LANDTAG MECKLENBURG-VORPOMMERN **Drucksache 8/6260**
8. Wahlperiode **04.02.2026**

UNTERRICHTUNG

durch den Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern

20. Tätigkeitsbericht zum Datenschutz

Berichtszeitraum: 1. Januar 2024 bis 31. Dezember 2024

Zugeleitet mit Schreiben des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern vom 4. Februar 2026.

Vorwort

Die Gesellschaft ist in einem Wandel begriffen. Sie digitalisiert sich immer mehr, analoge Prozesse werden sukzessive weniger. Dabei ist die Digitalisierung mehr als ein „Nice-to-have“, das vieles bequemer und schneller macht. Sie ist eine zwingende Notwendigkeit. Bedingt durch den Fachkräftemangel und die demografische Entwicklung werden wir viele Abläufe und Prozesse digitalisieren müssen, wenn wir die Angebote in gleichem Umfang wie bisher aufrechterhalten wollen. Das betrifft den öffentlichen Sektor genauso wie die Privatwirtschaft. Wo jedoch zunehmend digitalisiert und vernetzt wird, werden die theoretischen Zugriffsmöglichkeiten auf personenbezogene Daten immer größer. Die Gefahren nehmen deutlich zu und damit auch das grundrechtlich verankerte Bedürfnis nach Datenschutz. Diesem Bedürfnis wollen und müssen wir Rechnung tragen. Datenschutz ist Grundrechtsschutz, er gewährleistet die Menschenwürde im digitalen Raum. Dabei ist er keine rechtliche Hürde oder ein Hindernis, er ist unabdingbar in einem demokratischen Rechtsstaat. Wo Datenschutz abgebaut wird, verlieren Menschen ihre Rechte. Dessen muss man sich immer bewusst sein.

Dabei ist es wichtig, den Datenschutz frühzeitig in Entwicklungen einzubringen. Prinzipiell stellt seine Einhaltung nämlich bei Weitem keine so große Herausforderung dar, wie vielfach angenommen wird. Die Probleme entstehen meist erst dann, wenn er zu Prozessbeginn nicht mitgedacht wird und erst zum Ende hin – oder gar erst im Nachgang – implementiert werden muss. Wer etwas bauen will und sich im Vorfeld nicht über Bauvorschriften informiert, muss sich schließlich auch nicht wundern, wenn er im Baugenehmigungsverfahren mit unliebsamen Bedingungen, Auflagen oder gar einer Versagung konfrontiert wird. Im Datenschutz ist das ganz ähnlich. Es ist deshalb zu begrüßen, dass die Datenschutzbehörde von vielen Ministerien und nachgeordneten Behörden mittlerweile sehr oft bereits zu Beginn von Vorhaben beratend eingebunden wird. Es bleibt zu hoffen, dass sich diese Entwicklung weiter fortsetzt.

Darüber hinaus ist auch die Vermittlung von digitalen Kompetenzen ein wichtiges Anliegen meiner Behörde. Soziale Medien sind „die“ Kommunikationsplattformen dieser Zeit. Mit all ihren Vorteilen bringen sie aber auch Hass, Hetze oder Desinformation mit sich. Negative Aspekte, denen man sich ebenfalls stellen muss. Künstliche Intelligenz ist eine Technologie, die unsere Gesellschaft in beinahe allen Bereichen dauerhaft und grundlegend verändern wird. Die Gefahren sind ebenso groß wie der mögliche Nutzen. Auch davor kann und darf man die Augen nicht verschließen. Es ist deshalb wichtig, dass die Menschen diesen Herausforderungen informiert und kompetent gegenübertreten. Ein großer Teil dieser Kompetenzen muss natürlich im klassischen Bildungssystem vermittelt werden. Allerdings ist die Aufgabe zu komplex, als dass man Kitas, Schulen und Hochschulen mit ihr allein lassen könnte. Es handelt sich um eine gesamtgesellschaftliche Aufgabe, die von vielen Akteuren auf allen Ebenen angegangen werden muss. Wir werden unseren Teil mit unseren Medienkompetenzprojekten jedenfalls weiterhin leisten.

Mit dem vorliegenden 20. Tätigkeitsbericht möchte ich Sie über wichtige datenschutzrechtliche Themen sowie über ausgewählte Beratungs- und Beschwerdefälle informieren, mit denen sich meine Behörde im Berichtsjahr 2024 befasst hat. Ich bedanke mich ausdrücklich bei meinen Mitarbeiterinnen und Mitarbeitern für ihren Einsatz und ihr Engagement. Ich danke ebenso den Partnerinnen und Partnern in der öffentlichen Verwaltung sowie in den Unternehmen unseres Landes, die uns bei der Wahrnehmung unseres Auftrages unterstützten, und baue auch weiterhin auf eine vertrauensvolle Zusammenarbeit.

Sebastian Schmidt
Landesbeauftragter für Datenschutz und Informationsfreiheit
Mecklenburg-Vorpommern

Inhaltsverzeichnis

Teil A – 20. Tätigkeitsbericht zum Datenschutz

Berichtszeitraum: 1. Januar 2024 bis 31. Dezember 2024

1. Entwicklung der Behörde/Presse- und Öffentlichkeitsarbeit

Im Berichtszeitraum wurden weitere strukturelle Anpassungen innerhalb der Behörde vorgenommen. Diese ermöglichten etwa die zielgerichtete Beratung der Landesregierung im Bereich Künstliche Intelligenz (KI) oder die Durchführung von Kontrollen vor Ort.
Weiterhin wurde das EU-finanzierte Familienprojekt #DigitaleVorbilder – Familien gehen online. im Referat „Presse, Kommunikation und Medienbildung“ durchgeführt. Zusätzlich zu den Ergebnissen des Projektes fand ein Fachtag für pädagogische Fachkräfte statt. Das Ziel war es, mit den Materialien des Familienprojektes #DigitaleVorbilder die Elternarbeit in den Einrichtungen des Landes zu unterstützen. Der Fokus der Zusammenarbeit auf europäischer Ebene wurde weiter ausgebaut.

1.1 Zahlen, Daten, Fakten

Die Anzahl der Eingaben und Beschwerden, die es zu bearbeiten galt, steigerte sich im Berichtszeitraum 2024 noch einmal von 898 im Jahr 2023 auf 969 Beschwerden im Jahr 2024. Allerdings reduzierten sich die Datenpannenmeldungen gemäß Artikel 33 der Datenschutz-Grundverordnung (DS-GVO) im Berichtszeitraum auf 290 Meldungen gegenüber 401 Meldungen in 2023. Wir nahmen bereits in der Vergangenheit eine deutlich gesteigerte Sensibilität der Verantwortlichen in Bezug auf die Sicherheit von informationstechnischen Systemen wahr. Das spiegelt sich auch in unserem Beratungsaufkommen sowohl im öffentlichen als auch im nicht öffentlichen Bereich wider. Unsere Hinweise wurden dabei als sehr hilfreich und praktikabel angesehen. Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (LfDI M-V) wird den beratenden Charakter der Behörde weiterhin aufrechterhalten.

2. LfDI MV kontrolliert weiterhin verstärkt vor Ort

In der Theorie scheint es so einfach: Nach der DS-GVO muss ein Verantwortlicher dokumentieren und nachweisen können, dass er alle angemessenen Maßnahmen ergriffen hat, um datenschutzkonform zu agieren. Gelingt ihm dieser Nachweis nicht, kann die Datenschutzaufsichtsbehörde Maßnahmen ergreifen oder Bußgelder erlassen. Die DS-GVO, deren Macher/-innen vor allem die Schaffung zentraler Datenschutzaufsichtsbehörden in den Mitgliedstaaten vor Augen hatten, ermöglichte so Verfahren, die auch rein schriftlich über größere Entfernungen vonstattengehen könnten. Allerdings zeigt die Praxis, dass Verfahren rein nach Papierlage mit sehr strengen Maßnahmen zulasten der Verantwortlichen enden können, die sich bei genauerer Betrachtung eventuell als überzogen darstellen.

Insofern ermöglichen die föderalen Strukturen in Deutschland im Rahmen der vorhandenen personellen Ressourcen sinnvollerweise auch Ermittlungen vor Ort. Auch wenn der Begriff „Kontrolle“ zunächst nicht so angenehm klingt, erhalten unsere Teams, die im Berichtszeitraum verstärkt vor Ort im Einsatz waren, durchweg positives Feedback.

Denn tatsächlich verbirgt sich hinter dem Begriff „Kontrolle“ eher selten eine echte Durchsuchung, viel häufiger handelt es sich um Beratungs- und Informationsgespräche. Das gibt uns die Möglichkeit, genau zu erläutern, was konkret mit einem angeforderten Dokument gemeint ist und warum es vorzuhalten wäre. Wir können sofort gezielte Nachfragen stellen und an uns gerichtete Fragen beantworten. Bei nicht eingriffsintensiven Verfahren kann das sogar dazu führen, dass Verfahren vor Ort eingestellt werden können, ohne dass weiterer Aufwand auf die Verantwortlichen zukommt. Gerade bei der Videoüberwachung durch Privatpersonen, die öffentlichen Raum filmen, aber eigentlich nur ihr eigenes Grundstück schützen wollen, ist die Vor-Ort-Kontrolle – soweit sie personell machbar ist – ein schneller und unbürokratischer Weg, einen datenschutzkonformen Zustand herzustellen (siehe Punkt 5.2).

Natürlich gibt es auch deutlich förmlichere Kontrollen, in denen wir beispielsweise auch die Technik beim Verantwortlichen in Augenschein nehmen. So kontrollierten wir etwa eine Reha-Klinik, über die sich ein Patient beschwert hatte. Hier hatte uns die Papierlage zunächst skeptisch gemacht, weil sich der Verantwortliche eher ungünstig für sich selbst geäußert hatte. Bei der Kontrolle vor Ort konnte der in der Beschwerde geäußerte Vorwurf aber vollständig ausgeräumt werden. Doch selbst wenn sich in solchen Kontrollen ein Verdacht bestätigt, kann ein Verwaltungsverfahren teilweise vermieden werden, weil der Verantwortliche bereits unsere mündliche Einschätzung zum Anlass nimmt, einen datenschutzwidrigen Zustand ohne förmliche Anordnung abzustellen.

Und auch in laufenden Bußgeldverfahren, in denen wir selbstverständlich auf die notwendigen Belehrungen achten, wenn wir vor Ort mit den Betroffenen ins Gespräch kommen, treten nicht selten Umstände zutage, die zumindest die Bußgeldhöhe noch zugunsten der Verantwortlichen beeinflussen können.

Leider können wir aus Kapazitätsgründen nicht alle eingehenden Fälle mit Kontrollen vor Ort bearbeiten. Und auch nicht jeder Fall ist dafür geeignet. Sind wir aber vor Ort, profitieren in der Regel alle Beteiligten davon.

3. Technik und Organisation

Der aktuelle Berichtszeitraum war geprägt von Beratungsanfragen zum Thema Künstliche Intelligenz (KI). Dabei zeigte sich zum einen, dass der Einsatz von KI in sämtlichen Bereichen, z. B. in der Wirtschaft, Bildung oder Verwaltung, und unterschiedlichen Dimensionen angestrebt wird, sich zum anderen jedoch viele Projekte noch am Anfang bzw. in der Planungsphase befinden. Eine neue Herausforderung stellt dabei insbesondere die am 1. August 2024 in Kraft getretene europäische Verordnung über Künstliche Intelligenz (KI-VO[1]) dar. Da die KI-Verordnung vor allem den rechtlichen Rahmen für die Marktregulierung von KI bildet, kann in einigen Fällen auch ein Spannungsverhältnis zu den Inhalten anderer Rechtsakte wie der DS-GVO entstehen. So regelt die KI-Verordnung, mit Ausnahme von sehr eng gefassten Sonderbestimmungen, nicht den Umgang mit personenbezogenen Daten, sondern verweist hier auf die DS-GVO, die dann parallel angewendet werden muss.

[1] URL: https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_de [aufgerufen am 14.04.2025].

Solange dieses Spannungsverhältnis nicht auf europäischer Ebene harmonisiert wird, birgt es einige Hürden und muss beim Einsatz von KI in sämtlichen Bereichen im Blick behalten werden.

Bemerkenswert ist das in Mecklenburg-Vorpommern bereits vorhandene technische Know-how, wie z. B. im Zentrum für Künstliche Intelligenz (KI MV) oder im Regionalen Zukunftszentrum Mecklenburg-Vorpommern+ (ZMV+) sowie die Umsetzungsgeschwindigkeit, die in einigen Anwendungsbereichen erreicht wird.

3.1 Arbeitskreis „Technische und organisatorische Datenschutzfragen“

Die Datenschutzkonferenz (DSK) hat dem LfDI MV seit 1993 die Leitung des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ (AK Technik) übertragen. Dieses Gremium koordiniert das Zusammenwirken der deutschen Datenschutzaufsichtsbehörden im Technikbereich. Wir berichten darüber regelmäßig.

Es ist eine gute Tradition, dass hierzu auch Gäste aus Datenschutzaufsichtsbehörden der Schweiz und Liechtensteins, der katholischen und der evangelischen Kirche sowie des öffentlich-rechtlichen Rundfunks eingeladen werden. Im Berichtszeitraum neu hinzugekommen ist eine Vertretung des Medienbeauftragten für den Datenschutz bei der Bayerischen Landesmedienanstalt, stellvertretend für die Datenschutzaufsicht über private Rundfunkveranstalter und Medien. Im Berichtszeitraum fanden zwei Sitzungen des AK Technik statt, die 82. Sitzung als Videokonferenz und die 83. Sitzung in Schwerin.

In den beiden Sitzungen nahmen die geplanten Leitlinien des Europäischen Datenschutzausschusses (EDSA) zu Anonymisierung und Pseudonymisierung wie auch in den Vorjahren breiten Raum ein. Aufgrund der hohen Bedeutung dieser Begriffe, nicht zuletzt auch für die tägliche Arbeit in den Datenschutzaufsichtsbehörden, veranstaltete der AK Technik zusätzlich einen mehrstündigen Workshop zu den beiden Leitlinienentwürfen. Zum Ende des Berichtszeitraums zeichnete sich dann ab, dass die Leitlinien zur Pseudonymisierung Anfang 2025 verabschiedet werden würden.

Die Weiterentwicklung des Standard-Datenschutzmodells (SDM) bildete einen weiteren Schwerpunkt in beiden Sitzungen. In der 82. Sitzung verabschiedete der AK Technik die Version 3.1 des SDM, welche anschließend auch von der DSK bestätigt wurde. Gegenüber der Version 3.0 wurde vor allem das Kapitel D2.2 überarbeitet. Dort geht es um die Mittel der Verarbeitung. Hintergrund dieser Änderung ist, dass der rechtskonforme Einsatz von Mitteln zur Verarbeitung personenbezogener Daten, insbesondere von technischen Betriebsmitteln, von den für die Verarbeitung personenbezogener Daten Verantwortlichen nachzuweisen ist. Darüber hinaus haben die Mitglieder Vorschläge für die DSK erarbeitet, mit denen die Arbeit am SDM intensiviert und auf eine breitere Basis gestellt werden wird. Diese Vorschläge hat die DSK aufgenommen und verabschiedet.

Während der 82. Sitzung brachten die Mitglieder eine Zusammenarbeit des AK Technik mit der Föderalen IT-Kooperation (FITKO) auf den Weg. Die FITKO ist eine Anstalt des öffentlichen Rechts mit Sitz in Frankfurt am Main. Sie koordiniert im Auftrag des IT-Planungsrats die Digitalisierung der öffentlichen Verwaltung zwischen Bund und Ländern. Dazu steuert die FITKO Projekte und die Entwicklung von Produkten und Standards für die öffentliche Verwaltung, die in der Regel bundesweite Bedeutung haben.

Neben dem AK Technik arbeiten auch der AK Verwaltung und andere Gremien der DSK mit der FITKO zusammen, um gezielt auf die Einhaltung des Datenschutzes bei für die öffentliche Verwaltung so wichtigen Vorhaben der FITKO hinzuwirken.

In der 83. Sitzung sprach ein Gastreferent über den Mobilfunk-Standard der 6. Generation, der sich derzeit in Planung befindet. In diesem Normenwerk werden voraussichtlich Radar-Funktionen standardisiert werden, mit denen auch das Verhalten von Personen überwacht werden kann. Dies betrifft nicht nur Nutzer/-innen von Geräten nach dem neuen Standard, sondern auch Personen in deren Umgebung. Im Zusammenwirken von Endgeräten und Infrastrukturkomponenten könnte beispielsweise ermittelt werden, ob eine gesundheitlich beeinträchtigte Person in einer Wohnung stürzt, sodass automatisch Hilfe gerufen werden könnte. Ebenso kann eine solche Technik auch missbraucht werden. Beispielsweise könnten Unbefugte so feststellen, ob sich in nicht einsehbaren Räumen Menschen befinden, und diese sogar identifizieren. Derartige Anwendungen können teilweise auch schon mit bereits vorhandenen, drahtlosen, lokalen Netzen (Wireless LAN, WLAN) realisiert werden. Dort erfordern sie jedoch besondere Modifikationen an den bestehenden Systemen. Gemäß dem Mobilfunk-Standard der 6. Generation wären solche Funktionen zukünftig bereits ab Werk verfügbar. Um die Gefahren dieser Entwicklung sowie passende Gegenmaßnahmen aufzuzeigen, hat der AK Technik eine entsprechende Arbeitsgruppe ins Leben gerufen.

3.2 Einsatz von Künstlicher Intelligenz

Die Nutzung von Systemen, die KI für die Verarbeitung von Eingaben und die Erzeugung von Ausgaben einsetzen, erfreut sich weltweit rasant steigender Nutzungszahlen. Dies gilt sowohl für die großen Sprachmodelle, die Large Language Models (LLM), als auch für weitere Anwendungsfälle des maschinellen Lernens.

Es ist offensichtlich, dass die Anwendung von KI-Systemen in der Wertschöpfungskette einer Organisation einen zentralen Gewinn aufgrund einer besonders effizienten Nutzung und Verarbeitung großer Datenmengen darstellen kann. In Pilotprojekten innerhalb der Landesverwaltung Mecklenburg-Vorpommern wird ebenfalls deutlich, dass durch den Einsatz von KI in der öffentlichen Verwaltung ein klarer Effizienzgewinn erwartet wird. Diese Pilotprojekte, aber auch die vielfältigen Forschungsprojekte im Land bestätigen das starke Interesse. In jedem dieser Projekte wird jedoch deutlich, dass die Qualität der erzielten Ergebnisse direkt mit der Qualität und Quantität der verwendeten Trainingsdatensätze zusammenhängt, die sehr häufig eine Vielzahl von personenbezogenen Daten enthalten. Vor dem Hintergrund der digitalen Souveränität ergibt sich angesichts der weltpolitischen Lage jedoch die Herausforderung, dass sich viele Anbieter/-innen von KI-Systemen mit ihrem Geschäftssitz außerhalb der Europäischen Union (EU) befinden.

Die geschilderte Ausgangslage zeigt die Herausforderungen an einen verantwortungsvollen und informierten Umgang mit KI-Systemen und der damit verbundenen Verarbeitung von personenbezogenen Daten. Ergänzend zu den bestehenden Regelungen in der Datenschutz-Grundverordnung ist mit der KI-VO ein weiterer rechtlicher Rahmen erlassen worden, der in diesem Kontext Berücksichtigung finden muss.

Gerade vor dem Hintergrund, dass bei KI-Systemen Datenverarbeitungen in großem Umfang stattfinden und sich die Technologie momentan rasant weiterentwickelt, sind die rechtlichen Rahmenbedingungen, nicht zuletzt auch verstärkt im Sinne der Betroffenenrechte, einwandfrei zu klären.

Wir beraten daher im Rahmen unserer Möglichkeiten konstant und aktiv die Entwicklung und den Einsatz von KI, sowohl in der öffentlichen Verwaltung als auch im Rahmen von Forschungsprojekten. Dazu zählen beispielsweise Vorträge auf der IT-Sicherheitskonferenz an der Hochschule Stralsund, dem Neubrandenburger Geosymposium 2024 an der Hochschule Neubrandenburg oder im Rahmen diverser Weiterbildungen an der Fachhochschule für öffentliche Verwaltung, Polizei und Rechtspflege des Landes Mecklenburg-Vorpommern in Güstrow. Zudem haben wir einen permanenten Austausch mit dem Zentrum für Künstliche Intelligenz in Mecklenburg-Vorpommern etabliert und befinden uns im regelmäßigen Gespräch mit dem Ministerium für Bildung und Kindertagesförderung Mecklenburg-Vorpommern (BM MV) hinsichtlich des Einsatzes von KI in der Lehre. Weiterhin begleiten wir die Planungen zum Einsatz von KI im Rahmen eines Pilotprojektes im Finanzministerium Mecklenburg-Vorpommern.

3.3 Beratung zum Einsatz von Künstlicher Intelligenz an Schulen

Wie unter Punkt 3.2 des vorliegenden Berichtes angesprochen, befindet sich der LfDI MV in Beratungsgesprächen mit dem BM MV hinsichtlich des Einsatzes von KI im Bildungsbereich. Das Land setzt im Rahmen der Online-Weiterbildung von Lehrkräften bereits auf einen konkreten Anbietenden und verfügt hierzu über eine entsprechende Landeslizenz. Seitens dieses Anbietenden ist es nach einer Angebotserweiterung auch möglich, KI-Assistenzen für die Unterrichtsvorbereitung und ggf. auch im Unterricht einzusetzen. Um die datenschutzrechtlichen Aspekte des Einsatzes der KI-Assistenzen zu erörtern, wandte sich das BM MV an den LfDI MV. Diesbezüglich gab es im vorliegenden Berichtszeitraum drei gemeinsame Treffen. Inhalte der bisherigen Gespräche waren u. a. Punkte zu Verantwortlichkeiten beim Einsatz von KI sowie die vertraglichen Rahmenbedingungen im Bereich des Datenschutzrechtes. Insbesondere wurde die Gestaltung von Verträgen zur Auftragsverarbeitung thematisiert und das Erfordernis zur Erstellung einer Datenschutzfolgenabschätzung (DSFA). Neben den datenschutzrechtlichen Aspekten wurde seitens des LfDI MV der Hinweis gegeben, dass die Güte, d. h. die Qualität der Ausgaben einer KI, seitens der Betreiber im Rahmen des pädagogischen Einsatzes im Schulbereich kritisch geprüft werden sollte.

Ein Teilergebnis aus diesen Gesprächen ist die Herausgabe einer entsprechenden Mitteilung durch das BM MV an die öffentlichen Schulen im Land. In dieser wird darauf aufmerksam gemacht, dass für die Nutzung der KI-Assistenzen in Schule und Unterricht, d. h. insbesondere durch Schüler/-innen, die fortlaufenden Beratungen und Abstimmungen mit dem LfDI MV noch nicht abgeschlossen sind. Ein Einvernehmen mit dem LfDI MV für die Nutzung in Schule und Unterricht liege derzeit noch nicht vor. Die Nutzung der KI-Assistenzen in Schule und Unterricht ist daher noch nicht freigegeben.

Wir empfehlen dem Ministerium für Bildung und Kindertagesförderung des Landes Mecklenburg-Vorpommern, den Austausch mit unserer Behörde hinsichtlich der Beratung zum Einsatz von KI-Assistenzen in Schulen fortzuführen.

3.4 Projekt Integriertes Schulmanagementsystem

Auch im vorliegenden Berichtszeitraum wurden die Beratungen zwischen dem LfDI MV und dem Ministerium zum Projekt Integriertes Schulmanagementsystem (ISY MV) fortgeführt.

Die einzelnen Themen, zu denen sich ausgetauscht und beraten wurde, waren auch diesmal umfangreich und herausfordernd. Ein zeitintensiver Themenschwerpunkt war beispielsweise eine mögliche gemeinsame Verantwortung der unterschiedlichen Akteure im Schulbereich. Es galt zu erörtern, inwieweit diese Form der geteilten Verantwortung im Kontext Schule möglich ist. Diesbezüglich wurden auch Fragen zu möglichen Rückgriffen auf das aktuelle Schulgesetz diskutiert, um daraus für einzelne Fachverfahren die gemeinsame Verantwortung abzuleiten. Ferner wurde das Thema E-Mail-Bereitstellung für Lehrkräfte und deren Einführung besprochen. Im Rahmen dieser Einführung wurde die 2-Faktor-Authentifizierung bei der Anmeldung von Lehrkräften am zentralen Identitätsmanagementsystem des Landes etabliert. Hierzu ergingen im Vorfeld entsprechende beratende Hinweise durch den LfDI MV. Ebenso erfolgte die datenschutzrechtliche Beratung zu geplanten Modulen des integrierten Schulmanagementsystems, wie z. B. Onlinemanagement in Schulen (OMNIS) und dem Klassenbuch- und Stundenplan-Modul (KlauS). Neben diesen Beratungen zu aktuellen Themen des BM MV spricht der LfDI MV regelmäßig weitere Punkte an, welche sich aufgrund datenschutzrechtlicher und politischer Entwicklungen als Herausforderung für Verantwortliche darstellen könnten. Dies betrifft insbesondere den Prozess hin zur digitalen Souveränität und hierbei speziell die Einführung und Nutzung von Textverarbeitungs-Software aus dem Open-Source-Bereich. Alle angesprochenen Themen sind dabei Querschnittsthemen der zentralen Bereitstellung von Softwareprodukten im Schulbereich. Der LfDI MV hat bereits im letzten Tätigkeitsbericht[2] die Zentralisierung der Bereitstellung und Beschaffung von Softwareprodukten im Schulbereich adressiert. Die Erfahrung zeigt, dass die zentrale Bereitstellung von Softwareprodukten im Schulbereich viele Vorteile für die Schulen im Land mit sich bringt. So brauchen sich diese nicht mit Beschaffungsprozessen auseinanderzusetzen. Zusätzlich werden zentrale datenschutzrechtliche Fragestellungen im Vorfeld geklärt. Auf diese Weise werden Schulen entlastet und können so noch besser ihrem gesetzlichen Bildungsauftrag nachgehen.

Der Austausch mit dem BM MV sowie mit weiteren Teilnehmer/-innen, u. a. dem Zweckverband elektronische Verwaltung Mecklenburg-Vorpommern (eGo MV), wird seitens des LfDI MV als sehr konstruktiv, produktiv und zukunftsweisend im Sinne einer verwaltungsübergreifenden Zusammenarbeit wahrgenommen.

Wir empfehlen dem Ministerium für Bildung und Kindertagesförderung des Landes Mecklenburg-Vorpommern, den Austausch mit unserer Behörde, insbesondere zum Projekt ISY MV, fortzuführen und zu prüfen, ob und wie die zentrale Bereitstellung von Softwareprodukten im Schulbereich weiter ausgebaut werden kann.

[2] Siehe hierzu Punkt 3.7.1 Auftragsverarbeitung und Digitalisierung im Bereich Schule in URL: https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Taetigkeitsberichte/lfdmvtb18-19.pdf [abgerufen am 28.03.2025].

3.5 Austausch mit den Gemeinsamen Datenschutzbeauftragten an Schulen des Zweckverbands Elektronische Verwaltung in Mecklenburg-Vorpommern

Mit dem Voranschreiten der Digitalisierung im Schulbereich ist die Bedeutung des Datenschutzes weiter in den Vordergrund gerückt. Die Herausforderungen nehmen zu und eine datenschutzrechtliche Expertise ist an den Schulen umso mehr gefragt. Um dieser Entwicklung Rechnung zu tragen, ist es den öffentlichen Schulen im Land seit dem 1. März 2020 möglich, einen Datenschutzbeauftragten aus den Gemeinsamen Datenschutzbeauftragten an Schulen (GDSBaS) des eGo MV (eGo MV) zu bestellen. Die Datenschutzbeauftragten überwachen an den Schulen die Einhaltung der datenschutzrechtlichen Bestimmungen und sensibilisieren für den verantwortungsvollen Umgang mit personenbezogenen Daten, sowohl durch die Schulleitung als auch durch die Lehrkräfte selbst.

Die Vorteile sind dabei vielfältig. So tragen die Datenschutzbeauftragten nicht nur zur Minimierung rechtlicher Risiken und zur Vermeidung von Datenschutzverletzungen bei, sondern fördern auch das Vertrauen von Eltern und Schüler/-innen in die Schule als eine verantwortungsvoll agierende Institution.

Der LfDI MV befürwortet die Arbeit und das Wirken der GDSBaS des eGo MV an den Schulen ausdrücklich. Zudem steht der LfDI MV mit den GDSBaS im fachlichen Austausch über das Projekt ISY (siehe Punkt 3.3). Um den fachlichen Austausch weiter zu vertiefen, fand im Frühjahr und Winter des vorliegenden Berichtszeitraumes jeweils ein Treffen zwischen Vertreterinnen und Vertretern der GDSBaS und dem LfDI MV statt. Dabei standen wichtige Themen und Fragen wie die Verantwortlichkeiten im Schulbereich, die Nutzung privater Endgeräte, Fragen zur Archivierung und Löschung als auch Sachstandsmitteilungen aus dem Arbeitskreis Schule und Bildungseinrichtungen der DSK auf der Agenda. Die Treffen wurden durchweg positiv bewertet und es wurde vereinbart, dieses Format zwischen den GDSBaS und dem LfDI MV zu verstetigen.

Auch im Tagesgeschäft des LfDI MV zeigt sich die gute datenschutzrechtliche Arbeit der GDSBaS im Land. So wird bei Beratungsanfragen von Schulen immer wieder deutlich, dass dort nun datenschutzrechtliche Fachkenntnisse vorhanden sind. Zudem stehen dem LfDI MV bei Beschwerden im Schulbereich mit den GDSBaS fachliche Ansprechpartner/-innen zur Verfügung.

3.6 Elektronische Akte

Bereits seit dem Jahr 2016 begleiten wir beratend die Einführung einer elektronischen Akte für die Behörden Mecklenburg-Vorpommerns (E-Akte MV)[3].

Im vorliegenden Berichtszeitraum hat ein anbietendes Unternehmen den Zuschlag zur Einführung einer elektronischen Akte erhalten, sodass nun eine finale Zielarchitektur entworfen und ein Landesmaster auf einer Test- und Referenzumgebung umgesetzt wurde.

[3] Vgl. u. a. Punkt 4.1 in URL: https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Taetigkeitsberichte/lfdmvtb17.pdf [abgerufen am 27.03.2025].

In diesem Master, welcher auf der E-Akten-Software eGov-Suite basiert, werden nun die im Vorfeld ermittelten technischen und organisatorischen Anforderungen abgebildet und erste Pilotbehörden angeschlossen. Zu den organisatorischen Anforderungen zählen auch die Erstellung von zentralen Konzepten, z. B. hinsichtlich der Umsetzung von Informationssicherheit, der Protokollierung oder der Rechte- und Rollenvergabe, sowie die Gestaltung von Rahmendienstvereinbarungen, welche die Einführung, Umsetzung und Nutzung eines Dokumentenmanagements- und Vorgangsbearbeitungssystems als elektronische Akte regeln.

In diesem Zusammenhang berieten wir in einem konstruktiven Austausch das zuständige Projektteam im Rahmen der Sitzungen der Kommission für Informationssicherheit (KofIS) schwerpunktmäßig zum Thema der Mandantenfähigkeit. Hinter jedem Mandanten verbirgt sich dabei ein abgeschlossener Datenhaltungs- und Verarbeitungskontext eines Verantwortlichen. Die getrennte Verarbeitung im Rahmen von verschiedenen Verarbeitungstätigkeiten wird dabei als „Mandantentrennung“ bezeichnet. Die zur Datenverarbeitung eingesetzte Informationstechnik mit ihren einzelnen IT-Komponenten gilt dann als „mandantenfähig“, wenn sie in der Lage ist, zwischen verschiedenen Mandanten eine notwendige und erforderliche Trennung umzusetzen.

Die Abgeschlossenheit eines Mandanten bedingt zwangsweise auch eine sicherheitstechnische Isolation. Bei ausreichender Trennung der Datenverarbeitung dürfen u. a. Datenschutzprobleme oder -vorfälle eines Mandanten nicht zu Datenschutzproblemen oder -vorfällen anderer Mandanten führen.

Wäre beispielsweise in einem System die Möglichkeit gegeben, mandantenübergreifende Zugriffe auf eigene Daten oder Daten eines anderen Mandanten zu initiieren, oder wird diese Möglichkeit nur durch organisatorische Maßnahmen ausgeschlossen, läge keine Abgeschlossenheit vor und die Mandantenfähigkeit wäre nicht gegeben.

Eine Mandantenfähigkeit kann grundsätzlich durch verschiedene Trennungsgrade erreicht werden, wobei jedoch stets der Schutzbedarf aus Sicht der Informationssicherheit und aus Sicht des Datenschutzes, die in der Regel Hand in Hand gehen, zu berücksichtigen ist. Vernetzte, gemeinsam genutzte Dienste und Systeme bilden dabei grundsätzlich ein Risiko für das datenschutzrechtliche Trennungsgebot und die IT-Sicherheit, sodass es diesbezüglich stets einer Abwägung bedarf.

Im Rahmen unserer Beratungen wurde seitens des für die Einführung der E-Akte zuständigen Ministeriums für Inneres, Bau und Digitalisierung Mecklenburg-Vorpommern (MIBD MV) die Frage aufgeworfen, ob anstelle der ursprünglich geplanten, mehreren parallel laufenden Instanzen auch eine einzelne Landesinstanz ausreichen könnte. Hierbei verspricht man sich – insbesondere mit Blick auf die finanziellen Kosten und den administrativen Aufwand – ein deutliches Einsparungspotenzial.

Wie bereits erläutert, bringt der Betrieb auf nur einer Instanz, insbesondere bei einem hohen Schutzbedarf, verschiedene Auswirkungen mit sich, denen mit weiteren technischen und organisatorischen Maßnahmen (TOM) begegnet werden muss. Die Erfahrung zeigt, dass diese zusätzlichen Anforderungen nicht ohne Weiteres umzusetzen sind. Beispielhaft sei genannt, dass ganz andere Verfügbarkeitsanforderungen gelten, denn der Ausfall einer Komponente innerhalb der Instanz kann auch zum Stillstand aller Mandanten führen. Im konkreten Fall wäre dann die gesamte Landesverwaltung nicht mehr in der Lage, mit der E-Akte MV zu arbeiten, während bei einer sogenannten Mehrinstanzlösung nur einer oder wenige Mandanten betroffen wären. Dementsprechend ist zu prüfen, mit welchen Hochverfügbarkeitsmaßnahmen diesem Risiko zu begegnen und der womöglich höhere Aufwand zu bewerten ist.

Ein anderes Beispiel betrifft die Protokollierung. So dürfen sich sowohl die mandantenspezifische Nutzungsprotokollierung als auch die administrative Protokollierung nur auf Schritte zur Datenverarbeitung beziehen, die den jeweiligen Mandanten betreffen. Auch hier ist eine Umsetzung im Detail regelmäßig aufwendiger und komplexer.

Neben den genannten Beispielen können weitere datenschutzrechtliche Anforderungen auch dem Baustein 50 „Trennen“[4] des SDM entnommen werden.

Eine endgültige Entscheidung, welche Lösung seitens des zuständigen Ministeriums letztlich angestrebt wird, wurde im Berichtszeitraum noch nicht getroffen. Gleichwohl muss mit Blick auf generelle Risiken im IT-Projektmanagement festgehalten werden, dass sich ändernde Anforderungen – insbesondere, wenn diese einen größeren Umfang besitzen – einer der häufigsten Gründe sind, warum Digitalisierungsprojekte aus der Zeitschiene geraten oder gänzlich scheitern. Während häufig die Argumentation herangeführt wird, dass datenschutzrechtliche Anforderungen hierfür verantwortlich seien, zeigt sich in der Realität hingegen häufig, dass vielmehr sich ändernde Projektanforderungen und/oder eine verspätete Berücksichtigung der Anforderungen der IT-Sicherheit und des Datenschutzes dafür verantwortlich gemacht werden können.

3.7 Überarbeitung der Orientierungshilfe Digitale Dienste

Im vorangegangen Tätigkeitsbericht[5] informierten wir unter Punkt 4.8.2 bezüglich der Orientierungshilfe für Anbieter/-innen von Telemedien. Da die Digitalisierung einem stetigen Wandel unterliegt, wurde im vorliegenden Berichtszeitraum die Orientierungshilfe für Anbieter/-innen von Telemedien überarbeitet. Sie führt nun die Bezeichnung Orientierungshilfe für Anbieter/-innen von digitalen Diensten[6] (OH Digitale Dienste).

[4] URL: https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDMV2.0_Trennen_V1.0.pdf [abgerufen am 27.03.2025].

[5] URL: https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Taetigkeitsberichte/lfdmvtb18-19.pdf [abgerufen am 28.03.2025].

[6] URL: https://datenschutzkonferenz-online.de/media/oh/OH_Digitale_Dienste.pdf [abgerufen am 28.03.2025].

Die Anpassung wurde nötig, da gemäß Artikel 8 „Änderungsgesetz zur Einführung des Digitale-Dienste-Gesetzes“[7] (DDG) der Begriff „Telemedien“ im Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) nunmehr durch den Begriff „digitale Dienste“ ersetzt wurde. Als Folge wurde auch das TTDSG in das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) umbenannt. Gleichzeitig ist mit dem Inkrafttreten des DDG das Telemediengesetz (TMG) außer Kraft getreten.[8]

Inhaltlich wurde die Orientierungshilfe nun den neuen Begrifflichkeiten, weg von „Telemedien“ hin zu „digitalen Diensten“, angepasst. Weiterhin wurden Anpassungen hinsichtlich des Datentransfers in die Vereinigten Staaten von Amerika (USA) vorgenommen. Wenngleich die inhaltlichen Anpassungen nicht allzu umfangreich sind, ist in der Praxis immer wieder festzustellen, dass Verantwortliche den rechtlichen Rahmen rund um das Anbieten von digitalen Diensten weiterhin als Herausforderung betrachten. Auch die nachgelagerte Datenverarbeitung von personenbezogenen Daten gemäß der DS-GVO wird teilweise als Herausforderung angesehen.

Wir empfehlen Anbieter/-innen von digitalen Diensten aus dem öffentlichen und nicht öffentlichen Bereich, sich mit der neuen Version der Orientierungshilfe Digitale Dienste vertraut zu machen und ihre Dienste auf Datenschutzkonformität nach dem neuen TDDDG, auch hinsichtlich des Einsatzes von Cookies, zu prüfen. Darauf aufbauend ist zu prüfen, ob sich die anschließenden Datenverarbeitungen von personenbezogenen Daten auf eine entsprechende Rechtsgrundlage aus der DS-GVO stützen lassen. Bei Unregelmäßigkeiten sind Maßnahmen zu ergreifen, um dem Grundrecht der Betroffenen auf informationelle Selbstbestimmung zu entsprechen.

4. Bildungsauftrag der Behörde

Alle Bereiche der Gesellschaft sind durchdrungen von digitalen Geräten, Anwendungen, Services und Prozessen. Ob im Bildungs- oder Berufsalltag, in Verkehr und Mobilität, in der Verwaltung, beim Einkaufen, in der Arztpraxis, im Smart Home bis hinein ins Kinderzimmer – überall im Alltag werden Daten durch die Benutzung von technischen Alltagsunterstützern, digitalen Unterhaltungsangeboten oder Kommunikationsmitteln erzeugt. Die rasante Weiterentwicklung immer neuer Angebote erfordert von jedem Einzelnen eine stetige Auseinandersetzung mit den digitalen Anwendungen, den Chancen und Risiken ihrer Nutzung zum Schutz der eigenen Daten und Privatsphäre.

---

[7] Artikel 8 des Gesetzes zur Durchführung der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG sowie zur Durchführung der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten und zur Änderung weiterer Gesetze vom 6. Mai 2024 (BGBl. 2024 I Nr. 149).

[8] vgl. Artikel 37 des Gesetzes zur Durchführung der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG sowie zur Durchführung der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten und zur Änderung weiterer Gesetze vom 6. Mai 2024 (BGBl. 2024 I Nr. 149).

Die DS-GVO schützt die Grundrechte und -freiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten. Neben den hoheitlichen Aufgaben einer Datenschutzaufsichtsbehörde sollen die Aufsichtsbehörden gemäß Artikel 57 Absatz 1 Buchstabe b DS-GVO „[…] die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung sensibilisieren und sie darüber aufklären. Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder […]“. Dieser Aufgabe kommt der LfDI MV schon weit vor der Einführung der DS-GVO seit mehr als zehn Jahren engagiert nach[9].

Datenschutz ist langweilig? Auf gar keinen Fall. In unseren Veranstaltungen für Kinder und Jugendliche diskutieren wir die Notwendigkeit von Privatsphäre und wie schwer es die Anbieter/-innen einem machen, das zu verstehen. Wir besprechen Wahlmanipulationen übers Netz, den wertschätzenden Umgang im Netz und technische Tipps und Tricks. Eltern motivieren wir, sich mit der Medienwelt ihrer Kinder auseinanderzusetzen – manchmal auch mit einem Schockmoment. Wir fordern das Engagement der Eltern ein und zeigen ihnen, wie sie sich mit ihren Kindern gut und sicher durch die Medienwelt bewegen können. Pädagogische Fachkräfte ermuntern wir, sich mit der Vermittlung von Medienkompetenz/digitalen Kompetenzen zu beschäftigen, und geben ihnen die Möglichkeit, sich auszuprobieren.

Konkret informierte der LfDI MV im Zeitraum vom 1. Januar bis 31. Dezember 2024 in 45 Bildungsveranstaltungen verschiedene Zielgruppen im Land, darunter 13 online durchgeführte Webinare mit unbegrenzter Reichweite. Dadurch konnten wir insgesamt 2236 Personen, d. h. Schüler/-innen, Eltern und Familien, pädagogische Fachkräfte, sowie die allgemeine Öffentlichkeit erreichen. Die folgenden Abbildungen geben einen Überblick über unsere durchgeführten Bildungs- und Informationsangebote und deren Verteilung auf die jeweilig adressierten Zielgruppen (siehe Abb. 3 und 4). Nachfolgend berichten wir ausführlich zu unserem umfangreichen Bildungsangebot im Bereich Datenschutz und Medienkompetenz.

Wir fordern die Landesregierung dazu auf, weiter Sorge dafür zu tragen, dass der LfDI MV seine umfangreichen Bildungsangebote weiterhin für Menschen aller Altersgruppen aufrechterhalten kann. Des Weiteren raten wir der Landesregierung, eine Vernetzung medienpädagogischer Institutionen im Land mithilfe einer neuen „Kooperationsvereinbarung zur Förderung von Medienkompetenz in Mecklenburg-Vorpommern“ vermehrt zu unterstützen. Der LfDI MV bleibt hierbei ein bewährter Partner und unterstützt die Landesregierung bei der Vernetzung.

[9] Vgl. vorangegangene Tätigkeitsberichte 11.-19. in URL: https://www.datenschutz-mv.de/datenschutz/publikationen/taetigkeitsberichte/ [abgerufen am 24.02.2025].

4.1 Kinder und Jugendliche

Für den LfDI MV stehen im Bereich der digitalen Bildung seit vielen Jahren die Aufklärung und Sensibilisierung von Kindern und Jugendlichen im Vordergrund. Dazu gehören neben den Besuchen in verschiedenen Schulklassen zu Projekttagen auch das bundesweit anerkannte Medienscouts-MV-Projekt und die Zusammenarbeit innerhalb der Tage ethischer Orientierung – protect privacy im Bereich der 5. und 6. Klassen. Alle Angebote wurden im Berichtszeitraum weiter fortgesetzt und ausgebaut.

Medienscouts MV – Jugend klärt auf

Unser Jugendprojekt Medienscouts MV – Jugend klärt auf konnten wir im Berichtszeitraum planmäßig zweimal durchführen. Bei der örtlichen Auswahl ist es unser Hauptanliegen, jeweils einen Ort in Mecklenburg und einen in Vorpommern zu ermöglichen, um flächendeckend präsent zu sein. Somit bildeten wir im Frühjahr neue Medienscouts MV in Waren (Müritz) und im Herbst in Greifswald aus. Das Projekt wird in enger Zusammenarbeit mit unseren Kooperationspartner/-innen realisiert: mit dem Landeskriminalamt MV (LKA MV), der Landeskoordinierungsstelle für Suchtthemen MV (LAKOST MV), dem Landesjugendring Mecklenburg-Vorpommern e. V. (LJR MV), der ComputerSpielSchule Greifswald (CSG) und dem Medientrecker der Mediatope Rostock und Neubrandenburg der Landesmedienanstalt Mecklenburg-Vorpommern (MMV). Nur mithilfe dieser Partnerinstitutionen können wir in diesem Gemeinschaftsprojekt eine breite und aktuelle Themenvielfalt garantieren und zur flächendeckenden Vermittlung von Medienkompetenz in unserem Land beitragen. Die derzeit verstärkte Nutzung digitaler Medien und das Thema Medienkompetenz beeinflussen die gesamte Gesellschaft. Die rasante technische Entwicklung stellt uns alle vor neue Herausforderungen: Cybermobbing, Cybergrooming, KI, Fake News, Deepfakes, Abzockmaschen usw. Wir plädieren stets für stärkere Initiativen zu Medienschutzmaßnahmen seitens der Tech-Konzerne, obwohl die allererste Medienschutzkomponente die eigene Medienkompetenz darstellt. Die Aktualität der Ausbildungsinhalte unterstreicht den Mehrwert, Medienscouts an Schulen zu haben. 2024 konnten wir weitere 44 Jugendliche aus achten bis zehnten Klassen aus verschiedenen Schulen in MV als qualifizierte Medienscouts MV ausbilden, die durch eine Multiplikation des Wissens unerlässliche Themen der Medienkompetenz im Peer-to-peer-Austausch in Freundeskreise, in eigene sowie andere Schulklassen und in die Familien bringen. Die Besonderheit dieser Form von Aufklärung und Wissensvermittlung ist, dass sie vor allem auf Augenhöhe und ohne das Gefühl „des erhobenen Zeigefingers“ erfolgt. Besonders in der heutigen Zeit vertrauen Jugendliche einander häufig eher als Erwachsenen, wenn es um Themen oder Probleme im digitalen Raum geht. Darüber hinaus erreichten uns im Berichtszeitraum erstmalig Anfragen von förderbedürftigen Schüler/-innen. Nach einem ausgiebigen Austausch mit der Schulsozialarbeit der Einrichtungen konnten wir die Ausbildung auch Schüler/-innen aus Förderschulen ermöglichen, wenn die Bedingungen einer selbstständigen Fähigkeit, Inhalte an weitere Schüler/-innen zu multiplizieren und zu transportieren, vorhanden waren. Somit konnten wir einen Beitrag im Hinblick auf Inklusion leisten, denn auch förderbedürftige Schüler/-innen bewegen sich genauso oft in digitalen Räumen, und der Bedarf an Medienkompetenz ist hierbei nicht geringer als bei allen anderen. Die Vorteile davon, ausgebildete Medienscouts als Ansprechpartner/-innen in der Bildungseinrichtung zu haben, erkannten bereits einige Schulen und gründeten eine einrichtungsinterne Arbeitsgruppe, um den ehrenamtlichen Wissenstransfer innerhalb der Klassen nachhaltig zu verfestigen.

Uns erreichen dank der Vernetzung durch die datenschutzkonforme Medienscouts-App im geschlossenen Netzwerk Rückmeldungen, dass die ausgebildeten Medienscouts MV Klassenvorträge, Workshops oder ganze Projekttage im Bereich der digitalen Aufklärung begleiten und übernehmen. Einige von ihnen trauten sich sogar, die Themen für Eltern aufzubereiten. Die von Jugendlichen vermittelten Informationen finden einen besonders großen Anklang bei den Eltern, da die Medienscouts MV aus ihrer eigenen Perspektive als Jugendliche erzählen.

Die Eltern bringen mehr Verständnis für das eigene familiäre Umfeld auf, wenn sie hören, dass die Thematik nicht nur mit ihren eigenen Kindern stets zu Auseinandersetzungen führen, sondern es sich auch um allgemeine Themen der heutigen Zeit handelt. Die Perspektive der Medienscouts MV eröffnet ein Gespräch in den Familien, das zu mehr Empathie gegenüber den Wahrnehmungen der Jugendlichen führen kann. Bei Anfragen unterstützen wir die Jugendlichen in ihrer Tätigkeit als Medienscouts MV auch nach der Ausbildung mit fachlichen und personellen Ressourcen.

Bereits zur Entstehung des Projektes Medienscouts MV vor 13 Jahren waren medienpädagogische Themen und digitale Teilhabe ein überaus relevantes Thema. Mit den von Jahr zu Jahr steigenden Bildschirmzeiten aller Altersgruppen nehmen diese Themen nicht an Relevanz ab – im Gegenteil, sie nehmen weiterhin zu – wer sich im Netz bewegt, muss dies selbstbestimmt und kompetent tun. Die angehenden Medienscouts MV zeigen uns bei den Ausbildungswochenenden immer aufs Neue, dass Jugendliche großes Interesse an diesen zentralen Themen mitbringen. Privatsphäre, Cybermobbing, Mediensucht, Gaming sowie neue Entwicklungen im Bereich der KI sind Bereiche, über welche Jugendliche sprechen und mehr erfahren möchten. Die engagierten Medienscouts MV leisten in unserem Bundesland einen wichtigen Beitrag zur Aufklärung im Bereich der Medienkompetenz in ihrem Umfeld und schließen somit stückweise Lücken, die durch die mangelhafte Medienbildung und auf Konsum orientierte Nutzung der Online-Dienste zu beobachten sind.

Tage ethischer Orientierung – protect privacy

Des Weiteren gehört zu unserer Kinder- und Jugendarbeit die personelle und finanzielle Unterstützung der Tage ethischer Orientierung: protect privacy (TEO-PP) mit dem Motto „Mein Klick, meine Verantwortung?!“. Die Zukunft der Durchführung des jährlich stattfindenden Projektes war 2024 unklar und unsicher, da die zu diesem Zeitpunkt bestehenden Strukturen und Finanzierungen nicht verlängert wurden. Schließlich konnte das Angebot nur dank einer neuen Trägerstruktur zurückkehren.[10] Dafür kooperieren seit 1. Juli 2024 zunächst für drei Jahre der mecklenburgische und der pommersche Kirchenkreis, das Diakonische Werk MV und das Erzbistum Hamburg. Gleichwohl ist die Durchführung leider nur mit einer Eigenbeteiligung der Schüler/-innen in Höhe von 69 Euro möglich. Bei TEO PP[11] handelt es sich um ein schulkooperatives Lernprojekt mit einem Klassenfahrtcharakter für fünfte bis achte Klassen. Neben dem Wissenstransfer in Workshops werden begleitende medienpädagogische Angebote organisiert. Das Ziel ist, die Schüler/-innen zu bewegen, neue Medien und soziale Netzwerke zu verstehen, mit ihnen umgehen zu können und sie zu hinterfragen. Neben technischen Fragestellungen zielt das Projekt auf das Recht auf informationelle Selbstbestimmung und das Bewusstsein über Pflichten und Rechte im digitalen Raum ab.

[10] https://www.kirche-mv.de/nachrichten/2024/juli/teo-kehrt-nach-mv-zurueck [abgerufen am 22.11.2024].

[11] https://www.teo-mv.de/seite/723852/teo-protect-privacy.html [abgerufen am 22.11.2024].

Im heutigen Zeitalter, in dem ein Aufwachsen ohne Medien undenkbar ist, muss die Verantwortung für sich selbst und gegenüber anderen von jedem Einzelnen übernommen werden. Das gelingt am besten durch das Reflektieren des eigenen Verhaltens im Netz. Fragen nach dem Sinn des eigenen Lebens, nach Wertevorstellungen, Zielrichtungen, Verhaltensweisen, Verantwortlichkeiten spielen in den TEO-Veranstaltungen eine große Rolle. Während der Projekttage wird versucht, Kindern und Jugendlichen Freiräume aufzuzeigen und im Dialog Impulse für die persönliche Orientierung im Alltag zu geben.

Die Schüler/-innen zeigen regelmäßig großes Interesse an den Themen und können ihr Wissen und die vielseitigen sowohl positiven als auch negativen Erfahrungen, die sie im Internet bereits erlebten, mit anderen klassenübergreifend teilen. Die neue Lernumgebung und die neue Gruppendynamik sorgen für einen effektiveren und nachhaltigeren Lernerfolg. Vorab erhalten die Lehrkräfte während eines Trainings Inhalte der Workshops im direkten Austausch mit den Referentinnen und Referenten, damit sie vor der Veranstaltung in ihrem Unterricht gezielt Vorkenntnisse aktivieren und etwaige Wissenslücken schließen können.

Um vielfältige Lerneffekte zu erreichen, tragen zu dem Konzept von TEO PP verschiedene Institutionen mit ihren zentralen Themenbereichen der digitalen Realität bei. Inhaltliche Schwerpunkte wie Gaming und Influencer/-innen werden von der CSG behandelt, während wir mit den Teilnehmer/-innen das Thema Privatsphäre, Datenschutz und Tracking vertiefen. Unser Beitrag zielt hauptsächlich darauf ab, aufzuzeigen, wie wertvoll und schützenswert eigene Privatsphäre ist. Darüber hinaus erhalten seit den letzten Durchführungen zusätzlich die angehenden Erzieher/-innen die Gelegenheit, (medien-)pädagogische Themen (Mediensucht, Social Media und Cybermobbing) und Methoden mit den Gruppen auszutesten. Die Auseinandersetzungen mit der breiten Themenvielfalt fördern bei den Schüler/-innen das Verständnis für sozialethische Fragestellungen in unserer multimedialen Lebenswelt und lassen die Chancen und Risiken greifbarer erscheinen.

Die kontinuierlich hohe Nachfrage durch die Schulen unterstreicht zudem sowohl die Aktualität und die steigende Bedeutung der Themen für die Zielgruppe als auch die Notwendigkeit alternativer, schulübergreifender Lernformate, die eine tiefgehende Auseinandersetzung mit den Themen Mediennutzung und Datenschutzbewusstsein ermöglichen, die für die auf Digitalisierung ausgerichteten Zukunftsentwicklungen unabdingbar sind.

Das Fortbestehen des Projektes zeigt, dass Schulen Medienbildung als wichtig erachten, sie jedoch diese oft aufgrund von Zeit-, Personal- oder Ressourcenmangel nicht ausreichend umsetzen können. Die Umsetzung dieser Strategie an den Schulen bleibt oft von dem Engagement und der Unterstützung der Schulleitungen und Lehrkräfte abhängig. Daher ist es entscheidend, eine Vielzahl von schulischen und außerschulischen Bildungsangeboten und schulkooperativen Lernsettings zu fördern und kompetentes medienpädagogisches Fachpersonal für Kinder und Jugendliche bereitzustellen. Darüber hinaus ist die Durchführung nur mit einer Eigenbeteiligung in Höhe von 69 Euro möglich. Dies kann die Bildungschancengleichheit im Hinblick auf die Medienbildung bei den Schüler/-innen im Land beeinträchtigen.

Aktuelles zum Jugendportal YoungData.de

Im Jahr 2021 wurde durch die Datenschutzkonferenz des Bundes und der Länder (DSK) die Finanzierung für den Relaunch des Jugendportals www.youngdata.de beschlossen. Das Portal, welches von den Datenschutzaufsichtsbehörden des Bundes und der Länder in Zusammenarbeit mit der Datenschutzbeauftragten des Kantons Zürich betrieben wird, wurde in den Jahren 2022 bis 2023 vollständig neu gestaltet.[12]

Die überarbeitete Website wurde speziell auf das Nutzungsverhalten von Jugendlichen zugeschnitten, insbesondere durch eine mobile Version, die einen schnellen Zugriff über Smartphones ermöglicht. Sie bietet eine ansprechende Usability (Nutzer/-innenerfahrung), die die Auswahl der Themen, die Ansprache sowie die Texte berücksichtigt. Ein zentrales Ziel der Website ist es, Jugendliche im Alter von 13 bis 16 Jahren für das Thema Datenschutz zu sensibilisieren, indem lebensnahe Themen spannend und verständlich aufbereitet werden. Es ist wichtig, die komplexen Themen des Datenschutzes Jugendlichen zielgerichtet zu vermitteln. Sie müssen wissen, wie sie verantwortungsvoll mit ihren eigenen und fremden personenbezogenen Daten umgehen können, wenn sie Online-Dienste benutzen. Dies entspricht auch den Vorgaben des europäischen Gesetzgebers, der die Aufklärung und Sensibilisierung der Bürger/-innen über die Risiken, Rechte und Vorschriften im Zusammenhang mit der Verarbeitung personenbezogener Daten als eine der wesentlichen Aufgaben in Artikel 57 Absatz 1 Buchstabe b DS-GVO formuliert und insbesondere die Notwendigkeit spezifischer Maßnahmen für Kinder betont. Die DSK verfolgt gemeinsam dieses Hauptanliegen bereits seit 2013. Mit dem Relaunch spricht die Seite die Jugendlichen heutzutage viel mehr an. Zusätzlich bietet sie neben Top-Themen und News ein Glossar und eine Übersicht über spezielle Angebote der einzelnen Bundesländer für Jugendliche und Interessierte, um das Verständnis und die kritische Auseinandersetzung mit den Mechanismen der digitalen Gesellschaft zu fördern.

Die Redaktionsgruppe wird in gemeinsamer Federführung durch die zur Umsetzung des Relaunchs entstandene Arbeitsgruppe von Kolleginnen und Kollegen aus Mecklenburg-Vorpommern, Rheinland-Pfalz, Berlin, Baden-Württemberg und Thüringen unterstützt. Im Berichtszeitraum organisierte unsere Behörde regelmäßige redaktionelle Arbeitstreffen in Online- und Präsenzformaten. In der Zukunft ist nach Maßgabe der zur Verfügung stehenden Ressourcen eine redaktionelle Einbeziehung weiterer Aufsichtsbehörden in Form monatlicher Patenschaften angestrebt. Neben klassischen Datenschutzthemen wie Datensicherheit, Tracking und Privatsphäre werden ebenso aktuelle Themen zu sozialen Netzwerken, Apps, KI-Anwendungen und Umgang im Netz behandelt. Im Berichtszeitraum beteiligte sich der LfDI MV redaktionell an Artikeln und News mit der Fokussierung auf Passwörter, Nutzung der KI im schulischen Kontext, Medienschutzmaßnahmen bei der Nutzung von character.ai, Online-Shopping, Wahlbeeinflussung und politischem Tracking. Dabei streben wir an, uns bei der Planung der inhaltlichen Gestaltung an saisonalen und aktuellen Themen zu orientieren, wie z. B. Urlaub und Reisen im Sommer, Glücksspiel und Sportveranstaltungen begleitende Onlinewetten (z. B. Fußball-WM), Wahlmanipulation oder Onlineshopping in der Vorweihnachtszeit. Es ist von besonderer Bedeutung, dass Jugendliche nachvollziehen können, welche Rolle ihre Daten in der digitalen Welt spielen, wenn sie sich darin bewegen.

[12] Siehe 4.5 Das Jugendportal der DSK: youngdata www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Taetigkeitsberichte/lfdmvtb18-19.pdf [aufgerufen am 07.05.2025].

Organisatorisch wurden 2024 für das Betreiben der Webseite notwendige technische Updates durchgeführt, damit weiterhin die höchsten Schutzmaßnahmen gewährleistet werden können. Darüber hinaus wurden Werbematerialien wie Roll-ups, Flyer und Plakate erstellt, um die Webseite bei den Jugendlichen zu promoten (bei Schulbesuchen oder Veranstaltungen wie z. B. bei der didacta 2024 in Köln). Im weiteren Verlauf werden technische Implementierungen und inhaltliche Anpassungen zur Barrierefreiheit der Webseite umgesetzt, um neuen Anforderungen des 2025 in Kraft getretenen Barrierefreiheitsstärkungsgesetzes (BFSG) gerecht zu werden und die Webseite zur barrierefreien Nutzung auszubauen.

Die Redaktionsgruppe von YoungData greift weiterhin aktuelle Medien- und Datenschutzthemen auf und bringt die Website kontinuierlich auf den neuesten Stand. Die Datenschutzaufsichtsbehörden des Bundes und der Länder im Rahmen der DSK in Kooperation mit dem Kanton Zürich werden weiterhin ihr Fachwissen teilen, damit sich Jugendliche und alle Interessierten verantwortungsbewusst, mündig und selbstbestimmt in der digitalen Welt bewegen können. Digitale Kompetenz, Medienkompetenz und Datenschutzbewusstsein sind in einem auf Digitalisierung ausgerichteten Land von entscheidender Bedeutung. Das gilt unabhängig vom Alter und ist notwendig, um die Teilhabe jeder und jedes Einzelnen an demokratischen Prozessen zu wahren.

Wir empfehlen der Landesregierung den Austausch mit unserer Behörde bezüglich der medienpädagogischen Best-Practice-Projekte und deren Ausbaumöglichkeiten. Der Hauptvorteil dieser landesweiten Projekte besteht darin, die Vermittlung der Medienkompetenz auch in strukturschwächeren und/oder ländlichen Regionen abdecken zu können. Somit tragen sie zur Chancengleichheit bei. Es gibt derzeit keine vergleichbaren Formate und Bildungsangebote zur Vermittlung von Medienkompetenz für Kinder und Jugendliche in MV. Um diese Kompetenzen weiter zu fördern, ist es notwendig, die schulische und außerschulische Medienbildung zu vernetzen. Auf diese Weise kann die Medien- und Demokratiebildung junger Menschen in unserem Land deutlich unterstützt werden.

4.2 Pädagogische Fachkräfte

Unsere Behörde ist seit Jahren eine konstante und verlässliche Institution bei der Vermittlung von Medienkompetenz, Datenschutzbewusstsein und der Förderung von digitalen Kompetenzen für pädagogische Fachkräfte. Neben der Organisation eigener Fachtagungen im Rahmen des Netzwerks Medienaktiv MV und des Projekts #DigitaleVorbilder – Familien gehen online. wurden wir mit unserer Fachexpertise zu Fachtagungen eingeladen. Dazu zählen im Berichtszeitraum z. B. die stetige Unterstützung der Kinder- und Jugendmedienschutztagungen des BM MV und Schulungen der lokalen Arbeitskreise Schulsozialarbeit. Somit konnten wir unsere fachlichen Inhalte zur Datenschutzsensibilisierung und Medienbildung bei der 6. Kinder- und Jugendmedienschutztagung „Medien erleben – Kinder begleiten (!)“ des Medienpädagogischen Zentrums (MPZ) vom BM MV mit zwei Workshops unterstützen und an die Lehrkräfte und pädagogisches Fachpersonal weitergeben: „Digitale Kompetenzen leicht: Methoden und Anwendungsbereiche in unterschiedlichen Altersgruppen zu Datenschutzbewusstsein und Privatsphäre“ und „Learning aus #DigitaleVorbilder – Familien gehen online: Womit erreiche ich Familien für Themen der digitalen Medienerziehung?“.

Zusätzlich fanden im vorliegenden Berichtszeitraum noch weitere Fachtagungen für pädagogische Fachkräfte, an denen wir als LfDI MV mitwirkten, sowie die etablierte Fortbildungsreihe „Spielen, Zappen, Klicken – Medienerziehung in Kita und Familie als Beitrag zur Primärprävention von Mediensucht“ statt.

Fachtag „Hey MV! Wie läuft’s mit Medienerziehung und Datenschutz?“

Im Rahmen des EU-finanzierten Projekts #DigitaleVorbilder – Familien gehen online. (siehe Kapitel 4.3) fand am 4. Juli 2024 der Fachtag „Hey MV! Wie läuft’s mit Medienerziehung und Datenschutz?“ in Güstrow für interessiertes pädagogisches Fachpersonal als anerkannte Fortbildung des BM MV statt.[13] Rund 70 Fachkräfte aus den Bereichen Schule, (Schul-)Sozialarbeit, polizeiliche Prävention und Medienbildung kamen zusammen, um sich über Datenschutzsensibilisierung, Medienerziehung und Aufklärungsarbeit der Elternhäuser ihrer Bildungseinrichtungen auszutauschen. Ein zentraler Schwerpunkt lag auf der Frage, wie Familien Kinder und Jugendliche im Netz sicher begleiten können. Dabei standen praxisnahe Ansätze zur Förderung eines verantwortungsvollen Medienumgangs in Familien im Fokus. Für zahlreiche Workshops holte das Projektteam viele Referenten und Referentinnen an Bord, um den Teilnehmer/-innen wertvolle Inputs, Best-Practice-Erfahrungen und Impulse anzubieten. Dabei wurde auch diskutiert, welche Hürden es zu überwinden gilt, um Eltern als Mitverantwortliche für die Medienerziehung ihrer Kinder zu motivieren, und wie ein wertschätzender Austausch seitens der Fachkräfte gestaltet werden kann. Um die Eltern als Zielgruppe zu erreichen, erkannten wir die Notwendigkeit, Erkenntnisse und entstandene Materialien des Projekts an diejenigen weiterzugeben, die in ihrer Arbeit tagtäglich mit Kindern, Jugendlichen und deren Familien in Kontakt treten: die pädagogischen Fachkräfte in Mecklenburg-Vorpommern.

Das LKA MV gab praxisnahe Einblicke sowohl in die Präventionsarbeit als auch in Intervention und Deeskalation bei potenziellen Straftatbeständen im Schulalltag. Die Evangelische Suchtkrankenhilfe mit Kompetenzzentrum für exzessive Mediennutzung und -abhängigkeit MV, vertreten durch Dr. phil. Detlef Scholz, thematisierte in seinem erfolgreichen Klassiker „Entspannter Umgang mit digitalen Medien in der Familie“ Strategien für eine entspannte Medienerziehung in Familien. Über die Stärkung der Netzwerk- und Elternarbeit in der Medienbildung informierte die Regionalbeauftragte für Medienbildung von MPZ. Der LfDI MV stellte Methoden zur Datenschutzsensibilisierung und verschiedene digitale und analoge Werkzeuge zur Unterstützung der Medienerziehung unterschiedlicher Altersgruppen vor. Neben weiteren medienpädagogischen Workshops präsentierte der LfDI MV die im Hinblick auf Nachhaltigkeit und langfristige Verfügbarkeit entstandenen Bildungsprodukte der #DigitaleVorbilder-Mediathek: Webinare und Vorträge der Medienfachleute als Videos, mehrsprachige Kurzclips, Graphic Recordings als Plakate, Infokarten und mehrsprachige Broschüren. Die Fachkräfte erhielten spielerische Anregungen, wie diese vielfältigen Materialien sowohl analog als auch digital in der eigenen medienpädagogischen Elternarbeit einzubinden wären. Diese Materialien sind und bleiben weiterhin digital verfügbar. Die Broschüre „Orientierungshilfe Datenschutz: Ein Familienguide im digitalen Dschungel“ wurde in gedruckter Form zum Ende des Berichtszeitraums an zahlreiche pädagogische Einrichtungen von Kita bis Schule, von Mehrgenerationenhaus bis Familiencafé verschickt. Die Nachfrage ist weiterhin ungebrochen.

[13] https://www.datenschutz-mv.de/datenschutz/publikationen/DigitaleVorbilder/Fachtag_Guestrow [abgerufen am 12.11.2024].

Der Fachtag zeigte eindeutig: Medienkompetenz und Datenschutz sind zentrale Herausforderungen der digitalen Gesellschaft, und der interdisziplinäre Dialog bleibt weiterhin ein wichtiger Schlüssel zur Unterstützung von Familien und wurde anhand der Resonanz der Teilnehmer/-innen als große Bereicherung empfunden. Darüber hinaus wurde der Wunsch nach regelmäßigen kostenlosen Schulungen, Handreichungen und Vernetzungsmöglichkeiten deutlich formuliert, um Fachkräfte in ihrer Aufklärungsarbeit weiter zu stärken.

Medienaktiv MV-Fachtag: „Dem Hass nicht ins Netz gehen – medienpädagogische Ansätze zur Demokratiebildung“

Das landesweite Netzwerk der Medienbildung Medienaktiv MV führte am 5. November 2024 im Digital Garden Schwerin einen Fachtag unter dem Titel „Dem Hass nicht ins Netz gehen – medienpädagogische Ansätze zur Demokratiebildung“ erfolgreich durch. Die positive Resonanz und die engagierte Teilnahme der pädagogischen Fachkräfte zeigten, wie groß der Bedarf an medienpädagogischen Konzepten und demokratischen Leitlinien in der Bildungsarbeit ist. Die Teilnehmer/-innen verfolgen das gemeinsame Ziel, jungen Menschen Orientierung zu bieten, um sicher und selbstbewusst im digitalen und analogen Raum zu agieren. Die Veranstaltung bot pädagogischen Fachkräften einen praxisorientierten Einblick in Handlungsstrategien im Hinblick auf Hass im digitalen Raum und stellte dabei die Demokratiebildung als zentrales Thema in den Fokus. Durch die Keynotes, Workshops und Diskussionsräume konnten die Teilnehmer/-innen wertvolle Impulse für ihre tägliche Arbeit mit Kindern und Jugendlichen gewinnen. Mit der Unterstützung von Fachkräften sowie Partnerinnen und Partnern des landesweiten Netzwerks Medienaktiv MV wurden im Rahmen des Fachtags nicht nur aktuelle Herausforderungen diskutiert und inhaltliche Unterrichtseinheiten vorgestellt, sondern auch die Vernetzung stand im Vordergrund. Der Fachtag griff die dringende Herausforderung auf, dass Hass im Netz immer lauter wird und mittlerweile zum Alltag gehört. Die Konsequenzen zeigen sich zunehmend nicht nur im digitalen, sondern auch im analogen Leben. Aus der Studie der GMK „Lauter Hass – leiser Rückzug“ stellte Melina Honegg vor, dass Hass im Internet nicht nur soziale und gesundheitliche Folgen für Einzelne mit sich bringt, sondern auch die Meinungsfreiheit unserer Gesellschaft gefährdet und unsere demokratische Grundordnung bedroht. Die Teilnehmer/-innen erhielten praxisnahe Einblicke in verschiedene aktuelle medienpädagogische Herausforderungen, wie die Erkennung von Fake News und KI-generierten Inhalten, um Falschmeldungen online zu entlarven, die Radikalisierung in der Gaming-Szene bzw. wie Spiele als Plattform zur Verbreitung dieser Ideologien genutzt werden, versteckte Hassbotschaften und Codes in sozialen Medien und die Demokratiebildung in der Bildungspraxis. Der LfDI MV ist der Meinung, dass Medien- und Demokratiebildung zusammen gedacht werden müssen. Die Beeinflussung durch Desinformation, Social Bots, KI und Fake News findet online statt. Dafür brauchen die pädagogischen Fachkräfte Unterstützung. Der LfDI MV ist die tragende Säule des Netzwerkes Medienaktiv MV und hilft dabei, die beteiligten Institutionen zu koordinieren.

Kursreihe für pädagogische Fachkräfte im frühkindlichen Bereich: „Spielen, Zappen, Klicken“

Die modulare Fortbildungsreihe „Spielen, Zappen, Klicken – Medienerziehung in Kita und Familie als Beitrag zur Primärprävention von Mediensucht“, die auf die Inhalte der Bildungskonzeption für 0- bis 10-jährige Kinder in Mecklenburg-Vorpommern (BIKO M-V) abgestimmt ist, begleitet die pädagogischen Fachkräfte und Einrichtungen dabei, ein Medienkonzept für ihre Einrichtung zu erarbeiten und dieses anschließend in der Praxis umzusetzen. Damit leistet die Fortbildungsreihe einen aktiven und notwendigen Beitrag zur Primärprävention im Bereich der Medienerziehung. Unter der Koordination der LAKOST MV wird das Fortbildungsprogramm für Erzieher/-innen der Kitas und Horte seit 2018 jährlich mit einem modularisierten Ausbildungsdurchgang durchgeführt. Die Fortbildungsreihe umfasst acht Module und einen praxisorientierten Studientag in der Einrichtung der Teilnehmer/-innen. Die Kursreihe unterstützt Träger und Einrichtungen der frühkindlichen Bildung in der Erfüllung des Kindertagesförderungsgesetzes (KiföG M-V) zur Medienbildung und beinhaltet die Themenschwerpunkte des neu eingeführten Kapitels der BIKO M-V. Der LfDI MV brachte sich mit seiner Fachexpertise als Mitverfasser des Kapitels der BIKO M-V zur frühkindlichen Medienbildung bereits ein und übernimmt seitdem in Zusammenarbeit mit den Projektpartner/-innen und freien Medienpädagoginnen und Medienpädagogen die Realisierung von zwei Ganztagsmodulen mit medienpädagogischer Thematik. Dank der Finanzierung durch den Verband der Ersatzkassen MV (vdek e. V.) konnte die Fortbildung auch im Berichtszeitraum weiter fortgeführt werden.

Wir empfehlen der Landesregierung, regelmäßige und kostenlose Schulungen, Handreichungen, Materialien und regelmäßige Vernetzungsmöglichkeiten für pädagogische Fachkräfte in der Ausbildung sowie im weiteren Werdegang zu entwickeln und zu verfestigen. Aus unserer medienpädagogischen Praxis heraus sehen wir die Notwendigkeit, einen interaktiven und interdisziplinären Austausch zwischen allen relevanten Beteiligten der Bildungs-, Medienbildungs- und Präventionsarbeit zu ermöglichen, um mit der rasanten Entwicklung der Digitalisierung Schritt halten zu können. Eine Vernetzung der bestehenden Einzelmaßnahmen erachten wir als dringend notwendig.

4.3 Eltern & Familien

Um dem in Artikel 57 Absatz 1 Buchstabe b DS-GVO formulierten Bildungsauftrag bestmöglich nachzukommen und vor allem Kinder über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung ihrer Daten zu sensibilisieren und aufzuklären, ist es unerlässlich, auch die Gruppe der Eltern und Familienmitglieder gezielt mit Bildungs- und Informationsangeboten zu adressieren. Die Kernfamilie als Ort der elementaren Bildung und Sozialisation vermittelt nicht nur grundlegende Wert- und Normvorstellungen, sondern auch Wissen und schafft somit die Basis für die Entwicklung verschiedener Kompetenzen und Handlungsmuster. Mit Blick auf die heutigen digitalen Herausforderungen ist es eine verantwortungsvolle und gleichzeitig sehr umfangreiche Aufgabe, den Kindern einen kompetenten und sicheren Umgang mit den digitalen Medien mit auf den Weg zu geben.

Nur wenn Vor- und Nachteile bzw. Chancen und Risiken bei der Nutzung digitaler Angebote bekannt sind, können diese auch gegeneinander abgewogen und nach einem erlernten Wertesystem entschieden werden. Medienkompetenz als eine Entscheidungskompetenz ist die Grundlage für Datenschutzbewusstsein und einen sicheren und selbstbestimmten Umgang mit digitalen Medien. Die meisten Eltern sind sich ihrer Verantwortung zwar bewusst, die Medienkompetenz ihrer Kinder bestmöglich zu fördern, jedoch fühlen sich nur die wenigsten Familien dieser Herausforderung wirklich gewachsen. Diese Wahrnehmung bestätigt sich regelmäßig bei den vielen durch unsere Behörde durchgeführten Bildungs- und Informationsangeboten für Eltern und Familien. Im Folgenden geben wir einen Überblick zu dem Projekt Medienguides MV und dem EU-Projekt #Digitale Vorbilder – Familien gehen online. sowie zu Informationsangeboten im Rahmen organisierter Elternabende.

Medienguides MV

Im Frühjahr 2024 führte der LfDI MV sein Bildungsangebot für Eltern Medienguides MV – Eltern. Medien. Kompetenz zum dritten Mal erfolgreich durch. An zwei Samstagen im Frühjahr wurden weitere Medienguides MV in Rostock ausgebildet. Ziel des Projektes ist es, dass die ausgebildeten Medienguides MV nicht nur die eigene Familie für Medienthemen stärken, sondern ihr Wissen im Anschluss auch an andere Familien weitergeben. Die Teilnehmer/-innen erhofften sich neben Tipps und Tricks zum sicheren Umgang mit Medien in der Familie vor allem klare Regeln und konkrete Handlungsempfehlungen, z. B. ab welchem Alter ein Kind ein eigenes Smartphone haben sollte, wie viel Medienkonsum unbedenklich sei und wie sich feste Medienregeln am besten umsetzen ließen. Die Überraschung der Teilnehmer/-innen war zunächst groß, als wir gemeinsam mit unseren Projektpartnern von der LAKOST MV, dem Kompetenzzentrum für Medienabhängigkeit, der CSG sowie vom LKA MV deutlich machten, dass es keine allumfassenden Regeln und Empfehlungen geben kann. Denn die Medienerziehung ist so unterschiedlich wie die Familien selbst. Vielmehr liegt das Ziel der Ausbildung zum Medienguide MV darin, das eigene Mediennutzungsverhalten kritisch zu hinterfragen, um daraufhin die Medienerziehung in der eigenen Familie verbessern zu können.

In den einzelnen Workshops zu Privatsphäre und Datenschutz, Medienkonsum und Mediensucht, Mediennutzung aus Kindersicht sowie Cybermobbing und Cybercrime wurde zunächst wichtiges Wissen innerhalb der jeweiligen Themenfelder vermittelt. Durch unser offenes Format, das kontinuierlich Raum für Diskussionen und somit Gelegenheit zum Einordnen und Reflektieren des eigenen Mediennutzungsverhaltens bot, war es den Eltern möglich, ihre ganz persönlichen Fragen einzubringen und so individuelle Erkenntnisse für sich und die eigene Familie zu gewinnen. Insbesondere durch die medienpraktischen Angebote der CSG und Radio LOHRO konnten die Teilnehmer/-innen selbst aktiv werden und z. B. derzeit angesagte Games ausprobieren, in digitale Spielewelten mittels VR-Brille eintauchen oder eine Hörgeschichte technisch und inhaltlich selbst gestalten. Für den Berichtszeitraum lassen sich im Nachgang der durchgeführten Medienguides MV-Ausbildung mehrere erfolgreich durchgeführte Veranstaltungen der ausgebildeten Medienguides MV resümieren. So wurde auf Initiative eines Teilnehmers ein zweitägiger Elternabend zum Thema „Medien in der Familie“ an einer Rostocker Schule organisiert und mit Unterstützung unterschiedlicher Projektpartnerinnen und -partner ausgerichtet, an dem insgesamt 80 Eltern teilnahmen.

Der LfDI MV unterstützte hier mit zwei Fachvorträgen zum Thema „Privatsphäre und Datenschutz – Alles eine Frage der Einstellung“. Die Verstetigung dieses thematischen Medien-Elternabends zu einer jährlich stattfindenden Informationsveranstaltung für Eltern wird an der Schule derzeit umgesetzt. An einer Grundschule im Landkreis Nordwestmecklenburg informierte eine Teilnehmerin via Online-Elternbrief über ihre Ausbildung als Medienguide MV und führte im November 2024 gemeinsam mit der Schulleitung einen thematischen Elternabend als Workshop-Format zum Thema „Medienkompetenz und Datenschutzbewusstsein“ durch. Der LfDI MV beriet die Verantwortlichen des Elternabends zu inhaltlichen und organisatorischen Fragen, übersandte zur Vorbereitung der Veranstaltung umfangreiches Informationsmaterial und bleibt auch weiterhin als fester und verlässlicher Ansprechpartner für die Medienguides MV verfügbar. Der Eingang neuer Anmeldungen zum nächsten Ausbildungsdurchgang der Medienguides MV 2025 im direkten Nachgang des Elternabends in Nordwestmecklenburg legt die Vermutung nahe, dass hier andere Eltern unmittelbar von unserem Format überzeugt werden konnten.

Die im vorliegenden Berichtszeitraum ausgebildeten Medienguides MV signalisieren uns kontinuierlich, wie wichtig ihnen die Vernetzung untereinander ist, um sich gegenseitig über erfolgreich durchgeführte Veranstaltungen zu informieren, interessante Artikel oder Beiträge auszutauschen bzw. sich untereinander Ratschläge und Tipps zur Umsetzung von Ideen an den Schulen und Einrichtungen ihrer Kinder zu geben und sich auch bei diesen Veranstaltungen in Person zu unterstützen. Durch das Angebot der eigens zu diesem Zweck entwickelten Medienguides-MV-App ist es unserer Behörde ebenfalls möglich, die Teilnehmer/-innen auch nach ihrer Ausbildung mit aktuellen Informationen und Hinweisen zum Thema Datenschutz zu versorgen, regelmäßig zu wichtigen Medienthemen zu informieren oder Veranstaltungshinweise weiterzuleiten. Das vertrauensvolle Miteinander der Ausbildungstage und das als Medienguide MV gewonnene Gefühl, den Herausforderungen der Medienwelt als Eltern nicht hilf- oder ratlos gegenüberzustehen, spornt die Teilnehmer/-innen an, weiterhin aktiv zu bleiben und möglichst viele andere Eltern zu erreichen und zu informieren. So sind aktuell auch für das Schuljahr 2024/2025 Durchführungen weiterer thematischer Elternabende durch unsere diesjährig ausgebildeten Medienguides MV geplant.

#Digitale Vorbilder – Familien gehen online.

Mit der Zielsetzung, das Thema Datenschutz für Familien verständlich und erlebbar zu machen, führte der LfDI MV gemeinsam mit dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) das Projekt #Digitale Vorbilder – Familien gehen online. mit einer Laufzeit vom 1. November 2022 bis zum 31. Oktober 2024 erfolgreich durch[14]. Im Rahmen dieses durch das EU-Programm „Citizens, Equality, Rights and Values-2021-DATA (CERV-2021-DATA)“ finanzierten Projektes wurden im vorliegenden Berichtszeitraum verschiedene analoge und digitale Bildungs- und Informationsangebote für Familien durchgeführt. Zehn Veranstaltungen der bereits im November 2023 gestarteten zwölfteiligen Online-Seminarreihe fanden 2024 statt. Themenspezifische Inhalte wie z. B. „Tatort Internet“, „Die zehn Datenschutz-Mythen“, „TikTok, Snapchat & Co.“, „Rechte, Pflichten, Verantwortung“ oder „TikTok, sag mir, wen ich wählen soll“ wurden in leicht verständlicher Weise als moderierte Beratungsrunden mit Expertinnen und Experten angeboten.

[14] Vgl. u. a. Punkt 4.6 in URL: https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Taetigkeitsberichte/lfdmvtb18-19.pdf [abgerufen am 12.02.2025].

Die Live-Übertragungen fanden jeweils abends um 19 Uhr statt, sodass eine Teilnahme für die Eltern mit ihrem Familienalltag gut vereinbart werden konnte. Die Zahl von bis zu 300 Teilnehmer/-innen in einzelnen Veranstaltungen offenbarte eine hohe Nachfrage und ein deutliches Interesse der Zielgruppe an umfangreichen Informationen zu Datenschutz- und Medienthemen mehr als deutlich. Insbesondere die rege aktive Teilnahme mittels der Chatfunktion in den Webinaren verdeutlichte das Bemühen der Eltern, ihre Kinder bestmöglich bei der Nutzung digitaler Angebote zu begleiten. Eine Vielzahl der dort gestellten Nachfragen bezog sich auf technische Einstellungen und Hilfsmittel, mit denen die eigenen Daten optimal geschützt werden können. Insbesondere im Webinar zum Thema „Rechte, Pflichten und Verantwortung von Familien im digitalen Raum“, in dem der LfDI MV seine umfangreiche Expertise zur Verfügung stellte, wurden Datenschutzeinstellungen thematisiert. Gleichzeitig wurde aber auch herausgestellt, dass die größte Herausforderung für Eltern darin besteht, ein ausgewogenes Verhältnis von Kontrolle und Vertrauen in der Medienerziehung ihrer Kinder aufzubauen, dieses kontinuierlich alters- und entwicklungsspezifisch anzupassen und stets mit den Kindern im Dialog bezüglich der Mediennutzung zu bleiben. Alle Webinare wurden aufgezeichnet und bearbeitet und sind mit Untertitelung in verschiedenen Sprachen dauerhaft online abrufbar. Zusätzlich befinden sich auf der Projektwebseite[15] verschiedene Vorträge und Interviews von Fachleuten zu einzelnen Themenschwerpunkten im Bereich Medienkompetenz. Aus dem filmischen Material entstanden auch Kurzclips, die einzelne wichtige Aussagen der Vorträge aufgreifen. Die Kurzclips sind zudem in mehreren Sprachen (Deutsch, Englisch, Französisch, Spanisch, Russisch, Hocharabisch und Gebärdensprache) verfügbar. Die Vorträge und Aufzeichnungen der Onlinereihe können je nach Browser und Verbreitungsweg in allen Sprachen untertitelt werden. Zusätzlich gibt es die Inhalte auch als Podcast. Vor allem die Kurzclips und/oder Podcasts sind niedrigschwellige und flexibel abrufbare Bildungsangebote, nicht nur für Familien. Sie lassen sich gut in der pädagogischen Arbeit der Einrichtungen einsetzen.

Neben diesen Online-Angeboten führte der LfDI MV im Rahmen des Projektes #Digitale Vorbilder auch analoge Informationsveranstaltungen in Form von Elternabenden und Elterncafés durch. Auf diesen Veranstaltungen konnten im Berichtszeitraum Eltern über Datenschutzthemen und Medienkompetenzförderung aufgeklärt werden. Im intensiven Austausch mit den Eltern standen wie gewohnt die Themen Smartphone-Nutzung, Social Media und Online-Gaming im Zentrum unserer Aufklärungsarbeit. Die eigenen Daten nur möglichst sparsam preiszugeben und genau abzuwägen, zu welchem Zweck diese abgefragt werden, bleibt unsere elementare Botschaft an Eltern, Familien und Kinder. Besonders hervorzuheben ist die Broschüre „Orientierungshilfe Datenschutz: Ein Familienguide für den digitalen Dschungel“, mit deren Veröffentlichung im Oktober 2024 sämtliche Expertisen des Projektes ausführlich und zugleich kompakt zusammengefasst wurden. Je ein Belegexemplar wurde an alle Bildungseinrichtungen in MV versendet, um diese gezielt in der medienbezogenen Elternarbeit zu unterstützen. Die Einrichtungen konnten die Broschüre nachbestellen, um sie in ihre Aufklärungsarbeit zu integrieren. Dabei wurden im Berichtszeitraum fast 5.000 Exemplare mit Unterstützung der Landtagsverwaltung versandt. Die Nachfrage nach den Broschüren bleibt ungebremst. Während die deutsche Version als gedruckte Variante vorliegt, ist die Broschüre online ebenfalls auf Englisch, Französisch, Spanisch und als barrierefreie Version verfügbar.

[15] URL: https://datenschutz-hamburg.de/digitalevorbilder/materialien [abgerufen am 12.02.2025].

Eine immense Bereicherung für unsere Bildungsarbeit mit der Zielgruppe Eltern stellt die nachhaltige und dauerhafte Verfügbarkeit der Projektmaterialien über die genannte Projektwebseite dar. So konnten wir bei allen Informationsveranstaltungen auf konkrete Bildungsinhalte und bereitgestellte Materialien der #Digitalen Vorbilder verweisen. Interessierte können weiterhin auf alle produzierten Inhalte des EU-Projektes zugreifen. Der LfDI MV wird auch zukünftig bei der Durchführung von Bildungsveranstaltungen für Eltern und Familien verstärkt und schwerpunktmäßig auf die Projektmaterialien der #Digitalen Vorbilder verweisen und insbesondere die Broschüre für seine Aufklärungsarbeit nutzen. Die Umsetzung weiterer Onlineseminare unter #DigitaleVorbilder sowie die Produktion der Bildungsmaterialien sollen auch in der Zukunft durch den LfDI MV fortgeführt werden. Folgerichtig werden wir Finanzierungsmöglichkeiten prüfen und suchen, um die Fortführung des Familienprojektes umsetzen zu können. Entsprechend bekräftigen wir unsere Empfehlung an die Landesregierung aus dem vorangegangenen Tätigkeitsbericht erneut.

Elternabende

Neben den bereits dargestellten Angeboten führte der LfDI MV im vorliegenden Berichtszeitraum auch eine Vielzahl einzelner/separater Informations- und Bildungsveranstaltungen für Eltern durch. Einladungen für die Durchführung thematischer Elternabende oder anderer Formate wie z. B. Elterncafés erhielten wir sowohl direkt von Bildungseinrichtungen (d. h. Schulen und Horte bzw. durch die jeweiligen Einrichtungsträger) als auch durch andere Bildungsakteure im Land, die unsere Beteiligung an Bildungs- und Präventionsangeboten für Eltern und Familien anfragten. So begleiteten wir u. a. die LAKOST MV bei der Durchführung eines Elternabends in Brüsewitz, sensibilisierten dort für eine sparsame Datenpreisgabe bei der Nutzung digitaler Angebote und stellten ausführlich unsere Bildungsprojekte Medienscouts MV und Medienguides MV vor. Zum wiederholten Male unterstützten wir das Präventionsprojekt „Hassfreie Zone“ des gemeinschaftlichen Bildungsprogramms Helden statt Trolle des LKA MV und der Landeszentrale für politische Bildung Mecklenburg-Vorpommern (LpB MV), welches in Barth stattfand. Bei Themen wie „Kinderbilder im Netz“ sensibilisierten wir die Eltern und Kinder für mehr Datenschutzbewusstsein, den Umgang mit Familienfotos und die Kontrolle der Privatsphäreeinstellungen. Als besonders bereichernd und zielführend für die Präventionsarbeit empfanden wir den gemeinsamen Austausch mit Eltern und teilweise mit Kindern zu den Themen und individuellen Fragen der Mediennutzung innerhalb der Familien. Weitere thematische Elternabende führten wir auf Anfrage von Schulen durch. Für die teilnehmenden Eltern standen vor allem Fragen zur Nutzung von Social-Media-Angeboten durch ihre Kinder in der 5. bzw. 6. Klasse im Vordergrund. Entsprechend informierten wir umfänglich zu Sicherheits- und Privatsphäreeinstellungen bei Diensten, wie z. B. WhatsApp, Instagram und TikTok. Dies beinhaltete ebenfalls die Themen der Mediennutzung innerhalb der Familien und die Kompetenzförderung ihrer Kinder mit den online verfügbaren Informationsangeboten des Projektes #Digitale Vorbilder.

Es bleibt weiterhin ein Themenschwerpunkt, wie die Familien zu erreichen sind, die nicht die Bildungsangebote nutzen. Durch unsere Erfahrungen aus dem niederschwelligen Projekt #DigitaleVorbilder und den Austausch mit den Kolleginnen und Kollegen des Arbeitskreises Datenschutz und Medienkompetenz der DSK auf Bundesebene wird der LfDI MV auch weiterhin verstärkt den Fokus auf die medienkompetenzfördernden Angebote für diese Zielgruppe legen.

Wir empfehlen der Landesregierung, Projekte wie #Digitale Vorbilder – Familien gehen online. durch die Bereitstellung von Ressourcen zu fördern und zu unterstützen. Hierdurch kann ein niedrigschwelliger Zugang zu umfassenden Themen der Medienerziehung für Familien in Mecklenburg-Vorpommern gewährleistet werden. Der LfDI MV steht der Landesregierung jederzeit zur Verfügung, um inhaltlich und strategisch über die Projektergebnisse und deren weitere Verwendungsmöglichkeiten zu beraten, sodass auch zukünftig eine größtmögliche Zahl interessierter Familien in Mecklenburg-Vorpommern Zugang zu den aufbereiteten Bildungsmaterialien erhält.

4.4 Die Datenschutzaufsichtsbehörden des Bundes und der Länder: AK Datenschutz und Medienkompetenz & youngdata.de

Die DSK arbeitet mit Arbeitskreisen zu verschiedenen Themengebieten. Im Berichtszeitraum übernahm der LfDI MV die Leitung des Arbeitskreises Datenschutz und Medienkompetenz der DSK. Zuvor hatte die Aufsichtsbehörde in Thüringen die Leitung des Arbeitskreises inne. Durch personelle Veränderungen und das bundesweit beispielgebende Engagement des LfDI MV in der Vermittlung von Datenschutzbewusstsein und Medienkompetenz übernahm Mecklenburg-Vorpommern die Leitung des Arbeitskreises. In der jährlich stattfindenden Sitzung informieren sich die Aufsichtsbehörden untereinander über Bildungsprogramme und Initiativen sowie Unterrichtsmaterialien zur Vermittlung von Medienkompetenz.

Ziel ist es, die hoheitliche Aufgabe nach Artikel 57 Absatz 1 Buchstabe b DS-GVO mit konkreten Umsetzungen bundesweit zu koordinieren und sichtbar zu machen. Die europäische Gesetzgebung formulierte klar in der DS-GVO die Sensibilisierung und Aufklärung der Bürger/-innen über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten als zentrale Aufgabe. Der LfDI MV kommt dieser Aufgabe seit mehr als 12 Jahren konsequent nach, ebenso das Kollegium im Bundesgebiet. Bei der Vernetzung der Aufsichtsbehörden zu diesem Thema gibt es viele Synergieeffekte. So gibt es beispielsweise eine Kooperation mit Pixi, die in kleinen Büchern und Videos schon für kleinere Kinder das Thema Datenschutz und Informationsfreiheit anhand leicht verständlicher Beispiele aufbereitet. Jede Aufsichtsbehörde setzt die Aufgabe nach Artikel 57 Absatz 1 Buchstabe b DS-GVO mit einem unterschiedlichen Fokus auf eine oder mehrere Zielgruppen um. Die Vernetzung und der Austausch ermöglichen es uns, gemeinsam verschiedene Materialien für die Erfüllung des Aufklärungsauftrags zu nutzen.

Damit wurde ein Jugendportal zum Datenschutz und zur Informationsfreiheit ansprechend und informativ gestaltet, sodass Jugendliche selbstbestimmt und souverän durch unsere digitale Welt gehen können – die Grundidee des Datenschutzes. Digitale Kompetenz und Datenschutzbewusstsein sind jedoch für jeden Menschen – unabhängig vom Alter – in der digitalen Gegenwart unerlässlich. Alle Menschen sind eingeladen, sich auf youngdata.de über die Themen Datenschutz, Fake News, Demokratiebildung, Menschenrechte, Technik und vieles mehr zu informieren.

Weiterhin gehört die Arbeitsgruppe youngdata.de (siehe 4.1) zum Arbeitskreis Datenschutz und Medienkompetenz und wird vom LfDI MV aktiv geführt.

4.5 Vom FSJ Politik und Demokratie beim LfDI MV

Der LfDI MV bietet für junge Erwachsene jährlich die Möglichkeit an, ein Freiwilliges Soziales Jahr (FSJ) zu absolvieren. Dieses beginnt gewöhnlich am 1. September und endet am 31. August des Folgejahres. Die Zeiten sind bei Bedarf jedoch individuell anpassbar. Wichtig ist dabei allerdings, dass ein FSJ mindestens sechs Monate umfassen muss.

Im folgenden Abschnitt berichtet unser FSJ-Absolvierender aus dem Jahr 2024/2025 von seinen Eindrücken dieser Möglichkeit und von seinen persönlichen Erfahrungen:

„Wie vielen anderen jungen Erwachsenen war mir nicht klar, wohin mein Weg mich nach dem Abitur führen sollte. Ich wollte nicht übereifrig von einer Schulbank zur nächsten wechseln und ein Studium oder eine Ausbildung beginnen, mein Zuhause verlassen, meine Freunde zurücklassen und in eine andere Stadt ziehen. Außerdem bin ich keinesfalls davon überzeugt, ohne jegliche Arbeitserfahrung und Zeit für Selbstverwirklichung nach der Schulzeit sofort und unüberlegt ein Studium anzugehen, welches man dann womöglich nach ein oder zwei Semestern abbricht. Mir war bewusst, dass ich Zeit brauchte, um eine überdachte Entscheidung treffen zu können.

Nach tagelangen Überlegungen und viel Recherche stieß ich auf die Idee, ein Freiwilliges Soziales Jahr im Bereich Politik und Demokratie zu machen, in welchem ich mich persönlich weiterentwickeln möchte. Somit ist es mir möglich, Arbeitserfahrung zu sammeln und parallel Anreize für meine Zukunft mitzunehmen. Außerdem interessierte mich Politik schon immer sehr. Bei der Auswahl eines FSJ in Demokratie und Politik bestand die Möglichkeit, zwischen verschiedenen Einsatzstellen, die dieses Thema bedienen, zu wählen. Die Stelle im Referat Presse, Kommunikation und Medienbildung bei dem LfDI MV sprach mich besonders an. Die Entscheidung, mein FSJ zu beginnen, bereue ich keinesfalls.

In einer zunehmend digitalen Welt ist der Schutz unserer persönlichen Daten enorm wichtig. Als FSJ in der Medienbildung beim Landesdatenschutz kann ich mich aktiv in verschiedenen Bereichen einbringen, eine interessante Kombination aus Engagement, Kreativität und Technologie. Ich lerne viel über die wichtigen Themen Medien und Datenschutz und kann mich nebenbei auch selber weiterentwickeln. Dies ist möglich durch die abwechslungsreiche Arbeit, die ich als FSJler übernehme, welche mir tiefe Einblicke in diese gesellschaftsrelevanten Themen ermöglicht. Beim LfDI MV ist es darüber hinaus möglich, dass man in die Themen der Referate für Recht und Technik reinschnuppern kann. Meine Aufgaben im Referat Medienbildung reichen vom Artikel-Schreiben und organisatorischer Arbeit über das Designen von Posts bis hin zum aktiven Mitwirken bei verschiedensten Projekten und Tagungen zur Vermittlung von Medienkompetenz in MV. Diese Projekte richten sich an Lehrer/-innen und Erzieher/-innen sowie Eltern, aber auch an Kinder und Jugendliche. So findet beispielsweise zweimal jährlich die Ausbildung der Medienscouts MV statt. Etwa 30 Jugendliche aus ganz MV kommen zusammen und lernen kostenfrei von verschiedensten Institutionen, wie Medien unseren Alltag beeinflussen. Die Themen hierbei sind u. a. Cybermobbing, Fake News, Gaming und Social Media, aber auch, wann man sich strafbar macht durch das Teilen von Inhalten.

Das erlernte Wissen wird im Anschluss an den jeweiligen Schulen weitergegeben. So können viele Schüler/-innen erreicht werden, die ebenfalls sicher und kritisch mit Medien umgehen lernen müssen.

Als FSJ beim LfDI MV hilft man demnach nicht nur sich selbst, sondern auch der Gesellschaft, indem man sowohl Erwachsene als auch Jugendliche für Gefahren im Netz sensibilisiert und über Medienkompetenz aufklärt. Ein weiterer bemerkenswerter Vorteil meines FSJ ist, dass man einen Landtagsausweis erhält. Mit diesem kann man Landtagssitzungen oder Ausschüsse verfolgen und live an der Demokratie in MV teilhaben.

Mein FSJ zeigt, dass es nicht nur ein Jahr der Orientierung sein muss, sondern auch eine echte Chance bieten kann, Verantwortung zu übernehmen, die eigene Zukunft aktiv mitzugestalten und dabei etwas Sinnvolles für die Gesellschaft zu tun. Ich sehe dieses FSJ als eine sehr wertvolle Vorbereitung auf meine berufliche Zukunft."

Wir sind unseren FSJler/-innen für das Einbringen ihrer Erfahrung und für frische Ideen in unsere weitere (Bildungs-)Arbeit sehr dankbar. Gleichzeitig freut es uns, dass wir als LfDI MV jungen Menschen die Möglichkeit anbieten können, Orientierung zu bieten und Einblicke in den Arbeitsalltag unserer Behörde zu gewährleisten. Dank des Landtagausweises ist es möglich, zusätzlich bei Interesse das politische Geschehen aus unmittelbarer Nähe zu beobachten.

5. Wirtschaft

Im Bereich der Wirtschaft überwacht der LfDI MV die Einhaltung der DS-GVO über alle Branchen hinweg, von der Agrarwirtschaft bis zur Zimmerei, sofern diese personenbezogene Daten verarbeiten. Tatsächlich ist dies in den meisten Betrieben und Unternehmen der Fall. Zumindest Kundendaten und/oder auch Beschäftigtendaten werden hier verarbeitet. Die nachfolgenden Fallschilderungen aus dem Bereich Wirtschaft sind exemplarisch für die Bandbreite der Aufsichts- und Beratungstätigkeit des LfDI MV.

5.1 Videoüberwachung in Fitnessstudios

Immer mehr Fitnessstudios nutzen Videokameras, um ihre Studioräumlichkeiten zu überwachen. Dies geschieht teilweise durch Videobeobachtung, bei welcher eine Live-Übertragung der Bilder auf einen Monitor erfolgt, teilweise auch durch Videoaufzeichnung, bei welcher die Aufnahmen gespeichert und später ausgelesen werden können, oder natürlich auch durch eine kumulative Anwendung beider Verfahren. Gerade in der heutigen Zeit öffnen immer mehr Fitnessstudios, die weitestgehend personallos geführt werden. Die Betreiber/-innen wählen als Sicherheitsmaßnahme gern die Videokamera, um sich aus zuvor genannten Gründen geschützt bzw. vorbereitet zu fühlen. Hier gilt es jedoch, im Vorfeld abzuwägen, ob dieses gewählte Mittel der Videoüberwachung tatsächlich die beste Option für Betreiber/-innen und Betroffene mit Blick auf Datenschutzbelange ist.

In einer neu gegründeten Unterarbeitsgruppe Videoüberwachung Fitnessstudio der Datenschutzaufsichtsbehörden der Länder, zu der sich bereits alle Bundesländer in einer konstituierenden Sitzung online trafen, soll mittels eines Arbeitspapiers Orientierungshilfe Videoüberwachung in Fitnessstudios erläutert werden, wie eine Videoüberwachung auf den Trainingsflächen und in den anderen Bereichen eines Fitnessstudios im Einklang mit der DS-GVO möglich ist. Dabei will die Orientierungshilfe die in der Praxis auftretenden vielfältigen Varianten der Videoüberwachung aufgreifen.

Die häufigsten Begründungen für eine Videoüberwachung in einem Fitnessstudio waren demnach die Vermeidung von Diebstählen und Vandalismus oder das Registrieren bzw. Lokalisieren medizinischer Vorfälle. Besonders bei personallos geführten Fitnessstudios in Mecklenburg-Vorpommern wurden diese Begründungen angeführt. Bei den durch unsere Behörde durchgeführten Vor-Ort-Kontrollen von Videoüberwachungen in Fitnessstudios fiel auf, dass dabei sowohl Mitarbeiter/-innen als auch Aufenthaltsbereiche mitgefilmt werden.

Eine Rundumüberwachung des sozialen Lebens kann auch anhand zivilrechtlicher Maßstäbe nicht mit dem Schutz vor Diebstahl gerechtfertigt werden. Regelmäßig überwiegen hier die schutzwürdigen Interessen der Betroffenen. Eine Videoüberwachung in einem öffentlich zugänglichen Betriebs- oder Geschäftsbereich ist möglich, wenn sie zur Wahrung berechtigter Interessen der Verantwortlichen erforderlich ist und schutzwürdige Interessen der Beschäftigten sowie Gäste nicht überwiegen.

Darüber hinaus ist eine Videoüberwachung von Aufenthaltsbereichen in einem Fitnessstudio im Regelfall datenschutzrechtlich unzulässig. In Sitzbereichen halten sich Gäste typischerweise über längere Zeit auf, erholen und unterhalten sich. Die Rechtsprechung ordnet dieses Verhalten dem Freizeitbereich der Gäste zu[16]. Persönlichkeitsrechte sind hier besonders zu schützen. Eine Videoüberwachung stört die unbeeinträchtigte Kommunikation und den unbeobachteten Aufenthalt der Studiobesucher/-innen und greift intensiv in deren Rechte[17] ein. Bereiche, die zum längeren Verweilen, Entspannen und Kommunizieren einladen, dürfen daher regelmäßig nicht mit Kameras überwacht werden.

5.2 Vor-Ort-Kontrollen bei Videoüberwachungen

In einer Vielzahl von Beschwerden, die den LfDI MV im vorliegenden Berichtszeitraum erreichten, geht es um Videoüberwachungen, die den Eindruck erwecken, dass auch der öffentliche Bereich mit aufgenommen werden könnte. Dabei handelt es sich zumeist um Videoüberwachungen im nachbarschaftlichen Kontext oder um Videoüberwachungsanlagen, die von Unternehmen installiert wurden.

Bei Videokameras in Wohn- und Gewerbegebieten herrscht eine große Unsicherheit darüber, was hier überhaupt erlaubt ist und wie eine Videokamera auf dem privaten Grund oder einem Betriebsgelände eingestellt werden muss. Dabei ist die Lage vor Ort für die betroffene Person und für die verantwortliche Person regelmäßig gar nicht so leicht einzuschätzen.

---

[16] Vgl. AG Hamburg, Urteil vom 22. April 2008 – 4 C 134/08.

[17] Vgl. OH Videoüberwachung durch nichtöffentliche Stellen, Punkt 5.3 in URL: https://www.datenschutzkonferenz-online.de/media/oh/20200903_oh_v%C3%BC_dsk.pdf [aufgerufen am 23.04.2025].

Bei unklaren oder sich widersprechenden Sachverhalten wird daher grundsätzlich eine unangekündigte Vor-Ort-Kontrolle durch den LfDI MV durchgeführt. Im Jahr 2024 führten die Mitarbeiter/-innen unserer Behörde insgesamt 26 unangekündigte Vor-Ort-Kontrollen zur Videoüberwachung im gesamten Landesbereich durch.

Bei einer Kontrolle dieser Art wird die konkrete Situation direkt vor Ort geprüft und beteiligte Personen können unmittelbar beraten werden. Auf diese Weise kann oftmals ein langwieriger Schriftverkehr vermieden werden. In einem persönlichen Gespräch können sich die beteiligten Personen sachlich und verständlich mit den Mitarbeiter/-innen des LfDI MV austauschen. Ärger, Wut oder Enttäuschung über eine platzierte Videokamera oder die entsprechende Beschwerde darüber können zusätzlich durch eine vermeintlich unverständliche Verwaltungssprache und mangelnde Einbeziehung der beteiligten Personen im schriftlichen Verwaltungsverfahren entstehen. Dagegen können verständliche Hinweise und Erläuterungen vor Ort Verständnis und eine Sensibilisierung für den Datenschutz schaffen. So werden zahlreiche Widersprüche, Klagen und weitere Beschwerden vermieden. Darüber hinaus bleiben vielen Bürger/-innen so auch zusätzlicher Ärger, Aufregung, schlaflose Nächte und gesundheitliche Beeinträchtigungen erspart.

5.3 Videoüberwachung auf einem Musikfestival

Durch einen Zeitungsartikel wurden wir auf eine umfassende Videoüberwachung auf einem Musikfestival mit 75.000 Besucher/-innen pro Tag aufmerksam. Demnach sollten durch den Verantwortlichen 60 Videokameras betrieben werden, die rund um die Uhr hochauflösende Bilder von allen Bereichen des Festivalgeländes erfassen. Neben dem Geschehen vor den Bühnenbereichen sollten dabei insbesondere auch die dortigen Zelt- und Campingplätze gefilmt werden.

Eine Videoüberwachung von Zelt- und Campingplätzen ist im Regelfall datenschutzrechtlich unzulässig. Auf Zelt- und Campingplätzen halten sich Gäste typischerweise über längere Zeit auf – sie schlafen, essen, trinken und unterhalten sich. Die Rechtsprechung ordnet dieses Verhalten dem Freizeitbereich der Gäste zu. Persönlichkeitsrechte sind hier besonders zu schützen. Eine Videoüberwachung stört die unbeeinträchtigte Kommunikation und den unbeobachteten Aufenthalt der Gäste und greift intensiv in deren Rechte ein. Die vermeintliche Gefahr, ein möglicherweise entstehendes Feuer nicht rechtzeitig zu entdecken, besteht in diesem Zusammenhang in der Regel nicht, da sich neben den Gästen auch ausreichend Personal auf dem Gelände befindet, das bei entsprechenden Vorfällen unmittelbar die Feuerwehr verständigen kann. Bereiche, die zum längeren Verweilen, Entspannen und Kommunizieren einladen, dürfen daher regelmäßig nicht mit Kameras überwacht werden.

Dementsprechend wurde mit dem Verantwortlichen vor Beginn des Festivals eine angemeldete Vor-Ort-Kontrolle durchgeführt, bei der wir uns die Videoüberwachungsanlage erläutern ließen. Die Bilder der Videoüberwachungsanlage liefen in der gemeinsamen Führungsstelle des Veranstalters auf. Diese Führungsstelle wurde dauerhaft von den jeweils zuständigen Vertreter/-innen von Veranstalter, Sicherheitsdienst, Polizei, Ordnungsamt, Feuerwehr und Rettungskräften besetzt.

Der Zugang zu diesem Raum wurde durch den Veranstalter kontrolliert. In der gemeinsamen Führungsstelle liefen die Bilder von den 20 fest installierten Kameras (ohne Zoomfunktion) auf einem geteilten Monitor auf. Diese Kameras lieferten kein ständiges Livebild, sondern nur ein jeweils einzelnes Bild, welches nach kurzer Zeit aktualisiert wurde. Zusätzlich befand sich eine zoom- und schwenkbare Kamera im oberen Bereich der Hauptbühne. Diese wurde genutzt, um Brände nach Sichtung auf den anderen Kameras zu verifizieren oder um Rettungskräfte bei einem Einsatz in das richtige Gebiet zu navigieren.

Ein Personenbezug bei der Datenerfassung ließ sich entsprechend durch die Bilder der Kameras in den Bereichen vor den Bühnen feststellen, nicht jedoch in dem Bereich der Zelt- und Campingplätze. Hier wurde nach DIN EN 62676-4 maximal ein „Detektieren“ mit einer Auflösung von maximal 25 Pixel/Meter erreicht. Die Qualitätsstufe „Detektieren“ ermöglicht demnach lediglich eine Anwesenheitsermittlung. Auf diese Weise kann lediglich festgestellt werden, ob eine Person oder ein Objekt im Sichtfeld vorhanden sind. Eine Identifizierung ist folglich nicht möglich. Die Videoüberwachung betraf somit nicht die Personen auf den Zelt- und Campingplätzen.

Anders verhielt es sich in den Bereichen vor den Bühnen. Hier waren die Personen von der Videoüberwachung betroffen. Entsprechend prüfte unsere Behörde, ob eine datenschutzrechtliche Zulässigkeit nach Artikel 6 Absatz 1 Buchstabe f DS-GVO vorliegt.

Dabei darf die Videoüberwachung nur in Betrieb genommen werden, wenn schutzwürdige Interessen der Betroffenen nicht überwiegen.

Grundsätzlich waren die Bilder der Betroffenen als Gäste eines Festivals hier dem Freizeitbereich zuzuordnen, in welchem die Persönlichkeitsrechte besonders zu schützen sind. Eine Videoüberwachung stört die unbeeinträchtigte Kommunikation und den unbeobachteten Aufenthalt der Besucher/-innen und greift intensiv in deren Rechte ein. Neben den Besucher/-innen befanden sich auch Personal des Veranstalters, Polizei und Feuerwehr vor Ort, die bei entsprechenden Vorfällen unmittelbar reagieren konnten. Jedoch stößt ein analoges Sicherheitskonzept bei 75.000 Besucherinnen und Besuchern pro Tag auf dem Musikfestival organisatorisch an seine Kapazitätsgrenzen. Hier ist eine zentrale Einsatzleitung unabdingbar, um die gesamte Lage schnellstmöglich zu erfassen, Einsatzkräfte zu lenken und um Besucher/-innenströme zu leiten. Abgemildert wurde die Videoüberwachung entsprechend durch die Beschränkung auf ein reines Monitoring und durch die Exklusivität der Zugriffsmöglichkeit durch die Führungsstelle der Einsatzleitung. Die Videoüberwachung konnte somit zu den o. g. Zwecken und unter Einhaltung der mit dem LfDI MV besprochenen Vorgaben zu einem späteren Zeitpunkt bei der Durchführung des Festivals stattfinden.

5.4 Einholung von Selbstauskünften bei Mietinteressierten

Es kommt regelmäßig vor, dass Vermieter/-innen, Makler/-innen oder Hausverwaltungen persönliche Angaben von Mietinteressierten erheben, bevor eine Wohnraumbesichtigung stattfindet. Auf Basis der erfragten Daten soll dann vorab eine Entscheidung über einen Besichtigungstermin getroffen werden. In diesem Zusammenhang erreichte uns im vorliegenden Berichtszeitraum eine Beschwerde. An der Beantwortung dieser Fragen müssen Vermieter/-innen ein berechtigtes Interesse haben bzw. dürfen nur solche Daten erhoben werden, die zur Durchführung des Besichtigungstermins erforderlich sind.

Auf Basis einer Interessenabwägung muss das Recht der Mietinteressierten auf informationelle Selbstbestimmung Beachtung finden. In diesem Zusammenhang können sich Beschwerden ergeben, wonach personenbezogene Daten zu früh, d. h. noch vor dem Besichtigungstermin, erhoben wurden, wie beispielsweise Mieterselbstauskünfte oder Bonitätsauskünfte.

Bezüglich der Datenerhebung kann zwischen bis zu drei Zeitpunkten differenziert werden:

[A] dem Besichtigungstermin,
[B] der vorvertraglichen Phase, in welcher die Mietinteressierten den künftigen Vermieter/-innen mitteilen, eine konkrete Wohnung anmieten zu wollen, und
[C] der Entscheidung der künftigen Vermieter/-innen für eine/einen bestimmte/n Mietinteressierte(n) (Erstplatzierte).

Die Zulässigkeit der Erhebung personenbezogener Daten der Mietinteressierten richtet sich zum Zeitpunkt des Besichtigungstermins regelmäßig nach Artikel 6 Absatz 1 Buchstabe f DS-GVO. Spätestens nach der Erklärung der Mietinteressierten, eine konkrete Wohnung anmieten zu wollen, entsteht ein vorvertragliches Schuldverhältnis zu den künftigen Vermieter/-innen, sodass dann Artikel 6 Absatz 1 Buchstabe b DS-GVO maßgebend ist.

Streben Mietinteressierte zunächst nur eine Besichtigung der Räumlichkeiten an, so ist es in aller Regel nicht erforderlich, Angaben zu den wirtschaftlichen Verhältnissen zu erfragen. Lediglich Angaben zur Identifikation wie Name, Vorname und Anschrift dürfen erfragt werden. Zur Überprüfung und Dokumentation des Namens der Mietinteressierten sind Vermieter/-innen befugt, sich den Personalausweis vorzeigen zu lassen. Eine Ausweiskopie darf jedoch nicht angefertigt werden, da dies nicht erforderlich und nicht zulässig wäre. Auch die Erhebung der personenbezogenen Daten in Form von Mieterselbstauskünften oder Bonitätsauskünften zu diesem Zeitpunkt ist unzulässig.

Bei eingehenden Beschwerden dieser Art ist der Verfahrensweg grundsätzlich folgender: Ist der Verantwortliche hinsichtlich der vorliegenden Beschwerde noch nicht in Erscheinung getreten, wird dieser über den Verstoß informiert und für die Zukunft gewarnt (Artikel 58 Absatz 2 Buchstabe a DS-GVO). Tritt der Verantwortliche nach der Warnung ein weiteres Mal in dieser Problematik in Erscheinung, wird er verwarnt (Artikel 58 Absatz 2 Buchstabe b DS-GVO). Tritt der Verantwortliche ein drittes Mal in Erscheinung, werden andere Sanktionsmöglichkeiten bis hin zur Einleitung eines Ordnungswidrigkeitenverfahrens (Artikel 83 DS-GVO) geprüft.

Abschließend lässt sich zusammenfassen, dass zum Zeitpunkt eines Besichtigungstermins lediglich Angaben zu Name, Vorname, Anschrift, Telefon und E-Mail-Adresse sowie im Falle einer Sozialwohnung der Wohnberechtigungsschein gefordert werden dürfen. Nachzulesen ist dies ebenfalls in den Ausführungen der Orientierungshilfe zur Einholung von Selbstauskünften bei Mietinteressierten der Datenschutzkonferenz[18].

[18] URL: https://www.datenschutzkonferenz-online.de/media/oh/2024-01-24_DSK-OH_Mietinteresse_V1.0.pdf [abgerufen am 16.04.2025].

Zum Zeitpunkt der Bekanntgabe eines Anmietinteresses dürfen dann zusätzliche Angaben wie Personenanzahl, ehemalige/r Arbeitgeber/-in oder Angaben zu Einkommensverhältnissen gefordert werden. Erst nach Entscheidung des Vermietenden für den oder die Mietinteressierte/n sind auch Nachweise in Form von Gehaltsabrechnungen, Kontoauszügen oder Einkommensteuerbescheiden vorzulegen. Nicht erforderliche Angaben können auf diesen Nachweisen geschwärzt werden.

5.5 Auskunfteien

Der Europäische Gerichtshof (EuGH) hat Ende des Jahres 2023 zwei wichtige Entscheidungen über die Zulässigkeit von Datenerhebungen aus öffentlichen Registern und deren Speicherdauer sowie die Übermittlung und Verwendung von Scorewerten getroffen.

Auskunfteien speichern Daten aus öffentlichen Schuldnerverzeichnissen der Gerichte und insbesondere Meldungen von ihren Vertragspartnern, etwa Kreditinstituten, Leasing-Gesellschaften, Versandhandelsunternehmen, Kreditkartengesellschaften und Telekommunikationsunternehmen. Es werden beispielsweise die Einziehung der Kreditkarte oder die Kündigung des Girokontos wegen missbräuchlicher Nutzung, die Abgabe einer eidesstattlichen Versicherung, fruchtlose Pfändungen, Lohnpfändungen oder Scheckrückgaben mangels Deckung gespeichert. Sie erteilen Auskünfte an ihre Vertragspartner zur Risikoeinschätzung von Geld- oder Warenkrediten. Aus datenschutzrechtlicher Sicht richtet sich die Verarbeitung der personenbezogenen Daten durch Auskunfteien grundsätzlich nach Artikel 6 Absatz 1 Buchstabe f DS-GVO.

Im ersten der beiden o. g. Verfahren ging es um die Erhebung von Daten über eine Restschuldbefreiung und deren Speicherung für drei Jahre. Im Insolvenzregister werden diese Daten nur sechs Monate abrufbar gehalten. Der EuGH hat nun entschieden, dass private Auskunfteien solche Daten jedenfalls nicht länger speichern dürfen als das öffentliche Insolvenzregister, d. h. also nicht länger als sechs Monate.

Im zweiten Fall ging es um den Bonitätsscore, den Wirtschaftsauskunfteien errechnen. Sie bewerten auf der Grundlage der von ihnen gespeicherten Daten die Kreditwürdigkeit von Kreditnehmern, d. h. die Wahrscheinlichkeit, ob der Kredit rechtzeitig und vollständig zurückbezahlt werden wird. Die Erstellung und Verwendung eines solchen Scores hat der EuGH als automatisierte Entscheidung über den Kredit angesehen. Insbesondere dann, wenn ihm die Kreditgeber „eine maßgebliche Rolle im Rahmen der Kreditgewährung beimessen“[19]. Eine automatisierte Entscheidung ist allerdings gemäß Artikel 22 DS-GVO grundsätzlich unzulässig und darf nur aufgrund einer Einwilligung oder einer gesetzlichen Erlaubnis getroffen werden.

[19] Vgl. EuGH, PRESSEMITTEILUNG Nr. 186/23, 7. Dezember 2023.

Aufgrund dessen wurde die in MV ansässige Wirtschaftsauskunftei zur Umsetzung dieser Entscheidungen im Mai 2024 durch den LfDI MV befragt und es wurden entsprechende Informationen nach Artikel 58 Absatz 1 Buchstabe a DS-GVO eingeholt. Die Wirtschaftsauskunftei teilte uns glaubhaft mit, dass die Prozeduren der Datenverarbeitung schon vor den genannten Urteilen des EuGH, d. h. mit den Schlussanträgen des Generalstaatsanwaltes, angepasst wurden. Insbesondere werden Informationen aus den Insolvenzbekanntmachungen über die Erteilung der Restschuldbefreiung nicht mehr länger als im öffentlichen Verzeichnis, d. h. also sechs Monate, gespeichert.

Hinsichtlich der Scorewerte wurde dem LfDI MV mitgeteilt, dass der von ihnen erstellte Bonitätsindex nicht ausschließlich automatisiert errechnet wird, sondern sich aus zahlreichen unterschiedlichen Faktoren zusammensetzt und abschließend durch eine menschliche Entscheidung, d. h. durch fachliche Bewertung der Mitarbeiter/-innen, gebildet würde.

6. Europäische Zusammenarbeit

Der LfDI MV ist eine nach dem Unionsrecht (Artikel 51 DS-GVO) unabhängige Datenschutzaufsichtsbehörde – gleichzeitig stimmen wir uns jedoch deutschlandweit in der DSK und europaweit im EDSA ab, um die datenschutzrechtlichen Vorgaben in der gesamten EU kohärent anzuwenden. Im föderal strukturierten Deutschland arbeiten wir in der DSK schon seit vielen Jahren gut zusammen. Auf europäischer Ebene spricht Deutschland mit einer Stimme als Teil der 31 europäischen Datenschutzaufsichtsbehörden – 28 in der EU, drei im Europäischen Wirtschaftsraum (EWR).[20] Auch Beratungsanfragen, Datenpannen oder Beschwerden machen nicht mehr an nationalen Grenzen halt – Bürger/-innen nutzen internationale Dienste und oft sitzen Verantwortliche oder Auftragsverarbeiter/-innen in anderen Ländern der Union. Vor allem, um solche grenzüberschreitenden Datenpannen oder Beschwerden gemeinsam zu bearbeiten, aber auch für den kollegialen Austausch ist der LfDI MV über das Binnenmarktinformationssystem (engl. Internal Market Information System [IMI]) mit den anderen Datenschutzaufsichtsbehörden in Kontakt. Im Berichtszeitraum haben wir Bürgerinnen und Bürger aus MV dabei unterstützt, ihre Rechte grenzüberschreitend wahrzunehmen (siehe Punkt 6.1).

Neben der konkreten Prüfung von Datenpannen, Beschwerden und Anfragen tauschen wir uns europaweit auch zu strategischen Fragen aus und bilden in den Subgroups (ESG) des EDSA internationale Teams, um Leitlinien, Zertifizierungen, Antworten an Interessensvertretungen aus der Wirtschaft oder Politik vorzubereiten. Die europäische Zusammenarbeit und das Mitwirken an den Aktivitäten des EDSA gehören zu den gemäß Artikel 57 Absatz 1 DS-GVO gesetzlich vorgeschriebenen Aufgaben des LfDI MV, auch als eher kleine Aufsichtsbehörde. Wir nehmen derzeit die stellvertretende Ländervertretung in der Enforcement ESG wahr. Der LfDI MV konnte sich dieses Jahr in mehreren Subgroups so einbringen, dass insbesondere auch Unternehmen in MV profitieren können (siehe Punkt 6.2).

[20] Siehe Übersicht der einzelnen Länder und Aufsichtsbehörden, URL: https://www.edpb.europa.eu/about-edpb/about-edpb/members_de [abgerufen am 19.03.2025].

Im Jahr 2024 engagierten wir uns besonders bei der Umsetzung der europaweit koordinierten Prüfaktion, engl. Coordinated Enforcement Framework (CEF). Die diesjährige Fragebogenaktion befasste sich auf den Vorschlag der Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI) hin mit dem Recht auf Auskunft gemäß Artikel 15 DS-GVO. Die Ergebnisse für MV helfen uns, unsere Beratungs- und Aufsichtstätigkeit an die Bedarfe vor Ort anzupassen (siehe Punkt 6.3).

6.1 Kooperationsverfahren

Wenn Bürger/-innen beim LfDI MV Beschwerde gegen einen Verantwortlichen mit Sitz in einem anderen Mitgliedstaat einlegen, muss zunächst die federführende Aufsichtsbehörde bestimmt werden. Neben der federführenden Aufsichtsbehörde können sich auch alle Behörden als betroffene Aufsichtsbehörde melden, wenn Menschen in ihrem Zuständigkeitsbereich von der Verarbeitung ebenfalls betroffen sind – beispielsweise bei großen Unternehmen hinter beliebten Apps, Bezahldiensten oder Onlineshops. Unter Nutzung des IMI prüften wir im Berichtszeitraum 854 Abfragen gemäß Artikel 56 DS-GVO zur Feststellung der federführenden und betroffenen Aufsichtsbehörden. Im Vergleich zum Jahr 2023, in dem wir insgesamt 687 solcher Abfragen prüften, gingen dementsprechend fast 200 Abfragen mehr ein. Weiterhin prüfen wir die entworfenen Entscheidungen der europäischen Kolleginnen und Kollegen, die durch wegweisende Entscheidungen z. B. gegenüber Big Playern auch Bürger/-innen in MV direkt betreffen. Im Jahr 2024 wurden 415 Beschlussentwürfe und 279 endgültige Beschlüsse über IMI mit uns geteilt.

Der LfDI MV gestaltete 2024 selbst mehrere Kooperationsverfahren aktiv mit. Zunächst konnte ein Verfahren eines Beschwerdeführers aus MV nunmehr in Zusammenarbeit mit der federführenden Datenschutzstelle im Fürstentum Liechtenstein abgeschlossen werden. Nach umfangreicher Prüfung stellten der LfDI MV und die Datenschutzstelle fest, dass die Daten des Beschwerdeführers rechtmäßig verarbeitet wurden, und die Beschwerde wurde daher gemäß Artikel 60 Absatz 8 DS-GVO abgewiesen. Ein andauerndes Verfahren einer Studentin aus MV gegen eine Universität konnte ebenfalls gemeinsam mit der zuständigen französischen Aufsichtsbehörde Commission Nationale de l'Informatique et des Libertés (CNIL) im Berichtszeitraum zur Zufriedenheit der Beschwerdeführerin abgeschlossen werden – die Universität hatte schlussendlich die gewünschten Informationen gemäß Artikel 15 DS-GVO bereitgestellt. Wir erhielten zwei grenzüberschreitende Beschwerden von Bürger/-innen aus MV, die bereits im Laufe weniger Monate im Sinne der Beschwerdeführer/-innen aus MV geklärt werden konnten – je eine gegen einen maltesischen und einen litauischen Onlineshop. Eine weitere Beschwerde einer Person aus MV gegen einen Anbieter von Onlineglücksspiel mit Sitz in Malta wurde Ende 2024 an die federführende Aufsichtsbehörde übermittelt und geprüft. Der LfDI MV konnte somit erneut gute Erfahrungen mit der vertrauensvollen und konstruktiven europäischen Zusammenarbeit machen.

Über die konkreten Fälle hinaus werden über IMI auch freiwillige Anfragen gemäß Artikel 61 DS-GVO geteilt, z. B. zu allgemeinen Fragen der Rechtsauslegung, zum Austausch über Best Practices bei der Prüfung von Sachverhalten oder zu internen Prozessen. Aus Kapazitätsgründen konnte der LfDI MV hier kaum aktiv teilnehmen. Im IMI wird auch über einstweilige Maßnahmen einzelner Behörden im Dringlichkeitsverfahren gemäß Artikel 66 DS-GVO informiert.

Die polnische Aufsichtsbehörde führte beispielsweise zwei solcher Dringlichkeitsverfahren gegen ein soziales Netzwerk, indem die weitere Verarbeitung der Daten von zwei Beschwerdeführer/-innen in Werbeanzeigen untersagt wurde, die gewaltvolle und betrügerische Fake News enthielten.

6.2 Gremienarbeit

Der LfDI MV ist ebenso wie alle europäischen Datenschutzaufsichtsbehörden gesetzlich verpflichtet, einen Beitrag zu den Tätigkeiten des EDSA zu leisten. In den ESG des EDSA sind immer die BfDI, eine Ländervertretung und eine stellvertretende Ländervertretung für Deutschland anwesend – die stellvertretende Ländervertretung ist jedoch eine permanente Vertretung. Der LfDI MV übernimmt die stellvertretende Ländervertretung in der Enforcement ESG. Durch Personalzuwachs konnte diese Aufgabe im Berichtszeitraum besser ausgefüllt werden, wenngleich die Teilnahme an Sitzungen in Brüssel für eine kleine Aufsichtsbehörde viele Kapazitäten bindet. Besonders engagiert haben wir uns bei der jährlichen koordinierten Prüfaktion der Enforcement ESG (siehe Punkt 6.3).

Im Rahmen der Compliance, E-Government and Health (CEH) ESG konnten wir 2024 zwei Mandate in Drafting-Teams übernehmen.

Zunächst beteiligten wir uns an der Überprüfung der Verhaltensregeln im Sinne des englischen Code of Conduct (CoC) gemäß Artikel 40, 41 DS-GVO des Antragstellers European Contract Research Organization Federation (EUCROF). Die Datenschutzaufsichtsbehörden sind gemäß Artikel 40 Absatz 1 DS-GVO verpflichtet, die Ausarbeitung dieser bereichsspezifischen Verhaltensregeln für kleine und mittlere Unternehmen zu fördern. Im vorliegenden CoC wurden durch den antragstellenden Fachverband Regelungen zur Verarbeitung von personenbezogenen Daten, darunter auch Gesundheitsdaten, durch Auftragsverarbeiter im Bereich der klinischen Forschung getroffen. Von der Anwendung des CoC profitieren hauptsächlich kleine und mittlere Unternehmen, die in dem Verband EUCROF organisiert sind, z. B. Labore oder IT-Dienstleister. Die federführende Prüfung des CoC erfolgte durch die französische CNIL, deren Einschätzung sowie die Unterlagen des Antragstellers durch das aus der CEH ESG heraus gebildete Drafting-Team überprüft und eine Stellungnahme des EDSA gemäß Artikel 64 Absatz 1 Buchstabe b DS-GVO formuliert wurde. Dabei konnte auf die EDSA-Leitlinien 01/2019 über Verhaltensregeln und Überwachungsstellen gemäß der Verordnung EU 2016/679[21] zurückgegriffen werden, welche europaweite Standards für die Prüfung von Verhaltensregeln setzt, inklusive der Akkreditierung der Stelle, die die Einhaltung dieser Verhaltensregeln überwacht.

[21] EDSA-Leitlinien 01/2019, Fassung 2.0, URL: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-0_de [abgerufen am 19.03.2025].

Der unter Mitarbeit vom LfDI MV erarbeitete Beschluss 12/2024[22] wurde im Sommer 2024 vom EDSA angenommen und enthält Anregungen und Empfehlungen für das französische Kollegium auch zur Weiterleitung an den Antragsteller, sodass nach entsprechender Anpassung des CoC durch den Antragsteller eine Genehmigung möglich wird. Die federführend zuständige CNIL konnte mithilfe des Beschlusses 12/2024 die angepassten Verhaltensregeln von EUCROF nunmehr genehmigen.

Da der EUCROF CoC grenzüberschreitend in der EU genehmigt wurde, profitieren auch kleine und mittlere Unternehmen aus dem Gesundheitssektor in MV von der Möglichkeit, die datenschutzrechtlichen Anforderungen mithilfe der genehmigten Verhaltensregeln des Verbandes leichter umzusetzen und mit der nachweisbaren Einhaltung der DS-GVO Wettbewerbsvorteile zu erlangen.

Am Ende des Jahres 2024 übernahm der LfDI MV zudem ein Mandat in der Überprüfung des World Anti Doping Codes der World Anti Doping Agency (WADA). Das Ziel des Codes ist die globale Regelung im Umgang mit personenbezogenen Daten der Sportler/-innen, z. B. Gesundheitsdaten, Biomaterialien wie Blut- und Urinproben oder Standortdaten unter Einhaltung der DS-GVO. Im Jahr 2025 soll die Prüfung abgeschlossen werden.
Der LfDI MV vertiefte außerdem seine Kenntnisse in der Prüfung von Verbindlichen Internen Datenschutzvorschriften (engl. Binding Corporate Rules [BCR]) gemäß Artikel 47 DS-GVO im Jahr 2024, indem wir an einem durch die International Transfer ESG des EDSA initiierten und durch die litauische Aufsichtsbehörde in Vilnius organisierten BCR Workshop teilnahmen.

6.3 Koordinierte Prüfaktion zum Auskunftsrecht – CEF 2024

Der EDSA führt seit 2020 jedes Jahr eine koordinierte Prüfaktion – CEF – durch, bei der die Datenschutzaufsichtsbehörden europaweit ein gemeinsames Thema prüfen. Die kohärente Aufsicht über die Umsetzung der datenschutzrechtlichen Vorgaben genauso wie die grenzüberschreitende Kooperation wird durch das CEF unterstützt. Dank des Personalzuwachses war es möglich, dass der LfDI MV nun seine Rolle in der Enforcement ESG (siehe Punkt 6.2) besser wahrnehmen konnte. In dem Zuge konnten wir nun erstmals an der koordinierten Prüfaktion teilnehmen. Auf Vorschlag der BfDI hin nahm die diesjährige Aktion das Auskunftsrecht gemäß Artikel 15 DS-GVO in den Fokus. Insbesondere sollte überprüft werden, wie die einschlägigen EDSA-Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht[23] in der Praxis angewendet werden.

Das Auskunftsrecht begegnet uns beim LfDI MV regelmäßig in Beratungsanfragen oder Beschwerden. Viele Bürger/-innen nutzen dieses grundlegende Recht, um bei Unternehmen oder Behörden z. B. sicherzustellen, dass ihre Daten korrekt sind oder rechtmäßig verarbeitet werden. Mit dem europaweit gemeinsam erarbeiteten und abgestimmten Fragebogen haben wir insgesamt zwölf Verantwortliche in MV befragt, darunter Behörden wie Ministerien und Stadtverwaltungen, Verbände oder Unternehmen aus dem Tourismus- und Gesundheitssektor.

[22] EDSA-Beschluss 12/2024, nur auf Englisch und Französisch verfügbar, URL: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-122024-draft-decision-french-supervisory_de [abgerufen am 19.03.2025].

[23] EDSA Leitlinien 01/2022, Version 2.1, URL: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012022-data-subject-rights-right-access_de [abgerufen am 19.03.2025].

In Deutschland beteiligten sich neben uns auch die Landesdatenschutzaufsichtsbehörden aus Bayern (BayLDA), Brandenburg, Niedersachsen, Rheinland-Pfalz, dem Saarland und Schleswig-Holstein sowie die BfDI selbst, sodass in Deutschland insgesamt 116 Verantwortliche befragt wurden. Auf europäischer Ebene nahmen weitere 22 mitgliedstaatliche Datenschutzaufsichtsbehörden teil, sodass insgesamt die Angaben von 1.185 Verantwortlichen ausgewertet wurden.

Der gemeinsam erstellte deutsche Beitrag für den Abschlussbericht des EDSA zum CEF 2024, der im Januar vom EDSA Plenum 2025 angenommen und veröffentlicht wurde, fällt insgesamt positiv aus.[24] Viele Verantwortliche im EWR und auch in MV können Auskunftsanträge von betroffenen Personen mit internen Weisungen und Prozessen gut bearbeiten und rechtskonform beantworten. Besonders im Gesundheitssektor mit besonders sensiblen Daten haben Verantwortliche aus MV sogar Best-Practice beisteuern können, um den Auskunftsinteressen der betroffenen Personen am besten gerecht zu werden. Ein Unternehmen demonstrierte beispielhaft, wie Bürger/-innen automatisierte Auskünfte über die von ihnen verarbeiteten Daten über ihr Nutzer/-innenkonto abfragen können.

In der Kohorte der zwölf befragten Verantwortlichen aus MV haben die öffentlichen Stellen etwas mehr Nachbesserungsbedarf gehabt – der LfDI MV begann bereits im Sommer 2024 vor der Auswertung des CEF 2024 damit, für die gesetzlich verankerte beratende und beaufsichtigende Rolle der behördlichen Datenschutzbeauftragten (bDSB) zu sensibilisieren,[25] damit diese nicht für die Erfüllung von Auskunftsbegehren eingesetzt und einem Interessenkonflikt ausgesetzt werden. Dieser Austausch mit den bDSB soll zukünftig verstetigt werden, denn in einem gemeinsamen Austausch vor Ort kann unsere Beratung besonders effizient und frühzeitig greifen und die Umsetzung der datenschutzrechtlichen Vorgaben in den öffentlichen Stellen erleichtern.

Insgesamt befragte der LfDI MV im Rahmen des CEF 2024 zwölf Verantwortliche und sprach nach Auswertung dieser Ergebnisse drei Warnungen gemäß Artikel 57 Absatz 2 Buchstabe a DS-GVO aus. Bei diesen Verantwortlichen waren bisher keine oder wenige Auskunftsanträge eingegangen und wir gaben viele Hinweise zur konkreten Umsetzung des Auskunftsrechts und der EDSA-Leitlinien 01/2022. Weitere Verantwortliche wurden zum Umfang und zur Art der Daten beraten, die zu beauskunften sind, beispielsweise auch pseudonymisierte Daten oder Sprachaufzeichnungen. Wir wiesen auch darauf hin, dass der Umfang des Auskunftsrechts nicht vom Verantwortlichen unzulässig eingegrenzt werden darf, z. B. durch entsprechend gestaltete Formulare, sondern ein allgemeiner Antrag mit Zugang zu einer Übersicht über alle personenbezogenen Daten möglich sein muss. Bei sehr wenigen Verantwortlichen hat eine anschließende, vertiefte Prüfung begonnen.

[24] Report 2024 Coordinated Enforcement Action. Implementation of the right of access by controllers. Adopted on 16 January 2025, URL: https://www.edpb.europa.eu/our-work-tools/our-documents/other/coordinated-enforcement-action-implementation-right-access_de [abgerufen am 19.03.2025].

[25] S. u. a. Information des LfDI MV zum Netzwerktreffen der behördlichen Datenschutzbeauftragten (bDSB) von Kommunen in MV, URL: https://www.datenschutz-mv.de/veranstaltungen/bDSB_Treffen/ [abgerufen am 19.03.2025].

Überraschend war europaweit, wie wenig Anträge auf Auskunft gemäß Artikel 15 DS-GVO bei den Verantwortlichen eingehen – in MV erhielten vier von zwölf Verantwortlichen im Jahr 2023 keinen Antrag und fast alle übrigen eine geringe ein- bis zweistellige Anzahl. Tendenziell gingen mehr Anträge bei Unternehmen und auch bei Verantwortlichen im Gesundheitssektor ein. Der LfDI MV wird die Ergebnisse der koordinierten Prüfaktion für zielgerichtete Beratung und Handlungsempfehlungen weiter verwenden.[26]

Die Teilnahme des LfDI MV am CEF 2024 zeigte auch, dass wir europaweit ähnliche Herausforderungen bei der Umsetzung von Betroffenenrechten haben und die teilnehmenden Behörden Synergien bei der Aufsicht nutzen können. Die im ganzen EWR gewonnenen Informationen stehen mit der Veröffentlichung des EDSA-Berichtes auch für weiterführende Auswertungen zur Verfügung.

7. Gesundheit

Gesundheitsdaten im Sinne der Allgemeinheit für Forschungszwecke nutzen und gleichzeitig die sensiblen Patientendaten schützen? Natürlich gibt es in diesem Spannungsfeld kein „Entweder-oder“. Vielmehr muss beides miteinander in Einklang gebracht werden. Hierfür setzen wir uns ein!

Im Berichtszeitraum haben sowohl das Land Mecklenburg-Vorpommern als auch der Bund Gesetze erlassen, die dieses Ziel verfolgen. Der LfDI MV war am Gesetzgebungsverfahren im eigenen Bundesland beteiligt. Weiterhin konnte eine Arbeitsgruppe unter unserer Federführung ein Papier finalisieren, das sich mit der Übermittlung von Gesundheitsdaten und Biomaterialien in Drittstaaten beschäftigt.

Darüber hinaus beschäftigten uns verstärkt Beschwerden gegen Gesundheitsämter. Über zwei davon werden wir im Folgenden exemplarisch berichten.

7.1 Erhebung von Gesundheitsdaten im Rahmen der Einschulungsuntersuchung

Im Berichtszeitraum befasste sich der LfDI MV mit einer Beschwerde zur Erhebung von Gesundheitsdaten im Rahmen der Einschulungsuntersuchung. Der Beschwerdeführer erhielt mit der Einladung zur Einschulungsuntersuchung auch einen Anamnesebogen für sein Kind. In der Einladung zur Einschulungsuntersuchung befand sich der Hinweis, dass das Ausfüllen des Anamnesebogens freiwillig sei. Deshalb füllte der Beschwerdeführer den Anamnesebogen nicht aus. Einige Monate nach der Einschulungsuntersuchung forderte der Beschwerdeführer Auskunft gemäß Artikel 15 DS-GVO über die im Rahmen der Einschulungsuntersuchung gespeicherten Daten seines Kindes von dem Gesundheitsamt, welches die Einschulungsuntersuchung durchgeführt hatte.

[26] Pressemitteilung des LfDI MV: Abschluss der europaweiten Prüfung zum Auskunftsrecht – Ergebnisse auch für Mecklenburg-Vorpommern, URL: https://www.datenschutz-mv.de/presse/?id=208042 [abgerufen am 19.03.2025].

Anhand der erteilten Auskunft stellte der Beschwerdeführer fest, dass das Gesundheitsamt trotz des Hinweises zur Freiwilligkeit der Angaben dennoch Anamneseinformationen, die im Rahmen der Einschulungsuntersuchung mündlich gegeben wurden, sowie Daten aus dem bei der Untersuchung vorgelegten Mutterpass elektronisch gespeichert hatte.

Die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle ist zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe, die dem Verantwortlichen übertragen wurde, erforderlich ist. Bei der Beurteilung der Erforderlichkeit ist ein strenger Maßstab anzulegen. Nach der Rechtsprechung des EuGH[27] ist eine Datenverarbeitung erforderlich, wenn sie „auf das absolut Notwendige“ beschränkt ist. Für die Verarbeitung von Gesundheitsdaten – wie in diesem Fall – gelten jedoch zusätzlich die Vorgaben von Artikel 9 DS-GVO. Demnach ist für die Verarbeitung von Gesundheitsdaten durch die Gesundheitsämter eine konkrete Rechtsgrundlage oder eine Einwilligung der betroffenen Person erforderlich. Die rechtliche Grundlage für die Durchführung der Einschulungsuntersuchung ist § 15 Absatz 3 des Gesetzes über den Öffentlichen Gesundheitsdienst im Land Mecklenburg-Vorpommern (ÖGDG M-V). In der Schulgesundheitspflege-Verordnung (SchulGesPflVO M-V) sind außerdem Art, Umfang und Zeitpunkte der Untersuchungen geregelt. In dieser Verordnung ist auch geregelt, dass das Ausfüllen des Anamnesebogens freiwillig ist. Die Erforderlichkeit für die Speicherung der Gesundheitsdaten aus dem Anamnesebogen ist schon deshalb nicht gegeben, da auch im Einladungsschreiben zur Einschulungsuntersuchung an die Eltern darauf hingewiesen wird, dass diese Angaben freiwillig sind. Das heißt, dass der für die schulische Entscheidung bedeutsame Gesundheits- und Entwicklungsstand sowie Krankheiten und Einschränkungen des Kindes auch dann festgestellt werden können, wenn der Anamnesebogen von den Eltern nicht ausgefüllt wird.

Wegen der fehlenden Einwilligung der Sorgeberechtigten in die Datenverarbeitung und einer nicht ausreichenden gesetzlichen Norm wurden die Gesundheitsdaten des Kindes im vorliegenden Fall unrechtmäßig verarbeitet. Der LfDI MV verpflichtete daher das Gesundheitsamt, die entsprechenden personenbezogenen Daten unverzüglich zu löschen. Außerdem regte der LfDI MV die Überarbeitung der SchulGesPflVO M-V an, um Rechtssicherheit bei der Speicherung der Untersuchungsergebnisse für die Ärztinnen und Ärzte der Gesundheitsämter zu schaffen, die die Einschulungsuntersuchung durchführen.

7.2 Vorlage des Masernschutznachweises bei Gesundheitsämtern

In der täglichen Praxis begegnen uns immer wieder Fragen zur Vorlage des Masernschutznachweises für Kinder. Das Masernschutzgesetz fordert seit dem 1. März 2022 die Vorlage eines Masernschutznachweises durch die Eltern gegenüber der Kindertagesstätte oder der Schule, die ein Kind besucht bzw. besuchen soll. Alle betroffenen Personen, die mindestens ein Jahr alt sind, müssen demnach eine Masern-Schutzimpfung oder eine Masern-Immunität belegen. Kinder ab zwei Jahren müssen entsprechend mindestens zwei Masern-Schutzimpfungen oder ein ärztliches Zeugnis über eine ausreichende Immunität gegen Masern nachweisen.

[27] EUGH Aktenzeichen C-73/07, ECLI:EU:C:2008:727 Rn. 56.

Wer wegen einer medizinischen Kontraindikation nicht geimpft werden kann, muss diese ebenfalls durch ein ärztliches Attest nachweisen.[28] Die Einrichtungen der Kindertagespflege und die Schulen sind gesetzlich verpflichtet, das zuständige Gesundheitsamt zu informieren, wenn Eltern keinen Nachweis des Masernschutzes vorlegen. Wenn der erforderliche Nachweis nicht innerhalb einer angemessenen Frist (mindestens zehn Tage) vorgelegt wurde, kann das Gesundheitsamt die nachweispflichtige Person zu einer Beratung einladen. Davon unabhängig kann das Gesundheitsamt jeweils im Einzelfall entscheiden, ob nach Ablauf einer angemessenen Frist ein Betretungsverbot, Geldbußen oder gegebenenfalls Zwangsgelder ausgesprochen werden. Ausnahmefälle gelten hier bei schulpflichtigen Kindern sowie bei Lieferengpässen der Impfstoffe. Die Landesregierung hat bisher nicht von der Möglichkeit des § 20 des Infektionsschutzgesetzes Gebrauch gemacht, wonach der Masernschutznachweis nicht gegenüber der Leitung der jeweiligen Betreuungseinrichtung, sondern direkt gegenüber dem Gesundheitsamt zu erbringen ist. Daher können Gesundheitsämter in Mecklenburg-Vorpommern ohne Vorlage einer entsprechenden Information der betreuenden Einrichtung oder Schule zu fehlenden Masernschutznachweisen nicht eigenständig aktiv werden.

Im Berichtszeitraum erließ ein Gesundheitsamt ein Zwangsgeld gegen eine Familie, obwohl ihm weder von einer Betreuungseinrichtung noch von einer Schule eine entsprechende Information über fehlende Masernschutznachweise der Kinder vorlag. Das Gesundheitsamt forderte vielmehr von den Eltern die Information, in welcher Einrichtung bzw. welcher Schule die Kinder betreut werden. Das Gesundheitsamt berief sich bei der Erhebung der Daten zur betreuenden Einrichtung bzw. Schule der Kinder darauf, dass es sich beim Masernschutznachweis um eine Maßnahme zur Gefahrenabwehr handele. Im Rahmen der uns vorliegenden Beschwerde musste daher die Rechtmäßigkeit der Datenerhebung überprüft werden.

Im Epidemiologischen Bulletin Nr. 32 des Robert Koch-Instituts ist die Zielstellung zur Erhöhung der Masern-Impfbereitschaft klar formuliert: „Die Elimination der Röteln und Masern durch Impfprogramme ist in 53 Mitgliedstaaten der Europäischen Region ein erklärtes Ziel des WHO-Regionalkomitees für Europa. Wiederholt wurden die Mitgliedstaaten aufgefordert, dieses Ziel konsequent zu verfolgen und umzusetzen.“[29] Auch die Gesetzesbegründung stellt auf eine Erhöhung der Impfquote ab[30]. Die Ausnahmeregelung, wonach schulpflichtige Personen auch ohne Vorlage eines gültigen Impfnachweises betreut werden dürfen und müssen, verdeutlicht, dass der Zweck der Aufgabe des Gesundheitsamtes hier in der Erhöhung der Impfquote liegt und damit selbstverständlich auch dem Schutz der Allgemeinheit dient – das Gesundheitsamt aber nicht die konkrete Gefahr abwehren soll und darf, die von einer nicht geimpften Person ausgeht. Eine Datenerhebung zu den Betreuungseinrichtungen der Kinder der betroffenen Familie aus den angeführten Gründen der Gefahrenabwehr war daher unzulässig.

[28] Vgl. § 20 Absatz 8 Satz 4, Absatz 9 Satz 1 Nummer 2 des Infektionsschutzgesetzes (IfSG).
[29] URL: https://www.rki.de/DE/Aktuelles/Publikationen/Epidemiologisches-Bulletin/2010/32_10.pdf?__blob=publicationFile&v=3 [aufgerufen am 23.04.2025].
[30] Vgl. BT-DFrs. 19/13452 S. 1.

7.3 Forschung mit medizinischen Daten – aber sicher?!

Im Berichtszeitraum hat der Landtag Mecklenburg-Vorpommern das Gesundheitsforschungsstärkungsgesetz Mecklenburg-Vorpommern beschlossen. Dieses ändert die bisherigen Regelungen zur Forschung im Landeskrankenhausgesetz Mecklenburg-Vorpommern (LKHG M-V) und enthält eine ausdrückliche Regelung zur Entwicklung und zum Training künstlicher Intelligenz. Der LfDI MV war frühzeitig in den Gesetzgebungsprozess involviert.

Wesentliche Änderung: Forschung mit den Daten der Patientinnen und Patienten aus den Krankenhäusern in Mecklenburg-Vorpommern ist auch ohne eine ausdrückliche Einwilligung möglich. Auch wenn es auf den ersten Blick nicht so aussieht: Damit bekommen diese sogar mehr Rechte. Nach der bisherigen Regelung war Forschung entweder mit einer Einwilligung möglich oder aber, wenn durch das zuständige Ministerium das besondere öffentliche Interesse an dem Forschungsvorhaben festgestellt wurde. Forscher/-innen bemängelten die bürokratischen Hürden und wiesen auf Risiken hin, wenn beispielsweise das KI-Training für wichtige medizinische Entwicklungen nur in Drittländern mit keinen oder weniger strengen Datenschutzvorschriften stattfinden könnte. Aus Sicht der Patientinnen und Patienten zeigten Kontrollen des LfDI MV, dass die Einwilligungen häufig im Zusammenhang mit dem Aufnahmeprozess eingeholt wurden. Zu beanstanden waren dabei insbesondere Defizite bei der Information zur Einwilligung. Zudem bestand kaum eine Möglichkeit, gegen die Datennutzung vorzugehen, wenn das zuständige Ministerium das besondere öffentliche Interesse an dem Forschungsvorhaben festgestellt hatte. Nach den neuen Regelungen können Patienten und Patientinnen der Nutzung ihrer Daten voraussetzungslos und jederzeit widersprechen. Neu ist zudem, dass ihnen eine „Bedenkzeit“ von vier Wochen ab Kenntnis ihrer Rechte eingeräumt wird. Vor Ablauf der Frist dürfen die Daten nicht weiter genutzt werden.

Weitere Voraussetzungen für die Datennutzung sind die Einbindung der Ethikkommission und des Datenschutzbeauftragten sowie die Erfüllung strenger Anforderungen an die Datensicherheit. In Deutschland ist grundsätzlich eine Ethikkommission zu beteiligen, bevor mit Patientendaten geforscht werden darf. Bereits bisher wurden dabei auch datenschutzrechtliche Belange mitgeprüft. Die neuen Regelungen übernehmen diese bereits gelebte Praxis und stellen die Beteiligung des Datenschutzbeauftragten an dem Verfahren sicher. Die Ethikkommission stellt u. a. das „öffentliche Interesse“ an dem Forschungsvorhaben fest. Hierbei geht es aber nicht mehr um ein „besonderes öffentliches Interesse“, sondern um die Frage, ob das Forschungsvorhaben einen medizinischen Nutzen für die Allgemeinheit verfolgt und dabei weitere ethische Grundsätze gewahrt bleiben.

Darüber hinaus regelt das LKHG M-V nunmehr auch, welche technischen Anforderungen an die Datenverarbeitung erfüllt sein müssen. Cyberangriffe auch auf Krankenhäuser nehmen zu. Dabei fällt oft auf, dass Angriffe auf das Krankenhausinformationssystem selbst häufig noch rechtzeitig abgewehrt werden können, aber Daten aus weniger gesicherten Bereichen der IT-Infrastruktur abfließen. Patientendaten, die aus dem Krankenhausinformationssystem für Forschungszwecke extrahiert und in anderen Laufwerken abgelegt werden, sind hier besonders gefährdet. Nach dem Gesetz sollen diese Daten nunmehr ausschließlich in einem gesicherten Forschungssystem verarbeitet werden.

Langfristig bieten die neuen Regelungen zudem die Chance, die Forschung mit anonymisierten und pseudonymisierten Daten voranzutreiben und Forscher/-innen unter Einbeziehung einer Treuhandstelle qualitativ und vor allem auch quantitativ hochwertige Datensätze, etwa auch zum KI-Training, zur Verfügung zu stellen. Auch diesen Prozess wird der LfDI MV weiterhin beratend begleiten.

7.4 Arbeitsgruppe zum Transfer von Gesundheitsdaten und Biomaterial in Drittländer

Im Auftrag der DSK und ihrer Taskforce Forschungsdaten (TFFD) leitete der LfDI MV eine Unterarbeitsgruppe, die sich mit der Übermittlung von Gesundheitsdaten (z. B. Laborberichte, Anamnese) und Biomaterialien (z. B. Blut- und Gewebeproben) an Drittländer beschäftigte. Hintergrund war ein entsprechender Austausch mit der durch das Bundesministerium für Bildung und Forschung (BMBF) geförderten Medizininformatik-Initiative (MII), angeleitet durch den Forschungsverbund TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V. (TMF).[31]

Die an der MII beteiligten Institutionen aus Wissenschaft und Forschung, darunter auch die Universitätsmedizin Greifswald, hatten bereits Muster entwickelt, um Patientinnen und Patienten über die standortübergreifende Nutzung ihrer medizinischen Daten und Bioproben für wissenschaftliche Forschungszwecke zu informieren und eine Einwilligung für die Verarbeitung einzuholen. Die DSK hatte nach einem konstruktiven Austausch bereits grünes Licht für die Nutzung der Einwilligungsdokumente in der Version 1.6b und der zugehörigen Handreichung in der Version 0.9b gegeben.[32] Die Forscher/-innen stützen sich dabei auf den sogenannten „Broad Consent“ – informieren also so spezifisch wie möglich über die Art von Forschungsprojekten zur Verbesserung der allgemeinen medizinischen Versorgung, welche vorab durch eine Ethikkommission genehmigt werden müssen, sowie über die Schutzmaßnahmen in der Verbundforschung und die Rechte der betroffenen Personen.

Nunmehr bat die MII um die Einschätzung der DSK zu der beabsichtigten Übermittlung der Gesundheitsdaten und Biomaterialien aus dem Forschungsverbund an Drittländer, um an internationalen Forschungsprojekten zu partizipieren. Zu diesem Zweck wurden die Maßnahmenvorschläge der TMF vom 24. August 2023 zum Drittlandtransfer, die Patienteneinwilligung in der Version 1.7.2 sowie die Nutzungsordnung in der Version 1.1 berücksichtigt.

[31] Siehe Hintergrundinformationen zur MII und TMF, URL: https://www.tmf-ev.de/unsere-arbeit/projekte/mii-begleitstruktur [abgerufen am 10.03.2025].

[32] Siehe Pressemitteilung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 24.04.2020, URL: https://www.datenschutzkonferenz-online.de/media/pm/20200427_Einwilligungsdokumente_der_Medizininformatik-Initiative.pdf [abgerufen am 10.03.2025].

Unter der Federführung des LfDI MV konnte die Arbeitsgruppe TFFD mit unseren Fachkräften aus der Datenschutzaufsicht der wissenschaftlichen Forschung und des Internationalen Datenverkehrs im Berichtszeitraum eine umfangreiche Analyse vorlegen, die die besonderen Rahmenbedingungen der MII im Einzelfall beleuchtet und auf aktuelle Beschlüsse der DSK sowie einschlägige Leitlinien des EDSA zurückgreift. Zusammenfassend wurde festgestellt, dass keine pauschalen Lösungen für die Übermittlung dieser besonders sensiblen Daten an unterschiedliche Drittländer gefunden werden können. In jedem Einzelfall muss die Rechtmäßigkeit der beabsichtigten Übermittlung für wissenschaftliche Forschungszwecke sowohl auf erster Stufe (gemäß Artikel 5, Artikel 6 Absatz 1, Artikel 9 Absatz 2 DS-GVO als Broad Consent) und auf zweiter Stufe (gemäß Artikel 44 ff. DS-GVO geprüft werden). Die TFFD hat den Forschenden insbesondere eine Liste möglicher Garantiemaßnahmen zukommen lassen, welche etwaige Informationsdefizite des Broad Consent im Einzelfall ausgleichen könnten. Auf zweiter Stufe wurden die rechtlichen Grenzen verschiedener Transferinstrumente für die vorliegende Konstellation geprüft, die durch den jeweiligen Verantwortlichen berücksichtigt werden müssen. Außerdem ist stets zu prüfen, ob auch eine hinreichende Information der Betroffenen über die (beabsichtigte) Übermittlung gemäß Artikel 13, 14 DS-GVO erfolgt – in diesem Zuge hat die TFFD konkrete Hilfestellungen für Verantwortliche zur Verfügung gestellt. Damit konnte die Unterarbeitsgruppe erfolgreich abgeschlossen werden. Darüber hinaus bringt sich der LfDI MV dauerhaft in den Austausch der TFFD der DSK mit den Forscher/-innen ein.

8. Öffentliche Verwaltung und Kommunales

Eine Vielzahl der uns vorliegenden Beschwerden dreht sich um die Frage, ob eine bestimmte Datenverarbeitung auf eine Rechtsgrundlage gestützt werden kann oder nicht. Eng mit der Erlaubnis ist auch die Erforderlichkeit verknüpft. Denn verarbeitet werden darf ohnehin nur das, was für die Erfüllung der Aufgabe der öffentlichen Stelle unbedingt erforderlich ist. Über zwei Beschwerden zu diesen Themen möchten wir exemplarisch berichten. Nicht oder nicht ordnungsgemäß beantwortete Auskunftsersuchen sind nach wie vor der wohl häufigste Beschwerdegrund. Daher berichten wir auch zu diesem Thema wiederholt.

8.1 „Hilfe! Ich werde beim Sonnenbad auf der Terrasse gefilmt“ – warum öffentliche Stellen nicht mit Drohnen über Privatgrundstücke fliegen dürfen

Was nicht ausdrücklich erlaubt ist, ist verboten. So lässt sich Datenschutzrecht für öffentliche Stellen grob zusammenfassen. Zwar gibt es im Polizeibereich klare Regelungen zum Einsatz von Drohnen, nicht aber für all die anderen öffentlichen Stellen. Diese sollten daher vorübergehend genau prüfen, wie sie Drohnen einsetzen.

Durch eine Journalistin wurden wir darauf aufmerksam gemacht, dass der Altgebäudebestand einer Kommune erfasst werden soll. Mit dieser Aufgabe wurde ein staatlich bestellter Vermesser beauftragt, der selbst entschied, zu diesem Zweck die Grundstücke mit Drohnen zu überfliegen und Bildaufnahmen zu erstellen. Die Grundstückseigentümer/-innen und Bewohner/-innen wurden nur sehr allgemein informiert, dass der Überflug in einem Zeitraum von zwei Wochen stattfinden sollte.

Die Bewohner/-innen konnten sich so kaum darauf einstellen, dass von ihrem Garten, ihrer Terrasse oder auch von Innenräumen durch Dachfenster Videoaufnahmen aus der Luft erstellt werden sollten. Orte, an die man sich privat zurückzieht und an denen man nicht durch Dritte beobachtet werden will. Das Datenschutzrecht schützt diese Privatsphäre – verankert im Grundgesetz und der EU-Grundrechte-Charta. Bei dem Überflug von Grundstücken werden personenbezogene Daten verarbeitet, die den höchstpersönlichen Lebensbereich erfassen können. Eine solche Datenverarbeitung darf nur erfolgen, wenn ein Gesetz dies erlaubt oder die betroffene Person eingewilligt hat. Der Bayerische Verwaltungsgerichtshof hatte schon zu Beginn des Berichtszeitraums entschieden, dass solche Drohneneinsätze nicht auf eine Generalklausel gestützt werden können[33]. Eine Generalklausel erlaubt öffentlichen Stellen allgemein, zur Erfüllung ihrer Aufgaben personenbezogene Daten zu verarbeiten. Eine solche findet sich auch in § 4 des Landesdatenschutzgesetzes (DSG M-V) für Mecklenburg-Vorpommern. Allerdings stellte hier der Gesetzgeber selbst schon in der Gesetzesbegründung klar, dass auf diese Norm keine eingriffsintensiven Datenverarbeitungen, sprich beispielsweise im Schul- oder Sozialbereich, gestützt werden könnten und hierfür Spezialgesetze geschaffen werden müssten. Auf § 4 DSG M-V konnte sich der Vermesser, der hier als öffentliche Stelle tätig war, dementsprechend nicht stützen und eine andere Rechtsgrundlage gab es nicht. Daher blieb nur die Möglichkeit, dem Vermesser den Einsatz von Drohnen über Wohngrundstücken zu untersagen. Der Bescheid des LfDI MV ist noch nicht rechtskräftig. Eine Klage beim Verwaltungsgericht Schwerin ist anhängig. Beim MIBD MV regte der LfDI MV bereits an, unabhängig von dem Rechtsstreit eine Regelung zu schaffen, die den Einsatz von Drohnen für öffentliche Stellen regelt. Zudem gibt es auch länderübergreifende Pläne in dieser Richtung. Besonderes Augenmerk sollte hier auf Regelungen zur Transparenz und zu technischen Maßnahmen gelegt werden, um möglichst wenig in die Privatsphäre der Bürger/-innen einzugreifen.

Zu betonen bleibt, dass nicht gleich jeder Drohneneinsatz durch öffentliche Stellen problematisch ist. Etwa für die Kontrolle von Bauwerken, die nicht als Wohnraum dienen, kann der Einsatz von Drohnen in den meisten Fällen auf § 4 DSG M-V gestützt werden, sofern dabei überhaupt personenbezogene Daten verarbeitet werden.

8.2 Jugendamt zwischen den Stühlen – die unzulässige Übermittlung von Einkommensunterlagen in Unterhaltsfragen

Zu den Aufgaben der Jugendhilfe für junge Volljährige gehört es, diese bis zur Vollendung des 21. Lebensjahres bei der Geltendmachung von Unterhaltsansprüchen zu beraten und zu unterstützen.

In dem uns vorgelegten Fall hatte ein volljähriges Kind von diesem Anspruch Gebrauch gemacht. Das Jugendamt nahm daraufhin eine Einkommensprüfung beider Elternteile vor und berechnete die jeweilige Höhe des Unterhaltes. Das Recht auf Auskunft bezüglich der Einkommensunterlagen der Eltern hat dabei aber nicht das Jugendamt bzw. der Landkreis, sondern das volljährige Kind selbst. In dem vorliegenden Fall bat jedoch dann der Vater das Jugendamt um Auskunft über das Einkommen der Mutter.

[33] Vgl. BayVGH, Beschluss vom 15.2.2024 – 4 CE 23.2267 VG München.

Das Jugendamt holte daraufhin das Einverständnis der Tochter ein und übermittelte die von der Mutter eingereichten Einkommensunterlagen an den Vater, ohne die Mutter vorher in Kenntnis zu setzen. Diese legte daraufhin beim LfDI MV eine Beschwerde ein.

Die datenschutzrechtliche Prüfung ergab, dass die Übermittlung der Einkommensunterlagen der Mutter an den Vater unzulässig war. Aus der gesetzlich normierten Pflicht des Jugendamtes, das Kind bei der Geltendmachung seines Unterhaltsanspruchs zu unterstützen, kann keine Erlaubnis für das Jugendamt zur Übermittlung der Einkommensunterlagen der Mutter an den Vater ohne deren Einverständnis hergeleitet werden. Außerdem hatte die Mutter auch die notwendigen Unterlagen zur Berechnung des Unterhalts eingereicht, sodass das Jugendamt in der Lage war, den Unterhalt zu berechnen.

Das Jugendamt wähnte sich zunächst im Recht. Das Amt handelte doch in dem Vertrauen auf die Informationen eines Rechtsgutachtens des Deutschen Institutes für Jugendhilfe und Familienrecht, dass im weiteren Verlauf des Beschwerdeverfahrens zu der konkret vorliegenden Fragestellung auch hinzugezogen wurde. Im Ergebnis des konstruktiven Austauschs konnte der LfDI MV jedoch darauf hinwirken, dass die Prozesse datenschutzkonform überarbeitet werden. Zulässig bleibt es, die Einkommensunterlagen der Eltern dem volljährigen Kind zu übermitteln.

8.3 Das Auskunftsrecht im Sozialdatenschutz – Grenzen und Möglichkeiten

Das Recht auf Auskunft ist im Sozialdatenschutz ein wichtiges und oft in Anspruch genommenes Betroffenenrecht. Es gibt betroffenen Personen einen Anspruch darauf, dass ein Verantwortlicher erklärt, ob und wie er personenbezogene Daten der Person verarbeitet. Weiterhin hat die betroffene Person ein Recht auf eine Kopie dieser Daten. Damit ähnelt das Auskunftsrecht dem Recht auf Akteneinsicht, ist dennoch nicht vollständig mit diesem identisch. Betroffene Personen und auch Verantwortliche wandten sich häufig mit Beschwerden bzw. Fragen zu diesem Thema an uns.

Im Bereich des Sozialdatenschutzes sind oftmals einige gesetzliche Besonderheiten zu beachten. Der Verantwortliche hat zu prüfen, ob es im Rahmen der Erfüllung des Auskunftsanspruches neben Artikel 15 DS-GVO und den Leitlinien des Europäischen Datenschutzausschusses zum Auskunftsrecht („Anforderungen der Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht“) auch sozialgesetzliche Bestimmungen zu beachten gibt.

Dies kann z. B. im Bereich des Kinderschutzes der Fall sein, also wenn eine mögliche Kindeswohlgefährdung gemeldet wird. Hier schützen etwa Artikel 15 Absatz 4 DS-GVO oder auch § 83 Absatz 1 Satz 1 des Zehnten Buches Sozialgesetzbuch (SGB X) den Hinweisgeber. Ihre Identität muss gegenüber den Eltern in der Regel nicht offenbart werden. Der Verantwortliche muss jedoch die widerstreitenden Interessen gegeneinander abwägen und kann die Auskunft nicht pauschal verweigern. Darüber hinaus wird in diesem Zusammenhang von Betroffenen häufiger das Akteneinsichtsrecht gemäß § 25 SGB X geltend gemacht. Den Beteiligten steht ein solcher Anspruch jedoch nur in einem laufenden Verwaltungsverfahren zu.

Dies wird entweder nicht berücksichtigt oder es wird angezweifelt, dass ein solches Verfahren abgeschlossen werden durfte. Im Bereich des Kinderschutzes und dann, wenn aufgrund einer anonymen Meldung ein Verwaltungsverfahren eingeleitet wird, kann zwar grundsätzlich Akteneinsicht verlangt werden. Jedoch ist auch hier eine Interessenabwägung vorzunehmen und gegebenenfalls das Informationsinteresse hinter das Interesse des Hinweisgebers auf Vertraulichkeit zu stellen.

Im Rahmen einer Auskunftserteilung gemäß Artikel 15 DS-GVO sind vom Sozialleistungsträger ggf. also noch weitere Vorschriften zu beachten. Häufig besteht zudem das Problem, dass die Daten von Betroffenen schwer oder nicht von den Daten Dritter getrennt werden können. Daten Dritter dürfen jedoch nur übermittelt werden, soweit schutzwürdige Interessen an der Geheimhaltung im Sinne des § 67d Absatz 2 SGB X oder nach Artikel 15 Absatz 4 DS-GVO nicht überwiegen. Allerdings muss der Verantwortliche auch hier abwägen und ggf. Schwärzungen vornehmen. Eine vollständige Verweigerung der Auskunft wird in der Regel nicht zulässig sein.

Oftmals zweifeln die Auskunftsberechtigten auch an, dass tatsächlich schutzwürdige Belange Dritter der Auskunft entgegenstehen würden. Pauschale Aussagen eines Jugendamtes hierzu müssen dann hinterfragt werden. Meistens verbergen sich hinter Auskunftsansprüchen in diesem Bereich immer noch weiterreichende Fragestellungen und Problempunkte, die mit betrachtet bzw. geprüft werden müssen. Nicht zuletzt stellt der oftmals sehr große Umfang der Inhalte und Akten ein großes Problem dar und auch die oft gegensätzlichen Darlegungen zum Inhalt der Akten. Neben unseren allgemeinen Empfehlungen zum Auskunftsanspruch ist im Sozialdatenschutz zu empfehlen, insbesondere auch die entsprechenden Regelungen aus dem SGB X hinzuzuziehen und die durchzuführenden Verhältnismäßigkeitsprüfungen nachvollziehbar darzulegen und zu dokumentieren. Denn der EuGH stellte mit seiner Entscheidung vom 27. Februar 2025 klar[34], dass der zuständigen Aufsichtsbehörde, also dem LfDI MV, die geschützten Daten Dritter zu übermitteln sind, wenn dies notwendig ist, um die einander gegenüberstehenden Rechte und Interessen abzuwägen und den Umfang des in Artikel 15 DS-GVO vorgesehenen Auskunftsrechts der betroffenen Person zu ermitteln.

8.4 Das Auskunftsrecht der betroffenen Person – noch immer eine Herausforderung für Behörden

Im Berichtszeitraum beschwerten sich, wie schon in den letzten Jahren, betroffene Personen über nicht oder unvollständig erteilte Auskünfte gemäß Artikel 15 DS-GVO bzw. darüber, dass die Formalitäten (Frist, Begründung) gemäß Artikel 12 DS-GVO nicht eingehalten wurden.

Das Auskunftsrecht nach Artikel 15 DS-GVO ist ein bedeutsames Betroffenenrecht. Betroffene Personen können von dem für die Datenverarbeitung Verantwortlichen eine Auskunft darüber verlangen, welche Daten über sie gespeichert sind bzw. verarbeitet werden. Verantwortliche müssen betroffene Personen außerdem u. a. über die Verarbeitungszwecke, die Herkunft der Daten, soweit diese nicht direkt beim Betroffenen erhoben wurden, oder über die konkreten Empfänger, an die diese Daten übermittelt wurden, informieren. Dieses Recht steht allen Bürger/-innen gegenüber öffentlichen Stellen (z. B. Behörden) und nicht öffentlichen Stellen (z. B. Wirtschaftsunternehmen, Verbänden, Vereinen etc.) zu.

[34] Vgl. EuGH (Erste Kammer), Urt. v. 27.2.2025 – C-203/22.

Durch das Auskunftsrecht werden die Bürger/-innen in die Lage versetzt, den Überblick und damit auch die Kontrolle über die Verarbeitung ihrer personenbezogenen Daten zu erhalten.

Die Inanspruchnahme des Auskunftsrechts ist grundsätzlich kostenlos. Der Verantwortliche muss der betroffenen Person die Informationen unverzüglich, in jedem Fall jedoch innerhalb eines Monats nach Eingang des Antrags zur Verfügung stellen. Die Frist kann im Ausnahmefall um weitere zwei Monate verlängert werden. Im Falle, dass der Verantwortliche auf den Antrag der betroffenen Person hin nicht tätig wird, muss er die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags, über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen, informieren. Insbesondere dieser Zeitdruck führt häufig zu Problemen. Das Zusammentragen der Daten sowohl aus elektronischen als auch aus manuellen Ablagesystemen kann sich für die Behörden sehr aufwendig gestalten. Zwar kann bei der betroffenen Person nachgefragt werden, in welchen Systemen sie eine Datenverarbeitung vermutet, besteht die betroffene Person aber ausdrücklich auf umfassende Auskunft, muss entsprechend recherchiert werden. Nicht selten führt dies dazu, dass die Auskunft nicht oder verspätet erteilt wird. Falls eine Auskunft jedoch verspätet erteilt oder etwa ohne Angabe von Gründen abgelehnt wird, ist das bereits als Datenschutzverstoß zu bewerten. Daher sind wir in den meisten Fällen verpflichtet, umgehend Maßnahmen zu ergreifen, damit dieser Verstoß abgestellt wird. In der Regel hören wir den Verantwortlichen an, bevor wir eine Maßnahme erlassen, die diesen verpflichtet, die Auskunft zu erteilen. Häufig wird dann in der Anhörung vorgetragen, der Auskunftsanspruch sei rechtsmissbräuchlich. Häufig ist dies jedoch nicht der Fall. Allein die Tatsache, dass die betroffene Person nicht primär die datenschutzrechtliche Überprüfung ihrer Daten verfolgt, macht den Auskunftsanspruch beispielsweise nicht rechtsmissbräuchlich. Zudem muss der Verantwortliche auch darlegen und nachweisen, woraus sich ein exzessives oder rechtsmissbräuchliches Verhalten ergibt.

Zugegeben, Auskunftsersuchen der betroffenen Person sind aufwendig. Hierbei können nur standardisierte Prozesse helfen. Wir empfehlen daher den Behördenleitungen dringend, verbindliche Verfahrensabläufe zu beschreiben und Zuständigkeiten für die Bearbeitung der Auskunftsersuchen nach Artikel 12 und 15 DS-GVO zu benennen. Hierzu sollten alle Behördenmitarbeiter/-innen regelmäßig in den Datenschutzschulungen auf diesen Rechtsanspruch der Bürger/-innen hingewiesen und mit den Prozessabläufen vertraut gemacht werden.

9. Innere Sicherheit

Im Berichtszeitraum wurde sowohl eine Prüfung bei der Landespolizei MV als auch beim Verfassungsschutz MV durchgeführt. Einerseits wurde die Kontrolle der gesetzlich vorgeschriebenen turnusmäßigen Prüfungen von eingriffsintensiven und verdeckten Maßnahmen der Polizei im Bereich der Gefahrenabwehr fortgeführt (siehe Punkt 9.1). Andererseits erfolgte beim Verfassungsschutz MV eine Prüfung der Antiterrordatei sowie der Rechtsextremismus-Datei (siehe Punkt 9.2).

Im Berichtszeitraum gingen beim LfDI MV nur wenige Beschwerden gegen die Landespolizei ein. Während Beschwerden in vorherigen Berichtszeiträumen häufig im Zusammenhang mit Auskunftsersuchen eingereicht worden sind, war gerade in dieser Hinsicht ein Rückgang der Anzahl der Beschwerden zu verzeichnen. Problematisch erwiesen sich jedoch Beschwerden gegen den Verfassungsschutz MV, da nach derzeitiger Rechtslage weder die Datenschutzaufsicht durch unsere Behörde über den Verfassungsschutz MV noch ein Beschwerderecht betroffener Personen in Bezug auf die Verarbeitungstätigkeiten durch den Verfassungsschutz MV hinreichend geregelt sind. In Anbetracht dieses rechtsstaatlich bedenklichen Zustandes sowie der ausstehenden Umsetzung von Vorgaben des Bundesverfassungsgerichts (BVerfG) aus der Rechtsprechung der letzten Jahre besteht ein dringender Novellierungsbedarf des Landesverfassungsschutzgesetzes (siehe Punkt 9.4).

Im Rahmen der umfassenden Änderung des Sicherheits- und Ordnungsgesetzes (SOG M-V) in der Novelle 2019/2020 wurde durch den Landesgesetzgeber beschlossen, dass die Landesregierung eine Evaluierung der Änderungen durchführt. Diese Evaluierung wurde im Berichtszeitraum – auch unter Beteiligung des LfDI MV – durchgeführt (siehe Punkt 9.3).
Darüber hinaus wurden im Berichtszeitraum durch die Landespolizei gesetzlich vorgeschriebene Beteiligungsverfahren durchgeführt (siehe Punkt 9.5). Insgesamt war eine gute und kooperative Zusammenarbeit zwischen der Landespolizei MV und dem LfDI MV zu verzeichnen.

9.1 Prüfung eingriffsintensiver und verdeckter Maßnahmen der Landespolizei

Bereits im letzten Tätigkeitsbericht[35] wurde darüber berichtet, dass eine Prüfung eingriffsintensiver und verdeckter Maßnahmen der Landespolizei MV im Bereich der Gefahrenabwehr durch den LfDI MV aufgenommen wurde.

Die Pflicht des LfDI MV zur Prüfung bestimmter polizeilicher Maßnahmen und Datenübermittlungen im Bereich der Gefahrenabwehr ergibt sich aus § 48b Absatz 6 SOG M-V. Diese Norm wurde zur Umsetzung der Vorgaben des BVerfG aufgenommen. Mit dem wegweisenden sog. BKAG-Urteil[36] hat das höchste deutsche Gericht die verfassungsrechtlichen Anforderungen an die Ausgestaltung eingriffsintensiver Befugnisse aus zahlreichen vorangehenden Entscheidungen weiterentwickelt und präzisiert. Dies betraf auch flankierende rechtsstaatliche Absicherungen, insbesondere zum Schutz des Kernbereichs privater Lebensgestaltung oder zur Gewährleistung von Transparenz, den individuellen Rechtsschutz und die aufsichtliche Kontrolle.

Da bei verdeckten Maßnahmen der Sicherheitsbehörden eine Transparenz der Datenerhebung und -verarbeitung sowie die Ermöglichung des individuellen Rechtsschutzes kaum sichergestellt werden können, kommt den Aufsichtsbehörden eine Kompensationsfunktion zu. So wurde durch das BVerfG die Vorgabe getroffen, dass Kontrollen verdeckter Maßnahmen durch die Aufsichtsbehörden in angemessenen Abständen – höchstens etwa zwei Jahren – gesetzlich vorzusehen sind.

---

[35] Vgl. Punkt 9.1 in 19. Tätigkeitsbericht; URL: https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Taetigkeitsberichte/lfdmvtb18-19.pdf [abgerufen am 27.02.2024].

[36] Bundeskriminalamt-Gesetz (BKAG): BKAG-Urteil; BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09.

Entsprechend wurde eine Kontrollpflicht des LfDI MV in § 48b Absatz 6 SOG M-V vorgesehen. Hiernach muss der LfDI MV die in § 46f Absatz 2 SOG M-V genannten Maßnahmen der Polizei sowie Datenübermittlungen an Drittstaaten und weitere zwischen- sowie überstaatliche Stellen im Abstand von längstens zwei Jahren zumindest stichprobenartig kontrollieren.

In Anbetracht der Regelungskompetenz des Landesgesetzgebers sind die nach § 48b Absatz 6 SOG M-V zu kontrollierenden polizeilichen Maßnahmen und Datenübermittlungen ausschließlich im Bereich der Gefahrenabwehr zu verorten. Insoweit handelt es sich um Maßnahmen, die es zum Ziel haben, von der Allgemeinheit oder dem Einzelnen Gefahren abzuwehren, durch die die öffentliche Sicherheit oder Ordnung bedroht wird. Dabei ist das Spektrum möglicher Szenarien breit gefächert: Es reicht von vermissten Personen bis hin zu terroristischen Aktivitäten. Die für die Gefahrenabwehr durch den Landesgesetzgeber im SOG M-V vorgesehenen Maßnahmen sind auch vielgestaltig. Sie umfassen beispielhaft den Einsatz von Vertrauenspersonen oder verdeckt Ermittelnden, die Telekommunikationsüberwachung, den verdeckten Einsatz technischer Mittel, insbesondere solcher zur Bild- und Tonaufnahme/-aufzeichnung, die sog. Online-Durchsuchung, die Rasterfahndung und den Einsatz technischer Mittel zur Wohnraumüberwachung.

Anhand dieser nur beispielhaft genannten verdeckten Maßnahmen ist offenkundig, dass diese besonders eingriffsintensiv sind, weil sie geeignet sind, um weit in die Grundrechte der betroffenen Personen einzugreifen bzw. in geschützte Lebensbereiche einzudringen. Dies gilt umso mehr angesichts der verdeckten Durchführung dieser Maßnahmen, sodass die hiervon betroffenen Personen währenddessen keine Kenntnis haben. Dementsprechend ist eine Kontrolle der Durchführung dieser Maßnahmen wichtig.

Der Prüfungsumfang seitens des LfDI MV bezieht sich vor allem darauf, wie Maßnahmen durchgeführt worden sind bzw. ob diese in Art, Dauer und Umfang im Einklang mit den jeweiligen Rechtsgrundlagen bzw. Anordnungen stehen. Darüber hinaus wird, soweit personenbezogene Daten des Kernbereichs privater Lebensgestaltung im Wege der Maßnahmen betroffen sind, die Einhaltung der Vorgaben hierzu geprüft. Daneben erfolgt ebenso im Falle der Betroffenheit von Dritten die Prüfung der Einhaltung weiterer Vorgaben sowie auch die nachträgliche Benachrichtigung betroffener Personen. Die meisten eingriffsintensiven Maßnahmen unterliegen einem Richtervorbehalt, sodass diese einer richterlichen Anordnung bedürfen. In diesen Fällen ist es aufgrund der justiziellen Unabhängigkeit ausgeschlossen, dass durch den LfDI MV die richterliche Entscheidung über das Vorliegen der Tatbestandsvoraussetzungen einer Maßnahme geprüft wird. Bei richterlich angeordneten Maßnahmen wird jedoch durchaus geprüft, ob die Maßnahmen im Umfang der Anordnung durchgeführt worden sind. In allen übrigen Fällen, die keiner richterlichen Anordnung bedürfen, wird seitens des LfDI MV selbstredend zudem geprüft, ob die jeweiligen Tatbestandsvoraussetzungen für die Anordnung dieser Maßnahmen vorlagen.

Die Kontrolle dieser Maßnahmen und Datenübermittlungen ist nach § 48b Absatz 6 SOG M-V zumindest stichprobenartig vorgesehen worden. Insoweit wurde durch den LfDI MV zunächst eine repräsentative Stichprobe aller kontrollpflichtigen Maßnahmen und Datenübermittlungen erhoben. Nach Auswahl der Stichproben wurde daraufhin die Prüfung der einzelnen Maßnahmen aufgenommen. Die Prüfung konnte nunmehr nahezu vollständig abgeschlossen werden. Bei den bisher durchgeführten Kontrollen wurden bislang keine datenschutzrechtswidrigen Verstöße festgestellt.

Ein abschließendes Ergebnis liegt jedoch noch nicht vor, da zu einzelnen Maßnahmen bisher noch die Bereitstellung von Informationen seitens der Landespolizei MV aussteht. Die Bereitstellung dieser Informationen wird zeitnah erwartet, sodass im nächsten Tätigkeitsbericht über die abschließenden Ergebnisse aus der andauernden Prüfung und dem darauffolgenden Prüfturnus berichtet werden kann.

Im Zuge der erstmaligen Aufnahme dieser Kontrollen war vor allem festzustellen, dass für die Durchführung gemeinsam mit der Landespolizei MV ein Verfahren etabliert werden muss. Hierzu stehen wir bereits in Abstimmung mit der Landesregierung.

9.2 Prüfung der Antiterror- und Rechtsextremismus-Datei

Der LfDI MV führte im Berichtszeitraum eine Prüfung der Antiterrordatei (ATD) und Rechtsextremismus-Datei (RED) beim Verfassungsschutz MV durch.

Bei der ATD und RED handelt es sich um sog. Verbunddateien, die von verschiedenen Sicherheitsbehörden des Bundes, der Landeskriminalämter sowie der Verfassungsschutzbehörden der Länder gemeinsam beim Bundeskriminalamt geführt werden. In den Dateien werden Erkenntnisse dieser Sicherheitsbehörden zentral zusammengeführt, um sie bundesweit zu gesetzlich vorgegebenen Zwecken nutzen zu können. Dabei dient die ATD dem Zweck der Aufklärung und Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland (§ 1 Absatz 1 des Antiterrordateigesetzes [ATDG]); die RED wurde zum Zweck der Aufklärung und Bekämpfung des gewaltbezogenen Rechtsextremismus, insbesondere zur Verhinderung und Verfolgung von Straftaten mit derartigem Hintergrund, errichtet (§ 1 Absatz 1 des Rechtsextremismus-Datei-Gesetzes [RED-G]). In den Dateien werden vor allem Informationen zu Ziel- und Randpersonen (z. B. Kontaktpersonen, Unterstützer), aber auch zu Vereinigungen/Gruppierungen aus dem Bereich des internationalen Terrorismus und des gewaltbezogenen Rechtsextremismus gespeichert. Beide Dateien sollen insbesondere die Zusammenarbeit zwischen den Nachrichtendiensten und den Polizeibehörden in Bund und Ländern verbessern.

Da eine Transparenz der Datenverarbeitung und die Ermöglichung individuellen Rechtsschutzes der in diesen Dateien gespeicherten Personen nur sehr eingeschränkt sichergestellt werden können, entschied das BVerfG, dass zur Kompensation einer aufsichtsbehördlichen Kontrolle in Form von turnusmäßigen Prüfungen in angemessenen Abständen eine umso größere Bedeutung zukommt[37]. Denn im Gegensatz zum klassischen Verwaltungshandeln finden Datenverarbeitungen im Rahmen der ATD und RED außerhalb jeder unmittelbaren Wahrnehmbarkeit statt. Sie erfolgen ohne Wissen der betroffenen Personen und können daher nur schwerlich gerichtlich überprüft werden. Durch den Bundesgesetzgeber wurden daher als Kompensationsmaßnahmen Pflichtprüfungen der Datenbestände in der ATD und RED durch die Datenschutzaufsichtsbehörden in regelmäßigen Abständen vorgesehen (§ 10 Absatz 2 ATDG; § 11 Absatz 2 RED-G). Dieser Verpflichtung kommt der LfDI MV mit seiner Prüfung beim Verfassungsschutz MV nach.

[37] BVerfG, Urt. v. 24.4.2013 – Az. 1 BVR 1215/07, Rn. 215 ff.

Der Gegenstand der Prüfung waren in der ATD und RED gespeicherte Daten, für die der Verfassungsschutz MV die datenschutzrechtliche Verantwortung trägt. Das sind Daten, die durch den Verfassungsschutz MV in die Verbunddateien eingegeben worden sind (§ 8 Absatz 1 ATDG; § 9 Absatz 1 RED-G). Dabei erstreckte sich die Prüfung konkret auf Personendatensätze sowie TOM.

Durch den Verfassungsschutz MV wurden dem LfDI MV die für die Prüfung erforderlichen Informationen bereitgestellt. Zu den jeweiligen geprüften Personendatensätzen wurden zudem die Voraussetzungen für deren Speicherung dargelegt und erläutert. Sowohl die geprüften TOM als auch die geprüften Personendatensätze waren datenschutzrechtlich nicht zu beanstanden. In keinem Fall konnte eine nicht nachvollziehbare oder unrechtmäßige Datenverarbeitung festgestellt werden. Für alle geprüften Personendatensätze lagen die jeweiligen gesetzlichen Vorgaben für eine Speicherung in den Dateien vor. Insgesamt konnten im Rahmen der Prüfung keine Mängel festgestellt werden. Vertiefte Ausführungen zu den Prüfungen und damit dem Inhalt der Dateien sind aufgrund des Geheimhaltungsgrades nicht möglich.

Unbenommen des positiven Prüfergebnisses kommt der LfDI MV jedoch – wie andere Datenschutzaufsichtsbehörden[38] – zu dem Schluss, dass die ATD und RED im Gegensatz zu anderen Kommunikationswegen der Sicherheitsbehörden nur einen vergleichsweise geringen Nutzen aufweisen dürften.

9.3 Evaluierung des Sicherheits- und Ordnungsgesetzes

Das SOG M-V wurde mit der Novellierung in den Jahren 2019/2020[39] umfassend geändert. Anlass dazu war einerseits eine Umsetzung unionsrechtlicher Vorgaben[40] im Rahmen der europaweiten Harmonisierung des Datenschutzrechts sowie eine Anpassung an die Rechtsprechung des BVerfG[41], andererseits erfolgte im Bereich der Gefahrenabwehr eine weitreichende Ausweitung von Befugnissen. Somit wurden bestehende Normen für einzelne Befugnisse mitunter angepasst, aber auch gesetzliche Regelungen über Befugnisse im Rahmen der Novelle neu aufgenommen. Dies betrifft beispielhaft Befugnisse wie die Online-Durchsuchung, die Quellen-Telekommunikationsüberwachung und die Ausschreibung zur gezielten Kontrolle.

In Anbetracht der umfassenden Änderungen des SOG M-V, die insbesondere auch Befugnisse mit weitreichenden Grundrechtseingriffen betreffen, wurde folgerichtig durch den Gesetzgebenden beschlossen, die Landesregierung zu einer Evaluierung der mit der Novelle vorgenommenen Änderungen zu verpflichten. In § 116 SOG M-V wurde folglich die Regelung aufgenommen, dass die Landesregierung dem Landtag bis zum 31. Dezember 2024 über die erzielten Wirkungen der Änderungen des SOG M-V aus der Novelle 2019/2020 berichtet.

---

38 Vgl. Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, 31. TB (2022), S. 94; 30. TB (2021), S. 85; 27. TB (2017/18), S. 78; vgl. auch Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, 32. TB (2023) S. 22; 31. TB (2022), S. 33; 29. TB (2020), S. 61.

39 Vgl. Landtag MV, Drucksache 7/3694.

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

41 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09; BKAG I.

Aufgrund dieser Verpflichtung wurde durch das Ministerium für Inneres, Bau und Digitalisierung MV eine Evaluierung durchgeführt, über deren Ergebnis auch der Landtag MV unterrichtet wurde.[42] Positiv hervorzuheben ist, dass in diesem Rahmen für Rechtsanwendende die Möglichkeit bestand, sich zu bestehenden Normen zu äußern und Änderungsbedarfe zu artikulieren. Neben der schriftlichen Gelegenheit zur Stellungnahme wurde durch das MIBD MV auch ein Symposium veranstaltet, das einem weiten Kreis von Rechtsanwendenden die Möglichkeit bot, sich zur Weiterentwicklung des SOG M-V auszutauschen und gemeinsam gesetzgeberische Handlungsnotwendigkeiten zu diskutieren. Hierbei kamen Vertreter/-innen aus der Wissenschaft, dem Hilfesystem zum Schutz von Frauen vor Gewalt, der Politik sowie den Polizei- und Ordnungsbehörden, Rechtsvertreter/-innen sowie der LfDI MV zu Wort. Zu bedauern bleibt, dass viele grundsätzliche Bedenken hinsichtlich der Bewertung der Änderungsbedarfe dann doch nicht in den Evaluierungsbericht eingeflossen sind. Dies betrifft insbesondere die Streichung von „Kettenverweisen“, die die Einhaltung verfassungsrechtlicher Vorgaben erschweren. Zudem muss die Verständlichkeit der Normen sowohl für Rechtsanwendende als auch für Bürger/-innen gewährleistet sein. Weiterhin wurden auch Bedenken hinsichtlich der Vereinbarkeit mit dem Unionsrecht, insbesondere in Bezug auf §§ 25, 48 SOG M-V, nicht aufgenommen.

Mit der Evaluierung bestand die Chance, das SOG M-V insgesamt auf den Prüfstand zu stellen. Mindestens aber war die Evaluationspflicht aus § 116 SOG M-V entsprechend dem Willen des Gesetzgebenden zu erfüllen, indem eine Evaluierung aller aus der Novelle 2019/2020 erzielten Wirkungen erfolgt. Es erscheint fraglich, ob der formulierte Evaluierungsgegenstand, der sich auf die neu aufgenommenen Befugnisse beschränken soll, dem gesetzlichen Auftrag nach § 116 SOG M-V entspricht. Dadurch blieben im Evaluierungsbericht wesentliche Änderungen im Zusammenhang mit der Anpassung an die DS-GVO und die Umsetzung der JI-RL unberücksichtigt.

Insoweit wird eindringlich an die Landesregierung appelliert, in einer potenziell folgenden Novelle auch Änderungsbedarfe über den Evaluierungsbericht hinaus zu berücksichtigen. In einem etwaigen Gesetzesvorhaben steht der LfDI MV gerne beratend auch in einer frühen Phase eines Entwurfes zur Verfügung.

9.4 Novellierung des Landesverfassungsschutzgesetzes

Das BVerfG stellte in drei wegweisenden Entscheidungen aus den Jahren 2022 und 2024 fest, dass einzelne Normen in verschiedenen Verfassungsschutzgesetzen verfassungswidrig und teilweise nichtig sind.[43]

Im Mittelpunkt der Entscheidungen stehen insbesondere die Anforderungen des Verhältnismäßigkeitsprinzips als Ausfluss aus dem Rechtsstaatsprinzip an die Tätigkeit der Verfassungsschutzbehörden. Anhand dieses zentralen Prüfungsmaßstabs sowie der Abwägung des Grundsatzes der streitbaren Demokratie und der individuellen Freiheitsrechte erklärt das BVerfG u. a. einzelne Regelungen im Zusammenhang mit Datenübermittlungen sowie der Ausgestaltung von nachrichtendienstlichen Befugnissen für verfassungswidrig.

---

[42] Landtag MV, Drucksache 8/4496.

[43] BVerfG, Urt. v. 26.4.2022 – 1 BvR 1619/17 (Bayerisches Verfassungsschutzgesetz),
BVerfG, Urt. v. 28.09.2022 – 1 BvR 2354/13 (Bundesverfassungsschutzgesetz),
BVerfG, Urt. v. 17.7.2024 – 1 BvR 2133/22 (Hessisches Verfassungsschutzgesetz).

Gleichwohl die betreffenden Grundsatzentscheidungen des höchsten deutschen Gerichts nicht unmittelbar zum Landesverfassungsschutzgesetz (LVerfSchG M-V) ergangen sind, gehen mit diesen für alle Verfassungsschutzgesetze in Bund und Ländern weitreichende Novellierungsbedarfe einher. Während weitgehend bereits Anpassungen der jeweiligen Verfassungsschutzgesetze erfolgten, steht eine Novellierung des LVerfSchG M-V immer noch aus. Dieser Zustand ist rechtsstaatlich überaus bedenklich. Dies wird im Weiteren dadurch verstärkt, dass nach der derzeitigen Rechtslage infolge einer ausgebliebenen Angleichung des LVerfSchG M-V an das DSG M-V noch nicht einmal die Datenschutzaufsicht über den Verfassungsschutz MV hinreichend geregelt ist.

Seitens des LfDI MV wurde zuletzt mehrfach gegenüber dem zuständigen Ressort der Landesregierung auf die datenschutzrechtlichen Änderungsbedarfe hingewiesen,[44] ohne dass im Berichtszeitraum eine Anpassung an die Vorgaben des Bundesverfassungsgerichts erfolgt ist.

Zur Wahrung der Rechtsstaatlichkeit und des Grundrechtsschutzes ist eine Anpassung des LVerfSchG M-V dringend geboten. Wir empfehlen der Landesregierung dringend, eine Gesetzesinitiative zur Änderung des LVerfSchG M-V in den Landtag einzubringen.

9.5 Beteiligungen durch die Landespolizei

Vor der Inbetriebnahme von neu anzulegenden Dateisystemen bzw. automatisierten Verfahren bestehen mitunter seitens der Polizeibehörden in bestimmten Kontexten nach § 500 der Strafprozessordnung (StPO) i. V. m. § 69 des Bundesdatenschutzgesetzes (BDSG) und § 48c Absatz 2 SOG M-V[45] Pflichten zur Vorabkonsultation mit dem LfDI MV. Die Pflicht zur vorherigen Anhörung tritt einerseits ein, wenn aus einer vorherigen Datenschutz-Folgenabschätzung hervorgeht, dass eine beabsichtigte Verarbeitung ein hohes Risiko für die Rechtsgüter betroffener Personen zur Folge hätte, wenn die verantwortliche Stelle keine Abhilfemaßnahmen treffen würde.

Andererseits besteht eine Beteiligungspflicht, wenn die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, Mechanismen oder Verfahren, ein hohes Risiko für die Rechtsgüter betroffener Personen zur Folge hat. Darüber hinaus sind weitere Unterrichtungs- und Beteiligungspflichten spezifisch geregelt. Der Zweck dieser Beteiligungspflichten besteht darin, dass Dateisysteme/Verfahren, in denen beabsichtigte Verarbeitungen von personenbezogenen Daten mit einem erhöhten Gefährdungspotenzial einhergehen, bereits im Vorfeld durch den LfDI MV geprüft werden können. Damit soll vor allem eine frühzeitige Einbindung der Aufsichtsbehörde geschaffen werden, damit diese präventiv tätig werden kann.

[44] Siehe beispielhaft Punkt 9.5 in 19. Tätigkeitsbericht; URL: https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Taetigkeitsberichte/lfdmvtb18-19.pdf [abgerufen am 27.02.2024].

[45] In Umsetzung von Artikel 28 JI-RL.

Im Berichtszeitraum wurden Beteiligungen des LfDI MV durch die Landespolizei im Rahmen der vorbenannten Pflichten durchgeführt. Unsere Behörde brachte sich in diesen Zusammenhängen vor allem beratend ein. Die Zusammenarbeit verbessert sich hier stetig.

Um dem Zweck der Konsultationspflichten gerecht zu werden, müssen die entsprechenden Beteiligungen tatsächlich auch vor der Inbetriebnahme von Verfahren erfolgen. Die Inbetriebnahme kennzeichnet in diesem Zusammenhang den Zeitpunkt der erstmaligen Verarbeitung von personenbezogenen Daten realer Personen (Echtdaten, nicht Testdaten) in neuen automatisierten Verfahren/Dateisystemen. Somit muss auch im Rahmen von Pilotphasen einzelner Verfahren bereits eine Beteiligung im Vorfeld stattfinden, wenn die Verarbeitung von Echtdaten beabsichtigt ist. Vor diesem Hintergrund waren vereinzelt Beteiligungen zu bereits bestehenden Verfahren nachzuholen. Gerade in Bezug auf jüngere bekannte Verfahren ist jedoch eine frühzeitige Einbindung des LfDI MV zu verzeichnen.

Bei Projekten zu Verfahren wurde mitunter der Eindruck erweckt, dass zwar Regelungen des Datenschutzes berücksichtigt wurden, ihre Einhaltung aber nicht durchgängig bereits bei Beginn bzw. der Planung eines Projektes gewährleistet war. Der LfDI MV rät in diesem Zusammenhang den initiierenden Polizeibehörden, das Datenschutzmanagement bei allen Projekten bereits in der Planungs-/Beauftragungsphase – insbesondere hinsichtlich personeller und materieller Kapazitäten – zu berücksichtigen. Hierbei ist nochmals zu betonen, dass das Datenschutzmanagement auch nicht der gesetzlichen Aufgabe der bDSB der Polizeibehörden entspricht. Gleichwohl die Tätigkeit der bDSB der Polizeibehörden überaus positiv hervorzuheben ist, müssen die Dienststellen gewährleisten, dass diese ihren gesetzlichen Aufgaben, primär der Kontrolle und Beratung, ohne Interessenkonflikte nachkommen können. In analoger Anwendung der §§ 48e ff. SOG M-V wird auf den Beitrag im vergangenen Tätigkeitsbericht hinsichtlich der Stellung und Aufgaben von bDSB hingewiesen.[46]

10. Vereine, Parteien und Beschäftigtendatenschutz

Kurz und knapp berichten wir in diesem Kapitel zum Thema Wahlwerbung der Parteien, die übrigens als Vereine eingetragen und daher in diesem Kapitel zu finden sind. Der Fall eines Vereins, der es mit der sicheren Aufbewahrung von Beschäftigtendaten nicht ganz so genau nahm, soll als mahnendes Beispiel dienen und wird vorliegend geschildert. Bei Beschäftigtendaten haben wir zur Verarbeitung von Personalnummern bei den Entgeltverhandlungen zwischen Kommunen und Leistungserbringern beraten – unsere Empfehlungen teilen wir im letzten Unterkapitel mit.

[46] Vgl. Punkt 8.6 in 19. Tätigkeitsbericht; URL: https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Taetigkeitsberichte/lfdmvtb18-19.pdf [abgerufen am 27.02.2025].

10.1 Ungesicherte Aufbewahrung von Personaldaten – Verwarnung eines Vereins

Im Berichtszeitraum erhielt der LfDI MV die Beschwerde einer betroffenen Person gegen ihren ehemaligen Arbeitgeber, einen gemeinnützigen Verein. Der Verein soll Personaldaten der ehemaligen Minijobberin an die Rechtsanwältin ihres leiblichen Vaters weitergegeben haben, welche in einem Sorgerechtstreit die Einkommens- und Lebensverhältnisse der Tochter aus dem Personalfragebogen zitierte. Weiterhin wurde die ehemalige Vorgesetzte als Zeugin benannt. Mit den Vorwürfen konfrontiert, wies der Verein zunächst jede Verantwortung von sich.

Die Beschwerdeführerin konnte darlegen, dass sie zum Zeitpunkt der Weitergabe ihres Personalfragebogens längst nicht mehr bei dem Verein beschäftigt gewesen war und keine Verbindung zwischen dem Verein und dem leiblichen Vater bestanden hatte. Als der ehemalige Arbeitgeber mit Auszügen aus den Gerichtsakten konfrontiert wurde, die auf den Personalfragebogen und die Vorgesetzte Bezug nehmen, wurden dann doch weitere Nachforschungen angestellt. Die neue Ehefrau des leiblichen Vaters wurde als Zeugin herangezogen – demnach habe sie bei einem Besuch im Verein unter dem Vorwand, zur Toilette zu gehen, die Personalunterlagen der Beschwerdeführerin offen einsehbar herumliegen sehen und unbemerkt kopiert, um dem bösartigen Treiben der Tochter im Unterhaltsstreit mit ihrem Partner ein Ende zu setzen. Sie bezeugte zudem, dass der Verein und die Vorgesetzte niemals gegen den Datenschutz verstoßen würden. Die Beschwerdeführerin und der LfDI MV hatten Zweifel an dieser Darstellung der Ereignisse, zumal lange nach dem Ende der geringfügigen Beschäftigung kein Grund dafür bestand, die Personalunterlagen zu bearbeiten. Darüber hinaus lebten der Vater und seine neue Partnerin in einem anderen Teil Deutschlands, ein zufälliger Besuch bei einem Verein in MV schien also unwahrscheinlich. Selbst wenn jedoch davon ausgegangen wird, dass die Schilderung des Beschwerdegegners zutrifft, muss der Verein die datenschutzrechtlichen Anforderungen erfüllen. Z. B. muss auch der Verein angemessene technische und organisatorische Maßnahmen zum Schutz von Beschäftigtendaten gemäß Artikel 32 DS-GVO ergreifen. Bei der Offenlegung des Personalfragebogens ehemaliger Beschäftigter mit der Möglichkeit zur Einsicht und Erstellung einer Kopie auf dem Weg zur Toilette kann von solchen Schutzmaßnahmen jedoch keine Rede sein. Unter Berücksichtigung der Umstände des Vereins und der Schäden, die durch die unrechtmäßige Offenlegung der Beschäftigtendaten entstanden sind, hat der LfDI MV erstmals eine Verwarnung gegen einen Verein erlassen. Von einem Bußgeldverfahren wurde vorliegend abgesehen. Das Klageverfahren des Vereins gegen den LfDI MV ist noch anhängig.

10.2 Datenschutz und Wahlen – wie gelangen Parteien an meine Adresse?

Vor anstehenden Wahlen finden viele Bürger/-innen persönliche Wahlwerbung politischer Parteien in ihren Briefkästen. So erhalten wir immer wieder Anfragen von Betroffenen, die sich nicht erklären konnten, wie Parteien an ihre Adresse gelangt waren, und danach fragten, ob dies erlaubt sei.

Aufgrund ihrer besonderen Bedeutung im demokratischen System und für die politische Meinungsbildung dürfen Parteien unter bestimmten Voraussetzungen Adressdaten aus dem Melderegister abfragen. Diese Sonderregelung ist in § 50 Absatz 1 des Bundesmeldegesetzes (BMG) zu finden. Danach dürfen die Meldebehörden im Zusammenhang mit Wahlen oder Abstimmungen auf Bundes-, Landes- oder Kommunalebene zeitlich begrenzt auf sechs Monate vor der Wahl Adressdaten von Wahlberechtigten an Parteien, Wählergruppen und andere Träger von Wahlvorschlägen weitergeben. Die Weitergabe der Daten ist auf Vor- und Nachname, eventuell einen Doktorgrad und die aktuelle Anschrift beschränkt. Zudem müssen Parteien eine konkrete Altersgruppe benennen, die sie ansprechen möchten, beispielsweise Erstwähler/-innen oder Seniorinnen und Senioren ab 65 Jahren. Die Parteien dürfen die erhaltenen Daten ausschließlich für Wahlwerbung nutzen. Eine Speicherung in eigenen Adressdatenbanken oder eine Weitergabe an Dritte ist unzulässig. Die Daten müssen spätestens einen Monat nach der Wahl gelöscht werden. Jede Bürgerin und jeder Bürger hat jedoch das Recht, der Weitergabe der Meldedaten zu widersprechen. Der Widerspruch ist formlos, kostenlos und dauerhaft gültig. Eine Begründung ist nicht erforderlich. Hierzu sollten als Hilfestellung die digitalen Formulare der Kommunen auf ihren Webseiten genutzt werden. Bei der Anmeldung eines Wohnsitzes müssen die Meldebehörden über das Widerspruchsrecht informieren.

10.3 Der ewige Streit um Personalnummern – was bei Entgeltverhandlungen zwischen Kommunen und Leistungserbringern wirklich hilft

Auch in diesem Berichtszeitraum war der LfDI MV erneut mit einer schon länger heiß diskutierten Frage befasst: Dürfen Kommunen, wenn sie mit Leistungserbringern über zukünftige Verträge verhandeln, vorab bereits Personalnummern der Leistungserbringer verarbeiten?

Hinter dieser sehr abstrakt klingenden Frage verbirgt sich Folgendes: Das SGB IX enthält Regelungen, wie Menschen mit Behinderung oder von Behinderung bedrohte Menschen am Leben teilhaben können. Der Staat, genauer die Kommunen, soll Leistungen zur Teilhabe erbringen. Als Leistungserbringer kommen dabei nicht nur die Kommunen selbst in Betracht, sondern auch freie Träger und andere Einrichtungen, die dann von den Kommunen beauftragt werden. Für solche Verträge enthält das SGB klare Regelungen. Eigentlich. Denn immer wieder ist umstritten, ob die Leistungserbringer bereits vor dem Vertragsschluss während der noch laufenden Verhandlungen anhand von Personalnummern nachweisen müssen, dass sie tatsächlich die ausgeschriebene Leistung mit dem erforderlichen Personal erbringen können. Die Kommunen wünschen sich dies – einige Leistungserbringer haben aber datenschutzrechtliche Bedenken.

Richtig kompliziert wurde die Situation für einen kirchlichen Leistungserbringer. Für diesen war gar nicht der LfDI MV die zuständige Datenschutzaufsichtsbehörde. Denn Kirchen können unter bestimmten, in der DS-GVO festgelegten Bedingungen eigenes Datenschutzrecht ausführen und eigene Datenschutzbeauftragte, sogenannte spezifische Datenschutzaufsichtsbehörden, benennen. Natürlich ähneln diese Datenschutzvorschriften stark der DS-GVO. Die für den Leistungserbringer zuständige spezifische Datenschutzaufsichtsbehörde hatte dem Leistungserbringer untersagt, die Personalnummern, die eine Kommune in den Vertragsverhandlungen vorgelegt haben wollte, zu übermitteln. Hierbei handele es sich um Beschäftigtendaten, für deren Übermittlung es keine Rechtsgrundlage gebe, jedenfalls sei die Übermittlung nicht erforderlich.

Nun saß der Leistungserbringer zwischen den Stühlen: Entweder übermittelte er die Daten und riskierte ein Bußgeld von seiner spezifischen Aufsichtsbehörde oder er übermittelte nicht und verlöre möglicherweise den Auftrag.

In dieser misslichen Lage wandte sich der Leistungserbringer an den LfDI MV als zuständige Aufsichtsbehörde für die Kommune. Denn wenn der Leistungserbringer keine Rechtsgrundlage für die Übermittlung hätte, glaubte er, dürfte die Kommune die Daten wahrscheinlich auch gar nicht erheben. Zu diesem Ergebnis gelangten wir nach einer ersten Prüfung auch und warnten die Kommune zunächst vor der Datenerhebung. Das SGB IX regelt klar, wann und wie in der vertraglichen Beziehung zwischen Leistungserbringer und Kommune personenbezogene Daten der Leistungserbringer verarbeitet werden dürfen: Nach Vertragsschluss, wenn die Kommune den Leistungserbringer prüft. Da die Kommune trotz Warnung weiterhin auf die Übermittlung der Personalnummern bestand, hörte der LfDI MV die Kommune vor Erlass eines Verwaltungsaktes, mit dem die Erhebung verboten werden sollte, an.

Da auch andere Kommunen gern weiterhin die Personalnummern erheben wollten, wurde eine Vereinbarung zwischen den Kommunen und den Leistungserbringern angepasst und die Personalnummern als notwendige Anlage für die Vertragsverhandlungen deklariert. Daraufhin sah der LfDI MV zunächst von dem Erlass der Maßnahme gegen eine einzelne Kommune ab und wandte sich stattdessen an das zuständige Ministerium für Soziales, Gesundheit und Sport des Landes Mecklenburg-Vorpommern, um das Problem grundlegend zu lösen.

In diesem Gespräch wurde schnell klar, warum die Kommunen glaubten, die Personalnummern zu benötigen. Häufig schließen die Leistungserbringer mit den Kommunen mehrere Verträge zur Leistungserbringung ab. Dabei muss aber sichergestellt sein, dass das benötigte Personal auch tatsächlich mit dem Stundenanteil für das jeweilige Projekt eingesetzt wird, wie in den Verhandlungen angegeben. Ein doppelter oder gar mehrfacher Einsatz derselben Arbeitskraft in verschiedenen Projekten muss vermieden werden. Daher wollten die Kommunen anhand der Personalnummern feststellen, bei welchen Verträgen dieses Personal noch eingesetzt würde. Diese Kontrolle sollte einerseits das Personal schützen und andererseits die Qualität der erbrachten Leistung gewährleisten – auch für den LfDI MV ein nachvollziehbares Argument. Doch stellte sich die Frage, ob Personalnummern tatsächlich geeignet sind, diesen Nachweis zu erbringen. Personalnummern sind in Deutschland ein Datum, das regelmäßig nur einer einzigen Person zugeordnet werden kann. Diese Person muss bei den Vertragsverhandlungen noch nicht beim Leistungserbringer angestellt sein, könnte während oder nach den Verhandlungen kündigen, in Elternzeit gehen oder vieles mehr. Arbeitgeber/-innen können nicht garantieren, dass die Person mit der Personalnummer, die in den Verhandlungen angegeben wird, auch tatsächlich dann die vertraglich geschuldete Leistung erbringt. Was sie aber zusagen können, ist das Vorhalten einer Stelle mit einer bestimmten Stundenzahl bzw. eine Stelle zu schaffen, die mit einem vereinbarten Stellenanteil festgelegte Tätigkeiten erbringt. Diese Informationen sind in Stellenbeschreibungen und Stellenbewertungen enthalten. Und diese Dokumente sind zunächst abstrakt. Natürlich können sie auch einer natürlichen Person zugeordnet sein, wenn die Stelle besetzt ist. Sie sind, anders als die Personalnummer, aber nicht fest einer natürlichen Person, sondern einer Stelle zugeordnet. Diese kann im Lauf der Zeit mit unterschiedlichen Personen besetzt werden.

Der LfDI MV empfiehlt daher den Kommunen, statt der Personalnummer die Stellenbeschreibungen und Bewertungen zu den vereinbarten Stellen anzufordern – natürlich ohne den Namen oder die Personalnummern der Beschäftigten, sollten die Stellen schon besetzt sein.

Aufmerksamen Leser/-innen wird ein kleiner Wertungswiderspruch nicht entgangen sein: Mit dieser Empfehlung werden letztlich pseudonymisierte Daten übermittelt, wenn die Stellen gerade besetzt sind. Die Stellennummer stellt hierbei eine Art Schlüssel dar, mit dem der Leistungserbringer – nicht aber die Kommune – die jeweilige Stelle einer natürlichen Person zuordnen kann. Tatsächlich lässt sich das jedoch bei den Verhandlungen kaum vermeiden. Wir haben daher auch angeregt, dass sich das zuständige Ministerium für Soziales, Gesundheit und Sport des Landes Mecklenburg-Vorpommern auf Bundesebene für eine klarstellende Regelung im SGB IX einsetzt.

11. Bußgeldstelle und Justiziariat

Das Beschwerderecht und dessen gerichtliche Überprüfbarkeit zählen zu den wichtigsten Errungenschaften der DS-GVO. Betroffene Personen sind nicht bloße Objekte einer Datenverarbeitung, sondern können sich aktiv zur Wehr setzen. Allerdings häufen sich die Fälle, in denen das Beschwerderecht missbraucht wird, um Verwaltungen oder Unternehmen lahmzulegen und einfach nur immensen Aufwand bei diesen Stellen zu erzeugen. Im Berichtszeitraum sind wichtige Entscheidungen dazu ergangen, wann eine Beschwerde nicht mehr bearbeitet werden muss, weil sie als rechtsmissbräuchlich einzustufen ist. Darüber hinaus konnten wir zunehmend Bußgeldverfahren zum Abschluss bringen.

11.1 Entscheidung des Verwaltungsgerichts Schwerin: Wann sind Auskunftsersuchen rechtsmissbräuchlich und exzessiv?

Nicht über jedes Auskunftsersuchen von Beschwerdeführern muss vom LfDI MV in der Sache entschieden werden. Wo die Grenze verläuft, hat das Verwaltungsgericht (VG) Schwerin in seiner Entscheidung im August 2024 umrissen. Eine Klage vor dem Verwaltungsgericht ist bereits unzulässig, wenn sie rechtsmissbräuchlich ist und ein Rechtsschutzbedürfnis fehlt. Dies ist der Fall, wenn eine schikanöse Ausnutzung des Rechtsschutzes vorliegt. Von einem solchen Missbrauch ist auszugehen, wenn die Absicht zu erkennen ist, dass die Klage nur den Sinn hat, den Beklagten oder das Gericht zu schädigen und unnötig zu belästigen.

Im zur Entscheidung vorliegenden Fall verfolgte die klagende Person einerseits das Ziel, verschiedene Behörden, die in anderen Verfahren nicht im Sinne der Beschwerdeführerin entschieden hatten, mit massenhaften Auskunftsanträgen lahmzulegen. Darüber hinaus ging es ihr darum, staatliche Behörden für von ihr als ungerecht empfundene familiengerichtliche Entscheidungen zu bestrafen und zu der erwünschten familienrechtlichen Entscheidung zu bewegen. Ein tatsächliches Interesse an der Feststellung von Datenschutzverstößen war nach Feststellung des Gerichts nicht erkennbar (VG Schwerin, 3 A 909/22SN).

Darüber hinaus ergibt sich nach Einschätzung des VG Schwerin aus Artikel 57 Absatz 4 DS-GVO, dass sich auch die Datenschutzaufsichtsbehörde bei offenkundig unbegründeten oder exzessiven Beschwerden weigern kann, tätig zu werden. Wenn aus Sicht der klagenden Person die Absicht verfolgt wird, sich für eine ungerechte Entscheidung zu rächen und gewünschte Entscheidungen zu erzwingen, ist nach der Auffassung des Verwaltungsgerichts das Interesse am Schutz der personenbezogenen Daten vor diesem Hintergrund nicht schutzwürdig. Denn die Arbeitsfähigkeit von Gerichten und Behörden wird durch ein solches Verhalten belastet, was sich auch auf deren Fähigkeit, Dritten Rechtsschutz zu gewähren oder Anträge in angemessener Zeit zu bescheiden, auswirken kann. Diese Interessen verdienen den Vorrang vor nicht schutzwürdigen Interessen klagender Personen.

In einem Vorabentscheidungsersuchen an den EuGH zeichnet sich im Berichtszeitraum eine wegweisende Entscheidung zur Frage der Exzessivität ab. Den Schlussanträgen des Generalanwalts vom 5. September 2024 in der Rechtssache C- 416/23 folgend, ist Artikel 57 Absatz 4 DS-GVO dahingehend auszulegen, dass Anfragen nicht alleine aufgrund ihrer Zahl während eines bestimmten Zeitraums als „exzessiv“ einzuordnen sind. Vielmehr muss die Aufsichtsbehörde nachweisen, dass das Vorliegen einer Missbrauchsabsicht der anfragenden Person gegeben ist. Diese Anforderung wäre jedenfalls in dem vorliegenden Fall leicht zu erfüllen gewesen: In einer E-Mail hatte die Beschwerdeführerin gegenüber dem LfDI MV angekündigt, von weiteren Beschwerden oder Anträgen nach Artikel 15 DS-GVO abzusehen, wenn ihr in der familienrechtlichen Streitigkeit Recht gegeben würde.

11.2 Neugierige Beschäftigte – Bußgelder wegen Datenabfragen aus dienstlichen Systemen

Leider gibt es sie: Beschäftigte im öffentlichen Dienst oder in Krankenhäusern, die ihre Befugnisse missbrauchen, um geschützte Daten von Bürger/-innen oder Patientinnen und Patienten auszuspionieren – und dabei ganze Berufsstände in Misskredit bringen.

Im Krankenhaus, bei der Polizei oder im Gericht – überall muss im Zweifel schnell auf personenbezogene Daten zugegriffen werden können. Technische Zugriffsbeschränkungen sind daher nur bedingt sinnvoll, um die Daten vor unbefugten Zugriffen zu schützen. Wichtig sind daher ergänzende organisatorische Maßnahmen, wie z. B. Belehrungen der Beschäftigten, dass nur zu bestimmten Zwecken auf die Daten in den Systemen bei öffentlichen Stellen oder im Krankenhaus zugegriffen werden kann, die jeweils von der oder dem Arbeitgeber/-in festgelegt sind. Um dies überprüfen zu können, werden die Zugriffe durch die Beschäftigten auf Meldesysteme oder Patientenakten protokolliert.

Auch der Gesetzgeber in Mecklenburg-Vorpommern misst dem Schutz der Daten von Bürgerinnen und Bürgern sowie Patientinnen und Patienten einen hohen Stellenwert bei und hat sowohl im DSG M-V als auch im LKHG M-V spezielle Bußgeldtatbestände geschaffen, um unbefugte Datenabfragen durch Beschäftigte zu sanktionieren. Möglich ist hier ein Bußgeld bis zu 50.000 Euro.

Problematisch bleibt jedoch, dass das Gericht, das letztlich über den Bußgeldbescheid entscheiden muss, immer wieder Zweifel hat, ob tatsächlich die oder der Beschäftigte, die oder der laut Protokoll auf die Daten zugegriffen haben soll, es auch tatsächlich gewesen ist: Äußerst freimütig wird dann vor Gericht oder schon in der Anhörung davon berichtet, wie entgegen jeder Dienstanweisung Passwörter weitergegeben oder offen liegen gelassen werden. Das obligatorische Abmelden beim Verlassen des Arbeitsplatzes sei demnach oftmals zu umständlich gewesen. Besondere Kreativität zeigt sich beim Umgehen automatischer Bildschirmsperrungen. Beim Toilettengang der Beschäftigten hätte dann also wirklich jede Person am PC gewesen sein können. Natürlich sind solche Einlassungen nur bedingt klug, da sie wiederum auch arbeitsrechtliche oder disziplinarische Konsequenzen haben können, die im Zweifel auch schmerzhafter als ein Bußgeld sind.

Rechtskräftig werden angefochtene Bußgelder aber häufig nur dann, wenn uns der Nachweis gelingt, dass die oder der Betroffene die Daten auch tatsächlich weiterverwendet hat. Geschehen ist dies beispielsweise im Fall eines Polizisten, der eine besondere Nähe zu einer politischen Partei aufwies und politisch anders Denkende auf Facebook mit seinem widerrechtlich erlangten Spezialwissen über diese Personen unter Druck gesetzt hat.

Der LfDI MV empfiehlt daher Polizei, öffentlichen Stellen und Krankenhäusern, die internen Authentifizierungsprozesse zu überprüfen. Je nachdem, wie sensibel die betreffenden Daten sind, die verarbeitet werden, kommen hier verschiedene Authentifizierungsmöglichkeiten in Betracht. Diese ermöglichen einerseits eine eindeutige Zuordnung der abrufenden Person und minimieren andererseits Anreize, eine erneute, mit der Eingabe eines langen Passwortes verbundene Anmeldung am Arbeitsplatz zu umgehen.

11.3 Patientenakten auf der Baustelle – Bußgeld gegen Krankenhaus wegen eines ungesicherten Aktenschranks

„Wer schreibt, der bleibt“ war früher ein weitverbreiteter Arbeitsgrundsatz. Heute steigt zunehmend das Bewusstsein, dass das Geschriebene dann auch sicher aufbewahrt oder gespeichert werden muss. Darüber hinaus können Datensparsamkeit sowie das Löschen und Vernichten von Daten nach Ablauf entsprechender Fristen hier Kosten, Aufwand und Nerven sparen. Diese Erfahrung machte auch ein Krankenhaus im vorliegenden Berichtszeitraum.

Durch eine anonyme Beschwerde wurden wir darauf aufmerksam gemacht, dass sich in einem frei zugänglichen Baustellenbereich eines Krankenhauses ein unverschlossener Schrank mit Patientenakten befinden solle. Wir nahmen dies sehr ernst und führten sofort eine Kontrolle durch. Auch wenn wir uns natürlich vor Ort als zuständige Datenschutzaufsichtsbehörde zu erkennen gaben und von einer Beschäftigten des Verantwortlichen begleitet wurden, ließ sich der Vorwurf unproblematisch bestätigen. Wir konnten unbehelligt ein älteres und offenes Gemäuer betreten und fanden in der zweiten Etage auf einer Baustelle tatsächlich einen in die Jahre gekommenen, defekten Aktenschrank mit über 100 Patientenakten. Daneben lag eine Matratze, die sehr wahrscheinlich keinem Beschäftigten des Krankenhauses, sondern unbefugten Dritten in eher jüngerer Vergangenheit als Schlafplatz gedient haben dürfte. Eine kursorische Durchsicht der Akten mit Zustimmung des Krankenhauses ergab, dass nicht nur der Schrank, sondern auch die Fälle in den Akten recht alt waren und längst hätten vernichtet sein müssen.

Das Krankenhaus reagierte unmittelbar und ließ die Akten sofort bergen und nach einer Sichtung vernichten. Ebenfalls sicherte man uns auch eine Verbesserung der Prozesse zur Aufbewahrung und Vernichtung von Daten zu. Gleichwohl ist nach der DS-GVO in solchen Fällen der Erlass eines Bußgeldes die Regel. Durch die Vor-Ort-Kontrolle wurden aber die besonderen Gegebenheiten und Herausforderungen, vor denen das Krankenhaus stand, sowie vor allem auch dessen sofortige Kooperationsbereitschaft sichtbar. Diese Umstände flossen unmittelbar in die Bemessung des Bußgeldes ein und führten deutlich zu dessen Reduzierung.

Teil B – Empfehlungen und Ergänzungen

1. Empfehlungen an die Landesregierung

Wir sprechen die folgenden bereichsspezifischen Empfehlungen aus:

Technik und Organisation

Thema: Beratung zum Einsatz von Künstlicher Intelligenz (KI) an Schulen – Kapitel 3.3

Wir empfehlen dem Ministerium für Bildung und Kindertagesförderung des Landes Mecklenburg-Vorpommern, den Austausch mit unserer Behörde hinsichtlich der Beratung zum Einsatz von KI-Assistenzen in Schulen fortzuführen.

Thema: Projekt Integriertes Schulmanagementsystem (ISY MV) – Kapitel 3.4

Wir empfehlen dem Ministerium für Bildung und Kindertagesförderung des Landes Mecklenburg-Vorpommern, den Austausch mit unserer Behörde, insbesondere zum Projekt ISY MV, fortzuführen und zu prüfen, ob und wie die zentrale Bereitstellung von Softwareprodukten im Schulbereich weiter ausgebaut werden kann.

Thema: Überarbeitung der Orientierungshilfe Digitale Dienste – Kapitel 3.7

Wir empfehlen Anbieter/-innen von digitalen Diensten aus dem öffentlichen und nicht öffentlichen Bereich, sich mit der neuen Version der Orientierungshilfe Digitale Dienste vertraut zu machen und ihre Dienste auf Datenschutzkonformität nach dem neuen TDDDG, auch hinsichtlich des Einsatzes von Cookies, zu prüfen. Darauf aufbauend ist zu prüfen, ob sich die anschließenden Datenverarbeitungen von personenbezogenen Daten auf eine entsprechende Rechtsgrundlage aus der DS-GVO stützen lassen. Bei Unregelmäßigkeiten sind Maßnahmen zu ergreifen, um dem Grundrecht der Betroffenen auf informationelle Selbstbestimmung zu entsprechen.

Bildungsauftrag

Thema: Unterstützung der Bildungsangebote und Vernetzung zur Förderung von Medienkompetenz – Kapitel 4

Wir fordern die Landesregierung dazu auf, weiter Sorge dafür zu tragen, dass der LfDI MV seine umfangreichen Bildungsangebote weiterhin für Menschen aller Altersgruppen aufrechterhalten kann. Des Weiteren raten wir der Landesregierung, eine Vernetzung medienpädagogischer Institutionen im Land mithilfe einer neuen „Kooperationsvereinbarung zur Förderung von Medienkompetenz in Mecklenburg-Vorpommern“ vermehrt zu unterstützen. Der LfDI MV bleibt hierbei ein bewährter Partner und unterstützt die Landesregierung bei der Vernetzung.

Thema: Medienkompetenz bei Kindern und Jugendlichen – Kapitel 4.1

Wir empfehlen der Landesregierung den Austausch mit unserer Behörde bezüglich der medienpädagogischen Best-Practice-Projekte und deren Ausbaumöglichkeiten. Der Hauptvorteil dieser landesweiten Projekte besteht darin, dass die Vermittlung der Medienkompetenz auch in strukturschwächeren und/oder ländlichen Regionen abgedeckt wird. Somit tragen sie zur Chancengleichheit bei. Es gibt derzeit keine vergleichbaren Formate und Bildungsangebote zur Medienkompetenz für Kinder und Jugendliche dieser Altersgruppen in MV. Um diesen Ausbau zu begünstigen, ist es notwendig, die schulische und außerschulische Medienbildung zu vernetzen, um Medien- und Demokratiebildung junger Menschen in unserem Land zu garantieren.

Thema: Medienkompetenz bei pädagogischen Fachkräften – Kapitel 4.2

Wir raten der Landesregierung, regelmäßige und kostenlose Schulungen, Handreichungen, Materialien und regelmäßige Vernetzungsmöglichkeiten für pädagogische Fachkräfte in der Ausbildung sowie im weiteren Werdegang zu entwickeln und zu verfestigen. Aus unserer medienpädagogischen Praxis heraus sehen wir die Notwendigkeit, einen interaktiven und interdisziplinären Austausch zwischen allen relevanten Mitstreitern in der Bildungs-, Medienbildungs- und Präventionsarbeit zu ermöglichen, um mit der rasanten Entwicklung der Digitalisierung Schritt halten zu können. Eine Vernetzung der bestehenden Einzelmaßnahmen erachten wir als dringend notwendig.

Thema: Medienkompetenz bei Familien und Eltern – Kapitel 4.3

Wir empfehlen der Landesregierung, Projekte wie #Digitale Vorbilder – Familien gehen online. durch die Bereitstellung von Ressourcen zu fördern und zu unterstützen. Hierdurch kann ein niedrigschwelliger Zugang zu umfassenden Themen der Medienerziehung für Familien in Mecklenburg-Vorpommern gewährleistet werden. Der LfDI MV steht der Landesregierung jederzeit zur Verfügung, um inhaltlich und strategisch über die Projektergebnisse und deren weitere Verwendungsmöglichkeiten zu beraten, sodass auch zukünftig eine größtmögliche Zahl interessierter Familien in Mecklenburg-Vorpommern Zugang zu den aufbereiteten Bildungsmaterialien erhält.

Innere Sicherheit

Thema: Evaluierung des Sicherheits- und Ordnungsgesetzes – Kapitel 9.3

Es wird eindringlich an die Landesregierung appelliert, in einer potenziell folgenden Novelle auch Änderungsbedarfe über den Evaluierungsbericht hinaus zu berücksichtigen. In einem etwaigen Gesetzesvorhaben steht der LfDI MV gerne beratend auch in einer frühen Phase eines Entwurfes zur Verfügung.

Thema: Novellierung des Landesverfassungsschutzgesetzes – Kapitel 9.4

Zur Wahrung der Rechtsstaatlichkeit und des Grundrechtsschutzes ist eine Anpassung des LVerfSchG M-V dringend geboten. Wir empfehlen der Landesregierung dringend, eine Gesetzesinitiative zur Änderung des LVerfSchG M-V in den Landtag einzubringen.

Vereine, Parteien und Beschäftigtendatenschutz

Thema: Pseudonymisierung der Daten (Personalnummer, Stellennummer) – Kapitel 10.3

Der LfDI MV empfiehlt den Kommunen, statt der Personalnummer die Stellenbeschreibungen und Bewertungen zu den vereinbarten Stellen anzufordern – natürlich ohne den Namen oder die Personalnummern der Beschäftigten, sollten die Stellen schon besetzt sein.

Bußgeldstelle und Justiziariat

Thema: Datenabfragen aus dienstlichen Systemen – Kapitel 11.2

Der LfDI MV empfiehlt Polizei, öffentlichen Stellen und Krankenhäusern, die internen Authentifizierungsprozesse zu überprüfen. Je nachdem, wie sensibel die betreffenden Daten sind, die verarbeitet werden, kommen hier verschiedene Authentifizierungsmöglichkeiten in Betracht. Diese ermöglichen einerseits eine eindeutige Zuordnung der abrufenden Person und minimieren andererseits Anreize, eine erneute, mit der Eingabe eines langen Passwortes verbundene Anmeldung am Arbeitsplatz zu umgehen.

2. Abkürzungsverzeichnis

Das Abkürzungsverzeichnis wird alphabetisch geführt.

AK	Arbeitskreis
AK Technik	Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der DSK
ATD	Antiterrordatei
ATDG	Antiterrordateigesetz
BayLDA	Bayerisches Landesamt für Datenschutzaufsicht
bDSB	behördliche Datenschutzbeauftragte
BDSG	Bundesdatenschutzgesetz
BfDI	Die Bundesbeauftragte für Datenschutz und Informationsfreiheit
BIKO M-V	Bildungskonzeption der 0- bis 10-Jährigen in Mecklenburg-Vorpommern
BKAG	Bundeskriminalamt-Gesetz
BMG	Bundesmeldegesetz
BM MV	Ministerium für Bildung und Kindertagesförderung des Landes Mecklenburg-Vorpommern
BVerfG	Bundesverfassungsgericht
CEF	Koordinierte Prüfaktion, Englisch: Coordinated Enforcement Framework
CEH	Compliance, E-Government and Health
CERV-2021-DATA	EU-Programm „Citizens, Equality, Rights and Values-2021-DATA”
CNIL	Commission Nationale de l’Informatique et des Libertés
CoC	Verhaltensregeln, Englisch: Code of Conduct
CSG	ComputerSpielSchule Greifswald (Projekt des Medienzentrums Greifswald e. V.)
DDG	Digitale-Dienste-Gesetz
DSFA	Datenschutzfolgenabschätzung
DSG M-V	Landesdatenschutzgesetz
DS-GVO	Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
E-Akte MV	elektronische Akte für Mecklenburg-Vorpommern
EDSA	Europäischer Datenschutzausschuss
eGo MV	Zweckverband elektronische Verwaltung Mecklenburg-Vorpommern

ESG	Expert Subgroup
EU	Europäische Union
EUCROF	European Contract Research Organization Federation
EuGH	Europäischer Gerichtshof
EWR	Europäischer Wirtschaftsraum
FITKO	Föderale IT-Kooperation (Anstalt öffentlichen Rechts)
FSJ	Freiwilliges Soziales Jahr
GDNG	Gesundheitsdatennutzungsgesetz
GDSBaS	gemeinsame Datenschutzbeauftragte an Schulen
HmbBfDI	Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit
IMI	Binnenmarktinformationssystem, Englisch: Internal Market Information System
IFG	Informationsfreiheitsgesetz
IfSG	Infektionsschutzgesetz
ISY MV	Integriertes Schulmanagementsystem Mecklenburg-Vorpommern
KI	Künstliche Intelligenz
KI MV	Zentrum für Künstliche Intelligenz Mecklenburg-Vorpommern
KI-VO	Verordnung der Europäischen Union über Künstliche Intelligenz
KiföG M-V	Kindertagesförderungsgesetz
KlauS	Klassenbuch- und Stundenplan-Modul
KofIS	Kommission für Informationssicherheit
LAN	Local Area Network (lokales Netzwerk)
LAKOST MV	Landeskoordinierungsstelle für Suchtthemen Mecklenburg-Vorpommern
LfDI MV	Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern
LJR MV	Landesjugendring Mecklenburg-Vorpommern e. V.
LKA MV	Landeskriminalamt Mecklenburg-Vorpommern
LKHG M-V	Landeskrankenhausgesetz Mecklenburg-Vorpommern
LLM	Large Language Models
LpB MV	Landeszentrale für politische Bildung Mecklenburg-Vorpommern
LVerfSchG M-V	Landesverfassungsschutzgesetz
MV	Mecklenburg-Vorpommern
MIBD MV	Ministerium für Inneres, Bau und Digitalisierung Mecklenburg-Vorpommern
MII	Medizininformatik-Initiative
MMV	Landesmedienanstalt Mecklenburg-Vorpommern
MPZ	Medienpädagogisches Zentrum

OH Digitale Dienste	Orientierungshilfe für Anbieter:innen von digitalen Diensten
OMNIS	Onlinemanagement in Schulen
ÖGDG M-V	Gesetz über den Öffentlichen Gesundheitsdienst Mecklenburg-Vorpommern
RED	Rechtsextremismus-Datei
RED-G	Rechtsextremismus-Datei-Gesetz
SDM	Standard-Datenschutzmodell
SchulGesPflVO M-V	Schulgesundheitspflege-Verordnung
SGB	Sozialgesetzbuch
SOG M-V	Sicherheits- und Ordnungsgesetz
StPO	Strafprozessordnung
TDDDG	Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz
TEO – PP	Tage ethischer Orientierung – protect privacy
TFFD	Taskforce Forschungsdaten
TMG	Telemediengesetz
TMF	Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V.
TOM	technische und organisatorische Maßnahmen
TTDSG	Telekommunikation-Telemedien-Datenschutz-Gesetz
USA	Vereinigte Staaten von Amerika
vdek e. V.	Verband der Ersatzkassen e. V. Mecklenburg-Vorpommern
WADA	World Anti-Doping Agency
WKM MV	Wissenschaft, Kultur, Bundes- und Europaangelegenheiten Mecklenburg-Vorpommern
WLAN	Wireless Local Area Network (drahtloses lokales Netzwerk)
ZMV+	Regionales Zukunftszentrum Mecklenburg-Vorpommern+

3. Stichwortverzeichnis

E

F

G

I

J

K

L

M

N

O

P

R

S

T

V

W

Y