelle leicht zugängliche, herkömmliche Verschlüsselungslösungen, die für rechtmäßige Zwecke konzipiert worden seien, für ihre Vorgehensweisen nutzen. Gleichzeitig hänge die Strafverfolgung zunehmend vom Zugang zu elektronischen Beweismitteln ab, um Terrorismus, organisierte Kriminalität, sexuellen Missbrauch von Kindern (insbesondere dessen Online-Aspekte) sowie eine Vielzahl anderer Cyberstraftaten und durch den Cyberraum ermöglichter Straftaten wirksam zu bekämpfen. Für die zuständigen Behörden könne der Zugang zu elektronischen Beweismitteln von wesentlicher Bedeutung sein, nicht nur um erfolgreiche Ermittlungen durchzuführen und damit Kriminelle vor Gericht zu bringen, sondern auch um die Opfer zu schützen und zur Gewährleistung der Sicherheit beizutragen.

Diese Erwägungen sind überzeugend. Eines der wichtigsten Ermittlungsinstrumente sind TKÜ-Maßnahmen, welche gerade im Bereich der schweren und organisierten Kriminalität Täterstrukturen, Tatabsprachen und Tatbegehungen nachvollziehbar machen. Welche gravierenden Auswirkungen die Verschlüsselung hat, zeigen auch die durch die ausländischen Strafverfolgungsbehörden erfolgreich geführten Verfahren im Zusammenhang mit der Nutzung sog. „Kryptohandys“. Es wurde sehr deutlich, dass gerade die organisierte Kriminalität bereit ist, zum Teil hohe Summen zu investieren, um „überwachungssicher“ kommunizieren zu können. Durch die erfolgreich geführten Ermittlungen konnten unter anderem Einblicke in Strukturen des organisierten Betäubungsmittel-Handels in Deutschland erlangt werden, wie sie den Ermittlern jahrelang trotz intensiver Aufklärungsbemühungen verschlossen geblieben waren.

Verschlüsselungstechnologien werden nahezu flächendeckend über fast alle Kommunikationskanäle hinweg (Messenger, E-Mail usw.) verwendet, ohne dass es zu ihrer Nutzung eines monetären Einsatzes bedürfte. Deren Einsatz hat deswegen auch im Bereich der „Alltags- und Massenkriminalität“ Einzug gehalten, welche mitunter nicht mehr aufklärbar ist. Verschlüsselungen führen zudem nicht nur dazu, dass bestimmte Beweismittel nicht zugänglich sind, sondern verhindern auch die Sicherung der Tatbeute in Form von Kryptowährungen. Der Ansatz des Rates der Europäischen Union, Lösungen zu suchen, welche es den Behörden einerseits ermöglichen, ihre Untersuchungsbefugnisse auszuüben, die nach ihrem innerstaatlichen Recht der Verhältnismäßigkeit, Notwendigkeit und gerichtlichen Kontrolle unterliegen und dabei andererseits die gemeinsamen europäischen Werte und die Grundrechte zu achten sowie die Vorteile der Verschlüsselung zu wahren, ist daher zu begrüßen.

Zu 8.2 Kommunales

Zu 8.2.3 Datenschutzgerechte Ausgestaltung eines Briefumschlages

Sowohl durch den behördlichen Datenschutzbeauftragten des damaligen Ministeriums für Inneres und Europa als auch den Landesbeauftragten für den Datenschutz wurde festgestellt, dass im betreffenden Fall der in Art. 5 Abs. 1 lit. f der Verordnung (EU) 2016/679 verankerte Grundsatz der Vertraulichkeit verletzt wurde. Es konnte nicht ausgeschlossen werden, dass der Briefumschlag mit dem infrage stehenden Stempel Dritten zugänglich gemacht wird. Sowohl der Empfehlung des Landesbeauftragten für den Datenschutz zur Modifizierung des Stempels als auch den Hinweisen des behördlichen Datenschutzbeauftragten wurde bisher nicht durch die Verwaltung gefolgt. Es läuft gegenwärtig ein Anhörungsverfahren.

Zu 8.2.4 Sichere E-Mail-Kommunikation mit Behörden

Mit Blick auf die Empfehlungen zu den „Anforderungen an die Verschlüsselung von E-Mails“ sowie der durch die DSK gegebenen „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“ folgt die Landesregierung grundsätzlich den Ausführungen des Landesbeauftragten für den Datenschutz. Die Landesregierung weist darauf hin, dass bei der Verwendung einer Ende-zu-Ende-Verschlüsselung zum Schutz der E-Mail-Kommunikation Interdependenzen zu den bestehenden Sicherheitsarchitekturen sowie zu weiteren Sicherheitsmaßnahmen zu beachten sind. Um die datenschutzrechtlichen Anforderungen sowie die Ziele der Informationssicherheit zu gewährleisten und nachhaltig zu erhöhen, beabsichtigt die Landesregierung, die Standardisierung der von ihr betriebenen informations- und kommunikationstechnischen Verfahren sowie Infrastrukturen fortzuführen. Die referenzierten Protokolle und Sicherheitsstandards, insbesondere zur Gewährleistung der Vertraulichkeit sowie zum Schutz vor Manipulationen (Integrität) beim Versand von E-Mails kommen in der Landesverwaltung bereits zum Einsatz. Hierbei wird die Technische Richtlinie 02102-2 des Bundesamts für Sicherheit in der Informationstechnik (BSI) berücksichtigt.

Die Landesregierung hat zur Sensibilisierung und sicheren Kommunikation mit den Kommunen im Jahr 2020 zwei Runderlasse herausgegeben. Diese richten sich an die Landkreise, die kreisfreien und großen kreisangehörigen Städte sowie die unteren Rechtsaufsichtsbehörden und geben Hinweise zur Anwendung der Verordnung (EU) 2016/679, zu sicheren Kommunikationswegen und enthalten weitere Empfehlungen.

Die jährlichen Beratungen der unteren Rechtsaufsichtsbehörden werden zum Anlass genommen, die der Rechtsaufsicht des Ministeriums für Inneres, Bau und Digitalisierung unterstehenden kommunalen Körperschaften auf die Wahrung der notwendigen Sorgfalt beim Umgang mit elektronischer Kommunikation sowie auf die vorhandenen Möglichkeiten der Verschlüsselung hinzuweisen. Ein entsprechender Informationsaustausch zu den der unteren Rechtsaufsicht unterstehenden kommunalen Körperschaften wird ebenfalls empfohlen.

Zu 8.4 Polizei

Zu 8.4.1 Bußgeldverfahren gegen Polizeibeamtinnen und Polizeibeamte und Verwarnung gegen das Landesamt für zentrale Aufgaben und Technik der Polizei, Brand- und Katastrophenschutz Mecklenburg-Vorpommern (LPBK M-V)

Zum berichteten Sachverhalt fanden im Jahr 2020 mehrere Gespräche mit dem Landesbeauftragten für den Datenschutz seitens des Landesamtes für zentrale Aufgaben und Technik der Polizei, Brand- und Katastrophenschutz (LPBK M-V) und letztmalig am 17. Oktober 2020 unter Beteiligung des Staatssekretärs des damaligen Ministeriums für Inneres und Europa im Zusammenhang mit der Klage des LPBK M-V gegen die Verwarnung statt.

Leider ist festzustellen, dass der Landesbeauftragte für den Datenschutz auch in seinem Bericht für das Jahr 2020 weiterhin Ausführungen macht, die die Landesregierung so nicht teilt und um deren Klarstellung sich das LPBK M-V bereits in den genannten Gesprächen vergeblich bemüht hat. Korrekt dargestellt wurde die Thematik der Datenauslagerung, die auf einem technischen Problem beruhte, das umgehend ausgeräumt wurde, allerdings auch keinen Einfluss auf das Ermittlungsergebnis hatte.

Entgegen der Sachverhaltsdarstellung, waren die in Rede stehenden Anfragen gerade nicht identisch gewesen. Zum einen hatte die Kriminalpolizeiinspektion (KPI) Rostock um weitergehende Informationen gebeten, zum anderen hatte der Landesbeauftragte für den Datenschutz mit einer nicht korrekten Vornamen-Nachnamen-Kombination angefragt. Der der KPI übermittelte Zugriff wurde durch den zuständigen Sachbearbeiter als Ermittlungshinweis angesehen, hat jedoch keine Relevanz im vom Landesbeauftragten für den Datenschutz verfolgten Verfahren. Beide Antworten zu den Anfragen wurden mit der Information versehen, dass keine Protokolldaten festgestellt wurden, waren im Ergebnis also inhaltsgleich. Insofern waren die Vorwürfe, wie auch die Verwarnung unbegründet.

Aus diesem Grunde wurde am 8. Oktober.2020 Klage beim Verwaltungsgericht erhoben.

Der Tätigkeitsbericht verknüpft in diesem Zusammenhang die Rücknahme der Klage mit der Zusage einer verbesserten Zusammenarbeit durch das LPBK M-V, was den Anschein eines Schuldeingeständnisses erweckt. Dieses ist jedoch nicht der Fall, da die Rücknahme der Klage im Ergebnis des gemeinsamen Gesprächs zwischen Landesbeauftragten für den Datenschutz und dem Staatssekretär des damaligen Ministeriums für Inneres und Europa am 17. Oktober 2020 ohne Anerkennung des vorgeworfenen Pflichtverstoßes erfolgte und eine weitere außergerichtliche Klärung vereinbart wurde.

Bereits im Rahmen der Gespräche zwischen Landesbeauftragten für den Datenschutz und LPBK M-V und im dokumentierten Schriftverkehr wurde zudem betont, dass das LPBK M-V angesichts der langjährigen guten Zusammenarbeit diese auch gerne fortführen möchte und bilateralen Abstimmungsgesprächen offen gegenübersteht. Der gesetzliche Auftrag des Landesbeauftragten für den Datenschutz wurde und wird weiterhin aktiv unterstützt.

Zu 8.5 Schule

Zu 8.5.1 Projekt Integriertes Schulmanagement-System (ISY)

Die Landesregierung 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. Auch für die Bewältigung der besonderen Herausforderungen im jetzigen Berichtszeitraum war der Austausch mit dem Landesbeauftragten für den Datenschutz sehr hilfreich. Aufgrund des ISY-Projektfortschritts ergibt sich ein erhöhter Abstimmungsbedarf zum Datenschutz. Diesem wird seit Anfang 2020 durch monatliche Gespräche Rechnung getragen. Das Angebot, den Landesbeauftragten für den Datenschutz auch künftig im Sinne vertrauensvoller Zusammenarbeit frühzeitig in neue Projekte mit Bezug zu datenschutzrechtlichen Grundsatzfragen einzubinden und die Empfehlung, den Austausch des ISY-Projektes mit dem Landesbeauftragten für den Datenschutz weiter fortzuführen, begrüßt die Landesregierung ausdrücklich.

Zu 8.6 Soziales

Zu 8.6.1 Kein Kita-Essen ohne Schufa-Auskunft?

Ausgehend von § 11 Absatz 2 des Kindertagesförderungsgesetzes ist eine vollwertige und gesunde Verpflegung von Kindern bis zum Eintritt in die Schule während der gesamten Betreuungszeit ein integraler Bestandteil des Leistungsangebotes der Kindertageseinrichtungen. Demnach ist mit Aufnahme des Kindes in eine Kindertageseinrichtung unabhängig vom sozio-ökonomischen Hintergrund eine Vollverpflegung sichergestellt. Wenngleich die dafür anfallenden Kosten primär von den Eltern zu begleichen sind, erscheint eine vorherige Schufa-Abfrage und Bonitätsprüfung unverhältnismäßig. Daher wird das Vorgehen des Landesbeauftragten für den Datenschutz begrüßt.