Der Landesbeauftragte für
DATENSCHUTZ und
INFORMATIONSFREIHEIT
Mecklenburg-Vorpommern



19. Tätigkeitsbericht zum Datenschutz

» Berichtszeitraum: 1. Januar 2022 bis 31. Dezember 2023

und

9. Bericht über die Umsetzung des Informationsfreiheitsgesetzes M-V

» Berichtszeitraum: 1. Januar 2022 bis 31. Dezember 2023

Impressum

Redaktion:
Der Landesbeauftragte für Datenschutz und
Informationsfreiheit Mecklenburg-Vorpommern (LfDI MV)

Postanschrift:
Schloss Schwerin
Lennéstraße 1
19053 Schwerin

Dienststelle:
Werderstraße 74 a
19055 Schwerin

Telefon: 0385 59494-0
E-Mail: info@datenschutz-mv.de
Website: www.datenschutz-mv.de
www.informationsfreiheit-mv.de

Vorgelegt im Oktober 2024, Sebastian Schmidt, LfDI MV

Bildnachweise:
© Cover: christophkadur (Adobe Stock), © Freepik, KI-Unterstützung; © Vorwort: Ecki Raff

Disclaimer zum Gendern:
Im vorliegenden Tätigkeitsbericht schreiben wir Personenbezeichnungen mit Doppelpunkt, um die Lesbarkeit durch Screenreader zu ermöglichen. Personenbezeichnungen aus Gesetzestexten, die im generischen Maskulinum geschrieben sind, sind aufgrund der Zitierbarkeit der Gesetzestexte im Original übernommen. Alle Texte adressieren ausdrücklich alle Geschlechter.

19. Tätigkeitsbericht zum Datenschutz

Berichtszeitraum: 1. Januar 2022 bis 31. Dezember 2023

und

9. Bericht über die Umsetzung des Informationsfreiheitsgesetzes M-V

Berichtszeitraum: 1. Januar 2022 bis 31. Dezember 2023

Vorwort



Sebastian Schmidt · Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern

Auch mehrere Jahre nach Einführung der Europäischen Datenschutz-Grundverordnung (DS-GVO) nimmt die Sensibilität der Öffentlichkeit für das Thema Datenschutz in Mecklenburg-Vorpommern zu. Noch nie wurden der Aufsichtsbehörde so viele Datenpannen gemeldet, noch nie gingen bei ihr so viele Beschwerden ein. Dabei ist die Lage in Sachen Datenschutz objektiv nicht schlechter geworden, die Sensibilisierung für das Thema hat schlicht erheblich zugenommen. Eine große Rolle bei dieser Sensibilisierung hat sicherlich auch die Aufklärungs- und Informationsarbeit der Aufsichtsbehörde gespielt. Die Menschen werden sich der Schutzbedürftigkeit und des Wertes ihrer Daten zunehmend bewusster, und das begrüßen wir außerordentlich.

Neben unserer klassischen aufsichtsbehördlichen Funktion nehmen wir unseren Beratungs- und Informationsauftrag sehr ernst. Viele Datenschutzverstöße werden aus Unwissenheit begangen und können durch schlichte Aufklärungsarbeit bereits im Vorfeld verhindert werden. In der Praxis zeigt sich diese Präventionsarbeit als sehr effektiv. Gleichwohl werden dadurch Kontrollen und Sanktionen nicht überflüssig. Alle Instrumente müssen, wie die Zahnräder eines Uhrwerks, perfekt ineinander greifen. Nur dann kann ein möglichst effektiver Datenschutz gewährleistet werden.

Aus diesem Grunde ist die Behörde verstärkt dazu übergegangen, auch anlasslose Kontrollen in verschiedenen Bereichen durchzuführen. Diese Kontrollen wurden teilweise auch von den Verantwortlichen sehr positiv aufgenommen und verstärkten deren Problembewusstsein für datenschutzrelevante Themen. Überdies zeigten sich auch Effekte bei anderen Akteuren, die diese Kontrollen zur Kenntnis und zum Anlass für Verbesserungen in ihrem Verantwortlichkeitskreis nahmen.

Nach wie vor ist jedoch im Bereich des Datenschutzrechtes noch viel in Bewegung. Einige Bereiche sind noch nicht umfassend geregelt, viele Detailfragen noch unbeantwortet. Mit der KI-Verordnung hat die EU ein zweites großes unmittelbar geltendes Regelwerk auf den Weg gebracht, weitere werden folgen. Über eine verstärkte Beteiligung auf europäischer Ebene ist es möglich, sich als Bundesland Mecklenburg-Vorpommern in wichtige Prozesse frühzeitig einzubringen. Eben dieses soll durch eine verstärkte Mitarbeit in entsprechenden Arbeitsgruppen des EDSA gewährleistet werden. Aber auch auf nationaler Ebene gibt es noch viel zu tun. Das zuvor angesprochene Thema „KI" muss auf nationaler Ebene durch Anwendungsstrategien, bestimmte Regelwerke und Orientierungshilfen flankiert werden. Hier sind es die DSK und nicht zuletzt jede einzelne Aufsichtsbehörde für sich, die unterstützen müssen. Dieser Aufgabe sind wir uns bewusst und nehmen sie auch gerne an.

Als besonders wichtig haben sich jedoch die Projekte zum Thema Medienbildung gezeigt. In diesem Bereich prallen zwei Problemfelder aufeinander: auf der einen Seite eine technische Entwicklung, die immer rasanter wird, und auf der anderen Seite der fehlende Wissensvorsprung der Älteren am wichtigsten Lernort für Kinder, ihren Familien. In digitalen Medien lauern viele Gefahren, derer sich die meisten Menschen – egal ob jung oder alt – kaum bewusst sind. Wie funktionieren die Algorithmen sozialer Medien oder welche Gefahren bergen Deepfakes für das soziale und politische Miteinander? Was ist Realität und wie kann ihre Wahrnehmung in digitalen Medien beeinflusst werden? Die Vermittlung von Medienkompetenz ist eine der größten Herausforderungen dieser Zeit. Sie muss unterstützt und ausgebaut werden. In unserer Beratungs- und Aufklärungsfunktion werden wir auch hier künftig einen wichtigen Teil unsere Arbeit sehen.



Sebastian Schmidt

Landesbeauftragter für
Datenschutz und Informationsfreiheit
Mecklenburg-Vorpommern

Teil A 19. Tätigkeitsbericht zum Datenschutz

1. Entwicklung der Behörde 10

1.1. Statistik 10

2. Verstärkte Kontrollen und Beratungen vor Ort 11

3. Technik und Organisation 12

3.1. Arbeitskreis „Technische und organisatorische Datenschutzfragen" 13

3.2. Einsatz von Künstlicher Intelligenz 15

3.3. Cybersicherheit 17

3.4. Gesetz zur Errichtung des Landesamtes Zentrum für Digitalisierung M-V 19

3.5. Sicherheit bei der Übertragung von E-Mails beim LfDI MV 21

3.6. Einsatz von Videokonferenzsystemen 23

3.7. Datenschutz und Schule 24

3.7.1. Auftragsverarbeitung und Digitalisierung im Bereich Schule 24

3.7.2. Integriertes Schulmanagementsystem ISY MV 26

3.8. Telemedien 26

3.8.1. Arbeitsgruppe Microsoft-Onlinedienste 27

3.8.2. Orientierungshilfe für Anbietende von Telemedien 28

3.9. Versendung von Newslettern ohne Einwilligung 29

4. Bildungsauftrag der Behörde 30

4.1. Medienscouts MV – Jugend klärt auf! 31

4.2. Medienguides MV – Eltern.Medien.Kompetenz 32

4.3. Tage ethischer Orientierung: protect privacy – „Mein Klick, meine Verantwortung" 33

4.4. Modulare Fortbildungsreihe „Spielen, Zappen, Klicken" 35

4.5. Das Jugendportal der DSK: youngdata.de 36

4.6. #Digitale Vorbilder – Familien gehen online. 38

4.7. Das landesweite Netzwerk der Medienbildung Medienaktiv M-V 41

5. Europäische Zusammenarbeit und Internationaler Datenverkehr 42

5.1. Kooperationsverfahren über IMI 43

5.2. Untersuchung zum NIPT und möglichen Übermittlungen genetischer Daten nach China 44

5.3. AG Transfertools von Gesundheitsdaten und Biomaterialien in Drittstaaten 46

5.4. DSK Anwendungshinweise zum Angemessenheitsbeschluss für die USA 46

5.5. EDSA Streitbeilegungsverfahren zu TikTok 47

6. Beschäftigtendatenschutz **49**

6.1. Kontrollen in Callcentern 49

6.2. Kontrolle eines Landkreises 50

6.3. EuGH-Urteil vom 30. März 2023 Rs. C-34/21 zu den Anforderungen an gesetzliche Regelungen zum Beschäftigtendatenschutz 51

7. Videoüberwachung **53**

7.1. Klingelkameras 53

7.2. Videoüberwachung durch Wahlkreisbüro 55

7.3. Videoüberwachung mit Wildkameras in den Wäldern 56

7.4. Videoüberwachung in Kommunen 57

8. Behörden, Gesundheit und Soziales **59**

8.1. Gemeindevertreter:innen benötigen datenschutzkonforme mobile Endgeräte 59

8.2. E-Mail-Kommunikation im Rahmen von Gemeindevertretungen 60

8.3. Standardprozesse für Auskünfte nach Art. 15 DS-GVO durch die Kommunen 62

8.4. Förderung von Mini-Solaranlagen 64

8.5. SEPA-Lastschriftverfahren bei Zahlungen an Kommunen 65

8.6. Stellung und Aufgaben der behördlichen Datenschutzbeauftragten 66

8.7. Rechtsprechung des EuGH zum Recht auf Kopie der Patientenakte 70

9. Innere Sicherheit **71**

9.1. Kontrolle besonders eingriffsintensiver und verdeckter Maßnahmen 72

9.2. Unzutreffende Speicherung in polizeilichen Informationssystemen 74

9.3. Auskunftsrecht gegenüber der Polizei 76

9.4. Unberechtigte Datenabfragen in der Landespolizei MV 78

9.5 Novellierungsbedarfe des SÜG M-V und des LVerfSchG M-V 80

10. Justiz **81**

10.1. Unsichere E-Mail-Konten bei Gerichtsvollzieher:innen 81

10.2. Verlorener USB-Stick mit Missbrauchsmaterial 82

11. Verkehr **83**

11.1. Verkehrsanalyse und Hinweispflicht an der Warnowquerung 83

11.2. Kennzeichenerfassung auf Parkplätzen 85

11.3. Nutzung von Dashcams in Kraftfahrzeugen 86

11.4. Videoüberwachung in öffentlichen Verkehrsmitteln 87

12. Vereine **88**

12.1. Datenschutz im Kleingartenverein 88

13. Bußgeldstelle und Justiziariat **89**

13.1. Bei dem Verwaltungsgericht anhängige Verfahren 89

13.2. Mitarbeiterexzesse weiterhin Schwerpunkt der Bußgeldstelle 91

14. Begleitung von Rechtssetzungsvorhaben **92**

14.1. Novellierung der Kommunalverfassung M-V 93

14.2. Anpassung des SOG M-V an die Vorgaben des Bundesverfassungsgerichts 95

Teil B 9. Bericht über die Umsetzung des Informationsfreiheitsgesetzes M-V

1. Informationsfreiheit in Mecklenburg-Vorpommern – Bedeutung, Zahlen und Fakten 98

2. Bildungsministerium gibt Abituraufgaben der vergangenen Jahre heraus 99

3. Der LfDI MV ist bei seiner Aufgabenerfüllung zu unterstützen 100

4. Ein laufendes Klageverfahren kann einem Auskunftsanspruch entgegenstehen 100

5. Transparenz setzt eine ordnungsgemäße Aktenführung voraus 101

6. Die Angabe einer Adresse ist nicht immer erforderlich 102

7. Das Schriftformerfordernis verlangt eine eigenhändige Unterschrift 103

8. Protokolle nicht-öffentlicher Sitzungen sind nicht automatisch vertraulich 104

9. Die Geschäftsordnung einer Gemeindevertretung steht einem Anspruch auf Informationszugang nicht entgegen 105

10. Ablehnung des Informationszugangs kann rechtmäßig sein 106

11. Bei einem Drittbeteiligungsverfahren kann sich der Informationszugang verzögern 106

12. Strenge Voraussetzungen beim Zugang zu personenbezogenen Daten 108

Teil C Ergänzungen

1. Empfehlungen | Zusammenfassung **110**

» Technik und Organisation 110

» Datenschutz und Bildung 111

» Beschäftigtendatenschutz 113

» Behörden, Gesundheit und Soziales 113

» Informationsfreiheit – IFG M-V 113

2. Abkürzungsverzeichnis **114**

3. Stichwortverzeichnis **117**

Teil A

19. Tätigkeitsbericht zum Datenschutz

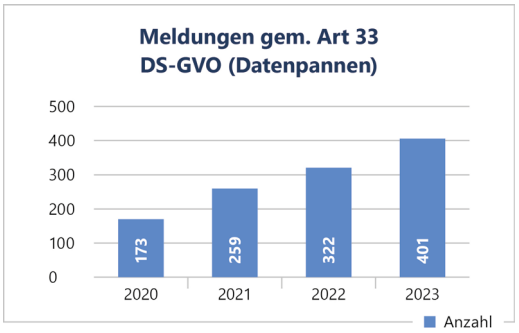
Berichtszeitraum: 1. Januar 2022 bis 31. Dezember 2023

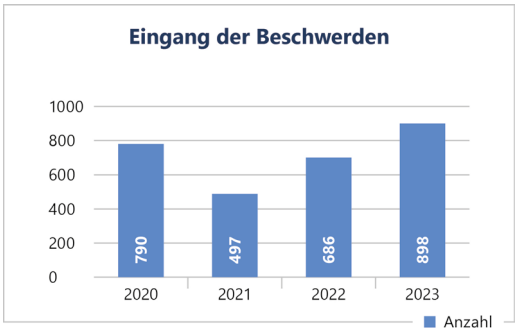
1. Entwicklung der Behörde

Im Berichtszeitraum wechselte der Landesbeauftragte für Datenschutz und Informationsfreiheit in eine neue Amtsperiode. Weiterhin konnte die Behörde durch die Personalbedarfsplanung im Einvernehmen mit dem Landesrechnungshof MV (LRH MV) Personalstellen entsperren. Begründet wurden die Entsperrungen mit bisher nicht durchgeführten (Pflicht-) Aufgaben, wie beispielsweise „anlasslosen Kontrollen" oder einem erhöhten Beratungsbedarf der Landesregierung zu Themen wie Einsatz Künstlicher Intelligenz (KI), Novellierung der Sicherheits- und Ordnungsgesetzes (SOG M-V) oder das Gesundheitsforschungsstärkungsgesetzes. Personell verstärkt wurde der Bereich Technik (LD3), um die stetig wachsenden technischen Neuerungen und Anfragen als Datenschutzaufsichtsbehörde umsetzen zu können und das Referat zuständig für den Datenschutzes im öffentlichen Bereich (LD2).Gleichzeitig sollte der organisatorische Aufbau der Behörde umgestaltet werden. Die Stabsstelle der Medienbildung wurde um die Presse- und Öffentlichkeitsarbeit erweitert und in ein eigenes Referat umgewandelt. Durch die EU-Fördergelder für das Familienprojekt *#Digitale Vorbilder – Familien gehen online.* wurde ebenfalls im Referat „Presse, Kommunikation und Medienbildung" eine für das EU-Projekt bezogene Stelle geschaffen. Zudem hat die Behörde ihre Zusammenarbeit auf europäischer Ebene gestärkt. Um als Mecklenburg-Vorpommern in Europa bereits frühzeitig wichtige Impulse setzen zu können, ist eine Mitarbeit in den Subgroups des Europäischen Datenschutzausschusses (EDSA) notwendig. In der Vergangenheit war dies leider nicht immer möglich. Diese Mitarbeit wurde forciert und soll perspektivisch weiter ausgebaut werden.

1.1. Statistik

Uns erreichten im Jahr 2022 bereits 322 Meldungen (Datenpannen) gem. Art. 33 Datenschutz-Grundverordnung (DS-GVO) und im Jahr 2023 dann sogar 401 Meldungen gem. Art. 33 DS-GVO. Das schließt einerseits auf die deutlich gesteigerte Sensibilität der Verantwortlichen und auf der anderen Seite jedoch auch auf die „Anfälligkeit" informationstechnischer Systeme. Während die Anzahl der Eingaben und Beschwerden im Jahr 2021 noch rückläufig war, hat sie sich im Jahr 2022 auf 686 Beschwerden erhöht und im Jahr 2023 noch einmal mehr auf 898 Beschwerden, die es zu bearbeiten galt. Gleichwohl folgte der LfDI MV seiner Strategie des stark beratenden Charakters weiterhin.





2. Verstärkte Kontrollen und Beratungen vor Ort

Der LfDI MV hat im Berichtszeitraum wieder verstärkte Kontrollen im Land durchgeführt, sowohl um Verantwortliche für die Einhaltung der datenschutzrechtlichen Anforderungen zu sensibilisieren, als auch um mögliche Verstöße zu überprüfen. Bei Hinweisen oder Beschwerden, die plausibel machen, dass insbesondere grundlegende Prozesse des jeweiligen Verantwortlichen, besonders sensible Daten oder viele Bürger:innen betroffen sind, kann eine Kontrolle vor Ort die Sachverhaltsermittlung deutlich beschleunigen und eventuelle Verstöße können schneller abgestellt werden. Bei diesen anlassbezogenen Prüfungen werden die Verantwortlichen zum gemeldeten Verstoß befragt und die betreffenden Dateisysteme durch uns eingesehen (wie zum Beispiel Einstellung von Videokameras, Verzeichnisse oder Dokumentenmanagement-Systeme, angewendete Zugriffbeschränkungen oder praktische Durchführung von Prozessen). Wir erleben bei unseren Kontrollen und Beratungen vor Ort einen konstruktiven und kooperativen Umgang sowie viel positives Feedback.

Ein Schwerpunkt unserer Kontrollen lag im Bereich Beschäftigtendatenschutz.[1] Bei Beschäftigten in Callcentern wurde uns ein sehr hoher Kontrolldruck gemeldet. Durch mehrere stichprobenartige Kontrollen mit dem Ziel der Sensibilisierung für die Einhaltung des Datenschutzes, sind wir dem nachgegangen (siehe Punkt 6.1.). Bei einem Landkreis wurde insbesondere dazu beraten, wie Beschäftigte zu schützen sind, wenn sie als Bürger:innen Dienstleistungen des Landkreises in Anspruch nehmen. Ablauf und Ergebnisse dieser Kontrolle werden in einem späteren Kapitel genauer beleuchtet (siehe Punkt 6.2.). Nach Hinweisen auf einen möglichen Transfer von genetischen Daten von Schwangeren nach China mit unabsehbaren Folgen haben wir außerdem eine landesweite Umfrage durchgeführt, um den Schutz von betroffenen Personen in Mecklenburg-Vorpommern sicherzustellen (siehe Punkt 6.2.). Die stichprobenartige Umfrage fand in Koordination mit Kolleg:innen der anderen europäischen Datenschutzaufsichtsbehörden statt, insb. mit Slowenien. Weiterhin nahm der LfDI MV die Kontrolle von gesetzlich vorgeschriebenen, turnusmäßigen Prüfungen von eingriffsintensiven und verdeckten Maßnahmen der Polizei im Bereich der Gefahrenabwehr auf (siehe Punkt 10.1.).

Wir konnten im Berichtszeitraum mit den Kontrollen vor Ort einer Vielzahl von Beschwerden betreffend einer Videoüberwachung nachgehen (siehe Punkt 7.). Viele Büger:innen fühlten sich durch den Einsatz der Überwachungskameras in ihrem Persönlichkeitsrecht eingeschränkt und überwacht, da Sie den Eindruck haben, dass Kameras über die Grenzen von privaten Grundstücken hinaus filmen. Bei der Mehrzahl dieser Kontrollen waren alle Beteiligten sehr kooperativ und die Einhaltung der Vorgaben im Hinblick auf die DS-GVO konnten vor Ort sofort umgesetzt werden. Dabei musste immer wieder festgestellt werden, dass oft Unkenntnis darüber besteht, wie eine Videoüberwachung datenschutzkonform eingesetzt werden kann und welche datenschutzrechtlichen Konsequenzen eine nicht datenschutzkonforme Videoüberwachung für den Verantwortlichen nach sich zieht. Die Hinweispflichten wurden mit Geltung der DS-GVO erweitert, d. h. auch für eine datenschutzkonforme Videoüberwachung gelten die Informationspflichten gem. Art. 13 DS-GVO, die durch den Verantwortlichen umzusetzen sind.

1 Vgl. Hinweis auf unserer Website in URL: https://www.datenschutz-mv.de/datenschutz/publikationen/Callcenter/ [abgerufen am 03.04.2024]

Gerade mit der datenschutzkonformen Umsetzung der Informationspflichten kann zukünftigen Beschwerden zu einer Videoüberwachungsanlage entgegen gewirkt werden. Der LfDI MV empfiehlt dabei die Nutzung eines vorgelagerten und eines nachgelagerten Hinweisschildes, damit Betroffene informiert werden, bevor sie den videoüberwachten Bereich betreten.

Überwiegend im Bereich der nachbarschaftlichen Videoüberwachung häufen sich die Beschwerden. Wir können allerdings nur im Rahmen der Zuständigkeit für den öffentlichen Raum tätig werden. In Fällen, in denen der öffentliche Raum von der Videoüberwachung nicht betroffen ist, können die Persönlichkeitsrechte lediglich im zivilrechtlichen Verfahren durchgesetzt werden. Mit einer einfachen Änderung der Ausrichtung der Kameras kann oftmals schon ausgeschlossen werden, dass öffentliche Flächen, Nachbarn und sonstige Betroffene erfasst werden, die den Eindruck von einer Aufzeichnung haben könnten. Gegebenenfalls lassen sich auch mittels Blenden am Objektiv der Kamera bestimmte Bereiche abdecken. Es ist grundsätzlich zu beachten, dass das Schwärzen, Pixeln oder Ausblenden öffentlicher Bereiche oder von Nachbarschaftsgrundstücken durch Kameraeinstellungen zwar ein datenschutzfreundliches Werkzeug darstellt, es jedoch unter Umständen bei Betroffenen weiterhin einen „Überwachungsdruck" erzeugen kann, da diese Einschränkungen für Betroffene nicht erkennbar sind.

3. Technik und Organisation

Der Berichtszeitraum war zum einen stark geprägt vom aufkommenden Thema der Künstlichen Intelligenz (KI), zum anderen jedoch auch weiterhin vom Thema Cybersicherheit. So erreichte den LfDI MV auch in diesem Berichtszeitraum eine konstant hohe Anzahl an Datenpannenmeldungen, insbesondere ausgelöst durch Cyberangriffe. Offensichtlich ist dabei, dass es Cyberkriminelle nicht einfach nur auf große finanzkräftige Unternehmen abgesehen haben, sondern bei ihren Angriffen verstärkt breitflächig vorgehen. Somit ist und bleibt die Gewährleistung von IT-Sicherheit eine stetige Herausforderung und es gilt, diese flächendeckend auf einem hohen Niveau zu etablieren. Dies stellt kleinere Unternehmen und insbesondere auch Kommunalverwaltungen, die laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) auch überproportional häufig von Cyberangriffen betroffen sind, vor enorme Herausforderungen. Das BSI formulierte jüngst die Vision von einer Cybernation Deutschland[1]. Auch der LfDI MV möchte die IT-Sicherheit im Land in die Breite tragen verschafft sich derzeit einen Überblick, um praxisorientiert und zielgerichtet Unterstützungsleistungen anbieten zu können.

1 URL: https://www.bsi.bund.de/DE/Das-BSI/Cybernation/cybernation_node.html [abgerufen am 22.02.2024]

3.1. Arbeitskreis „Technische und organisatorische Datenschutzfragen“

Die Datenschutzkonferenz (DSK) hat zur Koordination ihrer Aktivitäten auf technischem Gebiet den Arbeitskreis „Technische und organisatorische Datenschutzfragen“ (AK Technik) eingerichtet. Seit vielen Jahren obliegt dem LfDI MV die Leitung dieses Arbeitskreises. Der LfDI MV berichtet hierüber regelmäßig[1].

Die Sitzungen des Arbeitskreises fanden seit der 80. Sitzung abwechselnd als Präsenzsitzungen und als Videokonferenzen statt, nachdem während der Corona-Pandemie ausschließlich Videokonferenzen durchgeführt werden mussten. An den Sitzungen nahmen als Gäste auch wieder Vertreter:innen aus der Schweiz und aus Liechtenstein sowie von spezifischen Aufsichtsbehörden der evangelischen und der katholischen Kirche und des Rundfunks teil.

Auf der 76. Sitzung des AK Technik brachten die Teilnehmer:innen eine Änderung der Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“[2] auf den Weg, die dann auf der Datenschutzkonferenz am 16. Juni 2021 beschlossen wurde. Präzisiert wurde darin, was Personen, die Berufsgeheimnisse wahren müssen, zum sicheren Austausch von E-Mails tun müssen. Zu dieser Berufsgruppe gehören beispielsweise Ärzt:innen sowie Anwält:innen. Außerdem wurde der Baustein „Planen und Spezifizieren“ des Standard-Datenschutzmodells (SDM) verabschiedet[3]. Zu den weiteren Themen gehörten auch Kontaktnachverfolgungssysteme, wie sie zur Bekämpfung der COVID-19-Pandemie eingesetzt werden.

Zur 77. Sitzung des AK Technik hörten die Mitglieder und Gäste einen Vortrag zu Werkzeugen und Methoden zur Analyse von Apps für Smartphones und von Websites. Außerdem nahmen die Mitglieder den SDM-Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“[4] an. Ferner beschäftigten sie sich mit dem Umgang mit Meldungen zu Schwachstellen in informationstechnischen Systemen.

Auf der 78. Sitzung wurde der Entwurf von Leitlinien des Europäische Datenschutzausschusses (EDSA) zu Anonymisierung und Pseudonymisierung ausführlich diskutiert, um die deutschen Vertreter:innen in der dafür zuständigen Arbeitsgruppe (AG) auf europäischer Ebene zu unterstützen.

1 Vgl. Punkt 4.2 in URL: https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Taetigkeitsberichte/lfdmvtb16.pdf [abgerufen am 22.02.2024]

2 URL: https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Broschueren/20210616_OH_E-Mail.pdf [abgerufen am 22.02.2024]

3 Vgl. Punkt 7.1 in URL: https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Taetigkeitsberichte/lfdmvtb16.pdf [abgerufen am 22.02.2024]

4 URL: https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0b_Zugriffe_regeln_V1.0.pdf [abgerufen am 22.02.2024]

Zur 79. Sitzung wurde das neu gefasste SDM 3.0[1] abschließend beraten. Dieses wurde nach der Sitzung im Umlaufverfahren angenommen. Die Datenschutzkonferenz hat das SDM 3.0 anschließend in der 105. Sitzung beschlossen und veröffentlicht.

Neuerungen des SDM 3.0 sind insbesondere die Abschnitte:

» D2.1 Aufbereitung einer Verarbeitungstätigkeit in Vorgänge oder in Phasen eines Datenlebenszyklus
» D2.5 Überblick über die Modellierungstechniken des SDM („SDM-Würfel")
» D3 Risiken und Schutzbedarf

Ein weiteres wichtiges Thema der 79. Sitzung waren erneut die Leitlinien des EDSA zu Anonymisierung und Pseudonymisierung.

Auch in der der 80. Sitzung nahm die Diskussion zu diesen Leitlinien breiten Raum ein. Ein weiteres wichtiges Thema war das „Positionspapier zu cloudbasierten digitalen Gesundheitsanwendungen"[2]. Dieses Positionspapier entstand im Unterarbeitskreis „Digitalisierung im Gesundheitswesen", der von den Arbeitskreisen „Technik" und „Gesundheit und Soziales" getragen wird. Ergebnisse von Unterarbeitskreisen bedürfen der Zustimmung durch die jeweiligen Arbeitskreise, bevor sie der DSK zur Entscheidung vorgelegt werden. Darüber hinaus befassten sich die Mitglieder des Arbeitskreises mit dem Einsatz von Content Delivery Networks (CDN), welche insbesondere zur Lastverteilung von Websites genutzt werden. Hierzu hat der Arbeitskreis die Position[3] des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) zur Kenntnis genommen und keinen Bedarf zur Erstellung eines eigenen Papiers gesehen.

Die 81. Sitzung begann ebenfalls mit einer Erörterung zum Stand der Leitlinien des EDSA zur Anonymisierung und Pseudonymisierung sowie zur Anwendung der E-Privacy-Richtlinie. Außerdem wurde die Anfrage der französischen Datenschutzaufsichtsbehörde Commission Nationale de l'Informatique et des Libertés (CNIL) zur Gesichtserkennung auf Flughäfen besprochen. Ferner diskutierten die Mitglieder, in welcher Form die Zusammenarbeit mit dem BSI intensiviert werden soll.

In den Sitzungen des Arbeitskreises wurden stets Fragen erörtert, die sich aus der Zusammenarbeit unter den Datenschutzaufsichtsbehörden in der Europäischen Union ergeben. Dies betraf im Berichtszeitraum unter anderem die Interpretation von „Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten"[4] des EDSA. Hier beschäftigte sich der AK Technik damit, unter welchen Umständen eine kryptographische Verschlüsselung einen wirksamen Schutz personenbezogener Daten bietet.

1 URL: https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode-V30a.pdf [abgerufen am 22.02.2024]

2 URL: https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/20231106_Beschluss_cloudbasierte_digitale_Gesundheitsanwendungen.pdf [abgerufen am 22.02.2024]

3 Schreiben an ITZ Bund und Beschaffungsamt des BMI zu Beschaffungen mit Cloud-Bezug in URL: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2022/StgN_Cloud-ITZ-BeschA.html [abgerufen am 22.02.2024]

4 URL: https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_de.pdf [abgerufen am 22.02.2024]

Verschlüsselungsverfahren büßen über die Zeit an Stärke ein. Dies liegt nur zum Teil an der zunehmenden verfügbaren Rechenleistung, da diese recht gut vorhersagbar ist und in die Gestaltung der Verfahren und ihrer Parameter, z. B. die Schlüssellänge, einbezogen werden kann. Wichtiger sind eventuelle neu gefundene Erkenntnisse, die das Brechen der Verfahren unvorhersehbar erleichtern können. Beide Effekte führen dazu, dass häufig zusätzliche Maßnahmen getroffen werden müssen, um die Vertraulichkeit personenbezogener Daten langfristig sicherzustellen. Insbesondere sind auch verschlüsselte Daten stets zu löschen, wenn ihre weitere Verarbeitung nicht mehr zulässig ist. Es genügt nicht, nur den zur Entschlüsselung benutzten Schlüssel zu löschen.

In der Zusammenarbeit unter den europäischen Aufsichtsbehörden kommt den Leitungen der DSK-Arbeitskreise und AG's verstärkt eine Koordinierungsrolle zu. So obliegt ihnen die Federführung, wenn eine abgestimmte Position der in der DSK vertretenen Behörden im Themenbereich des jeweiligen Arbeitskreises zu formulieren ist. Ein Anlass hierfür sind Anfragen unserer europäischen Partnerbehörden zur freiwilligen gegenseitigen Amtshilfe nach Art. 61 DS-GVO.

Auch der Vorsitz des AK Technik bearbeitete im Jahr 2021 erste Fälle dieser Art. In den Jahren 2022 und 2023 setzte sich dies fort. Dabei ging es vorrangig um Anwendungsfälle von Biometrie[1].

3.2. Einsatz von Künstlicher Intelligenz

Der vergangene Berichtszeitraum war stark geprägt von den Entwicklungen rund um die KI.

Die einfache und breite Verfügbarkeit großer Sprachmodelle, so genannter Large Language Models (LLM), wie ChatGPT von OpenAI, Gemini (ehemals Bard) von Google oder dem Microsoft Copiloten (ehemals Bing Chat), haben zu einer sehr stark gestiegenen Wahrnehmung von KI und deren Möglichkeiten in der Öffentlichkeit geführt. Wirtschaft und Verwaltung sehen ebenfalls ein großes Potential im Einsatz von KI-Anwendungen und haben teilweise bereits damit begonnen, diese in ihren Arbeitsalltag zu integrieren.

Dieses sprunghafte Interesse und die schnelle Einführung diverser KI-Anwendungen stellte auch den LfDI MV vor neue Herausforderungen. So stiegen einerseits die Anfragen in Form von Beratungsersuchen und Vortragswünschen zum Thema massiv an, andererseits galt es, den Verantwortlichen und den Anwender:innen Hilfestellungen in Form von Orientierungshilfen und Leitlinien an die Hand zu geben.

Grundsätzlich ist die Thematik der KI für den LfDI MV kein komplett neues Thema. Bereits im Jahr 2019 haben wir uns mit den Datenschutzaspekten beim Einsatz von KI auseinandergesetzt. So entstand unter unserem Vorsitz des AK Technik das „Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen" (siehe Punkt 3.1).

1 Vgl. Punkt 7.1.1 in URL: https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Taetigkeitsberichte/lfdmvtb15.pdf [abgerufen am 22.02.2024]

Da die Entwicklungen in der KI seitdem jedoch große Sprünge machten, befassen wir uns auch weiterhin mit einer Überarbeitung dieser Version, die ebenfalls neue Techniken in den Blick nimmt. Um einen Überblick über die datenschutzrechtlichen Kriterien liefern zu können, welche für die datenschutzkonforme Nutzung von KI-Anwendungen zu berücksichtigen sind, entwickelt der LfDI MV einen Handlungsleitfaden.

In unserer täglichen Beratungspraxis zeigte sich auch in diesem Berichtszeitraum, dass es regelmäßig an verbindlichen Vorgaben zur Nutzung von KI-Anwendungen sowie deren Grenzen fehlt. Eine Strategie zum Umgang mit KI wurde von Seiten der Landesregierung mittlerweile angekündigt, liegt aber noch nicht vor. Insbesondere mit Blick auf strategische Ziele und die darauf aufbauenden Handlungsfelder ist eine solche Strategie erforderlich. Derzeit ist zu beobachten, wie sich die Ressorts einzeln auf den Weg machen, um den Einsatz von KI auszugestalten. In diesem Zusammenhang treffen wir regelmäßig auf die Problemlage hinsichtlich der Trainings von KI-Modellen mit Daten von Trägern der öffentlichen Verwaltung und insbesondere auch von personenbezogenen Daten und den hierfür nicht vorhandenen Rechtsgrundlagen.

Festzuhalten bleibt, dass die Empfehlungen, die wir bereits im 15. Tätigkeitsbericht an die Landesregierung abgegeben haben, weiterhin Bestand haben. So wiesen wir darauf hin, dass bereits bei den Planungen zum Einsatz von KI-Systemen die damit verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen sorgfältig zu analysieren und die Risiken beim Betrieb derartiger Systeme durch technische und organisatorische Maßnahmen (TOM) auf ein verantwortbares Maß zu reduzieren sind. Diese Empfehlungen haben nach wie vor ihre Gültigkeit.

Wir empfehlen der Landesregierung, bereits bei den Planungen zum Einsatz von KI-Systemen die damit verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen sorgfältig zu analysieren und die Risiken beim Betrieb derartiger Systeme durch technische und organisatorische Maßnahmen auf ein verantwortbares Maß zu reduzieren. Gleichzeitig empfehlen wir der Landesregierung, in einer IT-Strategie darzulegen, wie der zukünftige Einsatz von KI in der Landesregierung ausgestaltet sein sollte. Hierzu bedarf es mit Blick auf den Einsatz und das Training von KI-Modellen auch flankierender rechtlicher Rahmenbedingungen, in denen auch geregelt wird, wo die Grenzen einer Nutzung liegen.

3.3. Cybersicherheit

Der LfDI MV hat bereits im vergangenen Tätigkeitsbericht über die konstant hohe Anzahl an Datenpannenmeldungen (Art. 33 DS-GVO „Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörden“) berichtet.

Im Berichtszeitrum hat die Anzahl an Datenpannenmeldungen ihr konstant hohes Niveau beibehalten (vgl. 1. Zahlen und Fakten), insbesondere mit Blick auf die weiterhin hohe Anzahl an Ransomware-Attacken. Bei dieser Form der Kriminalität werden die Daten des Opfers verschlüsselt und das Opfer anschließend mit einem nicht unerheblichen Lösegeld (englisch: Ransom) erpresst[1].

Durch den Angriffskrieg von Russland auf die Ukraine hat sich die IT-Sicherheitslage jedoch insgesamt noch weiter verschärft. So hat das BSI die Gefährdung in seinen letzten beiden Lageberichten[2] wie folgt auf den Punkt gebracht: „Die Gefährdungslage im Cyberraum ist so hoch wie nie.“ Diese Einschätzung können wir auf Grundlage der bei uns eingegangenen Meldungen und Anfragen von Bürger:innen sowie von Unternehmen und öffentlichen Einrichtungen unterstreichen.

In einer gemeinsamen Pressemitteilung[3] mit dem Landeskriminalamt Mecklenburg-Vorpommern (LKA M-V) haben wir bereits frühzeitig vor möglichen Cyber-Angriffswellen auf Einrichtungen und Unternehmen im Land sowie vor Betrugsversuchen bei den Bürger:innen gewarnt und zur Erhöhung der IT-Sicherheit aufgerufen. Es zeigt sich dabei regelmäßig, dass eine große Anzahl an Vorfällen mit den gängigsten Maßnahmen hätte verhindert werden können. Hierzu zählen insbesondere das zeitnahe Einspielen aktueller Sicherheitsupdates und regelmäßiger Backups der Daten und Konfigurationen. Ein weiterer wichtiger Baustein ist das Sensibilisieren von Mitarbeitenden, gerade im Umgang mit E-Mails und Passwörtern.

Im Rahmen unserer vielfältigen Aktivitäten zur Sensibilisierung und Erhöhung der IT-Sicherheit im Land waren wir als Sachverständige im Ausschuss für Inneres, Bau und Digitalisierung des Landtages Mecklenburg-Vorpommern eingeladen und berichteten zum Thema „Cyberkriminalität verhindern – Mecklenburg-Vorpommerns kritische Infrastruktur vor Angriffen aus dem Netz schützen[4]“. Zudem war der LfDI MV bei der IT Sicherheitskonferenz in Stralsund eingeladen, um einen Vortrag über die Auswirkungen von Cyberangriffen und Abwehrmaßnahmen mit Blick auf den Datenschutz zu halten. Im Berichtszeitraum beteiligten wir uns weiterhin an der gemeinsamen Veranstaltungsreihe „Roadshow Kommunen“, die vom BSI und dem Ministerium für Inneres, Bau und Digitalisierung M-V organisiert wurde.

1 Vgl. Punkt 4.2 in URL: https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Taetigkeitsberichte/lfdmvtb17.pdf [abgerufen am 22.02.2024]

2 URL: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/221025_Lagebericht.html https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html [abgerufen am 22.02.2024]

3 URL: https://www.datenschutz-mv.de/presse/?id=178879&processor=processor.sa.pressemitteilung [abgerufen am 22.02.2024]

4 URL: https://www.landtag-mv.de/fileadmin/media/Dokumente/Parlamentsdokumente/Drucksachen/8_Wahlperiode/D08-0000/Drs08-0249.pdf [abgerufen am 22.02.2024]

Hierbei zeigte sich noch einmal sehr deutlich, wie unterschiedlich die Kommunen im Bereich der IT-Sicherheit aufgestellt sind. So erbringen diese durchschnittlich 80 Prozent der Verwaltungsleistungen und beherbergen dafür eine hohe Anzahl an teils auch sehr sensiblen personenbezogenen Daten von Bürger:innen, z. B. Daten zum Kindergeld und dem Wohnsitz oder Steuerunterlagen. Doch unabhängig von ihrer teils sehr unterschiedlichen Größe und finanziellen Ausstattung müssen alle dasselbe hohe IT-Sicherheitsniveau gewährleisten können. Es ist offensichtlich, dass dies in der heute ausgeprägten digitalen Arbeitswelt, gepaart mit einer stetig zunehmenden Digitalisierung von Verwaltungsleistungen, ohne ausreichende Unterstützung durch das Land kaum noch zu bewältigen ist. Hierzu zählt einerseits eine ausreichende finanzielle und personelle Ausstattung, aber insbesondere auch das Angebot an Schulungen für Administrator:innen und mit der IT-Sicherheit beauftragte Personen. Als ebenso unerlässlich sieht der LfDI MV die Stärkung des Computer-Notfallteams des Landes, dem Computer Emergency Response Team MV (CERT MV) und dessen Befugnissen an, um auch im kommunalen Bereich ausreichend tätig werden zu können. Hierzu zählt neben der wichtigen Arbeit in der Prävention und tagesaktuellen Analyse vor allem auch die Unterstützungsleistung für den Fall erfolgreicher Angriffe auf die IT-Infrastruktur selbst.

Um ein möglichst genaues Bild zur Lage des Datenschutzes und der IT-Sicherheit im kommunalen Bereich zu gewinnen und insbesondere auch, um den Bedarf und Wunsch an notwendigen und zielgerichteten Unterstützungsleistungen zu ermitteln, startete der LfDI MV im Berichtszeitraum eine umfassende Befragung der Kommunen. Hierbei wurden zielgerichtet Fragestellungen ausgewählt, die zeitgleich bei der Planung und Umsetzung der Anforderungen an die Informationssicherheit und den Datenschutz unterstützend wirken können. Der LfDI MV plant, die Ergebnisse der Umfrage in 2024 veröffentlichen zu können.

Wir empfehlen der Landesregierung, sich weiterhin für eine Stärkung der IT-Sicherheit einzusetzen und vorhandene Strukturen und Unterstützungsleistungen auszuweiten, insbesondere mit Blick auf den kommunalen Raum. Zudem empfehlen wir eine Stärkung des CERT MV sowie dessen Befugnissen.

3.4. Gesetz zur Errichtung des Landesamtes Zentrum für Digitalisierung M-V

In der Koalitionsvereinbarung 2021-2026[1] wurde festgehalten, dass der IT-Betrieb der Landesverwaltung nach den Grundsätzen der Homogenisierung, Standardisierung und Zentralisierung sowie der Nachhaltigkeit („Green IT“) aufgestellt werden soll. Neben der Einführung des standardisierten IT-Arbeitsplatzes (MV-PC) in allen Landesbehörden sollen die Ressorts und nachgeordneten Behörden auch dadurch entlastet werden, dass der IT-Betrieb innerhalb der Landesverwaltung zentralisiert wird. Zu diesem Zweck wurde das Landesamt Zentrum für Digitalisierung Mecklenburg-Vorpommern (ZDMV) errichtet.

Mit dem Gesetz zur Errichtung des Landesamtes Zentrum für Digitalisierung Mecklenburg-Vorpommern (Errichtungsgesetz ZDMV – ZDMVG) wurde dafür im Berichtszeitraum die notwendige Rechtsgrundlage geschaffen. Wir nutzten dabei im Rahmen der Ressortanhörung mehrfach die Gelegenheit zur Stellungnahme und zum Einbringen von Verbesserungsvorschlägen.

Grundsätzlich begrüßen wir die Errichtung des ZDMV, denn neben den entstehenden Synergieeffekten kann eine Zentralisierung auch genutzt werden, um eine IT-Strategie des Landes zu entwickeln, damit einhergehend einheitliche IT-Landesstandards durchzusetzen und insbesondere auch die im Koalitionsvertrag angestrebte digitale Souveränität umzusetzen. So kann von zentraler Stelle aus die aktuelle Abhängigkeit von proprietärer Software Stück für Stück reduziert und bei künftigen Software-Anschaffungen bzw. -Aufträgen verstärkt auf Open-Source-Produkte sowie Open-Source-Lizenzen gesetzt werden.

Weiterhin kann mit Blick auf die stetig zunehmenden Beratungsleistungen des LfDI MV zu unterschiedlichsten IT-Projekten im Land eine Zentralisierung auch die beratende und unterstützende Arbeit unserer Behörde erleichtern, wenn wir frühzeitig zu übergreifenden strategischen Anliegen gegenüber einer zentralen Einrichtung Stellung nehmen können. Aus diesem Grund haben wir auch explizit darum geworben, eine zentrale Datenschutz-Compliance Stelle beim ZDMV zu schaffen, mit einer den Datenschutz koordinierenden Person bei der jeweiligen Stelle vor Ort. Zudem könnten Datenschutzexpert:innen des ZDMV schon frühzeitig die datenschutzrechtlichen Aspekte neuer Fachverfahren und Projekte in den Blick nehmen und den aus der DS-GVO in Artikel 25 geforderten Privacy-by-Design und Privacy-by-Default Anforderungen Rechnung tragen oder bei der Erstellung der notwendigen Dokumentation mitwirken. Zudem entspricht die Schaffung einer Datenschutz-Compliance Stelle einem in unserer Beratungspraxis mehrfach geäußerten Wunsch öffentlicher Stellen, einen gemeinsamen Datenschutzbeauftragten etwa für mehrere nachgeordnete Behörden zu bestellen.

1 URL: https://spd-mvp.de/uploads/spdLandesverbandMecklenburgVorpommern/Downloads/Koalitionsvertrag-SPD-DIE-LINKE-MV-2021-2026.pdf [abgerufen am 22.02.2024]

Hier muss jedoch berücksichtigt werden, dass die mit diesem Wunsch verfolgten Ziele nicht mit einem gemeinsamen Datenschutzbeauftragten, sondern nur mit einer zentralen Datenschutz-Compliance Stelle erreicht werden können. Die Aufgaben des Datenschutzbeauftragten sind in Art. 39 der DS-GVO normiert und bestehen vor allem in der Kontrolle und Beratung. Damit unvereinbar wäre es, den Datenschutzbeauftragten, der stets weisungsfrei handelt, damit zu beauftragen, etwa Verzeichnisse über Verarbeitungstätigkeiten (Art. 30 DS-GVO), Informationen nach Art. 13 DS-GVO oder Datenschutz-Folgenabschätzungen (Art. 35 DS-GVO) zu erstellen. Diese Aufgaben darf der Datenschutzbeauftragte beratend begleiten, keinesfalls kann er aber dafür zuständig sein, dem Verantwortlichen obliegende datenschutzrechtliche Pflichten zu erfüllen.

Zwar ist die Gesetzgebung unserem Vorschlag nicht wörtlich gefolgt und hat die Begrifflichkeit der Datenschutz-Compliance Stelle nicht aufgegriffen. Dennoch lässt die Formulierung der Aufgabe des ZDMV in § 3 Abs. 1 Nr. 4 „Sicherstellung der Informationssicherheit und des Datenschutzes in der Landesverwaltung sowie Bereitstellung von Informationssicherheits- und Datenschutzbeauftragten für die Behörden des Landes“ die Möglichkeit offen, dass gerade nicht nur der Datenschutzbeauftragte gestellt wird, sondern auch der notwendige Unterbau im ZDMV vorhanden ist. Denn nur so können die angesprochenen Unterstützungsleistungen erbracht werden, insbesondere auch die Umsetzung der von uns ebenfalls geforderten Anwendung des SDM[1] und des IT-Grundschutzes[2] des BSI. Beide Standards sind etabliert und ermöglichen eine geeignete und angemessene Auswahl, Bewertung und Dokumentation von technischen und organisatorischen Maßnahmen anhand der vorhandenen Risiken. Dies gewährleistet einerseits die Identifizierung der notwendigen Maßnahmen zum Datenschutz und zur IT-Sicherheit sowie den gesetzlich notwendigen Nachweis ihrer angemessenen Umsetzung. Andererseits ermöglichen sie der Datenschutz-Aufsichtsbehörde und eben auch den Datenschutz- und IT-Sicherheitsbeauftragten vor Ort eine Kontrolle der Maßnahmen bereits anhand einer hinreichenden und vor allem prüffähigen Dokumentation.

1 URL: https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode-V30a.pdf [abgerufen am 22.02.2024]

2 URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html [abgerufen am 22.02.2024]

3.5. Sicherheit bei der Übertragung von E-Mails beim LfDI MV

Im vergangenen Berichtszeitraum erreichte uns eine Anfrage zur Umsetzung der Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“[1] in der eigenen Behörde. Wir bieten dabei mehrere Wege für eine sichere Kommunikation an, die abhängig vom Risiko gewählt werden können und einen angemessen Schutz darstellen.

Grundsätzlich ist es so, dass Daten, die im Klartext über das Internet transportiert werden, weitgehend ungeschützt sind. Überall entlang des Übertragungsweges können sie mitgelesen oder sogar verfälscht werden, zum Beispiel von den Betreibenden der Zwischenstationen oder von extern Angreifenden. Dabei weiß die absendende Person in der Regel nicht einmal, welchen Weg die Nachrichten nehmen werden.

Für eine sichere Kommunikation mit unserer Dienststelle bieten wir daher mehrere Möglichkeiten an, z. B. die Ende-zu-Ende Verschlüsselung in Form von Pretty Good Privacy (PGP). Der dafür benötigte öffentliche Schlüssel kann auf unserer Webseite bezogen werden[2]. Zudem sind dort weitere Informationen zum Einsatz von PGP zu finden. Weiterhin gibt es auf unserer Seite mehrere Formulare, die online ausgefüllt werden können und uns dann ebenfalls auf verschlüsseltem Wege erreichen.

Dennoch nahmen wir die Anfrage zum Anlass, um das Schutzniveau und die Absicherung unserer E-Mailkommunikation weiter zu erhöhen. Hierzu tauschten wir uns mehrfach mit unserem Dienstleister, dem Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH (DVZ), welcher zugleich auch der IT-Dienstleister der Landesregierung ist, aus und führten diverse Verbesserungen durch.

Hierzu zählt zum einen die Einrichtung von Domain Name System Security Extensions (DNSSEC). DNSSEC ist eine Sicherheitserweiterung für das Domain Name System (DNS), die verwendet wird, um Domainnamen in IP-Adressen aufzulösen. DNSSEC schützt insbesondere vor Cache Poisoning, also einer Umleitung des Datenverkehrs an gefälschte IP-Adressen und der Fälschungen von Antworten. Derartige Umleitung können insbesondere dazu genutzt werden, um Phishing-Angriffe (z. B. das Abfangen von vertraulichen Informationen) durchzuführen oder Benutzer:innen auf schädliche Webseiten umzuleiten, die wiederum versuchen, Malware (bösartige Software) zu verbreiten oder weitere Angriffe auszuführen.

Weiterhin implementierten wir mit DomainKeys Identified Mail (DKIM) einen Mechanismus zur E-Mail-Authentifizierung. DKIM wird dazu verwendet, die Authentizität von E-Mails mit Hilfe digitaler Signaturen zu überprüfen. Hierdurch kann sichergestellt werden, dass eine E-Mail von einer authentischen Absendeadresse stammt und während der Übertragung nicht manipuliert wurde. Somit können insbesondere auch gefälschte E-Mails erkannt und E-Mail-Spoofing (gefälschte Absenderadresse) sowie Phishing bekämpft werden.

1 URL: https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Broschueren/20210616_OH_E-Mail.pdf [abgerufen am 27.02.2024]

2 URL: https://www.datenschutz-mv.de/datenschutzerklaerung/#email [abgerufen am 27.02.2024]

Zusammen mit DKIM richteten wir zudem Domain-based Message Authentication, Reporting and Conformance (DMARC) ein. DMARC ermöglicht es, genaue Richtlinien zu setzen, wie die E-Mails von der eigenen Domain (in unserem Fall „datenschutz-mv.de“) von E-Mail-Empfänger:innen behandelt werden sollen. DMARC hilft insbesondere dabei, E-Mail-Spoofing und Phishing-Angriffe zu bekämpfen, indem es die Authentizität von E-Mails verbessert und Domaininhaber:innen mehr Kontrolle darüber gibt, wie ihre E-Mails behandelt werden. Darüber hinaus sorgt DMARC dafür, dass Domaininhaber:innen detaillierte Berichte über den Zustellstatus ihrer E-Mails erhalten. Diese Berichte beinhalten wiederum Informationen darüber, wie beim Empfangen mit E-Mails von ihrer Domain umgegangen wurde und können dabei helfen, Fehlkonfigurationen festzustellen oder eine missbräuchliche Nutzung aufzudecken.

Schlussendlich implementierten wir mit Mail Transfer Agent Strict Transport Security (MTA-STS) einen Mechanismus zur Verbesserung der Sicherheit und Integrität von E-Mail-Übertragungen. Dieser zielt darauf ab, den Transport von E-Mails zwischen Mailservern sicherer zu machen, indem eine verschlüsselte Verbindung verwendet wird.

Auch hier können Berichte über den Status der Übertragung von E-Mails einschließlich Informationen darüber empfangen werden, ob die MTA-STS-Richtlinien ordnungsgemäß implementiert und durchgesetzt wurden. Dies ermöglicht es Domaininhaber:innen, Probleme zu identifizieren und zu beheben, die eine Zustellung der E-Mails beeinträchtigen können.

Auf Grundlage der positiven Erfahrungen im Rahmen der Einführung und des Betriebes der genannten Verfahren, insbesondere in der Zusammenarbeit mit der DVZ, haben wir uns dazu entschieden, zeitnah auch bei den Ministerien und nachgeordneten Behörden die Umsetzung der Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail zu prüfen.

Wir empfehlen der Landesregierung, die eigenen Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail zu prüfen und die angesprochenen Techniken ebenfalls zu implementieren.

3.6. Einsatz von Videokonferenzsystemen

Wir haben bereits in den vergangenen Berichtszeiträumen über den Einsatz von Videokonferenzsystemen berichtet[1].

Auch in diesem Berichtszeitraum gab es eine hohe Anzahl an Beratungsersuchen und Anfragen zu diesem Thema. Dies ist mit Blick auf die sich inzwischen weiträumig etablierten Möglichkeiten des mobilen Arbeitens, sowohl im öffentlichen als auch nicht-öffentlichen Bereich, wenig überraschend. Während im letzten Berichtszeitraum einer unserer Schwerpunkte auf der Behebung der oft mangelhaften oder nicht vorhandenen Informationspflicht gemäß Artikel 13 DS-GVO lag, richteten wir nun verstärkt den Blick auf die Anwendungen an sich. Dies ist nur folgerichtig, da die von uns aus der Corona-Pandemie geduldete Übergangsphase in Bezug auf die Nutzung von Videokonferenzdiensten, die ihre Datenschutzkonformität noch nicht nachweisen konnten, nicht mehr angenommen werden kann. Folglich trägt die bisherige Argumentation, wonach nur wenige, vorrangig US-amerikanische Anbieter in der Lage sind, Videokonferenzen stabil auf einem technisch hohen Niveau auszurichten, immer weniger. Uns gegenüber wurde dabei regelmäßig mit der Notwendigkeit einzelner Anwendungsmerkmale argumentiert. Demnach konnten nur einige wenige Anbieter die benötigten Features vorhalten, wie z. B. eine rein browserbasierte Teilnahmemöglichkeit, schnelle Einrichtungen, telefonische Zuschaltungsmöglichkeiten, sehr hohe Teilnehmendenzahlen, ausgeblendeter Videohintergrund oder integrierte Chatmöglichkeiten. Inzwischen hat sich der Markt jedoch auf die veränderte Arbeitswelt eingestellt und es haben sich viele weitere europäische Anbieter etabliert bzw. ihr Angebot entsprechend weiterentwickelt. Darunter sind auch viele Angebote entstanden, die auf Basis von Open-Source die digitale Souveränität besonders fördern[2].

Diesbezüglich führten wir im Berichtszeitraum auch mit der Landesregierung mehrfach beratende Gespräche und versuchten, auf eine schnellstmögliche Ablösung der derzeitig im Einsatz befindlichen Videokonferenzlösung hinzuwirken. Der Einsatz einer datenschutzkonformen Lösung würde nicht zuletzt auch die digitale Souveränität wahren und die aktuell im Land bestehende hohe Abhängigkeit von rein US-amerikanischen Hersteller:innen bzw. Anbieter:innen reduzieren. Dies erscheint uns insbesondere vor dem Hintergrund von sich auch im Land bereits etablierten Lösungen, die Ihre Praxistauglichkeit inzwischen umfassend nachgewiesen haben, kurzfristig umsetzbar zu sein. Für uns ist die bisherige Argumentationslinie der Landesregierung, dass eine Umstellung der pandemiebedingt gewählten Variante auf eine datenschutzkonforme Lösung sowohl aus kapazitiven als auch aus vergaberechtlichen Gründen nicht sofort umgesetzt werden könne, nicht mehr nachvollziehbar.

1 Vgl. u. a. Punkt 4.6 in URL: https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Taetigkeitsberichte/lfdmvtb17.pdf [abgerufen am 27.02.2024]

2 Vgl. Punkt 4.3.4 in URL: https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Taetigkeitsberichte/lfdmvtb16.pdf [abgerufen am 27.02.2024]

So zeigt bspw. das Ministerium für Bildung und Kindertagesförderung des Landes Mecklenburg-Vorpommern (BM MV) mit einer für die Schulen kostenlos verfügbaren Lösung auf Basis des Open-Source Tools „Big Blue Button“[1], dass Videokonferenzsysteme und deren datenschutzkonforme Ausgestaltung durchaus Hand in Hand gehen können. Auch der Landtag setzt inzwischen erfolgreich eine Videokonferenzlösung auf Basis des Open-Source Tools „Jitsi Meet“ ein, die zudem vom schleswig-holsteinischen IT-Landesdienstleister Dataport im Rahmen des dortigen Phoenix Projektes[2] zur Entwicklung eines digital souveränen Arbeitsplatzes betrieben wird.

Wir empfehlen der Landesregierung, das derzeit eingesetzte Videokonferenzsysteme schnellstmöglich gegen eine datenschutzkonforme Lösung auf Basis von Open-Source zu ersetzen.

3.7. Datenschutz und Schule

Um den Datenschutz im Schulbereich stetig zu verbessern, befindet sich der LfDI MV in regelmäßigem Austausch mit verschieden Akteur:innen. Hierbei stehen Themen rund um die Digitalisierung von Schule als auch grundsätzliche datenschutzrechtliche Fragestellungen im Fokus. Im Zuge der voranschreitenden Digitalisierung des Schulbereichs kristallisiert sich zunehmend heraus, dass alte Strukturen datenschutzrechtlicher Verantwortlichkeit durch die Beteiligten überdacht werden sollten. So könnten Wege gefunden werden, wie man den Herausforderungen rund um die Bereitstellung von digitalen Lern- und Lehrmitteln als auch der Bereitstellung von Verwaltungssoftware begegnen kann. Der nachfolgende Berichtsabschnitt vermittelt einen Einblick in die Arbeit des LfDI MV im Bereich Datenschutz und Schule in den Berichtsjahren.

3.7.1. Auftragsverarbeitung und Digitalisierung im Bereich Schule

In der täglichen Praxis begegnen uns im Bereich Schule immer wieder Fragen rund um die Auftragsverarbeitung und die datenschutzrechtliche Verantwortung. Wir möchten dies zum Anlass nehmen, die Sicht des LfDI MV zu diesem Thema darzustellen.

Grundsätzlich kommt eine Datenverarbeitung im Auftrag in Betracht, wenn der Verantwortliche eine geplante Datenverarbeitung nicht selbst durchführen kann oder möchte. Die Gründe, sich eines Auftragsverarbeiters zu bedienen, können dabei vielfältig sein. Grundvoraussetzung für eine Datenverarbeitung im Auftrag ist, dass der Verantwortliche über eine entsprechende Rechtsgrundlage zur Datenverarbeitung der Betroffenendaten verfügt. Im Bereich Schule ergibt sich diese regelmäßig aus dem Schulgesetz für das Land Mecklenburg-Vorpommern (SchulG M-V) und dem normierten Bildungs- und Erziehungsauftrag der Schulen. Außerdem muss die Verarbeitung der Betroffenendaten erforderlich sein. Verantwortlicher im Sinne des Datenschutzrechts ist derzeit die Schulleitung.

1 URL: https://www.bildung-mv.de/schule-digital/schulmanagementsystem-isy-mv/itslearning/ [abgerufen am 27.02.2024]

2 URL: https://www.dataport.de/pressemitteilung/dataport-bringt-open-source-arbeitsplatz-phoenix-heraus/

Kann der Verantwortliche, im Bereich der Schule also die Schulleitung, die Datenverarbeitung auf eine entsprechende Rechtsgrundlage stützen, darf dieser sich für die Durchführung auch eines Auftragsverarbeiters bedienen. Der Auftragsverarbeiter benötigt dann keine eigene Rechtsgrundlage zur Datenverarbeitung, wenn er die Daten ausschließlich auf Weisung des Verantwortlichen verarbeitet. Um diese Möglichkeit der Verarbeitung von personenbezogene Daten nutzen zu dürfen, ist es erforderlich, dass der Verantwortliche einen Vertrag zur Auftragsverarbeitung gemäß Artikel 28 Abs. 3 DS-GVO mit dem Auftragsverarbeiter abschließt. Im Rahmen der Digitalisierung des Schulbereichs hat der LfDI MV die Erfahrung gesammelt, dass Schulleitungen hier regelmäßig auf große Herausforderungen in der Vertragsgestaltung zur Auftragsverarbeitung stoßen, welchen sie nur mit unverhältnismäßig hohem Aufwand begegnen können. Dies betrifft nicht nur die vertraglichen Bedingungen hinsichtlich des Weisungsrechts gegenüber dem Auftragsverarbeiter, sondern auch die Einschätzung, ob durch den Auftragsverarbeiter zugesicherte TOMs angemessen und geeignet sind, um die Daten der Betroffen datenschutzgerecht zu verarbeiten. Durch das verbreitete Aufkommen von KI und LLM müssen sich nun auch Schulleitungen mit diesem Thema auseinander setzen und dies in den Verträgen zur Auftragsverarbeitung berücksichtigen (siehe Punkt 3.2.).

Die vorangegangenen Ausführungen zeigen, dass Schulleitungen im Bereich des Datenschutzes vor immer größer werdenden Herausforderungen stehen. Im Zuge des Digitalpakts Schule wird von allen Beteiligten stetig daran gearbeitet, die Digitalisierung an Schulen schnell voran zu bringen. Dabei werden auch Softwarelösungen, welche zumeist über Auftragsverarbeitende realisiert werden, seitens des Ministeriums für Bildung und Kindertagesförderung MV zentral bereitgestellt. Dies stellt auch aus unserer Sicht eine Entlastung für die Schulleitungen dar und sollte ebenfalls zum Anlass genommen werden, um die generelle Zuweisung der datenschutzrechtlichen Verantwortung der Schulleitungen zu prüfen. Denn aus datenschutzrechtlicher Sicht steht einer zukünftig schnelleren Umsetzung der Digitalisierung von Schule in Mecklenburg-Vorpommern entgegen, dass es im Bereich Schule zu viele Entscheidungsträger:innen hinsichtlich deren digitalen Ausstattung gibt. Eine Verschiebung zu zentralisierten Beschaffungsstrukturen sowie eine Verschiebung hin zu zentraler datenschutzrechtlicher Verantwortlichkeit im Bereich Schule würden die Schulleitungen deutlich entlasten. Somit könnten diese dann besser ihrem gesetzlichen Erziehungs- und Bildungsauftrag nachkommen und den Einsatz von digitalen Lehrmitteln im Unterricht planen, anstatt sich mit der Beschaffung von digitalen Lehrmitteln und den damit verbundenen datenschutzrechtlichen Fragestellungen auseinandersetzen zu müssen.

Wir empfehlen der Landesregierung, hinreichend zu prüfen, ob im Zuge der zentralen Beschaffung und Bereitstellung von digitalen Lösungen eine Neuausrichtung der datenschutzrechtlichen Verantwortung von Schulleitungen hin zu zentraler datenschutzrechtlicher Verantwortlichkeit denkbar ist.

3.7.2. Integriertes Schulmanagementsystem ISY MV

Im vorliegenden Berichtszeitraum führte der LfDI MV die Beratungen mit dem BM MV zum Projekt Integriertes Schulmanagementsystem (ISY MV) fort[1].

Im aktuellen Berichtszeitraum wurde das Thema der Einbindung von kooperativen Erziehungs- und Bildungsangeboten nach § 59 a Schulgesetz MV in die bestehende E-Learning Plattform des Landes weiter vertieft und mündete in einer zufriedenstellenden Zwischenlösung für die Beteiligten. Weiterhin wurde die Integration von Lehrkräften öffentlicher Schulen sowie derer in freier Trägerschaft in die Fort- und Weiterbildungsangebote des Instituts für Qualitätsentwicklung Mecklenburg-Vorpommern besprochen (IQ MV). Bei der Einführung einer Schulverwaltungssoftware in das Schulmanagementsystem wurde ebenfalls die Einbindung von Schulen in freier Trägerschaft thematisiert. Einen weiteren inhaltlichen Schwerpunkt der Gespräche bildeten die Datenschutz-Folgenabschätzung (DSFA) bezüglich der E-Learning Plattform des Landes und die Einbindung von Lehramtsstudierenden in diese bestehende E-Learning Plattform. Neben diesen wichtigen Punkten konnten auch erneut diverse Grundsatzfragen hinsichtlich des Datenschutzes erörtert werden, z. B. bezüglich der Ausgestaltung des über die E-Learning Plattform bereitgestellten Open Source Videokonferenzdienstes. Der Austausch mit dem BM M-V sowie mit den weiteren Gesprächsteilnehmer:innen, wie dem Zweckverband elektronische Verwaltung Mecklenburg-Vorpommern (eGo MV), wird seitens unserer Behörde regelmäßig als sehr konstruktiv und produktiv wahrgenommen.

Wir empfehlen dem Ministerium für Bildung und Kindertagesförderung des Landes Mecklenburg-Vorpommern, den Austausch mit unserer Behörde zum Projekt ISY MV weiter fortzuführen.

3.8. Telemedien

Im vorangegangen Berichtszeitraum wurde die Orientierungshilfe für Anbietende von Telemedien nach einem öffentlichen Konsultationsverfahren durch den Arbeitskreis Medien der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) überarbeitet. Weiterhin gab es neue Entwicklungen bei den Gesprächen zwischen der AG Microsoft-Onlinedienste der DSK und der Firma Microsoft. Im Folgenden berichtet der LfDI MV nun über den Stand der neuen Orientierungshilfe für Anbietende von Telemedien und über den Sachstand sowie die Ergebnisse aus den Gesprächen mit Microsoft.

1 Vgl. Punkt 5.2.1. in URL: https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Taetigkeitsberichte/lfdmvtb17.pdf [abgerufen am 27.02.2024]

3.8.1. Arbeitsgruppe Microsoft-Onlinedienste

Im vorliegenden Berichtszeitraum wurden die Gespräche zwischen der AG Microsoft-Onlinedienste und der Firma Microsoft beendet. Bei den Gesprächen standen die Online Services Terms (OST) und das dazugehörige Data Protection Addendum (DPA) der Firma Microsoft im Fokus. Hinter den Begriffen verbergen sich vertragliche Regelungen für die Bereitstellung eines Clouddienstes der Firma Microsoft, der beispielsweise die Bürosoftware Microsoft 365 mit Anwendungen wie Word, Excel oder PowerPoint beinhaltet. Die Datenverarbeitung findet dabei nicht auf den technischen Einrichtungen des datenschutzrechtlich Verantwortlichen, sondern auf denen der Firma Microsoft selbst statt. Wird der genannte Clouddienst vom Verantwortlichen zur Erfüllung seiner Aufgaben eingesetzt, ist ein Vertrag nach Art. 28 Abs. 3 DS-GVO erforderlich, da der Verantwortliche personenbezogene Daten durch die Firma Microsoft im Auftrag verarbeiten lässt. Weitere Informationen zur Historie der Gespräche mit Microsoft sowie zur AG Microsoft-Onlinedienste können unserem 16. und 17. Tätigkeitsbericht[1][2] entnommen werden.

Nach Beendigung der Gespräche zwischen der AG und Microsoft wurden der DSK die Arbeitsergebnisse in einem Abschlussbericht[3] vorgelegt. Die DSK äußerte sich zum Abschlussbericht am 24. November 2022 auf der 104. Datenschutzkonferenz in einer Festlegung[4]. Die DSK teilt in dieser Festlegung mit, dass der Nachweis von Verantwortlichen, Microsoft 365 datenschutzkonform zu betreiben, auf der Grundlage des von Microsoft bereitgestellten „Datenschutznachtrags vom 15. September 2022" nicht geführt werden kann. Dies gilt solange, bis insbesondere die notwendige Transparenz über die Verarbeitung personenbezogener Daten aus der Auftragsverarbeitung für Microsofts eigene Zwecke hergestellt wird und deren Rechtmäßigkeit belegbar ist. Im März 2023 traten wir aus der AG Microsoft-Onlinedienste aus, da die Grundsatzprobleme durch die AG ausreichend aufgezeigt wurden. Die AG Microsoft-Onlinedienste besteht jedoch weiterhin fort und beobachtet die Änderungen zu den vertraglichen Unterlagen hinsichtlich der Auftragsnehmereigenschaft von Microsoft.

Vor dem Hintergrund der Festlegung der DSK empfehlen wir allen Verantwortlichen in Mecklenburg-Vorpommern aus dem öffentlichen sowie aus dem nicht-öffentlichen Bereich, die bereits Onlinedienste von Microsoft (z. B. Microsoft 365 mit Word, Excel, PowerPoint) im Rahmen der Auftragsverarbeitung einsetzen oder deren Einsatz planen, zu prüfen, ob sie in der Lage sind, diese Produkte datenschutzgerecht einzusetzen. Prüfmaßstab ist aus aufsichtsbehördlicher Sicht die Festlegung der 104. DSK zu Microsoft 365 und der Abschlussbericht der Arbeitsgruppe. Insbesondere mit Blick auf die digitale Souveränität empfehlen wir den Verantwortlichen, den Einsatz alternativer Produkte zu prüfen, vorwiegend aus dem Open Source Bereich.

1 Vgl. URL: https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Taetigkeitsberichte/lfdmvtb16.pdf [abgerufen am 28.02.2024]

2 Vgl. URL: https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Taetigkeitsberichte/lfdmvtb16.pdf [abgerufen am 28.02.2024]

3 URL: https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf [abgerufen am 29.02.2024]

4 URL: https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365.pdf [abgerufen am 27.02.2024]

3.8.2. Orientierungshilfe für Anbietende von Telemedien

Um den Verantwortlichen datenschutzrechtliche Hilfestellungen beim Anbieten von Telemedien zu geben, hat die DSK die Orientierungshilfe für Anbietende von Telemedien entwickelt. Die Orientierungshilfe wurde mit Inkrafttreten des Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTDSG) überarbeitet. Hierzu berichteten wir bereits im vorangegangen 17. Tätigkeitsbericht[1].

Aufgrund der Bedeutung der Orientierungshilfe hat sich die DSK nach deren Herausgabe am 1. Dezember 2021 dazu entschieden, sie einem öffentlichen Konsultationsverfahren zu unterziehen. Die dabei erhaltenen Rückmeldungen und Anregungen wurden ausgewertet und anschließend der Öffentlichkeit in einem ausführlichen Auswertungsbericht[2] zugänglich gemacht. Auf der 104. Datenschutzkonferenz haben die Datenschutzaufsichtsbehörden des Bundes und der Länder die aktualisierte Version ihrer Orientierungshilfe für Anbietende von Telemedien[3] veröffentlicht. Die Version 1.1 (Stand Dezember 2022) berücksichtigt dabei die Ergebnisse des Konsultationsverfahrens und soll nun weitere Hilfestellungen für die datenschutzkonforme Ausgestaltung von Webseiten geben. Dabei steht der Einsatz von Cookies mit den Erfordernissen des § 25 TTDSG und denen des Art. 6 Abs. 1 DS-GVO im Vordergrund. Es werden verschiedene Anwendungsfälle betrachtet und das Zusammenspiel zwischen dem TTDSG und der weiteren Datenverarbeitung nach der DS-GVO erläutert.

Wir empfehlen den Anbietenden von Telemedien aus dem öffentlichen und nicht-öffentlichen Bereich, sich mit der neuen Version der Orientierungshilfe für Anbietende von Telemedien vertraut zu machen und ihre Telemediendienste auf Datenschutzkonformität sowie bezüglich des Einsatzes von Cookies nach dem TTDSG zu prüfen. Darauf aufbauend sollte geprüft werden, 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.

1 Vgl. Punkt 4.4. in URL: https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Taetigkeitsberichte/lfdmvtb17.pdf [abgerufen am 28.02.2024]

2 URL: https://www.datenschutzkonferenz-online.de/media/oh/20221205_oh_Auswertung_Konsultation_zur_Orientierungshilfe_fuer_Anbieter_von_Telemedien_final.pdf [abgerufen am 28.02.2024]

3 URL: https://www.datenschutzkonferenz-online.de/media/oh/20221205_oh_Telemedien_2021_Version_1_1_Vorlage_104_DSK_final.pdf [abgerufen am 28.02.2024]

3.9. Versendung von Newslettern ohne Einwilligung

Immer wieder erhalten wir Beschwerden von Bürger:innen über den Erhalt ungewollte Newsletter. Dabei muss grundsätzlich zwischen zwei Varianten unterschieden werden.

Bei der ersten Variante wurde ein Newsletter durch den Verantwortlichen an seine Kund:innen versendet. In diesem Fall informieren wir die Beschwerdeführer:innen darüber, dass der Versand von Werbe-E-Mails (Newslettern) an Kund:innen grundsätzlich möglich ist, sobald die Kund:innen dem Verantwortlichen ihre E-Mail-Adresse zur Verfügung gestellt haben (gem. Art. 6 Abs. 1 lit. f DS-GVO, Erwägungsgrund (EG) 47 der DS-GVO, i.v.m. § 7 Abs. 3 Gesetz gegen den unlauteren Wettbewerb (UWG)). Eine gesonderte Einwilligung wird in diesem Fall nicht benötigt. Sollten Kund:innen hiergegen allerdings bereits Widerspruch (gem. Art. 21 Abs. 2 DS-GVO) eingelegt haben, so ist der Versand von Werbe-E-Mails nachfolgend unzulässig.

In einer zweiten Variante kommt es zur Versendung von Newslettern an dritte Personen, die nicht Kund:innen des Verantwortlichen sind. In diesem Fall muss dem Verantwortlichen für eine Versendung des Newsletters die Einwilligung des Empfängers vorliegen. Diese Einwilligung kann mit einem Double-Opt-In-Verfahren eingeholt werden.

Beim Double-Opt-In-Verfahren muss zuerst die Aufnahme in den Newsletter-Verteiler beim Verantwortlichen „beantragt" werden. In den meisten Fällen ist dazu die Angabe der E-Mail-Adresse auf der Internetseite des Verantwortlichen ausreichend. Im zweiten Schritt erhält der oder die Interessierte eine E-Mail mit der Aufforderung, den soeben beantragten Newsletter mit einem Klick auf einen Bestätigungslink zu bestätigen. Wird dieser Link dann bestätigt, erhalten die interessierten Personen den Newsletter und der Verantwortliche kann gleichzeitig deren Einwilligung nachweisen. Wird der Link jedoch nicht bestätigt, ist die Versendung des Newsletters unzulässig.

Möchten die Empfänger:innen zukünftig doch keine Werbe-E-Mails mehr erhalten, ist es bei beiden Varianten nötig, dem Erhalt des Newsletters gem. Art. 21 Abs. 2 DS-GVO zu widersprechen. In den meisten Fällen wird dazu am Ende eines Newsletters ein Funktionsbutton zur Abmeldung bereitgestellt. Dieser stellt eine einfache Form des Widerspruchs dar.

Werden Verstöße gegen die hier beschriebenen Vorgehensweisen beim Versenden von Newslettern durch uns als Datenschutzaufsichtsbehörde festgestellt, stehen uns verschiedene Sanktionsmöglichkeiten gemäß Art. 58 Abs. 2 DS-GVO zur Verfügung, die bis hin zum Ordnungswidrigkeitenverfahren reichen.

4. Bildungsauftrag der Behörde

Die DS-GVO gibt unserer Behörde als zentrale Aufgabe die „Sensibilisierung und Aufklärung der Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten" nach Artikel 57 Abs. 1 lit. b. Die DS-GVO hebt in diesem Zusammenhang ausdrücklich die Notwendigkeit spezifischer Maßnahmen für Kinder hervor und führt im Erwägungsgrund 132 dazu weiter aus, dass jede Datenschutzaufsichtsbehörde Sensibilisierungsangebote auch an Personen im Bildungsbereich adressieren soll. Der selbstbestimmte Umgang mit seinen eigenen Daten und den Daten Anderer sowie die digitalen Kompetenzen gehören heutzutage zum notwendigen Grundwissen. Dieser Aufgabe kommt der LfDI MV bereits seit mehr als zwölf Jahren nach.

Neben Projekttagen und Workshops für Schüler:innen bieten wir auch Weiterbildungen zu Themen der Medienbildung für Lehrer:innen, pädagogische Fachkräfte sowie Erzieher:innen im ganzen Land an. Ebenso unterstützen wir die Einrichtungen z. B. bei Elternabenden, wenn es um das Thema Medien und Datenschutzbewusstsein in der Familie geht.

Bei all diesen Aufgaben arbeitet der LfDI MV mit vielen verschiedenen starken Partnern in unserem Land zusammen. Im landesweiten Netzwerk der Medienbildung „Medienaktiv M-V" nimmt der LfDI MV eine wichtige Rolle ein. Hier organisieren wir u. a. Fachtagungen für pädagogische Fachkräfte oder erarbeiten gemeinsame politische Forderungen zum Thema Medienbildung für unser Bundesland.

Auch im vorliegenden Berichtszeitraum führte der LfDI MV mit den „Medienscouts MV" und den „Medienguides MV" seine selbst initierten und bereits seit mehreren Jahren etablierten, landesweiten Bildungsprojekte erfolgreich durch. Neben diesen eigenen Angeboten unterstützte der LfDI MV auch Veranstaltungen und Tagungen anderer Ressorts fachlich mit Vorträgen und Workshops, wie z. B. die Kinder- und Jugendmedienschutztagungen des BM MV oder den Fachtag für Schülerzeitungsredakteur:innen des Ministeriums für Wissenschaft, Kultur, Bundes- und Europaangelegenheiten Mecklenburg-Vorpommern (WKM MV) zum Thema „Fake News & Deep Fakes". Ebenfalls nahmen wir schulartübergreifend an zahlreichen Schulprojekttagen teil und absolvierten eine Vielzahl an Klassenbesuchen im gesamten Bundesland, um die Medienkompetenz zu fördern.

Darüber hinaus gaben wir unsere Fachexpertise zur Anpassung der schulischen Rahmenplänen und der Ausgestaltung der Unterrichtsfächer mit Hinblick auf die Medienkompetenz gegenüber dem BM MV ab.

Der LfDI MV ist nicht erst seit dem Inkrafttreten des gesetzlich verankerten Bildungsauftrages der DS-GVO in 2016 eine der tragenden Säulen der Medienbildung in Mecklenburg-Vorpommern. Das folgende Kapitel gibt einen Überblick zu den von uns durchgeführten Bildungsangeboten und -formaten.

4.1. Medienscouts MV – Jugend klärt auf!

Im Berichtszeitraum führten wir unsere etablierten Veranstaltungen der „Medienscouts MV – Jugend klärt auf" (Medienscouts MV) im gewohnten Turnus, d. h. jeweils einmal im Frühjahr und einmal im Herbst, durch. Gemeinsam mit unseren Kooperationspartner:innen in diesem Projekt, also der Landeskoordinierungsstelle für Suchtthemen MV (LAKOST), dem LKA M-V, dem Landesjugendring Mecklenburg-Vorpommern e.V. (LJR M-V e.V.), der Landesmedienanstalt Mecklenburg-Vorpommern (MMV) und der ComputerSpielSchule Greifswald (CSG) bildeten wir erfolgreich weitere Generationen motivierter Medienscouts MV aus[1]. Das Ziel des Projektes ist es, engagierte Jugendliche im Umgang mit digitalen Medien fit zu machen, so dass sie ihr Wissen (nicht nur) an gleichaltrige Mediennutzer:innen weitergeben. Wissensvermittlung mit einem Peer-to-peer-Ansatz bedeutet, die gelernten Inhalte, neuen Erfahrungen und Tipps zum Umgang mit Medien anschließend auch im Freundeskreis, in der Familie oder in der Klassen bzw. der eignen Schule weiterzugeben. Zwischen Gleichaltrigen besteht oft ein ganz anderes Vertrauensverhältnis, wenn es um Aktivitäten im Netz und ganz besonders auch um negative Erfahrungen und Gefahren geht. Dementsprechend werden die Hinweise und Ratschläge der Medienscouts von Kindern und Jugendliche eher an- und ernstgenommen, als die Regeln, die von Erwachsenen oft mit dem erhobenen Zeigefinger ausgesprochen werden. Einige Medienscouts trauen sich sogar zu, Vorträge und Workshops für Eltern durchzuführen. Die Tipps aus Sicht der Jugendlichen kommen ebenfalls bei den Eltern besonders gut an, denn die Medienscouts MV denken und handeln als Jugendliche ebenso, wie das eigene Kind. Die Aktualität und Relevanz der Ausbildungsinhalte verdeutlichen gleichzeitig die Vorteile, einen Medienscout an der eigenen Schule zu haben. Themen wie Datensparsamkeit, Cybermobbing, Hass und Hetze im Netz, problematische Inhalte oder Kostenfallen in Games verlieren nicht an Brisanz, vielmehr nimmt die Menge an medialen Angeboten und damit das Risiko negativer Folgen bei mangelnder Medienkompetenz weiter zu. Über die Grenzen der eigenen Schule hinaus engagierten sich einige Medienscouts MV im Rahmen der Medienaktionstage des Projektes #Digitale Vorbilder (siehe Punkt 4.3.) im Herbst und Winter 2023, indem sie die Medienscouts MV dort vorstellten und anderen interessierten Kindern und Jugendlichen berichteten, was man als Medienscout MV alles lernen kann und wie ein Ausbildungswochenende abläuft.

Im Berichtszeitraum zeigte sich für uns nach über zehn Jahren der Durchführung zum ersten Mal in aller Deutlichkeit, wie wichtig die Möglichkeit für Jugendliche ist, ein Angebot wie die Medienscouts MV kostenfrei in Anspruch nehmen zu können. Nie zuvor haben wir im Vorfeld der Bildungswochenenden so viele Rückfragen zur Kostenerstattung von Fahrtkosten bzw. zur generell kostenfreien Teilnahme erhalten. Dies zeigt uns eindeutig, dass der finanzielle Hintergrund der Jugendlichen und ihrer Familien mehr und mehr eine elementare Rolle beim Zugang zu Bildungsangeboten und damit auch zu Formaten der Medienbildung spielt. Um die Chancengleichheit zu wahren ist es absolut notwendig, dass die Teilnahme an medienkompetenzfördernden Angeboten wie den Medienscouts MV für Jugendliche weiterhin kostenfrei möglich ist.

1 https://www.datenschutz-mv.de/presse/?id=189833&processor=processor.sa.pressemitteilung [abgerufen am 03.04.2024]

Projektjubiläum: 10 Jahre Medienscouts MV

Im Berichtszeitraum wurde zudem das 10-jährige Jubiläum von Medienscouts MV gefeiert. Das Projekt wurde 2012 vom LfDI MV initiiert und wird seither kontinuierlich von den gleichen Partner:innen unterstützt (siehe Punkt 4.1.). Anlässlich der Feierlichkeiten wurden bereits ausgebildete Medienscouts MV mehrerer Generationen des letzten Jahrzehnts zu einem Festempfang in das Digitale Innovationszentrum Schwerin (DIZ) eingeladen. Der Landedatenschutzbeauftragte sowie der Minister für Inneres und Digitalisierung Mecklenburg-Vorpommern begrüßten die anwesenden Medienscouts und Partner:innen des Projektes. Bei den Glückwünschen und Grüßen von Medienscouts der vergangenen Jahre wurde deutlich, wie engagiert die Jugendlichen waren und weiterhin sind. Das zahlreiche Erscheinen von Vertreter:innen aus Politik, Verwaltung und Schule zeigte den Jugendlichen die Wertschätzung für ihr Engagement. Dies bestärkt unsere Behörde, das Bildungsangebot auch weiterhin fortzusetzen und auszubauen. Neben der Bekanntheit innerhalb unseres Landes finden die Medienscouts MV als Projekt des LfDI MV auch große Beachtung im gesamten Bundesgebiet.

4.2. Medienguides MV – Eltern.Medien.Kompetenz

Im Berichtszeitraum konnte der LfDI MV den zweiten Durchgang des Eltern-Medien-Projektes „Medienguides MV" erfolgreich in Präsenz in Wismar durchführen, nachdem das Projekt in 2021 unter Corona-Bedingungen in einer hybriden Variante gestartet war. An zwei Samstagen lernten interessierte Eltern in jeweils ganztägigen Veranstaltungen alles zum Thema der Medienerziehung in der Familie. Hierbei wurden sie zu Themen wie dem sicheren Umgang mit den eigenen Daten und den Daten ihrer Kinder, nützlichen Einstellungen in Apps und auf Geräten, präventiven Maßnahmen gegen Cybergrooming in digitalen Spielen, Suchtgefahren, Mediennutzungszeiten und Mobbing aufgeklärt. Gemeinsam mit unseren Projektpartner:innen wie der LAKOST, dem LKA M-V und dem dazugehörigen Projekt „Helden statt Trolle", dem Kompetenzzentrum und Beratungsstelle für exzessive Mediennutzung und Medienabhängigkeit Schwerin der Evangelischen Suchtkrankenhilfe MV, der CSG sowie freien Medienpädagog:innen konnten wir alle Fachfragen beantworten. Vor allem konnten wir durch die vielen unterschiedlichen Perspektiven auf das Thema Mediennutzung in der Familie auch viele nützliche Tipps und praktische Hinweise für den Familienalltag geben. Das Interesse der Eltern, sich medienpädagogisch beraten zu lassen, die Medienerziehung selbst kreativer zu gestalten und gemeinsam mit den eigenen Kindern das Netz zu entdecken, wächst genauso rasant, wie die derzeitige Entwicklung der neuen Technologien. Die Tatsache, dass andere Elternhäuser von den gleichen Problemen betroffen sind, schafft Vertrauen und durchbricht die Scheu, eigene Probleme und Streitigkeiten bezüglich der Mediennutzung vor Fremden anzusprechen. Nicht nur die kompetente Begleitung der eigenen Kinder hinein in die digitale Welt spielte bei den motivierten Eltern eine Rolle, sondern vor allem auch die Möglichkeit, im privaten Umfeld die Tipps, Ideen und Werkzeuge an andere Eltern weiterzugeben und somit eine peer-to-peer Wissensvermittlung zu realisieren.

Die ausgebildeten Medienguides MV wollen auch an den Schulen und Kindertageseinrichtungen ihrer Kinder ehrenamtlich für Fragen und Themen der Medienkompetenz und -erziehung tätig werden. Genauso wie die Medienscouts MV bei den Jugendlichen kommt auch das Elternprojekt Medienguides MV bei den Teilnehmenden überaus gut an. Am meisten geschätzt wird dabei immer wieder die Verbindung zwischen Theorie und Praxis. Die Eltern werden in die Lage versetzt, Medien kreativ selbst zu erleben, können die Apps und Spiele selbst ausprobieren, von denen ihre Kinder fasziniert sind. Aufgrund mangelnder personeller Kapazitäten des LfDI MV musste die Durchführung der Veranstaltung im Jahr 2023 ausgesetzt werden. Im Jahr 2024 soll das Projekt jedoch wieder aufgenommen und fortgeführt werden. Bisher war es aufgrund der finanziellen und vor allem personellen Ressourcen nur möglich, einen Ausbildungszyklus im Jahr durchzuführen, obwohl der Bedarf und das Interesse der Eltern weit höher sind. Unser Bestreben in diesem Bereich ist es, dieses Projekt an den Durchführungsturnus des Jugendprojektes Medienscouts MV (siehe Punkt 4.1.) anzugleichen und zweimal jährlich anzubieten. Dies bedarf jedoch nicht nur weiterer finanzieller Kapazitäten, sondern auch verfügbarer, personeller Ressourcen seitens unserer Projektpartner:innen. Um die ausgebildeten Eltern besser und vor allem dauerhaft miteinander vernetzten zu können, wurde auch für dieses Projekt in 2024 eine App zur Kommunikation entwickelt. Somit können interessante Links und Informationen geteilt sowie fachliche Fragen direkt über eine Chatfunktion beantwortet werden.

Wir empfehlen der Landesregierung dringend, (außerschulische) Projekte der Medienbildung, die sich konkret an Eltern und Familien richten, stärker in den Fokus der bildungspolitischen Agenda zu nehmen. Die Vermittlung von Medienkompetenz und Medienerziehung kann nicht allein von Akteur:innen des Bildungssystems geleistet werden und muss in der Familie beginnen. Im Sinne der Erziehungs- und Bildungspartnerschaft zwischen Bildungseinrichtungen und Eltern muss es mehr Angebote für Eltern und Familien geben, um Medienkompetenz zu erlangen und so besser und vor allem gemeinsam auf die lebensweltlichen Anforderungen der Kinder und Jugendlichen reagieren zu können.

4.3. Tage ethischer Orientierung: protect privacy – „Mein Klick, meine Verantwortung“

Die Tage ethischer Orientierung sind ein viertägiges schulkooperatives Modell der Evangelisch-Lutherische Kirche in Norddeutschland (Nordkirche), das in enger Zusammenarbeit mit dem LfDI MV seit 2013 erfolgreich durchgeführt wird und ein Mal jährlich stattfindet. Die Projektbezeichnung „Tage ethischer Orientierung: protect privacy“ (TEO PP) soll deutlich machen, wie wertvoll und schützenwert die eigene Privatsphäre ist. Die Schüler:innen der 5. und 6. Klassen werden im Laufe der Veranstaltung für den Umgang mit Medien und Anwendungen im digitalen Zeitalter sensibilisiert und reflektieren ihr eigenes Nutzungsverhalten im Netz. Im Rahmen dieses Gemeinschaftsprojektes mit der Nordkirche und weiteren Projektpartner:innen werden die wichtigsten Themen bezüglich Chancen und Risiken der digitalen Realität und der verantwortungsvoller Umgang im Netz abgedeckt.

Inhaltliche Schwerpunkte wie Mediensucht, Social Media und Cybermobbbing werden von der LAKOST übernommen, zu Gaming und Influencer:innen informiert die CSG, der LfDI MV arbeitet mit den Schüler:innen zum Thema Datenschutz und Tracking. Diese Auseinandersetzung mit dieser Themenvielfalt hilft dabei, ein sozialethisches Verständnis innerhalb unserer multimedialen Lebenswelt zu entwickeln. Die Vermittlung der Bildungsinhalte in außerschulischem Kontext, zugleich aber mit einem Klassenfahrtcharakter, stärkt den Zusammenhalt und zeigt sich gerade deshalb als besonders effektiv und nachhaltig: bekanntes Kollektiv, andere Lernumgebung, neue Informationen. Vorab erhalten die Lehrkräfte die Inhalte der einzelnen Workshops im direkten Austausch mit den Referent:innen, damit sie in ihrem Unterricht Vorkenntnisse aktivieren bzw. Wissenslücken bereits vor der Lernfahrt füllen können. Sie unterstützen bei der Durchführung und kümmern sich gemeinsam mit der Nordkirche um die Gestaltung der Freizeitaktivitäten. Die Kinder zeigen regelmäßig großes Interesse an den angebotenen Themen und überraschen die Lehrkräfte mit ihrem Wissen und den vielseitigen Erfahrungen, die sie bereits im Netz gemacht haben, sowohl in positiver als auch in negativer Hinsicht. Fächerübergreifende Medienbildung hat häufig wenig Platz in den Lehrplänen, obwohl mittlerweile fast alle Rahmenlehrpläne an die übergeordnete Strategie „Bildung in der digitalen Welt" der Kultusministerkonferenz (KMK)[1] angepasst sind. Deren Umsetzung am Lernort Schule ist jedoch weiterhin stark abhängig von Engagement, Willen und Ressourcen der Schulleitungen und Lehrkräfte. TEO PP bietet seit 2013 kontinuierlich für viele Schulen eine ausgezeichnete Möglichkeit, sich innerhalb eines Klassenkollektivs mit der eigenen Mediennutzung und dem Umgang mit digitalen Anwendung in einem gesonderten Rahmen so intensiv auseinanderzusetzen. Die begleitenden Lehrkräfte erhalten ebenfalls die Chance, Inhalte der Medienbildung praktisch umzusetzen, neue Methoden auszuprobieren und Erfahrungen auf pädagogischer sowie ethischer Ebene zu sammeln. Die über viele Jahre unverändert hohe Nachfrage durch die Schulen zeigt einerseits die Aktualität und Wichtigkeit der thematischen Inhalte für die spezifische Altersgruppe der 5.- und 6. Klässler:innen. Andererseits unterstreicht dieses hohe Interesse der Schulen aber vor allem die Notwendigkeit alternativer, schulkooperativer Lernformate zur umfassenden Auseinandersetzung mit Themen der Mediennutzung und Datenschutzbewusstsein, wie sie durch TEO PP angeboten werden. Die regelmäßigen Feedback-Runden mit den teilnehmenden Schüler:innen zeigen ebenfalls den immer größer werdenden Stellenwert medialer Themen im privaten und schulischen Kontext. Der Bedarf an Aufklärung im Bereich der Medienbildung bleibt in allen Altersgruppen stetig sehr hoch. Eine verantwortungsbewusste Nutzung der Medien muss gelernt werden. Das jährliche Fortbestehen dieses Projekt weist darauf hin, dass die Schulen Medienbildung als wichtig erachten, sie diese oft jedoch aus Personal-, Zeit- oder Ausstattungsgründen nicht entsprechend durchführen können. Folglich braucht es mehr, damit Medienbildung als Querschnittsaufgabe gelingt – nämlich eine Pluralität und Diversität von schulischen Bildungsangeboten, schulkooperativen Lernsettings wie beispeilsweise TEO PP und kompetenten Ansprechpartner:innen für Kinder und Jugendliche. Zu letzteren zählen neben den Lehrkräften eben auch die Eltern und Familien (siehe Punkt 4.2.) sowie gleichaltrige Freund:innen (siehe Punkt 4.1.).

1 URL: https://www.kmk.org/fileadmin/Dateien/pdf/PresseUndAktuelles/2018/Digitalstrategie_2017_mit_Weiterbildung.pdf [abgerufen am 03.04.2024]

Wir empfehlen der Landesregierung den Austausch mit unserer Behörde sowie mit der Nordkirche bezüglich der TEO-Projekte, deren zukünftige Weiterführung aufgrund auslaufender Fördermöglichkeiten über den Europäischen Sozialfond (ESF) unklar ist. Einen möglichen Wegfall des Formates TEO PP sehen wir äußerst kritisch, da es kein vergleichbares Bildungsangebot zur ethischen/politischen Orientierung für Kinder und Jugendliche dieser Altersgruppe im Land gibt. Bei gleichzeitiger Reduzierung dieser nicht fest in den Lehrplänen verankerten Themen zur Medienkompetenz befürchten wir eine starke Beeinträchtigung der ethischen/politischen Bildung junger Menschen in unserem Land.

4.4. Modulare Fortbildungsreihe „Spielen, Zappen, Klicken“

Die Kursreihe „Spielen, Zappen, Klicken“ ist eine modulare Fortbildungsreihe, die auf die Inhalte der Bildungskonzeption der 0-10 Jährigen in Mecklenburg-Vorpommern (BIKO MV) abgestimmt ist. Ziel ist es, die teilnehmenden pädagogischen Fachkräfte und Einrichtungen dabei zu begleiten, 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 wird das Fortbildungsprogramm für Erzieher:innen der Kitas und Horte seit 2018 jährlich mit einem modularisierten Ausbildungsdurchgang durchgeführt. Die Fortbildungsreihe umfasst 8 Module und einen praxisorientierten Studientag in der Einrichtung der Teilnehmenden. Die Kursreihe unterstützt Träger und Einrichtungen der frühkindlichen Bildung in der Erfüllung des Kindertagesförderungsgesetzes Mecklenburg-Vorpommern (KiFöG M-V) zur Medienbildung und beinhaltet die Themenschwerpunkte des neu eingeführten Kapitels der BIKO MV. Der LfDI MV brachte sich mit seiner Fachexpertise als Mitverfasser des Kapitels der BIKO MV zur frühkindlichen Medienbildung bereits ein und übernimmt seitdem in Zusammenarbeit mit den Projektpartnern und freien Medienpädagog:innen 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 Berichtszeitrum weiter fortgeführt werden. Mit dieser Fortbildungsreihe wird ein Werkzeug geschaffen, das pädagogischen Fachkräften auch die Kompetenz und Sicherheit im Umgang mit Themen der digitalen Mediennutzung innerhalb der Familien näherbringt und damit ebenfalls einen wichtigen Beitrag zur Elternarbeit leistet.

Der Kontakt mit den unterschiedlichsten Medien erfolgt bereits vor dem Eintritt in die Kita, denn Geräte und Bildschirme dringen von allen Seiten in die kindliche Lebenswelt ein. Den Medienkonsum für jüngere Kinder gänzlich zu vermeiden oder gar zu verbieten, ist in der heutigen Zeit keine Lösung mehr. Der spielerische Umgang und die Förderung der Entwicklungsprozesse von Kindern stehen bei der frühkindlichen Medienbildung im Fokus. Durch gemeinsames Entdecken der digitalen Geräte und Anwendungen ist es möglich, die Kinder für den zukünftigen Lebensweg medienkompetent zu machen. Dank der Vielfalt an Fachreferent:innen erfahren die Teilnehmenden der modularen Fortbildungsreihe, mit welchen alltagstauglichen Medien dieses Ziel in ihren Einrichtungen gut integrierbar und erreichbar ist.

Darüber hinaus erstellen die Teilnehmenden als Abschluss der Fortbildung ein pädagogisches Medienkonzept für ihre Einrichtungen und setzen somit selbst entworfene, praxistaugliche Medienprojekte um. Somit wird der erste Baustein in der frühkindlichen Medienerziehung bei den zuständigen Trägern gelegt. Weiterhin begleitet der LfDI MV die teilnehmenden Einrichtungen bei der Durchführung von Elternabenden, da aktuelle Bezüge der medienpädagogischen Inhalte und die entsprechende Wissensvermittlung an die Eltern ebenso notwendig sind, wie die Weiterbildung der Fachkräfte. Es ist eindeutig, dass die Mediennutzung ein immer wiederkehrendes Diskussionsthema in Familien darstellt und die Eltern für praktische Tipps zur Medienerziehung dankbar sind (siehe Punkt 4.6.).

Aufgrund der unsicheren Finanzierung der modularen Fortbildungsreihe „Klicken, Spielen, Zappen" durch den vdek e.V. fordert unsere Behörde seit Beginn des Weiterbildungsangebotes für pädagogische Fachkräfte in 2016 eine Verstetigung dessen Finanzierung auf Landesebene. Wir empfehlen der Landesregierung deshalb dringend, die Etablierung dieses Weiterbildungsangebotes zu prüfen und die Durchführung dauerhaft der LAKOST zu übertragen.

4.5. Das Jugendportal der DSK: youngdata.de

Die Datenschutzkonferenz des Bundes und der Länder (DSK) beschloss die Finanzierung des Relaunches des Jugendportals www.youngdata.de bereits 2021. Die bisherige Website wurde 2013 von der Datenschutzaufsichtsbehörde in Rheinland-Pfalz (LfDI RLP) ins Leben gerufen und verstetigte sich in der Folge sukzessive zu einem Angebot der DSK. Die Initiierung des Jugendportals durch den LfDI RLP war zu diesem Zeitpunkt ein Novum und wurde begeistert von den Kolleg:innen in den Ländern aufgenommen. Im vorliegenden Berichtszeitraum wurde diese Webseite der DSK in Kooperation mit der Datenschutzbeauftragten des Kantons Zürich komplett neu gestaltet. Sie wurde an das Nutzungsverhalten Jugendlicher angepasst, insbesondere durch eine mobile Version für den schnellen Zugriff über das Smartphone. Dabei will die Website lebensnahe Themen zum Datenschutz spannend und interessant aufbereiten und wendet sich vor allem an Jugendliche im Alter von 13-16 Jahren. Die Website ist nicht nur an die User Experience dieser konkreten Zielgruppe angepasst, sondern entspricht ihr auch in Themenauswahl, Wording, Ansprache, Textinhalten und visueller Gestaltung. Das Ziel ist es, zum Thema Datenschutz zu sensibilisieren und über den Umgang mit eigenen und fremden personenbezogenen Daten aufzuklären. Nach dem Willen des europäischen Gesetzgebers ist die Sensibilisierung und Aufklärung der Bürger:innen über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten eine zentrale Aufgabe. Der Art. 57 Abs. 1 lit. b DS-GVO hebt in diesem Zusammenhang ausdrücklich die Notwendigkeit spezifischer Maßnahmen für Kinder hervor. Diese Aufgabe ist ein gemeinsames Hauptanliegen der DSK. Die Seite youngdata.de stellt zusätzlich eine Übersicht über die speziellen Angebote der einzelnen Bundesländer für Jugendliche und Interessierte bereit. Dafür ist es notwendig, dass die Nutzenden die Mechanismen und Funktion unserer digitalen Kultur verstehen und kritisch hinterfragen.

Zur Realisierung des Relaunches bildete sich 2022 eine AG, die maßgeblich vom LfDI MV koordiniert wurde. Im Berichtszeitraum organisierte unsere Behörde regelmäßige Arbeitstreffen und kontinuierliche Absprachen in Online- und Präsenzformaten, entwickelte ein Logo und übernahm dann in gemeinsamer Verantwortlichkeit für die DSK die Abwicklung des bundesweiten Ausschreibungsverfahrens zum Relaunch mit den Agenturen. Die anschließende Umsetzung des Projektes wurde vorwiegend durch den LfDI MV organisiert und in engerer Zusammenarbeit durch die Datenschutzaufsichtsbehörden aus Rheinland-Pfalz, Hamburg, Berlin sowie den Bundesdatenschutzbeauftragten aktiv begleitet. So war der LfDI MV nicht nur verantwortlich für die inhaltliche Ausrichtung der Webseite, vielmehr übernahmen wir auch koordinierende Aufgaben im redaktionellen Bereich, stimmten Arbeitsprozesse mit der beauftragten Agentur ab und verfassten Inhalte und Artikel. Im Mai 2023 fand der Relaunch der Webseite statt. Damit wurde ein Jugendportal zum Datenschutz und zur Informationsfreiheit ansprechend und informativ gestaltet, so dass Jugendliche selbstbestimmt und souverän durch unsere digitale Welt gehen können – die Grundidee des Datenschutzes. Klassische Themen wie Datensicherheit, Tracking oder Privatsphäre als Ware gehören ebenso zu den Artikelinhalten wie Informationen zu sozialen Netzwerken, Apps oder Hate Speech. Natürlich werden auch neue Entwicklungen wie KI und ChatGPT so vermittelt, dass Jugendliche verstehen können, welche Rolle ihre Daten und persönlichen Informationen in diesem Kontext spielen.

Am 3. Dezember 2023 wurde die Webseite mit dem 3. Platz in der Kategorie „Jugendpreis Bildung" des renommierten Kindersoftwarepreises TOMMI ausgezeichnet. In der Begründung der Jugendjury heißt es: „Die Webseite YoungData gewinnt beim TOMMI den 3. Platz, weil es endlich mal für uns Jugendliche eine gute und verständliche Auswahl an Informationen zum Thema Datenschutz gibt. Zwar haben wir einiges schon vorher gewusst, aber eben vieles auch nicht. Der Aufbau ist sehr gut und vor allem haben wir verstanden, dass es beim Thema Datenschutz um uns als Menschen geht und nicht um Daten. So eine Seite würden wir uns auch für die Schule wünschen, wenn es um Medienkompetenz geht."[1]

Dies motiviert die YoungData-Redaktionsgruppe, auch in Zukunft aktuelle Medien- und Datenschutzthemen für Jugendliche aufzugreifen und die Webseite kontinuierlich zu aktualisieren und weiterzuentwickeln. Die DSK in Kooperation mit dem Kanton Zürich wird auch weiterhin ihr Fachwissen teilen, damit Jugendliche und alle Interessierten dieses nutzen können, um sich in unserer digitalen Gesellschaft selbstbestimmt und verantwortungsbewusst zu bewegen. Digitale Kompetenz und Datenschutzbewusstsein sind für jeden Menschen – unabhängig vom Alter – in der digitalen Gegenwart unerlässlich.

1 https://tommi.kids/magazin/spiele/platz-3-https-youngdata-de-konferenz-der-unabhaengigen-datenschutzbehoerden-des-bundes-und-der-laender-dsk-der-landes-beauftragte-fuer-datenschutz-und-informationsfreiheit-mecklenburg-vorpomme/ [abgerufen am 27.03.2024]

4.6. #Digitale Vorbilder – Familien gehen online.

Ende 2021 beantragte der LfDI MV gemeinsam mit dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) erfolgreich Fördergelder im Rahmen des EU-Programms „Citizens, Equality, Rights and Values-2021-DATA" (CERV-2021-DATA).

Das gemeinsam entwickelte Projekt mit dem Arbeitstitel „D.E.A.P. - Data, Education, Awareness, Protection" ist das erste EU-Projekt deutscher Datenschutzaufsichtsbehörden und folgt der Zielsetzung, das Thema Datenschutz für Familien verständlich und erlebbar zu machen. Diese Herangehensweise an Datenschutzthemen sowie unsere Planungen zur Umsetzung überzeugten das Auswahlkomitee. Der LfDI MV und der HmbBfDI erhielten rund 35% des Gesamtbudgets aus dem CERV-DATA-Fördertopf, um Familien im Bereich Datenschutzbewusstsein und Medienerziehung aufzuklären. Da dies das erste Mal überhaupt war, dass deutsche Datenschutzaufsichtsbehörden EU-Gelder zu diesem Zweck beantragt und erhalten haben, unterstreichen wir gemeinsam mit dem HmbBfDI unsere führende Rolle in der Erfüllung des Auftrages gemäß Art. 57 Abs. 1 lit. b der DS-GVO, Bürgerinnen und Bürger zu sensibilisieren und spezielle Angebote für Kinder und Jugendliche umzusetzen. Mit Eingang der Förderzusage der Europäischen Union im Frühjahr 2022 konnte das Projekt zum 1. November 2022 und einer Laufzeit bis zum 31.10.2024 starten. Schnell wurde dabei klar, dass der Projekttitel „D.E.A.P. – Data, Education, Awarness, Protection" nicht für die Ansprache von Familien hilfreich sein würde. Wir entwickelten einen Markennamen mit Logo und Slogan, der seitdem das Projekt in ganz Deutschland bekannt macht: *#Digitale Vorbilder – Familien gehen online*.

Der innovative Kern des Projektes liegt im Anspruch, Familien ganz niederschwellig erreichen zu wollen. Im Familienalltag sind digitale Medien und Apps nicht mehr wegzudenken. Die Faszination für die alltagserleichternden und unterhaltsamen digitalen Möglichkeiten ist sowohl bei Erwachsenen als auch bei Kindern und Jugendlichen ungebrochen und wächst stetig weiter. Gleichzeitig werden digitale Medien schnell zum Streitthema in der Familie, wenn es darum geht, welche Medien Kinder wie lange nutzen dürfen, welches die besten Sicherheitseinstellungen für Geräte und Apps sind und wie viele Informationen Kinder und Jugendliche im Netz von sich preisgeben. Das sind nur einige Themen, die in Familien zu Unsicherheiten führen. Medienkompetenz bedeutet, sich aktiv, kritisch und selbstbestimmt mit Medien auseinander setzen zu können. Dazu müssen neben den Vorteilen und Möglichkeiten von digitalen Medien auch deren Risiken und Gefahren gekannt werden, um ganzheitlich Handlungskompetenzen erwerben zu können. Das Projekt #Digitale Vorbilder setzt genau dort an. Es möchte Familien für die digitale Lebenswelt ihrer Kinder und für neue technologische Entwicklung begeistern, ihnen Hilfestellungen zum Schutz ihrer Privatsphäre aufzeigen und sie ermutigen, das eigene Mediennutzungsverhalten zu hinterfragen.

Mit Beginn des Jahres 2023 konkretisierten wir die Planung für die Projektumsetzung. Als Kooperationspartner für die gesamte mediale Aufarbeitung konnte der Bürger:innensender und Ausbildungskanal TIDE (TIDE) aus Hamburg gewonnen werden.

Wie im Projektantrag beschrieben ging es um die Durchführung von fünf vor-Ort-Veranstaltungen sowie zehn Online-Seminaren. Von den vor-Ort-Veranstaltungen sollten zwei in Hamburg und drei Veranstaltungen in Mecklenburg-Vorpommern stattfinden. Am 30. September 2023 startete die Umsetzung mit einem simultanen Familien-Medien-Nachmittag in Hamburg und in Schwerin. Im Herbst folgten in M-V noch weitere Termine in Torgelow (2. November 2023) und in Güstrow (4. Dezember 2023).

Um möglichst viele Familien zu erreichen, wurde das ganzheitliche Konzept der Medienaktionstage für die ganze Familie an einem Samstagnachmittag entwickelt. Die Nachmittage beinhalteten eine bunte Palette an medienpädagogischen Aktionen für Kinder, begleitet von interessanten Kurzvorträgen, Podiumsdiskussionen, verschiedenen Informationsständen landes- und bundesweiter Initiativen wie z. B. Blinde Kuh e.V, klicksafe, Schauhin.info, und Juuuport. Neben den beteiligten Datenschutzbehörden waren auch andere aktive Akteure der Medienbildung unseres Landes wie das LKA M-V und die LAKOST vertreten. So hatten die Familien viel Zeit, um sich intensiv und ganz individuell mit dem Thema Medienerziehung in der Familie, Datenschutzbewusstsein und neuen digitalen Herausforderungen auseinanderzusetzen. Gleichzeitig konnten sich die Kinder aktiv mit digitalen oder analogen Freizeitmöglichkeiten beschäftigen.

Im November 2023 startete dann ebenfalls die zehnteilige Online-Seminarreihe. In diesen zehn Veranstaltungen werden konkrete Inhalte wie z. B. „Gaming spielend sicher", „Die zehn Datenschutz-Mythen", TikTok, Snapchat & Co." oder „Cybermobbing" und „Verantwortung im digitalen Raum" thematisiert. Während der Laufzeit der Online-Seminare steigerte sich die Anzahl der Zuschauenden auf bis zu 300 Personen. Die ersten beiden Veranstaltungen fanden innerhalb des Berichtszeitraumes statt, die Durchführung aller weiteren Veranstaltungen wird entsprechend der Projektplanung in 2024 umgesetzt. Alle Seminare werden im Fernsehstudio des Medienprojektpartners TIDE aufgezeichnet und jeweils durch verschiedene Moderator:innen und Gäste zum entsprechenden Thema durchgeführt. Die Teilnehmenden haben dabei immer die Möglichkeit, über den Chat Fragen zu stellen, die dann live im Studio beantwortet werden können. Durch die Aufzeichnung der Seminare und der Vorträge auf den Medienaktionstage entsteht eine umfangreiche Sammlung vieler interessanter Videos, die auf der Projektwebsite www.digitale-vorbilder.eu zur Verfügung gestellt werden und für alle Interessierten abrufbar bleiben sollen.

Eine weitere Herausforderung bestand in der Zusammenstellung eines fachlichen Projektbeirates, der sich aus insgesamt sechs Institutionen beider Länder zusammensetzen sollte. Der Beirat des Projektes #Digitale Vorbilder wurde Anfang 2023 initialisiert und setzt sich aus folgenden Institutionen zusammen: Kindersuchmaschine Blinde Kuh e.V., Elternschule Wilhelmsburg, Stadtteilmütter der Diakonie Hamburg, Kinderschutzbund Landesverband Hamburg sowie das Kompetenzzentrum für Menschen mit Hör- und Sehbehinderungen Schwerin und das Kompetenzzentrum für exzessive Mediennutzung und -abhängigkeit der Evangelischen Suchthilfe MV. Der Beirat begleitet das Projekt regelmäßig und gibt durch seine fachliche Expertise zusätzliche Anregungen, wie die Zielgruppe gut erreichbar ist und welche Ansprache und Themen aus Sicht der Beiratsmitglieder wichtig sind.

Die Förderrichtlinien des EU-Programms CERV-2021-DATA sehen eine umfassende Evaluation des Projektes vor. Demensprechend wurden und werden bei allen durchgeführten Veranstaltungen, d. h. sowohl bei den Medienaktionstagen vor Ort als auch bei den Online-Seminaren, Befragungen aller Teilnehmenden anhand standardisierter Fragebogenerhebungen durchgeführt. Diese bilden die Grundlage zur Evaluation, die nach Abschluss des Projektes gemeinsam mit unserem Bericht beim Projektträger eingereicht wird.

Fazit

Ein EU-Projekt solch einer Größenordnung beansprucht Zeit und Kapazitäten in den durchführenden Aufsichtsbehörden. Gleichwohl haben wir bis jetzt festgestellt, dass das Interesse am Thema Datenschutz und Medienerziehung bei den Familien enorm groß ist. Die Menschen, die wir bisher erreicht haben, waren begeistert von der Fülle an Informationen und Möglichkeiten, die wir gemeinsam mit unseren Partner:innen aufzeigen konnten. Sie wollen alle #Digitale Vorbilder sein. Doch wir brauchen auch auf politischer Ebene Unterstützung. Neben einer Vernetzung brauchen bereits bestehende Beratungsstellen und Angeboten im lokalen wie auch digitalen Raum vor allem mehr Sichtbarkeit. Eine solche Vernetzung mit dem Ziel der Verstetigung bindet wiederum zeitliche und personelle Ressourcen, die oft nicht vorhanden sind.

Darüber hinaus wird immer wieder deutlich, dass erfolgreiche Medienbildung für Kinder und Jugendliche eine gesamtgesellschaftliche Aufgabe ist. Diese kann nur gelingen, wenn pädagogische Einrichtungen (Kindertagesförderung, Schule) und die dortigen Fachkräfte ebenso fit im Umgang mit Datenschutzthemen und Mediennutzung gemacht werden, wie Eltern und Familien in unserem Projekt #Digitale Vorbilder oder den Medienguides MV (siehe Punkt 4.2.). An dieser Schnittstelle messen wir insbesondere der Elternarbeit in pädagogischen Einrichtungen einen hohen Stellenwert bei. Diese sollte unserer Auffassung nach bereits im Rahmen der Aus- und Weiterbildungsinhalte für pädagogische Fachkräfte und Lehrer:innen verpflichtend sein und viel stärker auf eine Vermittlung von Medienkompetenz im familiären Kontext ausgerichtet werden.

Als Datenschutzaufsichtsbehörde tragen wir sehr gern unseren Teil zu dieser gesamtgesellschaftlichen Aufgabe und im Zuge unserer Verpflichtung nach Art. 57 Abs. 1 lit. b der DS-GVO bei. Das Projekt #Digitale Vorbilder soll auch nach Projektende bestehen bleiben, jedoch ist noch unklar in welchem Umfang. Das Wissen und die Materialien werden abrufbar bleiben unter: www.digitale-vorbilder.eu.

Wir raten der Landesregierung dringend an, eine Weiterführung des Projektes *#Digitale Vorbilder – Familien gehen online.* beim LfDI MV durch die Bereitstellung von Ressourcen zu unterstützen, damit ein niedrigschwelliger Zugang zu umfassenden Themen der Medienerziehung für Familien in Mecklenburg-Vorpommern weiterhin möglich ist. Der LfDI MV steht der Landesregierung jederzeit zur Verfügung, um inhaltlich und strategisch über die Projektergebnisse und deren weitere Verwendungsmöglichkeiten zu beraten, so dass auch weiterhin eine größtmögliche Zahl interessierter Familien in M-V vom gesammelten Expert:innenwissen profitieren kann.

4.7. Das landesweite Netzwerk der Medienbildung Medienaktiv M-V

Das Netzwerk Medienaktiv M-V wird vom LJRMV, der LAKOST M-V e.V., dem LKA MV, dem Kompetenzzentrum und Beratungsstelle für exzessive Mediennutzung und Medienabhängigkeit Schwerin der Evangelischen Suchtkrankenhilfe Mecklenburg-Vorpommern, der MMV und unserer Behörde organisiert, wobei die Planung und konzeptionelle Ausgestaltung beim LfDI MV liegt.

Den bundesweit beispielgebenden Charakter des Netzwerkes hat Medienaktiv M-V auch weiterhin inne. Nach unseren Erkenntnissen aus überregionalen Arbeitsgruppen der Suchthilfe, Prävention, Medienanstalten und Datenschutzaufsichtsbehörden sind jedoch auch die anderen Bundesländer auf dem Weg, sich institutionsübergreifend zu vernetzen und treiben Konzepte zur übergreifenden Medienkompetenzvermittlung aktiv voran. Der LfDI MV schätzt die Entwicklung in Mecklenburg-Vorpommern jedoch eher rückläufig ein. Aus Sicht des LfDI MV war das Instrument der „Kooperationsvereinbarung zur Förderung von Medienkompetenz in MV" eine gute Basis, um koordinierte Programme und Themen mit den verschiedenen Ressorts und Institutionen des Landes abzustimmen. Das Fehlen einer zentralen Koordination wird auch vom Medienaktiv M-V so gesehen.[1]

Im Berichtszeitraum lud das Netzwerk Medienaktiv M-V die schulischen und außerschulischen pädagogischen Fachkräfte zu seiner Herbsttagung „Medien.Sucht.Kompetenz - Reloaded" in das Bürgerhaus Güstrow ein. In den Jahren der Pandemie hat sich die Mediennutzung in der Gesellschaft intensiviert und gewandelt. So wurden die Vorteile von Videokonferenzen und digitalen bzw. hybriden Veranstaltungen entdeckt, gleichwohl mussten viele Menschen feststellen, wie schnell und einfach sie von digitalen Medien in ihren Bann gezogen werden konnten. Die Nutzungszeiten der Kinder und Jugendlichen änderten sich durch die Pandemie und ihre Folgen ebenfalls. Auf der Tagung wurde über mögliche Gefahren und über medienpädagogische Potenziale gesprochen, um den pädagogisch Tätigen das notwendige Wissen zur Verfügung zu stellen. Für diejenigen, die mit Kindern und Jugendlichen arbeiten, braucht es pädagogische Lösungen im Umgang mit zeitlich kritischer Mediennutzung, Fake News, verstörenden Inhalten und manipulativen Angeboten im Netz.

Weiterhin stand durch das zehnjährige Bestehen des Netzwerkes Medienaktiv M-V die Vernetzung der medienpädagogisch Tätigen im Land im Berichtszeitraum im Vordergrund. Die Vernetzung innerhalb Mecklenburg-Vorpommerns aufrechtzuerhalten und stetig neue Netzwerkpartner einzubinden, übernimmt unsere Behörde maßgeblich. Im Berichtszeitraum fand die Zusammenarbeit mit der Landeszentrale für politische Bildung MV (LpB MV) erstmalig statt.

Zeitgleich wurde im Medienaktiv-Netzwerk das Konzept „Mehr Medienkompetenz in Mecklenburg Vorpommern" der MMV in Abstimmung mit der Landesarbeitsgemeinschaft Medien (LAG MEDIEN MV) und der Landesgruppe MV der Gesellschaft für Medienpädagogik und Kommunikationskultur (GMK) vom Netzwerk als Arbeitsgrundlage aufgenommen.

1 vgl. https://www.medienaktiv-mv.de/medienpolitische-arbeit/forderungen-zur-medienbildung-2021 [abgerufen am 27.03.2024]

Aus Sicht des Netzwerkes kann das Konzept eine Diskussionsgrundlage sein, die jedoch den Blick für vorhandene Strukturen in der (Jugend-)Verbandskultur und weiteren Akteuren der Medienbildung in MV erweitert.

Erstmals im Berichtszeitraum fand der „Runde Tisch Medienkompetenz" der LpB MV statt, bei der auch das Netzwerk Medienaktiv M-V und der LfDI MV vertreten waren. Inwieweit die Vernetzung der Akteure der Medienbildung MV gelingen kann, wird sich erst in Zukunft zeigen.

Da kaum eine strukturelle Unterstützung zur Förderung von digitaler Kompetenzen/Medienkompetenz vorhanden ist, bleibt das Engagement der Akteure der Medienbildung in Mecklenburg-Vorpommern das Hauptpotenzial des Netzwerkes Medienaktiv M-V.

Das landesweite Netzwerk der Medienbildung Medienaktiv M-V wird auch zukünftig alle neuen Erkenntnisse, weitere Kooperationen und mögliche Schritte, wie die Vermittlung von Medienkompetenz und digitaler Kompetenzen in unserem Bundesland ausgestaltet werden kann, aktiv begleiten und im Dialog mit Politik erörtern. Unsere Behörde sieht darin die Möglichkeit, die Ziele von gesellschaftlicher Teilhabe, Demokratiebildung und notwendiger Chancengleichheit, weiterhin maßgeblich voranzutreiben.

Wir fordern die Landesregierung dazu auf, den LfDI MV gemeinsam mit den Kooperationspartnern des Netzwerkes Medienaktiv MV soweit zu unterstützen, dass eine Verstetigung der flächendeckenden Vernetzung der Akteur:innen der Medienbildung im Land verbindlich und dauerhaft umgesetzt werden kann.

5. Europäische Zusammenarbeit und Internationaler Datenverkehr

In Europa gibt es neben den unabhängigen Datenschutzaufsichtsbehörden in der Bundesrepublik insgesamt 30 weitere europäische Datenschutzaufsichtsbehörden (27 in der EU, 3 weitere im Europäischen Wirtschaftsraum)[1]. Es gehört zu unseren gesetzlich verankerten Aufgaben, gemeinsam mit unseren europäischen Kolleg:innen an der Einhaltung und Durchsetzung der DS-GVO zu arbeiten, insbesondere bei Anfragen oder Beschwerden von betroffenen Bürger:innen, aber auch über den kollegialen Austausch z. B. in Form von gegenseitiger Amtshilfe oder gemeinsamen Untersuchungen gemäß Art. 57 Abs. 1 lit. e, f, g, h DS-GVO. Zu diesem Zwecke ist der LfDI MV z. B. über das Binnenmarktinformationssystem (IMI: eng. Internal Market Information System) mit allen europäischen Datenschutzaufsichtsbehörden in Kontakt. Dort werden nicht nur Beschwerden gemeinsam bearbeitet, sondern auch fachliche Fragen auf Arbeitsebene diskutiert (siehe Punkt 5.1.).

1 Siehe folgende Übersicht der einzelnen Länder und Aufsichtsbehörden:
URL: https://www.edpb.europa.eu/about-edpb/about-edpb/members_de [abgerufen am 03.04.2024]

Die europäische Zusammenarbeit bezieht sich auf alle erdenklichen Inhalte. Schwerpunkte unserer Arbeit waren zuletzt Fragen des Internationalen Datenverkehrs, d. h. der Übermittlung personenbezogener Daten in Drittstaaten außerhalb des Europäischen Wirtschaftsraumes. In den folgenden Unterkapiteln wird dargelegt, wie wir uns insbesondere zum Thema der Übermittlung von personenbezogenen Daten (auch Gesundheitsdaten) in Drittstaaten auf deutscher und auf europäischer Ebene engagierten (siehe Punkte 5.2. bis 5.4.).

Neben der fallbezogenen Zusammenarbeit ist der LfDI MV auch dazu verpflichtet, einen Beitrag zur Tätigkeit des Europäischen Datenschutzausschuss (EDSA) zu leisten (Art. 57 Abs. 1 lit. t DS-GVO). Der EDSA als oberstes europäisches Gremium der Datenschutz-Aufsichtsbehörden ist auf Arbeitsebene in sogenannten Expert Subgroups (ESG) organisiert – ähnlich wie in Deutschland die DSK und ihre Arbeitskreise. In jeder ESG ist Deutschland durch eine Person vom BfDI und eine Person aus den Bundesländern vertreten. Auch wir als vergleichsweise eher kleinere Behörde von knapp 30 Personen, von denen circa 20 Mitarbeitende datenschutzrechtliche Sachverhalte prüfen, müssen diese Vorgabe erfüllen. Der LfDI MV ist in der Enforcement Subgroup, die sich mit der Durchsetzung des Datenschutzrechts durch Anordnungen und Bußgelder beschäftigt, stellvertretende Ländervertretung (siehe Punkt 5.5.).

5.1. Kooperationsverfahren über IMI

Betroffene können eine Beschwerde über einen möglichen Datenschutzverstoß bei jeder Aufsichtsbehörde in Europa einreichen. Es ist inzwischen immer öfter der Fall, dass der Beschwerdegegner ein global agierendes Unternehmen ist und daher Personen in anderen Ländern von der gemeldeten Verarbeitung personenbezogener Daten ebenfalls betroffen sind. Zumindest aber hat immer öfter der Verantwortliche für eine Verarbeitung seinen Sitz in einem anderen Land als dem, in der die betroffene Person lebt. Bei solch grenzüberschreitenden Fällen kommunizieren die Datenschutzaufsichtsbehörden in ganz Europa über das IMI miteinander und bearbeiten auf diese Weise gemeinsam die Beschwerdeverfahren oder gemeldete Datenpannen, die mehrere Aufsichtsbehörden betreffen. In den Jahren 2022/2023 hat der LfDI MV insgesamt 1.302 Verfahren gemäß Art. 56 DS-GVO bearbeitet und geprüft, ob mutmaßlich Menschen in Mecklenburg-Vorpommern von der Beschwerde oder Datenpanne betroffen sein könnten (615 in 2022 und 687 in 2023).

Viele Beschwerdeverfahren, die im Kooperationsverfahren bearbeitet werden, können wegen der komplexen Ermittlungen, Abstimmungsverfahren zwischen den Aufsichtsbehörden und geringen Personalressourcen in den Datenschutzaufsichtsbehörden etwas länger andauern. Ein Fall, der 2021 aus Mecklenburg-Vorpommern nach Slowenien zur federführenden Bearbeitung übermittelt wurde, konnte im Jahr 2022 abgeschlossen werden. Zwei weitere Beschwerden aus Mecklenburg-Vorpommern gegen ein großes Finanzunternehmen wurden 2022 in Zusammenarbeit mit der federführenden Aufsichtsbehörde in Luxemburg abgeschlossen. Wir übermittelten eine Beschwerde über IMI an die Datenschutzstelle im Fürstentum Liechtenstein und stehen seither zur Bearbeitung in engem Austausch. Eine weitere Beschwerde gegen eine Universität wird derzeit gemeinsam mit der federführenden Datenschutzaufsichtsbehörde in Frankreich bearbeitet.

Der LfDI MV schließ 2022 eine Beschwerde einer betroffenen Person aus Österreich mit einer Verwarnung ab, da das Unternehmen aus Mecklenburg-Vorpommern dem Auskunftsrecht gem. Art. 15 DS-GVO zunächst nicht entsprochen hatte. Eine weitere Beschwerde aus Österreich wurde von uns 2022 als federführende Aufsichtsbehörde zur Bearbeitung übernommen und im Jahr 2023 abgeschlossen. Die Beschwerde wurde gem. Art. 60 Abs. 8 DS-GVO abgewiesen, da sie nicht in den Anwendungsbereich der DS-GVO fiel.

In einer Vielzahl von Fällen ist der LfDI MV zudem als betroffene Aufsichtsbehörde an der Bearbeitung beteiligt und kann somit Einfluss auf die Entscheidung von Fällen mit zentraler Bedeutung nehmen (z. B. Beschwerden gegen global tätige Unternehmen wie Meta, PayPal oder Netflix), die auch Auswirkungen auf die Menschen in Mecklenburg-Vorpommern haben.

Neben der Bearbeitung konkreter Fälle stehen wir über IMI auch im umfassenden Kontakt über allgemeine Anfragen zur Rechtsauslegung, zum kollegialen Austausch von best practice-Beispielen oder auch zu Arbeitsprozessen in den jeweiligen Datenschutzaufsichtsbehörden in ganz Europa. Darunter fallen auch Anfragen zur Amtshilfe (Art. 61 DS-GVO) und Benachrichtigungen über einstweilige Maßnahmen einzelner Behörden (Art. 66 DS-GVO).

5.2. Untersuchung zum NIPT und möglichen Übermittlungen genetischer Daten nach China

Werden genetische Proben von Schwangeren aus Mecklenburg-Vorpommern nach China übermittelt? Diese Frage stellten wir uns, als wir aus Medienberichten erfuhren, dass ein Anbieter für einen genetischen Bluttest mutmaßlich die gewonnen Proben in Drittstaaten außerhalb des Europäischen Wirtschaftsraums (hier: China) übermitteln soll, um sie dort analysieren zu lassen. Aufgrund der hohen Sensibilität der betroffenen Gesundheitsdaten obliegt dieser Frage eine besondere Brisanz.

Das Verfahren des nicht-invasiven Pränataltest (NIPT) wird vielen Schwangeren im ersten Trimester nach einem ärztlichen Aufklärungs- und Beratungsgespräch in einer gynäkologischen Praxis oder Klinik angeboten – dabei wird ab der 10. Schwangerschaftswoche eine Blutprobe genommen. Diese Probe enthält genetische Daten (die DNA) der Schwangeren und auch Bruchstücke von Erbinformationen des Fötus. Die DNA-Bruchstücke des Fötus werden im Labor aus der Probe herausgefiltert und auf mögliche genetische Anomalien untersucht, vor allem auf Trisomien. Die genetische Untersuchung gibt an, mit wie hoher Wahrscheinlichkeit beim Fötus z. B. eine Trisomie (13, 18, 21) vorliegen könnte. Es gibt zahlreiche Anbieter der nicht-invasiven Pränataltests. Da die Praxis bzw. die Klinik den Anbieter auswählt, die Proben bei der Schwangeren erhebt und die Analyse in Auftrag gibt, ist sie Verantwortliche im Sinne der DS-GVO für die Verarbeitung dieser sensiblen Daten.

Die Übermittlung von personenbezogenen Daten in Drittstaaten außerhalb des Europäischen Wirtschaftsraumes kann zulässig sein, wenn die Anforderungen aus dem Kapitel V der DS-GVO erfüllt sind. In manchen Drittstaaten kann der Schutz personenbezogener Daten (insbesondere die Einhaltung des Kap. V DS-GVO) jedoch nicht sichergestellt werden.

Insbesondere China ist international dafür bekannt, die Rechte seiner Bürger:innen durch Überwachungsmaßnahmen wie Social Scoring zu beschneiden und ethnische Minderheiten zu diskriminieren.[1] Eine Studie im Auftrag des EDSA zum Zugriff öffentlicher Stellen kommt bei China zu dem Ergebnis, dass staatliche Stellen nach eigenem Ermessen und ohne faktische Kontrolle auf alle in China gespeicherten Daten zugreifen können.[2] Die Kontrolle über die Verarbeitung von nach China übermittelten Daten entzieht sich daher dem übermittelnden Verantwortlichen oder Auftragsverarbeiter. Es ist dementsprechend unmöglich zu sagen, zu welchen Zwecken Daten in China weiter verwendet werden könnten und welche Folgen dies womöglich auch für Betroffene haben könnte.

Da den Berufsverbänden keine Informationen zur Übermittlung von genetischen Proben aus einem NIPT nach China vorlagen, führte der LfDI MV eine Umfrage mit Stichproben bei per Zufall ausgewählten Verantwortlichen im Land durch.[3] Es wurden 12 Praxen und Kliniken angeschrieben und dazu befragt, ob Sie genetische Proben aus pränatalen Bluttests in Drittstaaten, z. B. nach China, übermitteln.

Bei der Untersuchung in MV stimmten wir uns sowohl mit den deutschen als auch mit allen europäischen Datenschutzaufsichtsbehörden ab und tauschten uns u. a. über IMI (siehe Punkt 5.1.) zu dem Thema NIPT und Drittlandübermittlungen aus. Da in Slowenien ein Unternehmen ansässig ist, dass einen NIPT dort anbietet, arbeiteten wir mit den slowenischen Kolleg:innen bei unseren jeweiligen Untersuchungen eng zusammen.

Am Ende der Untersuchung konnten wir feststellen, dass glücklicherweise keiner der befragten Verantwortlichen in Mecklenburg-Vorpommern genetische Daten von Schwangeren in Drittstaaten außerhalb des Europäischen Wirtschaftsraums übermittelt – auch nicht nach China. Es mussten somit keine weiteren Abhilfemaßnahmen ergriffen werden. Die Initiative des LfDI MV sensibilisierte gleichwohl die Öffentlichkeit, genauso wie Praxen und Kliniken nachhaltig für die Einhaltung der datenschutzrechtlichen Anforderungen im Umgang mit genetischen Daten, besonders auch bei beabsichtigten Drittlandsübermittlungen.

1 U. a. Björn Alpermann (2023): Chinas Umgang mit den Uiguren. In: Bundeszentrale für politische Bildung.
URL: https://www.bpb.de/themen/asien/china/541075/chinas-umgang-mit-den-uiguren/ [abgerufen am 03.04.2024]

ZDF (2020): Das Überwachte Volk – Chinas Sozialkredit-System.
URL: https://www.zdf.de/dokumentation/zdfinfo-doku/das-ueberwachte-volk-chinas-sozialkredit-system-102.html [abgerufen am 03.04.2024]

2 Milieu for EDPB (2021): Government access to data in third countries, S. 25.
URL: https://edpb.europa.eu/our-work-tools/our-documents/legal-study-external-provider/legal-study-government-access-data-third_en [abgerufen am 03.04.2024]

3 LfDI MV (2023): Umfrage: Möglicher Transfer von genetischen Daten in Drittstaaten.
URL: https://www.datenschutz-mv.de/datenschutz/publikationen/Analyse_von_Blutproben/ [abgerufen am 03.04.2024]

5.3. AG Transfertools von Gesundheitsdaten und Biomaterialien in Drittstaaten

Besonders Universitäten, aber auch Unternehmen, betreiben zur Verbesserung der medizinischen Behandlungsmöglichkeiten internationale wissenschaftliche Forschungen. Zu diesem Zwecke sollen Gesundheitsdaten (z. B. Diagnosen, Krankheitsgeschichte) und Biomaterialien (z. B. Blut- oder Gewebeproben) zwischen den beteiligten Forschungseinrichtungen oder Unternehmen ausgetauscht werden können. Auch die Universitätsmedizinen in Rostock und Greifswald engagieren sich für internationale medizinische Forschung im Rahmen des Verbundes Medizininformatik-Initiative (MII).[1] Sofern diese Daten in Drittländer außerhalb der EU und des europäischen Wirtschaftsraumes übermittelt werden sollen, müssen die Anforderungen des Kapitel V DS-GVO eingehalten werden, damit auch bei der Weiterverarbeitung die Rechte und Freiheiten der betroffenen Personen mit einem gleichwertigen Datenschutzniveau sichergestellt sind. In dem Kapitel V werden mehrere mögliche Übermittlungsinstrumente (Transfertools) aufgeführt, auf die eine Übermittlung gestützt werden könnte. Um die Forschenden zur Einhaltung der datenschutzrechtlichen Anforderungen für die Drittlandsübermittlung besser beraten zu können, hat die Taskforce Forschungsdaten der DSK eine AG gemeinsam mit Kolleg:innen aus dem Bereich Internationaler Datenverkehr gegründet. Die AG Transfertools von Gesundheitsdaten und Biomaterialien in Drittstaaten wird vom LfDI MV geleitet und erarbeitet konkrete Empfehlungen für Forschende der MII. Dabei haben die AG Mitglieder im Berichtszeitraum bereits einen konstruktiven Austausch mit Forschenden aufgenommen sowie konkrete Fallbeispiele und mögliche Übermittlungsinstrumente diskutiert. Der Arbeitsauftrag der AG soll im Jahr 2024 abgeschlossen werden.

5.4. DSK Anwendungshinweise zum Angemessenheitsbeschluss für die USA

Nachdem die letzten Angemessenheitsbeschlüsse „Safe Harbor" und „Privacy Shield" für die Übermittlung von personenbezogenen Daten in die Vereinigten Staaten von Amerika (USA) vom EuGH für ungültig erklärt worden waren, lag nunmehr am 10. Juli 2023 ein neuer Angemessenheitsbeschluss für Übermittlungen in die USA vor. Die Europäische Kommission erließ den Angemessenheitsbeschluss gem. Art. 45 DS-GVO auf Grundlage der Verträge im „EU-US Data Privacy Framework". Da viele global aktive Unternehmen ihren Sitz in den USA haben und auch Verantwortliche aus Mecklenburg-Vorpommern auf Dienste von diesen Unternehmen zurückgreifen wollen, sorgte das so geschaffene neue Instrument für Drittlandsübermittlungen gem. Kap V DS-GVO (siehe Punkt 5.2. und 5.3.) für Aufregung. Um Verantwortlichen und Betroffenen einen Überblick zur hauptsächlich englischsprachigen Dokumentation und zu daraus erwachsenden Rechten und Pflichten zu geben, erarbeitete die DSK in ihrem Arbeitskreis Internationaler Datenverkehr gemeinsame Anwendungshinweise. Wir beteiligten uns aktiv an der Erarbeitung der Anwendungshinweise, die seit 4. September 2023 online abrufbar sind.[2]

1 MII: Über die Initiative. URL: https://www.medizininformatik-initiative.de/de/ueber-die-initiative [abgerufen am 03.04.2024]

2 DSK (2023): Übermittlung personenbezogener Daten aus Europa an die USA - Anwendungshinweise zum Angemessenheitsbeschluss der Europäischen Kommission zum Datenschutzrahmen EU-USA (EU-US Data Privacy Framework) vom 10. Juli 2023. URL: https://datenschutzkonferenz-online.de/media/ah/230904_DSK_Ah_EU_US.pdf [abgerufen am 03.04.2024]; siehe auch DSK (2023): Pressemitteilung „Datenschutzkonferenz veröffentlicht Anwendungshinweise zum Angemessenheitsbeschluss zum EU-US Data Privacy Framework". URL: https://www.datenschutzkonferenz-online.de/media/pm/230904_DSK_PM_Anwendungshinweise_EU_US.pdf [abgerufen am 03.04.2024].

5.5. EDSA Streitbeilegungsverfahren zu TikTok

Im Rahmen seines Beitrages zur Tätigkeit des EDSA nahm der LfDI MV im Berichtszeitraum die stellvertretende Ländervertretung in der Enforcement Subgroup wahr (gemäß Art. 57 Abs. 1 lit. t DS-GVO). Im Berichtszeitraum vertrat der LfDI MV die deutschen Datenschutzaufsichtsbehörden der Bundesländer in einer Sitzung der Subgroup für Sanktionen und kommunizierte im Anschluss die Ergebnisse an die anderen deutschen Aufsichtsbehörden. Weiterhin beteiligten wir uns an dem Streitbeilegungsverfahren zu einem Beschlussentwurf aus Irland gegen TikTok Technology Limited, die insbesondere die grundsätzliche Fragen der Verarbeitung von personenbezogenen Daten der zahlreichen minderjährigen Nutzer:innen betraf.

Zum Verfahren: Nachdem die federführenden und betroffenen Datenschutzaufsichtsbehörden im Verfahren gem. Art. 56 DS-GVO via IMI bestimmt worden sind (siehe Punkt 5.1.), läuft die länderübergreifende Bearbeitung gem. Art. 60 DS-GVO konstruktiv und endet in aller Regel mit einem für alle beteiligten Aufsichtsbehörden zufriedenstellenden Verfahrensabschluss. In wenigen Fällen führen verschiedene Rechtsauffassungen dazu, dass ein maßgeblicher und begründeter Einspruch (Art. 4 Nr. 23 DS-GVO) gegen den entworfenen Bescheid der federführenden Aufsichtsbehörde eingelegt wird und selten sind Positionen derart konträr, dass die federführende Datenschutzaufsichtsbehörde den EDSA um eine Entscheidung im Streitbeilegungserfahren gem. Art. 65 DS-GVO ersucht. Die Erarbeitung des verbindlichen Beschlusses des EDSA erfolgt auf der Arbeitsebene sehr kurzfristig in der Enforcement ESG, um einen Beschluss des EDSA innerhalb eines Monats zu ermöglichen.

Im vorliegenden Fall teilte die federführende irische Datenschutzaufsichtsbehörde im September 2022 einen Beschlussentwurf gem. Art. 60 DS-GVO mit den europäischen Kolleg:innen, nachdem die Behörde 2021 auf eigene Initiative hin eine Prüfung der Plattform TikTok des Unternehmens TikTok Technology Limited für den Zeitraum 31.Juli bis 31. Dezember 2020 durchgeführt hatte. Die irischen Kolleg:innen stellten in ihrem Beschlussentwurf fest, dass die Voreinstellungen der Plattform TikTok gegen datenschutzrechtliche Bestimmungen verstoßen, z. B. gegen den Grundsatz der Datenminimierung sowie der Integrität und Vertraulichkeit, und dass das Unternehmen die Risiken für Kinder unter 13 Jahren, die die Plattform nutzen, nicht angemessen bewertet habe.[1] Nebstdem wurden Verstöße gegen Transparenzvorgaben (Art. 12 Abs. 1, Art. 13 Abs. 1 lit. e DS-GVO) festgestellt. Diese Feststellungen wurden nicht angefochten. In den maßgeblichen und begründeten Einsprüchen aus dem Oktober 2022 forderte Deutschland (Berlin und Baden-Württemberg) wegen sogenannter dark patterns[2], einen zusätzlichen Verstoß gegen den Grundsatz der Verarbeitung nach Treu und Glauben (englisch: fairness) gem. Art. 5 Abs. 1 lit. a DS-GVO festzustellen und damit verbundene Abhilfemaßnahmen zu ergreifen sowie eine Geldbuße zu verhängen.

1 Verstöße gegen Art. 25, Abs. 1, 2, Art. 24. Abs. 1, Art. 5 Abs. 1 lit. c, f DS-GVO.

2 Manipulierende Designs, die Nutzer:innen zu Entscheidungen im Sinne des Unternehmens drängen. Ein Beispiel aus dem vorliegenden Fall: bei der Erstellung eines Kontos bestand die Option zwischen einer Schaltfläche links mit „go private" für einen privaten TikTok Account oder auf der rechten Seite eine prominente Schaltfläche mit „Skip", die zu einem öffentlichen Account führte.

Während die irischen Kolleg:innen im Beschlussentwurf feststellten, dass TikTok Technology Limited in Bezug auf die Altersverifizierung der Nutzenden (mind. 13 Jahre) den Anforderungen des Art. 25 Abs. 1 DS-GVO entsprechen würde, fordern die Kolleg:innen aus Italien hier die Feststellung eines zusätzlichen Verstoßes gegen Art. 25 Abs. 1 DS-GVO, da die genutzten Maßnahmen zur Altersüberprüfung ineffektiv seien und Kinder unter 13 Jahren, die jedoch die größte Benutzergruppe abbilden, nicht hinreichend vor den erheblichen Risiken der Plattform schützen würden, sowie eine entsprechend erhöhte Geldbuße.

Nachdem im informellen Austausch keine Einigung erzielt werden konnte, ersuchte die irische Datenschutzaufsichtsbehörde im Mai 2023 den EDSA um die Beilegung des Konflikts. Dem EDSA lagen im Juni alle erforderlichen Unterlagen vor und die Enforcement ESG wurde unter Beteiligung des LfDI MV aktiv. Es wurde bald klar, dass die deutsche Position bis auf das geforderte Bußgeld mehrheitsfähig war. Die Prüfung der rund um die im Untersuchungszeitraum 31. Juli bis 31. Dezember 2020 angemessenen Maßnahmen zur Altersverifizierung erforderten längere Recherche und Debatten, sodass die Stellungnahmefrist des EDSA um einen weiteren Monat verlängert wurde.

Die schlussendlich durch den EDSA getroffene Entscheidung in Form eines verbindlichen Beschlusses vom August 2023 ist (auf Englisch) öffentlich abrufbar.[1] Der EDSA weist zwar die geforderten Bußgelder zurück, da diese nicht hinreichend begründet wären, schließt sich jedoch der deutschen Forderung an, dass die irische Datenschutzaufsichtsbehörde angesichts der dark patterns auf der TikTok Plattform einen Verstoß gegen den Grundsatz der Verarbeitung nach Treu und Glauben bzw. fairness gem. Art. 5 Abs. 1 lit. a DS-GVO feststellen muss. In dem Zuge müsse auch die Maßnahme ergehen, die Einhaltung dieses Grundsatzes anzuordnen. In Bezug auf die italienische Forderung, einen Verstoß gegen die Pflichten des Verantwortlichen gem. Art. 25 Abs. 1 DS-GVO bei der Altersverifizierung der minderjährigen Nutzer:innen festzustellen, lagen dem EDSA nicht genug Informationen vor, um die Einhaltung dieser Vorgaben (wie im irischen Beschlussentwurf) zu bestätigen. Da ernsthafte Bedenken, ob der im Untersuchungszeitraum gewählten Maßnahmen von TikTok Technology Limited zur Altersverifizierung bestehen, wurde die irische Datenschutzaufsichtsbehörde dazu angewiesen, bisher bestehende Aussagen dahingehend zu ändern, dass keine abschließende Bewertung zu Erfüllung der Anforderungen aus Art. 25 Abs. 1 DS-GVO möglich seien. Der überarbeitete irische Beschluss wurde noch im September 2023 erlassen und veröffentlicht.[2]

Das Thema Altersverifizierung bei der Nutzung von Online Plattformen und Netzwerken ist auch weiterhin ein Thema, das zukünftig – unabhängig vom vorgenannten Verfahren – in einer Taskforce der Europäischen Kommission gemeinsam mit Vertreter:innen u. a. der Datenschutzaufsichtsbehörden, aber auch des Jugendmedienschutzes, behandelt werden soll.

1 EDSA Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited (Art. 65 GDPR).
URL: https://www.edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-22023-dispute-submitted_de [abgerufen am 03.04.2024]

2 EDSA / DPC (2023): Decision in the matter of TikTok Technology Limited made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation.
URL: https://www.edpb.europa.eu/our-work-tools/consistency-findings/register-decisions/2023/decision-matter-tiktok-technology_en [abgerufen am 04.04.2024]

Wegen geringer Personalressourcen konnten wir uns im Zeitraum 2022/2023 nicht an weiteren (sehr arbeitsintensiven) verbindlichen Entscheidungen des EDSA, die sich fast alle auf das Unternehmen Meta Ireland Limited mit den Plattformen WhatsApp, Facebook und Instagram bezogen[1] oder weiteren Aktivitäten in der Enforcement Subgroup beteiligen. Gleichwohl traf der EDSA auch für Verantwortliche und betroffene Personen in Mecklenburg-Vorpommern wegweisende Entscheidungen und veröffentlichte Leitlinien, z. B. zum Auskunftsrecht gem. Art. 15 DS-GVO, zu Drittstaatenübermittlungen mittels Zertifizierung oder zur Berechnung von Geldbußen.[2]

6. Beschäftigtendatenschutz

Hinsichtlich des Beschäftigtendatenschutzes ist im Besonderen zu berücksichtigen, dass Arbeitgeber:innen gegenüber den Beschäftigten regelmäßig als wirtschaftlich und strukturell überlegener gelten. Insoweit sind die Beschäftigten als schwächere Vertragspartei ausreichend zu schützen. In diesem Berichtszeitraum beschäftigte sich der LfDI MV daher vertieft mit datenschutzrechtlichen Kontrollen in diesem Bereich. Demzufolge erfolgte im nicht-öffentlichen Bereich die Kontrolle zweier in Mecklenburg-Vorpommern ansässiger Callcenter (siehe Punkt 6.1.) und im öffentlichen Bereich führten wir eine Überprüfung eines Landkreises durch (siehe Punkt 6.2.). Von zentraler Bedeutung für unsere Arbeit ist weiterhin die Entscheidung des Europäischen Gerichtshofes (EuGH) vom 30. März 2023 in der Rechtssache C-34/21 gewesen, welcher nochmals die Erforderlichkeit eines eigenen Beschäftigtendatenschutzgesetzes unterstreicht (siehe Punkt 6.3.).

6.1. Kontrollen in Callcentern

Wir führten im Sommer 2023 Kontrollen in zwei Callcentern durch, die ihren Standort in Mecklenburg-Vorpommern haben. Wegen eines bezeichnenden Anstiegs von Beschwerden betroffener Arbeitnehmer:innen im Bereich des Beschäftigtendatenschutzes entschieden wir uns dazu, stichprobenartige, anlasslose Kontrollen mit dem Fokus auf Beschäftigtendaten durchzuführen. Mitarbeiter:innen in dieser Branche hatten uns aufgezeigt, dass sie einem extremen Kontrolldruck ausgesetzt seien. Daher war es unser Ziel, verantwortliche Arbeitgeber:innen für die Einhaltung der DS-GVO zu sensibilisieren und ein höheres Datenschutzniveau insbesondere auch im Bereich des Beschäftigtendatenschutzes zu erreichen.

1 Alle bindenden Entscheidungen des EDSA sind online abrufbar:
URL: https://www.edpb.europa.eu/our-work-tools/consistency-findings/binding-decisions_de [abgerufen am 03.04.2024]

2 Alle Leitlinien (Guidelines) und Empfehlungen (Recommendations) des EDSA sind (z. T. auch auf Deutsch) online abrufbar:
URL: https://www.edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_de [abgerufen am 03.04.2024]

Ende Juni 2023 wurde zunächst in Schwerin eine vor Ort Kontrolle in einem Callcenter durchgeführt, die in sehr kooperativer Weise verlief. Nach dieser Kontrolle forderten wir noch weitere Unterlagen an, die im Anschluss ausgewertet wurden. Eine weitere Kontrolle eines Callcenters im ländlichen Raum von Mecklenburg-Vorpommern verlief ebenfalls ähnlich. Die Beteiligten zeigten sich durchaus kooperativ und aufgeschlossen für Datenschutzanliegen im Bereich des Beschäftigtendatenschutzes.

Das Ziel der Kontrollen war es nicht, Verstöße zu sanktionieren, sondern für die Einhaltung datenschutzrechtlicher Vorgaben zu sensibilisieren. Im Zusammenhang mit diesen Kontrollen der Callcenter in unserem Bundesland ließ sich jedoch feststellen, dass die meisten Callcenter zwar Standorte in Mecklenburg-Vorpommern betreiben, diese aber nicht als selbstständige Niederlassungen zu bewerten sind und der dazugehörige Firmen- bzw. Hauptsitz außerhalb Mecklenburg-Vorpommerns liegt. Diese unterliegen dann nicht der Aufsichtsbefugnis des LfDI MV, sondern der Kontrollpflicht der Datenschutzaufsichtsbehörde in dem Bundesland, in dem die Callcenter ihren Hauptsitz haben.

6.2. Kontrolle eines Landkreises

Aufgrund zahlreicher Beschwerden im Bereich des Beschäftigtendatenschutzes, welche sich zunehmend auch gegen öffentliche Stellen als Arbeitgeber richteten, führte der LfDI MV im Sommer 2023 eine Kontrolle eines Landkreises in Mecklenburg-Vorpommern durch.

Im Vorfeld der Datenschutzkontrolle forderten wir zahlreiche Dokumente an. Der Fokus hierbei lag insbesondere auf vorhandene Dienstvereinbarungen, welche spezifische Rechtsgrundlagen für die Verarbeitung von personenbezogenen Daten im Beschäftigungsverhältnis darstellen können, sowie Formulare hinsichtlich der Informationspflichten gemäß Art. 13 DS-GVO, Auszüge aus dem Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO und das Rechte- und Rollenkonzept für die Personaldatenverwaltung.

Im weiteren Verlauf der Prüfung und nach Durchführung eines vor Ort Termins, in welchem sich aus den eingereichten Unterlagen ergebende Fragen klären ließen, verdeutlichte sich insbesondere die Notwendigkeit einer Festlegung und Erfassung von Prozessen, mithilfe derer neben der aktiven Verbesserung von Geschäftsprozessen auch der Rechenschaftspflicht gegenüber der Datenschutzaufsichtsbehörde gem. Art. 5 Abs. 2 DS-GVO nachgekommen werden kann.

Weiterhin lag im Rahmen dieser Prüfung ein besonderes Augenmerk auf dem Umgang mit Daten der Beschäftigten des Landkreises in den jeweiligen Fachämtern, wenn diese nicht als Beschäftigte, sondern als betroffene Bürger:innen auftreten und Dienstleistungen des Landkreises in Anspruch nehmen. Nicht selten werden in diesem Kontext auch sensible Daten, wie Angaben zu den sozialen sowie finanziellen Verhältnissen des jeweiligen Mitarbeitenden oder besondere Kategorien personenbezogener Daten i.S.v. Art. 9 DS-GVO, wie zum Beispiel Gesundheitsdaten, verarbeitet. Deren Kenntnisnahme durch Vorgesetzte oder Kollegen:innen könnte – wenn auch nur mittelbar – Auswirkungen auf das Beschäftigungsverhältnis haben. Es wurde deutlich, dass Verantwortliche diese Art von Fallkonstellation bislang nicht im Blick hatten.

Der LfDI MV wies daher eindringlich darauf hin, einen entsprechenden Prozess zum Umgang mit Vorgängen betreffend der eigenen Mitarbeiter:innen, die als Bürger:innen in den Fachämtern auftreten, zu etablieren. Dieser gewährleistet, dass der Kreis der kenntnisnehmenden Mitarbeitenden (bzw. Kolleg:innen) möglichst kleingehalten wird. Dies kann durch den Einsatz entsprechender TOMs, beispielsweise durch die Möglichkeit des Setzens von Sperrvermerken in den einzelnen Fachverfahren, sichergestellt werden.

Auch perspektivisch werden weitere Kontrollen von Kommunen im Bereich des Beschäftigtendatenschutzes in Betracht gezogen, um ein einheitliches Datenschutzniveau zu fördern und öffentliche Stellen in ihrer Funktion als Arbeitgeber:innen im Umgang mit personenbezogenen Beschäftigtendaten zu sensibilisieren.

6.3. EuGH-Urteil vom 30. März 2023 Rs. C-34/21 zu den Anforderungen an gesetzliche Regelungen zum Beschäftigtendatenschutz

Bereits in ihrer Entschließung vom 20. April 2022 (Die Zeit für ein Beschäftigtendatenschutz ist „Jetzt")[1] stellte die DSK fest, dass die bestehende bundesrechtliche Regelung des § 26 des Bundesdatenschutzgesetzes (BDSG) im Beschäftigtenkontext nicht hinreichend praktikabel, normenklar sowie sachgerecht ist und als Generalklausel sehr weite Interpretationsspielräume eröffnet. Diese Feststellung wurde im Berichtszeitraum 2023 durch das Urteil des EuGH vom 30. März 2023 in der Rechtssache C-34/21 bestätigt, in welchem über die europarechtskonforme Umsetzung des Beschäftigtendatenschutzrechts in Hessen entschieden wurde.

Grundsätzlich ist der Schutz personenbezogener Daten für alle Mitgliedsstaaten der Europäischen Union verbindlich in der DS-GVO geregelt. Die Mitgliedsstaaten dürfen jedoch aufgrund der Öffnungsklauseln bestimmte Fallkonstellationen eigenmächtig regeln. Eine solche Öffnungsklausel stellt beispielweise Art. 88 DS-GVO für den Beschäftigtendatenschutz dar. Nach Art. 88 Abs. 1 DS-GVO können die Mitgliedsstaaten spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten vorsehen. Diese müssen nach Art. 88 Abs. 2 DS-GVO geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Personen umfassen, z. B. im Hinblick auf die Transparenz der Datenverarbeitung und die Überwachungssysteme am Arbeitsplatz. In Mecklenburg-Vorpommern sind dies konkret § 26 Abs. 1 Satz 1 BDSG für den nicht-öffentlichen Bereich und § 10 Abs. 1 Satz 1 Landesdatenschutzgesetz (DSG M-V) für den öffentlichen Bereich sowie § 84 Abs. 1 des Landesbeamtengesetzes Mecklenburg-Vorpommern (LBG M-V) für Personalaktendaten im öffentlichen Dienst.

1 DSK vom 29. April 2022: Die Zeit für ein Beschäftigtendatenschutzgesetz ist „Jetzt"!
URL: https://www.datenschutzkonferenz-online.de/media/en/Entschliessung_Forderungen_zum_Beschaeftigtendatenschutz.pdf [abgerufen am 09.04.2024]

Die Ausführungen des EuGH lassen erkennen, dass das Gericht die Auffassung vertritt, dass die hessische Regelung des § 23 Abs. 1 Satz 1 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes (HDSIG) zur Verarbeitung personenbezogener Daten von Beschäftigten im öffentlichen Bereich keine spezifischere Bestimmung im Sinne des Art. 88 Abs. 1 DS-GVO ist. Die Vorschrift wiederholt lediglich die in Art. 6 Abs. 1 lit. b DS-GVO aufgestellte Bedingung, dass die Datenverarbeitung für die Erfüllung eines Vertrags erforderlich ist, fügt aber keine spezifischere Vorschrift im Sinne des Art. 88 Abs. 1 DS-GVO hinzu. Außerdem macht die Vorschrift nach Auffassung des EuGH keine dem Maßstab des Art. 88 Abs. 2 DS-GVO entsprechenden Vorgaben. § 23 Abs. 5 des HDSIG verweist lediglich – ebenso wie § 26 Abs. 5 BDSG – darauf, dass der Verantwortliche geeignete Maßnahmen ergreifen muss, um sicherzustellen, dass insbesondere die in Art. 5 DS-GVO genannten Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden.

Der EuGH stellte zudem klar, dass es den nationalen Gerichten zu beurteilen obliegt, ob die jeweiligen bundes- bzw. landesrechtlichen Regelungen die in Art. 88 DS-GVO vorgegebenen Voraussetzungen und Grenzen beachten. Hinsichtlich der hessischen Regelungen des § 23 Abs. 1 Satz 1 HDSIG und § 86 Abs. 4 des Hessischen Beamtengesetz (HBG) bleibt daher aktuell abzuwarten, wie und in welchem Umfang das VG Frankfurt über die Anwendbarkeit von § 23 Abs. 1 Satz 1 HDSIG entscheiden wird.

Da die Vorschrift des § 23 Abs. 1 HDSIG in ihrem Wortlaut in weiten Teilen mit den entsprechenden Regelungen der meisten Landesdatenschutz- und Beamtengesetze sowie mit § 26 Abs. 1 BDSG weitestgehend identisch ist, ist die Entscheidung des EuGH bundesweit, und somit auch in Mecklenburg-Vorpommern, von großer Bedeutung.

Insgesamt ist aus der Entscheidung abzuleiten, dass der nationale Gesetzgeber detailliertere Regelungen bezüglich des Beschäftigtendatenschutzes erlassen muss. Die DSK verabschiedete in diesem Zusammenhang bereits eine Entschließung zu dem Urteil („Europäischer Gerichtshof stärkt Forderung der DSK zur Schaffung spezifischer Regelungen zum Beschäftigtendatenschutz in Deutschland“[1]).

Wir empfehlen daher auch der Landesregierung, die bestehenden Regelungen zur Verarbeitung von Beschäftigtendaten im Landesdatenschutzgesetz und im Landesbeamtengesetz zu prüfen.

1 DSK Entschließung vom 11. Mai 2023. URL: https://www.datenschutzkonferenz-online.de/media/en/2023-05-11_DSK-Entschliessung_Beschaeftigtendatenschutz.pdf [abgerufen am 09.04.2024]

7. Videoüberwachung

Sobald es um den Schutz von Eigentum geht, sind Videokameras oft das Mittel der Wahl. Sie erweitern das Sichtfeld und haben sogar ein eigenes (Speicher-) Gedächtnis, jedenfalls soweit dies vom Benutzenden gewollt ist. Videokameras werden daher in Kraftfahrzeugen verbaut, von Privatpersonen auf dem eigenen Grundstück installiert und auch auf vielen öffentlichen Plätzen und in öffentlichen Gebäuden eingesetzt. Da die Anschaffungspreise der Videokameras oder gar von Videoüberwachungssystemen recht übersichtlich sind, ist ein solches Gerät recht schnell an einem privaten Wohnhaus oder in einem Betrieb installiert. Genauso schnell häufen sich dann die Beschwerden beim LfDI MV mit der Bitte um datenschutzrechtliche Überprüfung dieser Kamerasysteme.

Aus datenschutzrechtlicher Sicht steht einer Videoüberwachung unter Einhaltung der rechtlichen Voraussetzungen nichts im Wege. Eine Videoüberwachung, bei der nur personenbezogene Daten verarbeitet werden, die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten und ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen werden (Erwägungsgrund 18 zur DS-GVO), fallen nicht unter die Anwendung der DS-GVO. So kann das eigene Grundstück, welches von den Eigentümer:innen auch nur selbst genutzt wird, grundsätzlich bis zur eigenen Grundstücksgrenze überwacht werden. Sobald die Eigentümer:innen als Verantwortliche der Videokamera das Nachbargrundstück mit aufnehmen, kann der mögliche Eingriff der Verantwortlichen in die Persönlichkeitsrechte des Betroffenen durch diesen zivilgerichtlich geltend gemacht werden und im Rahmen von zivilgerichtlichen Abwehr- und Unterlassungsansprüchen abgestellt werden lassen (§§ 823, 1004 BGB).

Ein Großteil der eingereichten Beschwerden, in der die Zulässigkeit einer Videoüberwachung hinterfragt wird, richtet sich hingegen in den meisten Fällen nach Art. 6 Abs. 1 lit. f DS-GVO. Hierbei müssen die Wahrung berechtigter Interessen, die Erforderlichkeit und eine Interessenabwägung beachtet werden. Berücksichtigt werden somit nicht nur die berechtigten Interessen des Verantwortlichen, sondern auch die berechtigen Interessen Dritter. Im Folgenden werden exemplarisch drei Szenarien beschrieben, die zu Beschwerden beim LfDI MV im Berichtszeitraum geführt haben.

7.1. Klingelkameras

Der Einsatz sogenannter Klingelkameras wird in letzter Zeit immer beliebter. So suggerieren einige Hersteller, dass sich mit einer Klingelkamera via App von jedem Punkt der Welt aus und jederzeit optisch und akustisch feststellen lässt, wer vor der eigenen Tür steht. Dabei ist zu beachten, dass nicht alle zur Verfügung stehenden Funktionen einer Klingelkamera in Einklang mit dem Datenschutz stehen.

Beim Einsatz von Klingelkameras muss ebenso eine Abwägung der berechtigten Interessen gem. Art. 6 Abs. 1 lit. f DS-GVO erfolgen. Die Haus- oder Wohnungsbesitzer haben grundsätzlich ein berechtigtes Interesse daran, zu erfahren, wer vor ihrer Tür steht. Aber gleichwohl haben auch benachbarte Personen im Mehrfamilienhaus ein berechtigtes Interesse daran, nicht ständig vor ihrer Wohnungstür gefilmt zu werden.

Gerade in einem Mehrfamilienhaus besteht der betroffene Personenkreis aus Nachbar:innen und deren Besucher:innen, die in diesem Fall ständig der Kamera ausgesetzt sind und deren Interesse an einer Vermeidung dieser Überwachung höher zu werten ist. Anders könnte die Wertung ausfallen, wenn die Türklingelkamera auf dem eigenen Grundstück verwendet wird und Nachbar:innen oder andere Personen nicht betroffen sind.

Weiterhin ist bei der Interessenabwägung auch der Informationsgehalt der Daten zu berücksichtigen. Je mehr persönliche Informationen mit einer Klingelkamera erhoben werden, desto intensiver ist der Eingriff in die Rechte und schutzwürdigen Interessen der Betroffenen. Überwachungsmaßnahmen, denen ein Betroffener nicht ausweichen kann und die dauerhaft erfolgen, intensivieren einen Eingriff.

Dieser Eingriff in die Rechte und schutzwürdigen Interessen der Betroffenen kann darüber hinaus nach Art und Weise der Verarbeitung unterschiedlich intensiv erfolgen. Bei einer Klingelkamera soll lediglich beim Auslösen des Klingelknopfs an der Tür ein Bild in Echtzeit angezeigt werden. Dagegen ist beim anlasslosen Ausspähen des Geschehens vor der Tür oder bei einer Speicherung der Daten im Internet regelmäßig das Interesse der Betroffenen höher zu werten.

Grundsätzlich bestehen gegen eine Klingelkamera somit keine datenschutzrechtlichen Bedenken, wenn:

» die Kamera nur anlassbezogen durch das Klingeln an der Tür aktiviert wird,

» sie nur den unmittelbaren Eingangsbereich (Nahbereich) vor der Tür erfasst,

» sie nach kurzer Zeit automatisch wieder deaktiviert wird,

» keine Übertragung des Livebildes über das Internet erfolgt,

» keine dauerhafte Aufnahme der Bilder erfolgt und

» an der Tür bzw. an der Türklingel durch ein deutlich sichtbares Hinweisschild auf die Kamera aufmerksam gemacht wird.

Viele Klingelkameras verfügen jedoch über weitaus mehr als die genannten Funktionen. Wird eine Klingelkamera mit Funktionen betrieben, die nach datenschutzrechtlichen Gesichtspunkten nicht vertretbar sind, kann dies einen Verstoß gegen die DS-GVO darstellen, welcher mit einem Bußgeld geahndet werden kann.

7.2. Videoüberwachung durch Wahlkreisbüro

Durch eine Presseanfrage zur Zulässigkeit einer Videoüberwachung wurden wir auf eine Kamera aufmerksam, die augenscheinlich aus einem Wahlkreisbüro heraus den öffentlichen Raum, d. h. den Gehweg und die Straße in der Schweriner Altstadt filmte. Durch die Pressestelle der Partei wurde ein Bild der Überwachungskamera veröffentlicht, auf welchem ein Vertreter einer anderen Partei vor dem Wahlkreisbüros abgebildet war. Das Büro befindet sich im Erdgeschoß eines Mehrfamilienhauses. Um den Eingang zu den Wohnungen des Hauses zu betreten, muss man zuvor die Eingangstür des Büros passieren, deren obere Hälfte mit einer Glasscheibe versehen ist.

Unsere Auswertung der zur Videoüberwachung angeforderten Unterlagen und Bilder ergab, dass insgesamt zwei Kameras im Büro installiert waren. Eine war auf die Eingangstür zum Büro ausgerichtet, die andere, von der auch das o. g. Bild stammte, war auf die großflächige Fensterfront des Büros gerichtet. Jede Person, die den nach hinten gelagerten Eingang zum Flur der Wohnungen nutzen wollte, wurde durch die Scheibe der Tür von der Kamera erfasst. Von der Kamera, die auf die großflächige Fensterfront gerichtet war, wurden alle Personen erfasst, die das Büro auf dem Gehweg oder der Straße passierten. Zum Hintergrund der Installation der Kameras wurde ausgeführt, dass die Landtagsabgeordnete selbst und auch ihre Angestellte in der Vergangenheit Ziel von Anfeindungen worden war, bei welchen es nicht nur verbale Auseinandersetzungen, sondern auch körperliche Übergriffe gegeben hatte. Weiterhin war das Büro bereits Ziel von Schmierereien und Farbbeutelwürfen.

In Anbetracht dieser Vorfälle ist es grundsätzlich nachvollziehbar, eine Videoüberwachung zum Zweck der Aufklärung und Beweissicherung zu installieren, allerdings nicht in der beschriebenen Art und Weise, wobei der öffentliche Raum und damit alle Personen, die das Büro passierten, mitgefilmt wurden. Nach Art. 6 Abs. 1 lit. f DS-GVO und der einschlägigen Rechtsprechung ist eine Videoüberwachung zum Zwecke der Vandalismusbekämpfung und Aufklärung dann zulässig, wenn die Hausfassade filmt und gemessen von der Hauswand maximal einen Meter des öffentlichen Raumes miterfasst werden. In diesem Fall wäre es demnach legitim gewesen, einen Teil des Gehweges zu filmen. Weiterhin muss die Möglichkeit gegeben sein, dass Personen den Bereich vor dem Büro passieren können müssen, ohne von der Kamera erfasst zu werden.

Da die in der oben beschriebenen Form installierten Kameras datenschutzrechtlich unzulässig waren, erging eine Verwarnung durch den LfDI MV. Weiterhin wurde angeordnet, dass die Kameras datenschutzkonform einzustellen und auszurichten sind. Bis dahin wurde der Betrieb der Kameras untersagt. Zwei Wochen nach Zustellung des Untersagungs- und Anordnungsescheides erfolgte durch uns eine unangekündigte Kontrolle im Wahlkreisbüro. Hierbei wurde festgestellt, dass unserer Anordnung Folge geleistet wurde. Die Kameras wurden im abgeschalteten Zustand vorgefunden.

7.3. Videoüberwachung mit Wildkameras in den Wäldern

Datenschutzrechtliche Fragen der Videoüberwachung stellen sich nicht nur vor privaten Eingangsbereichen oder auf öffentlichen Straßen und Wegen. Auch innerhalb der Wälder Mecklenburg-Vorpommerns gibt es Videokameras. Diese werden vor allem durch Waldbesitzer:innen und Jäger:innen im Wald aufgestellt, um beispielsweise die Entwicklung der Tierbestände und deren Laufwege zu kontrollieren. Weiterhin können so auch Futterstellen oder Hochstände beobachtet werden, um diese vor wiederholter Beschädigung zu schützen. Die Aufnahme von Waldbesucher:innen ist bei solchen Kameras meist nicht gewollt, kann aber dennoch erfolgen.

Der Wald hat neben vielen anderen Funktionen auch eine Erholungsfunktion. Gemäß § 28 Abs. 1 S. 1 Landeswaldgesetz Mecklenburg-Vorpommern (LWaldG) ist es grundsätzlich jeder Person gestattet, den Wald zum Zweck der Erholung zu betreten. Werden Waldflächen oder Waldwege mit sogenannten Wildkameras überwacht und bestehen für diese Bereiche keine Betretungsverbote, handelt es sich dabei um eine Videoüberwachung öffentlicher Räume.

Bei einer Überwachung mittels Wildkamera ist den Persönlichkeitsrechten der betroffenen Waldbesucher:innen ein hoher Stellenwert einzuräumen. Sie nutzen den Wald in ihrer Freizeit und um sich zu erholen. Waldbesucher:innen müssen nicht mit einer (ggf. heimlichen oder versteckten) Kameraüberwachung rechnen. Liegt ein berechtigtes Interesse des Überwachenden nach Art. 6 Abs. 1 lit. f DS-GVO vor, kann eine Videoüberwachung mit einer Wildkamera zulässig sein, wenn die Aufnahme von Menschen äußerst unwahrscheinlich ist und mit allen verfügbaren Mitteln vom Betreibenden ausgeschlossen wird. Dies ist beispielsweise möglich, indem eine Kirr- oder Futterstelle nur unmittelbar auf Kniehöhe aufgenommen wird, d. h. die Kamera auf ungefähr einem Meter Höhe angebracht und direkt auf den Waldboden oder eine Futterstelle ausgerichtet ist. Bereiche, die sich in unmittelbarer Nähe zu einem Waldweg, einer Grillstelle und insbesondere einem Spielplatz befinden, dürfen grundsätzlich nicht überwacht werden. Eine Videoüberwachung ist somit nur im Einzelfall zulässig.

Wenn das Aufstellen einer Wildkamera im Wald zulässig sein sollte, ist ebenso wie auch bei anderen Videoüberwachungen auf eine transparente und umfassende Information gem. Art. 13 DS-GVO zu achten. So müssen an der Kamera Hinweise zum Umstand der Beobachtung (Piktogramm, Kamerasymbol), die Identität des für die Videoüberwachung Verantwortlichen (Name einschl. Kontaktdaten), die Kontaktdaten des betrieblichen Datenschutzbeauftragten (soweit bestellt, dann aber zwingend), Verarbeitungszwecke und Rechtsgrundlage in Schlagworten, die Angabe des berechtigten Interesses, die Dauer der Speicherung, ein Hinweis auf Zugang zu den weiteren Pflichtinformationen wie Auskunftsrecht, Beschwerderecht und ggf. weitere Empfänger der Daten angegeben werden. Diese Hinweise müssen im Bereich der Kamera stehen, bevor die betroffene Person in den Überwachungsbereich gelangt. Allein ein Hinweis bei Betreten des Waldes reicht hier nicht aus.

Die Kamera ist technisch so einzustellen, dass keine Videosequenzen, sondern Einzelbilder mit einigen Sekunden Abstand aufgenommen werden. Die Auflösung der Kamera sollte gering gewählt sein. Ist eine Überwachung von Tieren in der Nacht geplant, ist die Kamera tagsüber auszuschalten. Vor dem Einsatz einer Wildkamera müssen zudem immer mildere Mittel geprüft werden. Hier könnte beispielsweise der Einsatz von Wilduhren oder Infrarotkameras in Betracht kommen.

7.4. Videoüberwachung in Kommunen

Im vergangenen Berichtszeitraum informierten sich häufig Kommunen beim LfDI MV darüber, ob datenschutzrechtliche Bedenken bei der Installation einer Videokamera bestünden. Dabei ging es zum Beispiel um die Überwachung eines kommunalen Parkplatzes, einer kommunalen Müllsammelstelle oder auch eines öffentlichen Marktplatzes. Da eine Videoüberwachung regelmäßig erheblich in das Recht auf informationelle Selbstbestimmung eingreift, kann eine solche nur basierend auf einer Rechtsgrundlage durchgeführt werden. Die Kommunen hatten die entsprechenden Vorschriften der DS-GVO und des Landesrechts zu prüfen, wobei es nicht selten Unsicherheiten gab.

Als Rechtsgrundlagen für eine Videoüberwachung öffentlich zugänglicher Räume durch öffentliche Stellen kommen vor allem zwei verschiedene Rechtsgrundlagen in Betracht. Im Anwendungsbereich der DS-GVO ist zunächst Art. 6 Abs. 1 lit. e i.V.m. Art. 6 Abs. 2 bzw. 3 DS-GVO i.V.m. § 11 DSG M-V zu prüfen.

Gemäß § 11 Abs. 1 DSG M-V ist die Verarbeitung personenbezogener Daten mit Hilfe einer Videoüberwachung zulässig, wenn dies zur Wahrnehmung des Hausrechts, zum Schutz des Eigentums oder Besitzes oder zur Kontrolle von Zugangsberechtigungen erforderlich ist und keine Anhaltspunkte bestehen, dass überwiegende schutzwürdige Interessen der Betroffenen entgegenstehen.

Eine Videoüberwachung ist also nur zu diesen gesetzlich konkret festgelegten Zwecken erlaubt. Bezüglich der Wahrnehmung des Hausrechts ist zu beachten, dass öffentliche Stellen kein Hausrecht für den öffentlichen Verkehrsraum geltend machen können, der allen Personen zur Nutzung bereit steht. Es muss sich zumindest um befriedetes Besitztum handeln. In Bezug auf den Schutz des Eigentums oder Besitzes ist entscheidend, ob die Gemeinde selbst Eigentümerin der in Rede stehenden Örtlichkeit ist und sich für dieses Eigentum eine konkrete Gefahr anhand konkreter Vorfälle aus der Vergangenheit substantiiert darlegen lässt. Hinzu kommt, dass eine Videoüberwachung in diesem Zusammenhang auch erforderlich sein muss. Es ist also zu prüfen, ob alternative Maßnahmen in Frage kämen, die milder oder gleich wirksam sind.

Weiterhin dürfen keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen. Der mit der Beobachtung bzw. Aufzeichnung verfolgte Zweck muss also in einem angemessenen Verhältnis zu den schutzwürdigen Interessen aller Betroffenen im Einzelfall stehen. Eine Videoüberwachung ist besonders dann als ein intensiver Eingriff in die Rechte der Betroffenen zu gewichten, wenn diese sich normgerecht verhalten und damit keinen Anlass für eine Überwachung geben.

Selbst wenn die o. g. gesetzlichen Voraussetzungen vorlagen, dürfte es in den meisten geschilderten Fällen so gewesen sein, dass die schutzwürdigen Belange aller sich rechtstreu verhaltenden Bürger:innen gegenüber den Interessen an einer Videoüberwachung zur Verfolgung einiger weniger Personen, die Sachbeschädigungen oder Ordnungswidrigkeiten begangen hatten, überwogen haben, zum Beispiel auf einem Parkplatz oder bei der ordnungsgemäßen Abfallentsorgung. Die Schutzbedürftigkeit der Interessen aller Betroffenen war in Bezug auf den jeweiligen Einsatzort einer Videokamera im Einzelfall somit immer sorgsam zu prüfen.

Eine weitere Rechtsgrundlage für die Videoüberwachung des öffentlichen Raums besteht in § 32 Abs. 3 SOG M-V. Diese Rechtsgrundlage kommt dann in Betracht, wenn eine Videoüberwachung zu Zwecken der Gefahrenabwehr erfolgen soll. Die Aufgabe, Gefahren von der Allgemeinheit oder dem Einzelnen abzuwehren und somit die öffentliche Sicherheit oder Ordnung zu wahren, obliegt nicht nur der Polizei, sondern auch den Ordnungsbehörden (§ 2 Abs. 1 SOG M-V). So ist eine Videoüberwachung beispielsweise auch durch Landräte, Bürgermeister:innen oder Amtsvorsteher:innen als kommunale Ordnungsbehörden im Bereich der Gefahrenabwehr grundsätzlich möglich.

Konkret dürfen nach § 32 Abs. 3 SOG M-V personenbezogene Daten offen mit technischen Mitteln zur Bildaufzeichnung erhoben werden, soweit an öffentlich zugänglichen Orten wiederholt Straftaten begangen worden sind und konkrete Tatsachen die Annahme rechtfertigen, dass dort künftig mit der Begehung von Straftaten zu rechnen ist. Einerseits müssen somit an dem öffentlich zugänglichen Ort Straftaten in entsprechend hoher Anzahl begangen worden sein, die sich substantiiert anhand einer Kriminalstatistik darlegen lassen. Andererseits muss aus einer Kriminalitätsprognose hervorgehen, dass an diesem Ort auch in der Zukunft die Begehung von Straftaten zu erwarten ist. Eine Bewertung und Darstellung der Kriminalität anhand der polizeilich erhobenen Daten zu Straftaten an dem betreffenden Ort ist folglich unumgänglich. Ferner muss eine Videoüberwachung i.S.d. § 32 Abs. 3 SOG M-V im jeweiligen Einzelfall auch geeignet, erforderlich und angemessen sein. Häufig ist davon auszugehen, dass Videoüberwachungen öffentlicher Räume bereits an der Prüfung der Erforderlichkeit scheitern, da zumeist mildere, gleich geeignete Maßnahmen zur Verfügung stehen. Insbesondere in der Prüfung der Angemessenheit ist auch zu berücksichtigen, dass bei Videoüberwachungen des öffentlichen Raums eine Vielzahl von Personen von der Datenerhebung betroffen ist, obwohl von dieser keine Gefahr ausgeht. Stattdessen werden auch sich rechtskonform verhaltende Bürger:innen durch eine Videoüberwachung weitreichenden Grundrechtseingriffen ausgesetzt, die sich im Verhältnis zum Zweck – der Gefahrenabwehr – nur überaus selten als angemessen erweisen. Grundsätzlich kommt eine Videoüberwachung i.S.d. § 32 Abs. 3 SOG M-V somit lediglich an sog. Kriminalitäts-Hotspots in Betracht. Keineswegs erweisen sich hier nur vereinzelte, geringfügige Straftaten bzw. Bagatelldelikte als ausreichend. Eine Videoüberwachung nach § 32 Abs. 3 SOG M-V bedarf jeweils einer Anordnung durch die Leitung der zuständigen Behörde, in welcher u. a. auch die entsprechenden Gründe auszuführen sind. Über diese Anordnung ist der LfDI MV unverzüglich zu unterrichten (§ 32 Abs. 5 SOG M-V), woraufhin jeweils eine Prüfung durch uns eingeleitet wird. Soweit die datenschutzrechtlichen Voraussetzungen, beispielsweise Anforderungen an die Hinweisbeschilderung oder die Sicherheit der technischen Ausgestaltung nicht erfüllt werden, kann dies ein Einschreiten des LfDI MV begründen.

Wir haben den Eindruck gewonnen, dass den Kommunen die gesetzlichen Voraussetzungen für eine Videoüberwachung nicht immer bewusst waren. So haben sich auch Bürger:innen gemeldet, die den Einsatz von Videokameras hinterfragt bzw. sich beschwert haben, so dass die betreffende Kamera letztendlich entfernt werden musste. Positiv fällt auf, dass uns jedoch viele Kommunen im Vorfeld kontaktiert haben und wir einer rechtswidrigen Handhabung einer Videoüberwachung somit frühzeitig entgegenwirken konnten.

8. Behörden, Gesundheit und Soziales

Im Berichtszeitraum überwogen Beschwerden gegen öffentliche Stellen und Stellen des Gesundheitsbereichs, sowohl öffentlicher als auch nicht-öffentlicher Natur, wegen der Nichterfüllung von Betroffenenrechten (siehe Punkt 8.3.). Dieses Phänomen scheint sich nicht nur auf Mecklenburg-Vorpommern zu beschränken. Der EuGH erließ auch im Laufe des Berichtszeitraums maßgebliche Entscheidungen zu den Betroffenenrechten, die für Klarheit sorgen. Ein weiterer Beschwerdeschwerpunkt lässt sich bei Gemeinden und Gemeindevertretern erkennen (siehe Punkt 8.1. und 8.2.). Darüber hinaus setzten wir uns in zahlreichen Beratungen mit der Stellung der behördlichen Datenschutzbeauftragten auseinander (siehe Punkt 8.6.).

8.1. Gemeindevertreter:innen benötigen datenschutzkonforme mobile Endgeräte

Anlässlich eines Hinweises einer Gemeindevertretung überprüften wir in einer Gemeinde die Ausstattung der Gemeindevertretungen mit datenschutzkonformen mobilen Endgeräten. Mit der Übernahme eines Amtes in der Gemeindevertretung gibt es die Möglichkeit, gestaltend auf die Entwicklung der Kommune und Lebensumstände der Bürgerschaft einzuwirken. Die Handlungsfähigkeit der Gemeindevertretenden hängt in hohem Maße von Vorteilen der elektronischen Kommunikation untereinander und mit den Gemeindeverwaltungen ab. Mit dieser Aufgabe übernehmen sie gleichzeitig eine besondere Verantwortung gegenüber den Einwohner:innen der Gemeinde im Hinblick auf deren Persönlichkeitsrechte. Dazu zählt selbstverständlich auch das Grundrecht auf informationelle Selbstbestimmung. Es ist notwendig, dass im Rahmen dieser Tätigkeit persönliche Daten der Bürger:innen bekannt werden, mit denen sie umgehen müssen und die sie bei ihren Entscheidungen zu berücksichtigen haben. Darüber hinaus ist es erforderlich, in der Gemeindevertretung darauf zu achten, dass alle personenbezogenen Daten vor dem Zugriff Dritter, wie beispielsweise Familienangehörigen, Arbeitgebern oder Parteifreunden, zu schützen sind, ungeachtet der Form: in Akten oder als automatisierte Datei auf privaten oder dienstlichen Computern. Insbesondere bei der Nutzung privater oder beruflicher E-Mail-Accounts durch die Gemeindevertretenden ist nicht abschließend sichergestellt, dass nicht auch andere Personen Zugriff auf diesen Account haben. Dabei müssen Ausstattung und Konfiguration der Geräte dem notwendigen Schutzniveau der Datenverarbeitung entsprechen.

Wir empfehlen daher, die Gemeindevertretungen in ihrer Arbeit zu unterstützen und dafür eine datenschutzkonforme und sichere Arbeitsumgebung zur Verfügung zu stellen. Ausgewählte Anforderungen, die an die Beschaffung sicherer mobiler Endgeräte gestellt werden, sind beispielsweise in den Mindeststandards des BSI für Mobile Device Management[1] und in der Technischen Richtlinie des BSI (TR-03180 – KritKat Smartphone – Kriterienkatalog zur Bewertung des IT-Sicherheitsniveaus von Smartphones & Tablets)[2] dokumentiert.

8.2. E-Mail-Kommunikation im Rahmen von Gemeindevertretungen

Im Rahmen der datenschutzrechtlichen Anfragen wurde mehrfach die Problematik an uns herangetragen, ob Gemeindevertreter:innen[3] zur Ausübung ihres Mandats private oder berufliche[4] E-Mail-Accounts verwenden können. Im Ergebnis waren diese Anfragen damit zu beantworten, dass eine Verwendung privater oder beruflicher E-Mail-Accounts zu Zwecken der Mandatsausübung von Mitgliedern in kommunalen Vertretungsorganen nicht den datenschutzrechtlichen Anforderungen entspricht.

Die Nutzung von E-Mails für den Austausch zwischen Gemeindevertretung und Verwaltung, innerhalb der Gemeindevertretungen und ggf. mit Dritten ist eine Verarbeitung personenbezogener Daten im Sinne des Art. 4 Nr. 1 und 2 DS-GVO. Es können zum Beispiel personenbezogene Daten von Verwaltungsbediensteten, Sachkundigen, Bürger:innen sowie selbst von Mitgliedern der Gemeindevertretung aus dem geschlossenen Teil von Gemeindevertretungssitzungen sowie Protokollen, die nicht für die Öffentlichkeit bestimmt sind, betroffen sein. Spezielle Aufmerksamkeit erfordern die besonderen Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DS-GVO, wie zum Beispiel religiöse und weltanschauliche Überzeugungen, politischen Meinungen oder sogar Gesundheitsdaten. Für die Verarbeitung gilt der Grundsatz der Integrität und Vertraulichkeit nach Art. 5 Abs. 1 lit. f DS-GVO. Daher muss eine angemessene Sicherheit der personenbezogenen Daten gewährleistet werden. Es sind in diesem Zusammenhang TOMs notwendig, die eine unbefugte Offenlegung personenbezogener Daten an Dritte ausschließen. Insbesondere bei der Nutzung privater oder beruflicher E-Mail-Accounts durch die Gemeindevertretenden ist nicht abschließend sichergestellt, dass nicht auch andere Personen Zugriff auf diesen Account haben. Dabei müssen Ausstattung und Konfiguration der Geräte dem notwendigen Schutzniveau der Datenverarbeitung entsprechen. Ausgehend von dem Grundsatz der Vertraulichkeit und Integrität sind somit nach Art. 24 Abs. 1, Art. 32 Abs. 1 DS-GVO die geeigneten TOMs zu treffen, um ein dem Risiko angemessenes Schutzniveau zu leisten.

1 Mindeststandard des BSI für Mobile Device Management. URL:https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Mobile-Device-ManagementV2_0.pdf?__blob=publicationFile&v=2 [abgerufen am 19.03.2024]

2 BSI TR-03180 Kriterienkatalog zur Bewertung des IT-Sicherheitsniveaus von Smartphones & Tablets; URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03180/TR-03180_node.html#doc1105472bodyText1 [abgerufen am 19.03.2024]

3 Dies betrifft ebenso Mitglieder einer Stadtvertretung bzw. Bürgerschaft. Durchaus trifft dies aber auch auf Mitglieder weiterer kommunaler Vertretungsorgane zu.

4 Hierunter werden folgend E-Mail-Accounts aus beruflichen Tätigkeiten von Gemeindevertretungsmitgliedern außerhalb des Mandats verstanden.

Einerseits müssen in diesem Zusammenhang auch TOMs ergriffen werden, die eine unbefugte Offenlegung personenbezogener Daten an Dritte ausschließen. Gerade bei einem privaten E-Mail-Account ist jedoch nicht abschließend sichergestellt, dass neben dem Gemeindevertretungsmitglied auch weitere Personen, wie beispielweise Familienmitglieder, hierauf Zugriff haben, womit diesen unbefugt personenbezogene Daten zur Kenntnis gebracht werden könnten. Dies gilt insbesondere auch für E-Mail-Accounts aus beruflichen Tätigkeiten von Gemeindevertretungsmitgliedern außerhalb des Mandats, da hierbei möglicherweise der jeweilige Arbeitgeber Einsicht nehmen könnte. Ferner würde es auch besonders dem Grundsatz der Zweckbindung nach Art. 5 Abs. 1 lit. b DS-GVO zuwiderlaufen, wenn zum Zweck der Mandatsausübung verarbeitete personenbezogene Daten im Rahmen einer beruflichen Tätigkeit außerhalb des Mandats weiterverarbeitet werden würden.[1]

Andererseits müssen auch TOMs zur Integrität und Vertraulichkeit personenbezogener Daten durch den Verantwortlichen nicht nur ergriffen, sondern auch kontrollierbar, nachweisbar und durchsetzbar sein (vgl. u. a. Art. 5 Abs. 2 DS-GVO). Im Kontext von Gemeindevertretungen entscheiden deren Mitglieder i.d.R. nicht im eigenen Namen und meist auch nicht allein über Datenverarbeitungen ihrer Gemeinde. Die Mitglieder der Gemeindevertretung wirken vielmehr an den Entscheidungen der Gemeindevertretung mit, die ihrerseits als Organ der Gemeinde handelt. Das Handeln dieses Organs wird dann der Gemeinde zugerechnet, womit in der Folge die jeweilige Gemeinde als Gebietskörperschaft (vertreten durch die/den Bürgermeister:in) als Verantwortlicher i.S.d. Art. 4 Nr. 7 DS-GVO für Verarbeitungen personenbezogener Daten durch die Gemeindevertretung bzw. die Mitglieder der Gemeindevertretung gilt. Insoweit muss die Gemeinde als Verantwortlicher die Verarbeitung personenbezogener Daten durch die Gemeindevertretung kontrollieren und die Einhaltung datenschutzrechtlicher Bestimmungen nachweisen sowie durchsetzen können. Sofern jedoch Mitglieder der Gemeindevertretung private oder berufliche E-Mail-Accounts nutzen, kann dies nicht abschließend gewährleitstet werden, da sich diese der Sphäre der Gemeinde entziehen.

Ferner ist bei der Nutzung von privaten oder beruflichen E-Mail-Accounts durch Mitglieder der Gemeindevertretung nicht auszuschließen, dass aufgrund der Serverstandorte der Provider Übermittlungen personenbezogener Daten in ein Drittland erfolgen (Art. 44 DS-GVO). Für derartige Verarbeitungen personenbezogener Daten müssten zusätzlich die Voraussetzungen nach Art. 44 ff. DS-GVO, wie bspw. eines Angemessenheitsbeschlusses i.S.d. Art. 45 DS-GVO, vorliegen. Soweit E-Mail-Provider als Auftragsverarbeiter beteiligt werden, bedarf es vor allem auch eines Vertrages über die Auftragsverarbeitung nach Art. 28 Abs. 3 DS-GVO, der ebenso datenschutzrechtlichen Anforderungen entsprechen muss.

1 Zudem würde es für eine derartige Weiterverarbeitung generell an einer Rechtsgrundlage fehlen.

In unserer Beratungspraxis weisen wir daher insgesamt darauf hin, dass aus datenschutzrechtlicher Perspektive eine strikte Trennung zwischen der Sphäre der Ausübung des Mandats von Mitgliedern der Gemeindevertretung und der privaten sowie beruflichen Sphäre der Gemeindevertreter:innen vorzunehmen ist. Die Nutzung eines privaten oder beruflichen E-Mail-Accounts von Mitgliedern der Gemeindevertretung zur Ausübung ihres Mandats wird datenschutzrechtlichen Anforderungen, insbesondere der Gewährleistung des Grundsatzes der Integrität und Vertraulichkeit nach Art. 5 Abs. 1 lit. f DS-GVO, nicht gerecht. Als datenschutzrechtskonforme Alternative kommt stattdessen in Betracht, dass die Gemeinden den Gemeindevertreter:innen für die Ausübung ihres Mandats eine gemeindliche/dienstliche E-Mail-Adresse zur Verfügung zu stellen, für welche die Gemeinde die Einhaltung datenschutzrechtlicher Anforderungen gewährleisten kann. Für die Umsetzung durch die Gemeinden wird insbesondere die Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail" der DSK[1] empfohlen.

8.3. Standardprozesse für Auskünfte nach Art. 15 DS-GVO durch die Kommunen

Im Berichtszeitraum beschwerte sich eine zunehmende Zahl betroffener Personen über nicht oder unvollständig erteilte Auskünfte gem. Art. 15 DS-GVO bzw. darüber, dass die Formalitäten (Frist, Begründung) gem. Art. 12 DS-GVO nicht eingehalten wurden. Das Auskunftsrecht nach Art. 15 DS-GVO ist ein bedeutsames Betroffenenrecht. Demnach können betroffene Personen von dem für die Datenverarbeitung Verantwortlichen eine Auskunft darüber verlangen, welche Daten über sie gespeichert sind bzw. verarbeitet werden. Verantwortliche müssen betroffenen Personen außerdem u. a. über die Verarbeitungszwecke, die Herkunft der Daten, soweit diese nicht direkt beim Betroffen erhoben wurden, oder über die konkreten Empfänger, an die diese Daten übermittelt worden sind, informieren. Dieses Recht steht allen Bürger:innen gegenüber öffentlichen Stellen (z. B. Behörden) und nicht-öffentlichen Stellen (z. B. Wirtschaftsunternehmen, Verbänden, Vereinen etc.) zu. 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. Das Auskunftsrecht bezieht sich nicht nur auf sogenannte Stammdaten wie etwa Name, Adresse und Geburtsdatum, sondern beispielsweise auch auf die geführte Kommunikation und interne Vermerke der Behörde, soweit diese personenbezogene Daten enthalten. Häufig ergibt sich Inhalt und Sinn von Informationen, die sich auf eine betroffene Person beziehen, auch erst aus dem Verarbeitungskontext, z. B. durch Korrespondenz zwischen Verantwortlichem und betroffener Person. In diesem Fall sind in der Regel die entsprechenden Dokumente vollständig (in Kopie) herauszugeben. Hierbei ist von einem weiten Verständnis von personenbezogenen Daten auszugehen.

1 DSK, Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail, Orientierungshilfe vom 16.06.2021.
URL: https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Broschueren/20210616_OH_E-Mail.pdf [abgerufen am 03.04.2024]

Das Oberverwaltungsgericht (OVG) Greifswald[1] bestätigte im Berichtszeitraum eine Entscheidung des Verwaltungsgericht (VG) Schwerin[2] zu einer Anordnung des LfDI MV, wonach die Kopie eines Immobilien-Beweissicherungsgutachtens zu einem Gebäude nach Art. 15 Abs. 3 DS-GVO herauszugeben war. Die Inanspruchnahme des Auskunftsrechts ist grundsätzlich kostenlos. Der Verantwortliche muss der betroffenen Person die Informationen unverzüglich, in jedem Fall aber 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 aufwändig 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 aber verspätet erteilt wird. Falls eine Auskunft jedoch verspätet erteilt oder etwa ohne Angaben 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. Insofern ist dennoch zu betonen, dass allein die Tatsache, dass die betroffene Person nicht primär die datenschutzrechtliche Überprüfung ihrer Daten verfolgt, den Auskunftsanspruch nicht rechtsmissbräuchlich macht (siehe Punkt 8.7.).

Im Berichtszeitraum wurde allerdings in Fällen, in denen eine Vielzahl von Behörden mit identischen und umfangreichen Fragekatalogen konfrontiert waren, die offenkundig das Ziel verfolgten, die Arbeitsfähigkeit der betroffenen Behörden und Gerichte zu beeinträchtigen, eine exzessive Geltendmachung von Betroffenenrechten angenommen. Die Beschwerdeführerin klagte gegen diese Entscheidung. Eine Entscheidung des VG Schwerin steht noch aus.

Eine Zunahme der Geltendmachung des Auskunftsanspruchs ist auch gegenüber Jugendämtern zu beobachten. Hier ist der Anspruch grds. spezialgesetzlich in § 83 SGB X geregelt, wobei allerdings fraglich ist, ob die dortigen Einschränkungen von Art. 15 DS-GVO europarechtskonform sind. Einige Jugendämter kamen diesen Ansprüchen zunächst nicht oder nur teilweise nach und argumentierten diesbezüglich häufig mit den Rechten bzw. dem Schutz Dritter gem. Art. 65 Abs. 1 SGB VIII oder § 25 Abs. 2 SGB X, da gerade im Zusammenhang mit den Verfahren der Jugendämter eine Auskunft über personenbezogene Daten auch Angaben über Dritte, bspw. Kinder, Partner:innen oder Gutachter:innen enthalten kann.

1 OVG Greifswald, Beschluss vom 14. Dezember 2023 – 1 LZ 413/21 OVG.

2 VG Schwerin (1. Kammer), Urteil vom 29.04.2021 – 1 A 1343/19.

Unabhängig von der Frage, ob diese Regelungen den Auskunftsanspruch einschränken können, ist jedenfalls festzuhalten, dass dies nicht zu einer pauschalen Verweigerung der Auskunft führen darf. Zwar enthält auch Art. 15 Abs. 4 DS-GVO die Bestimmung, dass die Kopie die Rechte und Freiheiten anderer Personen nicht beeinträchtigen darf. Hier ist dennoch vom Verantwortlichen zu verlangen, dass etwa eine Schwärzung oder Teilentnahmen veranlasst. Stützt sich das Jugendamt auf § 65 Abs. 1 Nr. 1 SGB VIII und argumentiert damit, dass die in Rede stehenden Daten ihm zum Zwecke persönlicher und erzieherischer Hilfe anvertraut worden sind und keine Einwilligung von der Person vorliegt, die die Daten dem Jugendamt anvertrauten, darf dies nicht pauschal geschehen, sondern muss hinterfragt bzw. gegebenenfalls dargelegt werden. Bei den Gesprächen mit einigen Jugendämtern bzw. Landkreisen ist deutlich geworden, dass gerade bei Familienrechtsverfahren, bei denen es meistens um Sorge-, Umgangs- und Unterhaltsrecht geht, die Sachverhalte mehrere Personen betreffen und miteinander verwoben und schwer voneinander abzugrenzen sind. Nichtsdestotrotz müssen die Unterlagen unter diesem Gesichtspunkt geprüft und gegebenenfalls geschwärzt werden. Hinzukommen muss, dass dritte Personen danach gefragt worden sein müssen, ob die anvertrauten Daten im konkreten Fall offengelegt werden dürfen, bevor deren entgegenstehendes Interesse pauschal angenommen wird.

Wir empfehlen daher den Behördenleitungen verbindliche Verfahrensabläufe zu beschreiben und Zuständigkeiten für die Bearbeitung der Auskunftsersuchenden nach Artikel 12, 15 DS-GVO zu benennen. Hinzu sollten alle Behördenmitarbeitenden regelmäßig in den Datenschutzschulungen auf diesen Rechtsanspruch der Bürger:innen hingewiesen und mit den Prozessabläufen vertraut gemacht werden.

8.4. Förderung von Mini-Solaranlagen

Das Ministerium für Klimaschutz, Landwirtschaft, ländliche Räume und Umwelt Mecklenburg-Vorpommern gewährte eine Förderung für die Anschaffung und Installation von sogenannten Mini-Solaranlagen. Entsprechende Anträge konnten beim Landesförderinstitut Mecklenburg-Vorpommern gestellt werden, welches auch für die Verarbeitung der personenbezogenen Daten bei der Antragstellung verantwortlich war. Im Zusammenhang mit diesem Fördermittelverfahren erhielten wir Beschwerden. Diese bezogen sich auf das entsprechende Antragsformular, welches unter anderem die Forderung enthielt, dem Antrag eine vollständige Kopie des Personalausweises beizufügen.

Vor diesem Hintergrund forderten wir das Landesförderinstitut zur Stellungnahme auf. Danach ist Rechtsgrundlage für die Forderung nach einer Kopie des Personalausweises Art. 6 Abs. 1 lit. e DS-GVO i.V.m. § 4 Abs. 1 DSG MV, § 44 Landeshaushaltsordnung MV (LHO MV) sowie der Richtlinie für die Gewährung von Zuwendungen für steckerfertige Photovoltaik (PV)-Anlagen für Bürger:innen des Landes Mecklenburg-Vorpommern.

Das Land etablierte für dieses Förderprogramm im Interesse der Antragstellenden ein vereinfachtes Antrags- und Abrechnungsverfahren. Somit wurde die Zuwendung abweichend von den Festlegungen der LHO MV vor Bestandskraft des Zuwendungsbescheids ausgezahlt.

Ein derart vereinfachtes Verfahren erfordere nach Aussage des Landesförderinstituts geeignete Prüfroutinen zum Schutz vor missbräuchlichen Anträgen. Das hätten vor allem auch die Erfahrungen bei der Gewährung der Corona-Soforthilfen gezeigt. Daher müsse zumindest sichergestellt werden, dass der Antragsteller tatsächlich existiere und am angegeben Ort wohne. Für ein solches Massenverfahren für Privatpersonen sind uns die Argumente bezüglich der Erforderlichkeit dieser personenbezogenen Daten für die Antragstellung nachvollziehbar dargelegt worden. Die Vorlage der vollständigen Kopie des Personalausweises hielten wir dennoch für zu umfangreich und erachteten somit nicht als zulässig. Es wurde eine Schwärzung der nicht erforderlichen personenbezogenen Daten auf dem Personalausweis gefordert. Das Landesförderinstitut ist dem nachgekommen, sodass lediglich der vollständige Name und die dazugehörige vollständige Adresse lesbar sein mussten. Die entsprechenden Informationen zum Antragsverfahren auf der Homepage des Landesförderinstituts wurden um einen entsprechenden Hinweis ergänzt.

8.5. SEPA-Lastschriftverfahren bei Zahlungen an Kommunen

Im Berichtszeitraum gingen dem LfDI MV mehrere voneinander unabhängige Beschwerden zu, die im Zusammenhang mit Zahlungen von Bürger:innen an Kommunen bzw. dem hierzu genutzten SEPA-Lastschriftverfahren standen. Dieses Verfahren wird insbesondere häufig bei wiederkehrenden Zahlungen, beispielhaft im Kontext von steuerlichen Angelegenheiten oder bestimmten weiteren Abgabearten, eingesetzt. Gegenstand der Beschwerden war im Kontext des Lastschriftverfahrens die Angabe der Kontoverbindung von Bürger:innen in postalisch durch die Kommunen versandten Bescheiden.

Soweit das SEPA-Lastschriftverfahren genutzt werden soll, ist dieses an einen festgelegten Ablauf gebunden. Zunächst bedarf es der Erteilung des SEPA-Lastschriftmandats zur Autorisierung zukünftiger Zahlungen. Soweit Bürger:innen das SEPA-Lastschriftverfahren nutzen wollen, geht mit der Erteilung des Lastschriftmandats freilich die Angabe der jeweiligen Kontoverbindung/International Bank Account Number (IBAN) einher, damit von dem entsprechenden Konto Zahlungen eingezogen werden können. Im Weiteren muss vor jedem Zahlungseinzug eine sogenannte PreNotification/Vorabinformation erteilt werden. Mit dieser wird Zahlungsschuldnern innerhalb des SEPA-Verfahrens die Belastung mittels SEPA-Lastschrift angekündigt.

Eben diese Vorabinformation war Gegenstand der Beschwerden. Mit den jeweiligen Abgabebescheiden wurde die Vorabinformation über den Lastschrifteinzug erteilt, woran rechtlich zunächst keine Zweifel bestehen. Die Vorabinformation bedarf keiner bestimmten Form und kann beispielhaft unproblematisch mit einem Bescheid oder einer Rechnung erteilt werden. Im Wege der Information über den Lastschrifteinzug wurde jedoch durch die Kommunen in den postalisch versandten Schreiben jeweils die vollständige IBAN der betreffenden Bürger:innen angegeben. Diese befürchteten, soweit die Briefe in falsche Hände gelangen, dass ihre Kontodaten möglicherweise missbräuchlich genutzt werden könnten. Die Befürchtungen wurden zudem dadurch befördert, dass Postsendungen an die Beschwerdeführenden bereits abhandengekommen seien.

Tatsächlich wurde in einem Fall auch bekannt, dass der betreffende Bescheid mit Vorabinformation und Kontoverbindung nicht ordnungsgemäß zugestellt wurde, sondern der geöffnete Briefumschlag im öffentlichen Raum aufgefunden worden ist, womit die Kontoverbindung einem unbestimmten Empfängerkreis zugänglich gewesen war.

Insoweit es sich bei der Angabe der IBAN in der Vorabinformation um eine Verarbeitung personenbezogener Daten handelt, bemisst sich diese auch an den Grundsätzen der Datenminimierung sowie Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. c, f DS-GVO). Durchaus sind Gründe für die Angabe der IBAN in der Vorabinformation ersichtlich. Beispielsweise können Bürger:innen in einer derartigen Vorabinformation somit Fehlbuchungen oder veraltete Kontoverbindungen schneller erkennen. Es ist jedoch nicht ersichtlich, warum eine vollständige Angabe der IBAN erforderlich sein sollte. Eine rechtskonforme Vorabinformation verlangt lediglich, dass der Lastschriftschuldner mindestens 14 Tage vor dem Fälligkeitsdatum – oder unter Einhaltung einer Vereinbarung zu einer abweichenden Frist – über den Einziehungstag und Einziehungsbetrag zu unterrichten ist. Eine vollständige Angabe der IBAN von Bürger:innen in einer Vorabinformation im Rahmen des SEPA-Lastschriftverfahrens wäre somit nicht mit den Grundsätzen der Datenminimierung sowie Integrität und Vertraulichkeit vereinbar. Gegenüber den betreffenden Kommunen wurde in diesem Zusammenhang ein förmlicher Hinweis nach Art. 58 Abs. 1 lit. d DS-GVO erteilt. Ferner wurde auf eine Umstellung des Verfahrens hingewirkt, wonach Bestandteile der IBAN durch Platzhalter unkenntlich gemacht werden. Damit wird einerseits die Erkennung von Fehlbuchungen ermöglicht, andererseits wird der Schutz personenbezogener Daten, hier der Kontoverbindung, gewährleistet. Die betreffenden Kommunen stellten das Verfahren auf Anlass des Hinweises um.

8.6. Stellung und Aufgaben der behördlichen Datenschutzbeauftragten

Gemäß Art. 37 Abs. 1 lit. a DS-GVO besteht für Behörden/öffentliche Stellen die Pflicht einen behördlichen Datenschutzbeauftragten (bDSB) zu benennen (mit Ausnahme von Gerichten, soweit sie im Rahmen ihrer justiziellen Tätigkeit handeln). Einerseits sind bereits bei der Benennung vielfältige Voraussetzungen – insbesondere mit Blick auf die Vermeidung von Interessenskonflikten – zu berücksichtigen; andererseits sind bezüglich der Erfüllung des verantwortungsvollen und weitläufigen Aufgabenbereichs der bDSBs Anforderungen des Unionsgesetzgebers zu erfüllen. In der ganz überwiegend überaus positiv und konstruktiv geprägten Zusammenarbeit zwischen dem LfDI MV und den bDSBs von Behörden auf Kommunal- sowie Landesebene sind diesbezüglich vereinzelt Fragen aufgeworfen bzw. Anfragen an uns herangetragen worden.

Interessenkonflikte

Zunächst ist vor der Benennung eines bDSBs durch den Verantwortlichen zu prüfen, ob eine jeweilige Person für die Funktion des bDSB in Betracht kommt. Dies bezieht sich nebst der Qualifikation (Art. 37 Abs. 5 DS-GVO) besonders auf die Gewährleistung der Weisungsfreiheit und Vermeidung von Interessenkonflikten (Art. 38 Abs. 3 und 6 DS-GVO).

Denn grundsätzlich ist es nicht ausgeschlossen, dass ein bDSB neben Aufgaben, die mit dieser Funktion einhergehen, auch andere Aufgaben und Pflichten wahrnimmt (Art. 38 Abs. 6 DS-GVO). Vermehrt wird dies sogar den Regelfall darstellen. In diesem Fall ist sicherzustellen, dass zwischen der Erfüllung der Aufgaben des bDSBs nach Art. 38 Abs. 4, Art. 39 DS-GVO und den sonstigen Aufgaben kein Interessenkonflikt besteht und die Unabhängigkeit des bDSBs nicht gefährdet wird (Art. 38 Abs. 3 und 6 DS-GVO). Dabei kann sich ein Interessenkonflikt insbesondere daraus ergeben, dass es neben der Beratungsfunktion vordergründige Aufgabe eines bDSB ist, die Einhaltung datenschutzrechtlicher Vorschriften in der jeweiligen Behörde zu überwachen und zu kontrollieren. Soweit ein bDSB jedoch mit sonstigen Aufgaben betraut ist, im Rahmen dieser er über Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet, würde dies zu einer Konstellation führen, in der sich ein bDSB selbst kontrollieren müsste, mithin eine Interessenkollision vorläge bzw. keine effektive Kontrolle gewährleistet wäre. Eine Prüfung auf derartige etwaige Interessenkonflikte ist durch den Verantwortlichen sowohl vor einer Benennung eines bDSB als auch bei jeder Übertragung neuer sonstiger Aufgaben auf einen bereits benannten bDSB im Einzelfall durchzuführen. Gleichwohl diese Prüfung einer Einzelfallbetrachtung bedarf, lassen sich bestimmte Kategorien von sonstigen Aufgaben und Stellungen innerhalb einer Behörde benennen, die mit der Funktion des bDSB regelmäßig inkompatibel sind bzw. mit einem unzulässigen Interessenkonflikt einhergehen:

» Behördenleitung und herausgehobene Führungs-/Leitungspositionen

» Aufgabenbereiche, die Verarbeitungsvorgänge umfassen, die umfangreich sind oder besondere Kategorien personenbezogener Daten betreffen (bspw. beim Umgang mit Beschäftigtendaten in der Personalverwaltung: Leitung und nachgeordnete Beschäftigte betreffend)

» Leitung Justiziariat/Rechtsangelegenheiten (nicht aber auf Beschäftigte ohne Leitungsfunktion zutreffend)

» Leitung und/oder administrativ tätige Beschäftigte im Bereich der Informationstechnik

» Geheimschutzbeauftragte

» Informationssicherheitsbeauftragte (soweit nicht lediglich Kontrollaufgaben wahrgenommen werden)

» Gleichstellungsbeauftragte

Soweit öffentliche Stellen/Behörden einen externen bDSB nach Art. 37 Abs. 6 DS-GVO benennen, müssen auch in dieser Konstellation Interessenkonflikte ausgeschlossen sein. Insgesamt ist eine Unvereinbarkeit von Tätigkeiten grundsätzlich dann anzunehmen, wenn der bDSB u. a. sich selbst kontrollieren müsste bzw. wenn er zugleich im nennenswerten Umfang Aufgaben wahrnimmt, die nach der DS-GVO dem für die Verarbeitung Verantwortlichen zugeordnet sind. Dann wäre eine effektive Kontrolle durch den bDSB nicht gewährleistet.

Unterstützungspflicht/Bereitstellung erforderlicher Ressourcen

Das Aufgabenspektrum der (b)DSBs nach Art. 38 Abs. 4, Art. 39 DS-GVO ist überaus vielschichtig und mit umfangreichen Aufgaben verbunden. Insofern regelte der Unionsgesetzgeber, dass der Verantwortliche den (b)DSB bei der Erfüllung seiner Aufgaben unterstützen muss, indem er die für die Erfüllung dieser Aufgaben erforderlichen Ressourcen und den Zugang zu personenbezogenen Datenund Verarbeitungsvorgängen sowie die zur Erhaltung des Fachwissens erforderlichen Ressourcen zur Verfügung stellt (Art. 38 Abs. 2 DS-GVO).

Insbesondere bei Behörden mit einer großen Anzahl Beschäftigter, einem weitreichenden Zuständigkeitsbereich und/oder in denen aufgrund des spezifischen Aufgabenbereichs eine Vielzahl von komplexen oder risikoreichen Verarbeitungen (auch besonderer Kategorien personenbezogener Daten) vorgenommen wird, erweisen sich die zur Verfügung stehenden Ressourcen oftmals als Begrenzung der Aufgabenerfüllung. Unabhängig davon, wie ressourcenintensiv die Erfüllung der Aufgaben des bDSB entsprechend des jeweiligen Zuständigkeitsbereiches oder der Beschaffenheit der Verarbeitungen personenbezogener Daten in einer Behörde ausfällt, ist es Pflicht des Verantwortlichen dem bDSB die vollständige und effektive Erfüllung seiner Aufgaben zu ermöglichen. Die bereitzustellenden Ressourcen für die Aufgabenerfüllung umfassen daher auch die zur Verfügung stehende Arbeitszeit, etwaiges (Hilfs)Personal, ITGeräte, Software, Fachliteratur, die entsprechenden Räumlichkeiten sowie im Lichte von Art. 38 Abs. 3 Satz 3 DS-GVO ein regelmäßiges und unmittelbares Vortragsrecht bei der Behördenleitung.

Angenommen, dass die Funktion des bDSB nicht als alleinige Tätigkeit ausgeübt wird, sondern einem bDSB in einer Behörde hinzu sonstige Aufgaben zugewiesen sind, wird sich vermehrt die verfügbare Arbeitszeit als begrenzende Ressource für die Aufgabenerfüllung erweisen. Gerade bei öffentlichen Stellen müssen wir häufig feststellen, dass den bDSBs zur Aufgabenerfüllung nicht genügend Zeit zur Verfügung steht und Aufgaben nach Art. 38 Abs. 4, Art. 39 DS-GVO eher beiläufig nachgekommen werden muss. Regelmäßig wird der Eindruck erweckt, dass die Benennung als bDSB keine oder lediglich unzureichende Berücksichtigung in den Anteilen einer Stelle findet. Soweit jedoch Aufgaben der bDSBs schlicht zusätzlich übertragen werden, ohne eine Anpassung im Hinblick auf die Stellenanteile vorzunehmen, kann sich die verfügbare Arbeitszeit nicht als ausreichend erweisen. Eine Arbeitsbelastung durch sonstige übertragene Aufgaben nach Art. 38 Abs. 6 DS-GVO darf nicht dazu führen, dass die Aufgaben des bDSB nur unvollständig oder gar nicht erfüllt werden. Im Kontext von Behörden/öffentlichen Stellen ist es Aufgabe des bDSB intern die Verarbeitung von personenbezogenen Daten u. a. von Bürger:innen sowie Beschäftigten zu überwachen und den Verantwortlichen bei Ihrer Aufgabenwahrnehmung ausreichend zu beraten. Diese Aufgaben dürfen keinesfalls vernachlässigt werden. Wenn das dem bDSB zur Verfügung stehende Zeitkontingent zur vollständigen Aufgabenerfüllung unter Berücksichtigung arbeitsschutzrechtlicher Regelungen nicht ausreichend ist, muss der Verantwortliche den bDSB von den sonstig übertragenen Aufgaben ggf. anteilig oder vollständig entlasten oder die Erfüllung der Aufgaben des bDSB anderweitig gewährleisten. Dies kann bspw. auch dadurch erfolgen, dass dem bDSB (Hilfs-) Personal bereitgestellt wird.

Mit Blick auf die Räumlichkeiten, die dem bDSB vom Verantwortlichen zur Verfügung zu stellen sind, muss in diesen die Einhaltung der Geheimhaltungspflicht des bDSB aus Art. 38 Abs. 5 DS-GVO möglich sein. Auch gebietet die Vertraulichkeitsverpflichtung i.S.d. Art. 38 Abs. 5 DS-GVO, dass der bDSB jederzeit vertraulich kontaktiert werden kann. Aus den Pflichten zur Geheimhaltung und Vertraulichkeit folgt darüber hinaus, dass dem bDSB entsprechende Kommunikationsmittel zur Verfügung zu stellen sind. So ist beispielhaft ein E-Mail-Postfach (bspw. Funktionspostfach) zur Verfügung zu stellen, welches diese Anforderungen erfüllt bzw. mithin keine Einsicht durch andere Personen außer dem bDSB zulässt. Gleichsam müssen dem bDSB unter Wahrung der Geheimhaltungspflicht vertrauliche Telefonate möglich sein.

Falls der Pflicht zur Bereitstellung der erforderlichen Ressourcen oder der Unterstützungspflicht des bDSB durch den Verantwortlichen nicht nachgekommen wird, stellt dies einen Verstoß gegen Art. 38 Abs. 2 DS-GVO dar, der ein aufsichtsbehördliches Einschreiten gegen den Verantwortlichen begründen könnte. Zur Gewährleistung der Unterstützungspflichten und Bereitstellung der erforderlichen Ressourcen wird ein Austausch hierüber zwischen Behördenleitung und bDSB in regelmäßigen Abständen empfohlen, um etwaige erforderliche Maßnahmen für die Ermöglichung der vollständigen Aufgabenerfüllung des bDSB ableiten zu können.

Interne Einbindung und Meldung der bDSBs an den LfDI MV

Oftmals werden an den LfDI MV von Behörden/öffentlichen Stellen Fragestellungen zu komplexen Verarbeitungen personenbezogener Daten herangetragen, denen wir uns im Rahmen unser personellen Kapazitäten gerne annehmen. Durch einen frühzeitigen Einbezug des LfDI MV bei Vorhaben, die die Verarbeitung personenbezogener Daten betreffen, können etwaige Problematiken regelmäßig bereits im Vorfeld datenschutzrechtskonform gelöst werden. Einen offenen Austausch zwischen Behörden/öffentlichen Stellen und LfDI MV erachten wir als überaus begrüßenswert und unabdinglich.

Soweit eine Anfrage einer Behörde/öffentlichen Stelle jedoch nicht durch einen bDSB an uns herangetragen wird, geht hiermit regelmäßig unsere Rückfrage einher, ob der bDSB in das betreffende Vorhaben bereits eingebunden wurde. Diese Rückfrage bezieht sich jeweils auf Art. 38 Abs. 1 DS-GVO, wonach der Verantwortliche sicherstellen muss, dass der (b)DSB ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird. In Bezug auf diese Regelung ist nicht zu verkennen, dass es sich um eine Pflicht der verantwortlichen Stelle handelt. Vereinzelt wird bei Anfragen, die nicht durch einen bDSB an den LfDI MV herangetragen werden, der Anschein erweckt, dass der bDSB möglicherweise umgangen wird. Dies wäre jedoch nicht mit der Pflicht des Verantwortlichen zur frühzeitigen internen Einbindung des bDSB vereinbar und würde eine effektive Erfüllung der Aufgaben des bDSB gefährden. Weiterhin würde bei einer fehlenden Einbindung die Expertise der bDSBs ungenutzt bleiben.

Überdies ist darauf hinzuweisen, dass mitunter aufgrund der Aufgabe des bDSBs, der Zusammenarbeit mit der Aufsichtsbehörde und Anlaufstelle für diese (Art. 39 Abs. 1 lit. d, e DS-GVO), die Kontaktdaten des bDSB an die Aufsichtsbehörde mitzuteilen sind (Art. 37 Abs. 7 DS-GVO). Hierzu kann das auf unserer Website zur Verfügung stehende Meldeformular genutzt werden.[1]

Verantwortung für die Einhaltung datenschutzrechtlicher Bestimmungen

Abschließend ist darauf aufmerksam zu machen, dass die Verantwortung für die Einhaltung datenschutzrechtlicher Bestimmungen für Verarbeitungstätigkeiten des Verantwortlichen nicht dem bDSB obliegt. Der Unionsgesetzgeber stellt in Art. 24 Abs. 1 DS-GVO ausdrücklich klar, dass es die Pflicht des Verantwortlichen – und nicht die des bDSB – bleibt, sicherzustellen und nachzuweisen, dass die Datenverarbeitungen im Einklang mit den Regelungen der DS-GVO stehen. Gleichwohl sollte der bDSB seine Tätigkeiten in angemessener Weise dokumentieren, um ggf. nachweisen zu können, dass er seinen Aufgaben ordnungsgemäß nachgekommen ist. Der bDSB hat zwar primär eine interne Beratungs- und Kontrollfunktion gegenüber dem Verantwortlichen, doch können originäre datenschutzrechtliche Aufgaben sowie Verpflichtungen des Verantwortlichen grundsätzlich nicht auf den bDSB übertragen werden. Dies würde zur eingangs geschilderten Konstellation führen, in der sich ein bDSB selbst kontrollieren müsste. Damit bestünde eine unzulässige Interessenkollision und die Kontrollfunktion des bDSB würde leerlaufen.

Wir appellieren an alle öffentlichen Stellen sowohl auf Kommunal- als auch Landesebene – aber auch Verantwortliche darüber hinaus – den (b)DSBs im Einklang Art. 38 Abs. 2 DS-GVO die erforderlichen Ressourcen, insbesondere entsprechende Zeitkontingente, für die Aufgabenerfüllung zur Verfügung zu stellen, die (b)DSBs in alle mit dem Schutz personenbezogener Daten zusammenhängenden Frage einzubinden und die (b)DSBs bei der Erfüllung ihrer Aufgaben zu unterstützen.

8.7. Rechtsprechung des EuGH zum Recht auf Kopie der Patientenakte

Regelmäßig erreichen uns Anfragen und Beschwerden von betroffenen Personen, denen die Einsicht in ihre Patientenakte verwehrt, nur sehr beschränkt oder nur gegen Übernahme der Kopierkosten gewährt wird. Ein Grund für die Vielzahl der Beschwerden in diesem Bereich war eine offene Rechtsfrage, die der EuGH nunmehr klarstellte. Zwar regelt die DS-GVO unmittelbar im Art. 12 Art. und 15 Abs. 3 DS-GVO, dass betroffene Personen ein Recht auf Erhalt einer kostenlosen Kopie der über sie verarbeiteten personenbezogenen Daten haben. In Deutschland gibt es jedoch mit § 630g des Bürgerlichen Gesetzbuch (BGB) eine spezifische Regelung zur Einsicht in die Patientenakte. Verantwortliche legten vielfach dar, dass diese Regelung den europäischen Regelungen vorginge. Dieser Auffassung erteilte der EuGH in seinem Urteil vom 26. Oktober 2023 (C-307/22) eine klare Absage: begehren Patient:innen eine Kopie ihrer Patientenakte, ist die erste Kopie in der Regel kostenlos nach Art. 15 Abs. 3 DS-GVO zu erteilen.

1 URL: https://www.datenschutz-mv.de/kontakt/Mitteilung-von-Datenschutzbeauftragten/ [abgerufen am 15.03.2024]

Die Entscheidungsgrundlage des EuGH bildete die Auseinandersetzung mit einem Fall, indem eine Zahnärztin unter Berufung auf § 630g Abs. 2 BGB die Erstattung der Kosten für die erste Kopie der Patientenakte verlangte. Diese Kopie sei nicht gefordert worden, um einen Datenschutzverstoß geltend zu machen, sondern vielmehr brauchte der Patient diese Akte, um zivilrechtlich gegen die Ärztin vorzugehen. Nach Ausführungen des EuGH kommt es keinesfalls auf die Begründung oder auf die Motivation des Antrags (auf den Erhalt der Kopie) an, da das Auskunftsrecht hinsichtlich personenbezogener Daten auch ohne weitere Voraussetzung gemäß Erwägungsgrund 63 DS-GVO besteht, um sich der Verarbeitung bewusst zu werden und deren Rechtmäßigkeit überprüfen zu können. Die Ausübung des Auskunftsrechts hängt nach dem Wortlaut von Art. 15 DS-GVO von Motivation nicht ab. Somit ist es nach dieser Bestimmung nicht erforderlich, dass die betroffene Person ihren Antrag auf Auskunft begründen müsste. Der EuGH legte im Weiteren fest, dass der Patient einen Anspruch auf eine unentgeltliche erste Kopie seiner Akte hat. Durch eine nationale Regelung wie § 630g Abs. 2 BGB darf dem Patienten keine Kostenlast hierfür auferlegt werden. Erst für alle weiteren Kopien können Ärzt:innen ein angemessenes Entgelt verlangen.

9. Innere Sicherheit

Im Berichtszeitraum gingen dem LfDI MV auch datenschutzrechtliche Beschwerden gegen die Landespolizei MV zu. Der häufigste Beschwerdegegenstand bestand im Zusammenhang mit Auskunftsersuchen (siehe Punkt 9.3.). Darüber hinaus gingen bei uns Beschwerden zu etwaig unzulässigen Datenübermittlungen sowie aufgrund von unzutreffenden Speicherungen in polizeilichen Informationssystemen zu (siehe Punkt 9.2.). Ebenso waren unberechtigte Abfragen in polizeilichen Informationssystemen durch Beschäftigte der Landespolizei MV zu verzeichnen (siehe Punkt 9.4.). Aufgrund entsprechender Meldungen mussten wir in den jeweiligen Verfahren zumeist umfangreiche Informationen zur Bearbeitung der Verwaltungs- und Ordnungswidrigkeitenverfahren anfordern. Dabei konnten wir seitens der Polizei ein überwiegend kooperatives Verhalten und ein Interesse an der Aufklärung von Abfragen aus Informationssystemen ohne dienstliche Veranlassung beobachten. Weiterhin nahm unsere Behörde die Kontrolle von gesetzlich vorgeschriebenen, turnusmäßigen Prüfungen von eingriffsintensiven und verdeckten Maßnahmen der Polizei im Bereich der Gefahrenabwehr auf (siehe Punkt 9.1.). Insgesamt war eine gute und kooperative Zusammenarbeit zwischen der Landespolizei MV und dem LfDI MV im Berichtszeitraum zu konstatieren. Mit Blick auf das Sicherheitsüberprüfungsgesetz M-V und das Landesverfassungsschutzgesetz M-V ist insbesondere auf gesetzliche Novellierungsbedarfe hinzuweisen (siehe Punkt 9.5.).

9.1. Kontrolle besonders eingriffsintensiver und verdeckter Maßnahmen

Die Vereinbarkeit der Ausgestaltung von Befugnissen der Sicherheitsbehörden zu eingriffsintensiven und verdeckten Maßnahmen mit dem Grundgesetz ist immer wieder Gegenstand verfassungsgerichtlicher Rechtsprechung (siehe Punkt 14.2.). Ein ganz besonders wegweisendes Urteil des Bundesverfassungsgerichts (BVerfG) erging in diesem Zusammenhang zum Bundeskriminalamtgesetz (Urt. v. 20.04.2016 – 1 BvR 966/09; BKAG). Mit dieser Entscheidung wurden von dem höchsten deutschen 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 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.

Obwohl sich die Entscheidung unmittelbar nur auf das BKAG bezog, betrafen die grundsätzlichen Ausführungen u. a. auch Ermächtigungsnormen in den Gefahrenabwehrgesetzen der Länder. Mit der Novelle des SOG M-V im Jahr 2019/20 erfolgte durch den Landesgesetzgeber in Mecklenburg-Vorpommern somit nicht nur eine Umsetzung des Unionsrechts sowie – unter massiver Kritik – eine Ausweitung von Eingriffsbefugnissen der Polizei, sondern auch eine Umsetzung der Anforderungen aus der vorbenannten Entscheidung des BVerfG. Entsprechend wurde eine Kontrollpflicht des LfDI MV in § 48b Abs. 6 SOG M-V vorgesehen. Hiernach muss der LfDI MV die in § 46f Abs. 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 Abs. 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 sehr 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 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. Umso wichtiger ist die Kontrolle der Durchführung dieser Maßnahmen.

Die Kontrolle dieser Maßnahmen und Datenübermittlungen ist nach § 48b Abs. 6 SOG M-V zumindest stichprobenartig vorgesehen worden. Um die Auswahl der Stichproben möglichst repräsentativ zu gestalten und vorwiegend besonders eingriffsintensive Maßnahmen zu kontrollieren, bedurfte es zunächst der Kenntnis des LfDI MV, wie viele kontrollpflichtige Maßnahmen und Datenübermittlungen insgesamt durch welche Polizeibehörden der Landespolizei MV durchgeführt worden sind. Hierzu wurden die entsprechenden Informationen seitens des LfDI MV von der Landespolizei MV eingeholt. Nahezu vollständig lassen sich diese Informationen bereits auch den Berichten der Landesregierung nach § 48h SOG M-V zur Unterrichtung des Landtags M-V und der Öffentlichkeit entnehmen.

Anhand dieser Informationen ist zunächst ersichtlich, dass von denen im Rahmen der Novelle des SOG M-V im Jahr 2019/20 eingeführten eingriffsintensiven Befugnissen durch die Landespolizei MV nur selten bzw. mitunter gar nicht Gebrauch gemacht wurde. So erfolgte nach diesen Informationen im Gefahrenabwehrbereich bis 2022 beispielhaft kein Einsatz von Vertrauenspersonen oder verdeckt Ermittelnden, keine Quellen-Telekommunikationsüberwachung, keine Online-Durchsuchungen, keine Rasterfahndungen oder elektronischen Aufenthaltsüberwachungen. Dennoch wurden durchaus auch einzelne eingriffsintensive Maßnahmen durchgeführt, wie bspw. längerfristige Observationen oder vor allem der Einsatz technischer Mittel zur Bestimmung von Verkehrs- und Standortdaten. Unter den tatsächlich durchgeführten Maßnahmen hat der LfDI MV zur Kontrolle eine repräsentative Stichprobe erhoben, deren Prüfung derzeit noch andauert.

Der Prüfungsumfang seitens des LfDI MV bezieht sich vor allem darauf, wie Maßnahmen durchgeführt wurden bzw. ob diese in Art, Dauer und Umfang im Einklang mit den jeweiligen Rechtsgrundlagen bzw. Anordnungen stehen. Darüber hinaus wird die Einhaltung der Vorgaben geprüft, soweit personenbezogene Daten des Kernbereichs privater Lebensgestaltung im Wege der Maßnahmen betroffen sind. Währenddessen erfolgt 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. Trotzdem wird bei richterlich angeordneten Maßnahmen 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 auch geprüft, ob die jeweiligen Tatbestandsvoraussetzungen für die Anordnung dieser Maßnahmen vorlagen.

Bei den durchgeführten und abgeschlossenen Kontrollen wurden bislang keine Datenschutzrechtsverstöße festgestellt. Das abschließende Ergebnis liegt jedoch erst mit der Beendigung der Kontrollen vor. Über die Ergebnisse der zurzeit laufenden Kontrollen wird nach deren Abschließung im folgenden Tätigkeitsbericht berichtet. Im Laufe der erstmaligen Aufnahme dieser Kontrollen wurde vor allem festgestellt, dass es für die gemeinsame Durchführung einer Verfahrensetablierung bedarf. Hierzu steht der LfDI MV bereits in Abstimmung mit der Landesregierung MV.

9.2. Unzutreffende Speicherung in polizeilichen Informationssystemen

Im Berichtszeitraum zeigte eine Person mit einer Beschwerde an, dass von ihr unzutreffende personenbezogene Daten in polizeilichen Informationssystemen verarbeitet wurden. Konkret wurde der beschwerdeführenden Person im Rahmen einer Befragung durch die Polizei u. a. mitgeteilt, dass sie in der Vergangenheit einen Verstoß gegen das Betäubungsmittelgesetz (BtMG) begangen hätte; dies sei nach den Aussagen der Polizeivollzugsbeamten entsprechend in den polizeilichen Informationssystemen hinterlegt. Da die betroffene Person sich eine derartige Eintragung in den Datenbanken der Polizei nicht erklären konnte, wünschte sie die von ihr durch die Polizei verarbeiteten personenbezogenen Daten zu überprüfen. Hierzu stellte die beschwerdeführende Person einen Auskunftsantrag gegenüber der Landespolizei MV. Mit Verwunderung musste die betroffene Person in der durch die Polizei erteilten Auskunft feststellen, dass sie durchaus in einem Strafverfahren wegen eines Verstoßes gegen das BtMG als Beschuldigter/Tatverdächtiger geführt wird, obwohl dies nicht zutreffend ist. Daraufhin erhob die betroffene Person Beschwerde bei unserer Behörde.

Zur Ausermittlung des Sachverhalts wandten wir uns an die zuständige Polizeibehörde. Daraufhin wurde durch die Polizei eine unzutreffende Speicherung eingeräumt und eine Berichtigung vorgenommen. Es stellte sich heraus, dass die beschwerdeführende Person die Polizei lediglich in einer mit dem BtMG-Verstoß zusammengehörigen Angelegenheit zur Hilfe rief. Weil eine Vielzahl von Personen widerrechtlich das im Eigentum der beschwerdeführenden Person stehende Privatgelände betrat, zog sie als Geschädigter die Polizei hinzu. Die Einsatzkräfte unterstützten auch die betroffene Person bei der Durchsetzung des Hausrechts. Im Zuge dieses Einsatzes ergab sich zusätzlich bei einer gefahrenabwehrrechtlichen Nach- und Umschau in einem Fahrzeug, das den sich widerrechtlich auf dem Grundstück des Betroffenen aufhaltenden Personen zuzuordnen war, ein Zufallsfund von Betäubungsmitteln. Weil das Fahrzeug jedoch für alle Personen, die sich unbefugt auf dem Gelände aufhielten, zugänglich war, konnten die Betäubungsmittel nicht einer konkreten Person zugeordnet werden. Daher wurden alle vor Ort anwesenden Personen als Tatverdächtige erfasst. Dies betraf auch die beschwerdeführende Person, obwohl diese in keinerlei Zusammenhang zu dem Fahrzeug stand, in dem die Betäubungsmittel aufgefunden wurden. Somit wurde die betroffene Person, die eigentlich in diesem Fall als Geschädigter zu betrachten war, in polizeilichen Informationssystemen als Beschuldigter/Tatverdächtiger einer Straftat geführt. Die im Hinblick auf den BtMG-Verstoß gefertigte Strafanzeige, in welcher u. a. auch der Betroffene als Tatverdächtiger angeführt wird, wurde ebenso an die Staatsanwaltschaft übersandt.

Weil die Speicherung der personenbezogenen Daten vorliegend in einem Dateisystem zusammen mit Daten erfolgte, deren Speicherung sich nach dem Landesrecht bemisst, war die Angelegenheit rechtlich nach dem SOG M-V zu beurteilen (§ 483 Abs. 3 Strafprozessordnung). Nach § 39 Abs. 1 SOG M-V hat die verantwortliche Stelle angemessene Maßnahmen zu ergreifen, um zu gewährleisten, dass personenbezogene Daten, die unrichtig oder nicht mehr aktuell sind, nicht übermittelt oder sonst zur Verfügung gestellt werden. Zu diesem Zweck hat sie, soweit dies mit angemessenem Aufwand möglich ist, die Qualität der Daten vor ihrer Übermittlung oder Bereitstellung zu überprüfen. An diesen Maßnahmen fehlte es vorliegend, sodass ein Verstoß gegen § 39 Abs. 1 SOG M-V festzustellen war.

Aufgrund der Übersendung der unzutreffenden Daten an die Staatsanwaltschaft war auch § 45 Abs. 5 SOG M-V berührt: wenn unrichtige Daten übermittelt worden sind, muss die übermittelnde Stelle den Empfänger:innen unverzüglich u. a. über die Berichtigung oder Löschung in Kenntnis setzen. Diese Regelung ist überaus wichtig dafür, dass auch bei empfangenden Stellen unzutreffende Daten berichtigt werden können. Der LfDI MV sprach daher nach § 48b Abs. 1 SOG M-V i.V.m. Art. 58 Abs. 1 lit. d DS-GVO einen förmlichen Hinweis gegenüber der betreffenden Polizeibehörde dahingehend aus, dass es sich um einen Verstoß handelt, wenn der Pflicht nach § 45 Abs. 5 SOG M-V nicht nachgekommen wird. Ferner wurde der vorbenannte förmliche Hinweis auch auf § 45 Abs. 2 SOG M-V erstreckt, da die personenbezogenen Daten der betroffenen Person nicht nur zu berichtigen, sondern auch zu löschen waren. Dies musste bereits gelten, da das Verfahren durch die Staatsanwaltschaft zwischenzeitig eingestellt wurde und auch kein Restverdacht bestand.

Im gesamten Beschwerdeverfahren verhielt sich die betreffende Polizeibehörde überaus kooperativ. Umgehend nach dem förmlichen Hinweis wurde eine Löschung veranlasst und die Staatsanwaltschaft über die unzutreffende Übermittlung sowie die Löschung in Kenntnis gesetzt. Weiterhin wurden durch die betreffende Polizeibehörde Sensibilisierungsmaßnahmen ergriffen, die die Wiederholung eines ähnlich gelagerten Vorfalls nicht befürchten lassen. Von weiteren Maßnahmen, wie einer Beanstandung nach § 48b Abs. 3 SOG M-V, war vorliegend daher abzusehen. Dennoch können derartige Fehler für betroffene Personen folgenschwer sein, sodass diesen insbesondere in der polizeilichen Vorgangsbearbeitung mit weitreichenden Maßnahmen der Qualitätssicherung zu begegnen ist. Anhand dieses Praxiseinblicks zeigt sich einmal mehr, wie wichtig das Auskunftsrecht gerade gegenüber der Polizei sein kann.

9.3. Auskunftsrecht gegenüber der Polizei

Das Auskunftsrecht gegenüber der Polizei ist immer wieder Gegenstand von datenschutzrechtlichen Beratungsanfragen und Beschwerden. Dabei handelt es sich bei dem Auskunftsrecht um ein zentrales Schlüsselrecht. Mit dem Recht auf Auskunft werden betroffene Personen in die Lage versetzt, Kenntnis der von ihnen verarbeiteten personenbezogenen Daten zu erhalten und die Rechtmäßigkeit der Verarbeitung überprüfen zu können. Die erlangten Kenntnisse können sodann für die Ausübung weiterer Betroffenenrechte – wie einer Berichtigung, Löschung oder Einschränkung der Verarbeitung – genutzt werden, wodurch dem Auskunftsrecht eine Elementarfunktion zukommt. Für betroffene Personen ist es oftmals jedoch verständlicherweise schwierig, die korrekte Rechtsgrundlage auszumachen. Wir stehen hierbei zur Hilfe.

Das Auskunftsrecht als Grundrecht beruht zunächst auf Art. 8 Abs. 2 der Charta der Grundrechte der Europäischen Union (GRCh), welches der Unionsgesetzgeber in verschiedenen Rechtsakten – je nach den Zwecken einer Verarbeitung – umgesetzte. Für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, erließ der Unionsgesetzgeber die Richtlinie (EU) 2016/680[1], die sog. Richtlinie für Justiz und Inneres (JIRL), in welcher das Auskunftsrecht in Art. 14, 15 vorgesehen wird. Die JI-RL gilt nach Art. 288 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV) jedoch nicht unmittelbar in den Mitgliedstaaten, sondern war durch diese in nationales Recht umzusetzen. Diesbezüglich ist zu differenzieren: Für den Bereich der Strafverfolgung wurde das Recht auf Auskunft in § 57 BDSG umgesetzt. Da jedoch die Gesetzgebungskompetenz für das allgemeine Polizei- und Ordnungsrecht, welches ebenso die Gefahrenabwehr einschließt, den Ländern obliegt, wurde das Auskunftsrecht im Bereich der Gefahrenabwehr in Mecklenburg-Vorpommern in § 48 SOG M-V umgesetzt. In Fällen in denen die Polizei personenbezogene Daten zu Zwecken der Strafverfolgung in einem Dateisystem zusammen mit Daten verarbeitet, deren Speicherung sich nach den Polizeigesetzen richtet (bspw. Gefahrenabwehr), ist wiederum nach § 483 Abs. 3 Strafprozessordnung (StPO) u. a. für die Rechte der betroffenen Personen das für die speichernde Stelle geltende Recht maßgeblich. Mithin wäre in dieser Konstellation ebenso § 48 SOG M-V ausschlaggebend.

Zudem verarbeitet die Polizei auch personenbezogene Daten außerhalb des Anwendungsbereiches der JI-RL. Dies betrifft beispielhaft Verarbeitungen personenbezogener Daten im Rahmen von Beschäftigungsverhältnissen oder Sensibilisierungsmaßnahmen. Soweit in diesen Fällen der Anwendungsbereich der unmittelbar nach Art. 288 AEUV geltenden DS-GVO eröffnet ist, besteht das Auskunftsrecht nach Art. 15 DS-GVO.

1 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.

Weil es jedoch im Kontext der SOG-Novelle im Jahr 2020 Ziel des Gesetzgebers war, dass Rechtsanwendende der Stellen, die im Bereich der Gefahrenabwehr tätig sind, nicht verschiedene Regelungswerke berücksichtigen müssen,[1] erfolgte nicht nur die Umsetzung der JI-RL, sondern es wurden auch der DS-GVO entsprechende Regelungen getroffen.[2]

So wurden ausweislich des Wortlautes von § 25 Abs. 3 Nr. 5 SOG M-V mit § 48 SOG M-V zu Art. 15 DS-GVO spezifische Bestimmungen i.S.d. Art. 6 Abs. 2, 3 i.V.m. Abs. 1 lit. e DS-GVO erlassen und § 48 SOG M-V enthält zudem Beschränkungen i.S.d. Art. 23 Abs. d DS-GVO. Dieses Vorgehen begegnet weitreichenden Bedenken mit Blick auf die Vereinbarkeit mit dem Unionsrecht.

Die Mitgliedstaaten können zwar nach Erwägungsgrund 19 DS-GVO für zuständige Behörden nach der JI-RL in Bezug auf Verarbeitungstätigkeiten zu Zwecken, die dem Anwendungsbereich der DS-GVO unterfallen, spezifischere Bestimmungen beibehalten oder einführen, um die Anwendung der Vorschriften der DS-GVO anzupassen, sind aber hierbei durch die eng auszulegenden Beschränkungstatbestände nach Art. 23 DS-GVO begrenzt. Aufgrund der Ausgestaltung des § 48 SOG M-V ist anzunehmen, dass diese Regelung allenfalls Art. 14, 15 JI-RL entspricht. Ob eine ‚Abwandlung' des Auskunftsrechts nach Art. 15 DS-GVO im Umfang des § 48 SOG M-V zulässig ist und von den Öffnungs- und Spezifizierungsklauseln der DS-GVO gedeckt ist, erscheint überaus zweifelhaft und sollte in der Evaluierung nach § 116 SOG M-V aufgegriffen werden. Denn begehrt eine betroffene Person eine Auskunft i.S.d Art. 15 DS-GVO gegenüber der Polizei innerhalb des Anwendungsbereiches der DS-GVO, stellt sich daher die Frage, ob § 48 SOG M-V abschließend, lediglich in Ergänzung von Art. 12 i.V.m. Art. 15 DS-GVO oder stattdessen ausschließlich das Unionsrecht Anwendung findet. Insofern die Norm des § 48 SOG M-V mit Art. 15 DS-GVO kollidiert, ist jeder Rechtsanwendende zu einer europarechtskonformen Auslegung unter Beachtung des Vorrangs und der unmittelbaren Geltung des Unionrechts nach Art. 288 Abs. 2 AEUV sowie des Grundsatzes des „effet utile" verpflichtet. Danach sind Vorschriften so auszulegen, dass das Europarecht die höchstmögliche praktische Wirksamkeit entfalten kann.[3]

Jedenfalls dürfen Auskunftsanträge seitens der Polizei nicht abgelehnt werden, wenn betroffene Personen keine Rechtsgrundlage oder eine unzutreffende Rechtsgrundlage für das Auskunftsbegehren benennen. Durchaus ist dem LfDI MV zumindest in einem Fall aufgrund einer Beschwerde bekannt geworden, dass ein Auskunftsersuchen seitens der Polizei zunächst abgelehnt wurde, weil dieses seitens der betroffenen Person auf Art. 15 DS-GVO gestützt wurde. Die Polizei verarbeitete aber nur personenbezogene Daten des Antragstellers im Anwendungsbereich der JI-RL. Stattdessen haben Verantwortliche nach Art. 12 Abs. 2 DS-GVO/Art. 12 Abs. 2 JI-RL die Pflicht, betroffenen Personen die Ausübung der Betroffenenrechte zu erleichtern, was auch ein aktives Unterstützen erfordert.

1 Vgl. LT MV, Drs. 7/3694, S. 148

2 Vgl. A.a.O, S. 147: „Hierbei besteht das Ziel, datenschutzrechtliche Regelungen im SOG M-V zu schaffen, die sowohl der Umsetzung der Richtlinie (EU) 2016/680 dienen als auch den Regelungen der unmittelbar geltenden Verordnung (EU) 2016/679 entsprechen."

3 Vgl. HK LDSG MV/Kämpfe/Oehlrich/von Niessen § 6 Rn. 19

Dies schließt ein, dass der Wille des Antragstellers entsprechend auszulegen ist, unabhängig von einer ggf. unzutreffenden oder fehlenden Angabe einer Rechtsgrundlage. Betroffenen Personen darf es nicht zum Nachteil gereichen, dass das komplexe Regelungsgefüge zwischen Unions-, Bundes- und Landesrecht nicht unbedingt einfach nachvollziehbar ist.

Weiterhin ist darauf hinzuweisen, dass sowohl Art. 15 DS-GVO als auch § 57 BDSG/§ 48 SOG M-V alle verarbeiteten personenbezogenen Daten im jeweiligen Anwendungsbereich erfassen. Insoweit umfasst der Umfang dieser Auskunftsansprüche nicht lediglich elektronisch verarbeite personenbezogene Daten, sondern auch jene in analogen Akten.

Mit Blick auf die Ausübung von Betroffenenrechten steht der LfDI MV sowohl betroffenen Personen als auch Verantwortlichen beratend stets zur Verfügung.

9.4. Unberechtigte Datenabfragen in der Landespolizei MV

Im vorliegend berücksichtigten Berichtszeitraum waren unberechtigte Datenabfragen in polizeilichen Informationssystemen durch Beschäftigte der Landespolizei MV zu verzeichnen. Zumeist kam es zu unberechtigten Abfragen im elektronischen Vorgangsassistent (EVA) der Polizei, vereinzelt aber auch in weiteren Informationssystemen. Abfragen in polizeilichen Systemen ohne dienstliche Veranlassung stellen jeweils eine unzulässige Verarbeitung personenbezogener dar, bei welcher sich Beschäftigte eigenmächtig zu Verantwortlichen aufschwingen, indem sie Zwecke und Mittel der Verarbeitung eigenmächtig bestimmen und personenbezogene Daten entgegen der Weisung des Verantwortlichen ohne Rechtsgrundlage verarbeiten (sogenannter Mitarbeiterexzess).

Für die Feststellung und den Nachweis von unberechtigten Datenabfragen wird regelmäßig auf Zugriffsprotokollierungen zurückgegriffen. In den Informationssystemen der Polizei sind jegliche Zugriffe nach § 76 BDSG/§ 46e SOG M-V zu protokollieren, um deren Rechtmäßigkeit überprüfen und nachweisen zu können. Somit können in den Zugriffsprotokollierungen unberechtigte Abfragen entweder durch den LfDI MV oder die Polizei selbst festgestellt werden. Soweit durch die Polizei selbst unberechtigte Datenabfragen festgestellt werden, geht damit in der Regel auch das Bekanntwerden einer Verletzung des Schutzes personenbezogener Daten einher, die unserer Behörde gemeldet wird (§ 65 BDSG/§ 48d SOG M-V/Art. 33 DS-GVO). In der überwiegenden Anzahl der Fälle unberechtigter Datenabfragen erfolgte eine Meldung tatsächlich durch die Polizei selbst. Unberechtigte Datenabfragen wurden uns allerdings auch durch Anzeigen von Dritten oder Beschwerden betroffener Personen bekannt.

Sobald unberechtigte Datenabfragen bekannt werden, erfolgt eine konsequente Verfolgung durch den LfDI MV. Bisher wurden vorrangig aufgrund der Meldungen der Verletzungen des Schutzes personenbezogener Daten zunächst Verwaltungsverfahren eingeleitet, um aus diesen den Sachverhalt zu ermitteln und den Vorgang im Anschluss für die Verhängung von Bußgeldern intern an die Bußgeldstelle abzugeben (siehe Punkt 13.2.).

Da zwischenzeitig regelmäßig jedoch die jeweiligen unberechtigten Datenabfragen durch die Polizei nicht nur als Datenpannenmeldungen an uns übermittelt, sondern zudem auch als Ordnungswidrigkeitenanzeigen übersandt wurden, ging hiermit ein enormer sowie vor allem zeitintensiver Bearbeitungsaufwand einher. Es wurde insoweit von dem bisherigen Verfahren abgewichen, sodass zu Gunsten der Verfahrensökonomie unberechtigte Datenabfragen seitens unserer Behörde weitgehend nur noch im Ordnungswidrigkeitenverfahren verfolgt werden. Mitunter mussten Verfahren zu unberechtigten Abfragen aufgrund des Verdachts der Verwirklichung einer Straftat auch an die Staatsanwaltschaft abgegeben werden. Gleichzeitig erhielten wir andere Verfahren, die an uns durch die Staatsanwaltschaft abgegeben wurden, soweit eine Straftat nicht festgestellt werden konnte, aber eine Ordnungswidrigkeit in Betracht kam.

Bereits im letzten Tätigkeitsbericht[1] machten wir auf eine Entscheidung des Oberlandesgerichtes Rostock zu einem Rechtsstreit wegen der Verhängung eines Bußgeldes aufgrund einer unberechtigten Datenabfrage durch einen Beschäftigten der Landespolizei MV aufmerksam. Gleichwohl mehrere Bußgeldbescheide gegen Polizist:innen erlassen worden sind, waren hierfür auch einige Änderungen erforderlich. Mit dieser Entscheidung wurden Kriterien aufgestellt, die bei der Ausgestaltung von Datenabfragen durch Beschäftigte der Polizei zu berücksichtigen waren. Dementsprechend musste nach Auffassung des Gerichts durch die jeweilige Dienststelle konkret bestimmt sein, welche Befugnisse die Beschäftigten haben. Eine Verpflichtungserklärung auf die Datenschutzgrundsätze allein könne zur Ermittlung der jeweiligen Befugnisse nicht herangezogen werden. Eine Dienstpostenbeschreibung sei auch nicht geeignet, hieraus Aussagen über die Zulässigkeit der Nutzung bestimmter Datenverarbeitungssysteme abzuleiten, die ohne technische Beschränkung zur Bewältigung des täglichen Diensts den Beschäftigten zur Verfügung stehen. Soweit technische Einschränkungen nicht in Betracht kämen, müssten organisatorisch zumindest konkrete Anweisungen der Leitung vorliegen, die den Umgang mit der dienstlichen Software limitieren und auf deren Grundlage Beschäftigte schlussfolgern könnten, welche Systeme sie für welche Abfragen nutzen dürfen. Vor diesem Hintergrund wurden in der Landespolizei MV die Datenschutzbelehrungen angepasst und entsprechende Weisungen vorgenommen. Darüber hinaus wurden durch das Ministerium für Inneres, Bau und Digitalisierung MV sowie die bDSB der Polizeibehörden weitgehende Sensibilisierungsmaßnahmen getroffen. Zudem wurden technische Maßnahmen ergriffen und die Beschreibung der Zugriffsmöglichkeiten für die Polizeibeamt:innen angepasst. Unberechtigte Abfragen werden nicht nur durch unsere Behörde verfolgt, sondern auch durch die zuständigen Disziplinarstellen im Rahmen von Disziplinarverfahren. Infolgedessen lässt sich ein erhöhter Sensibilisierungsgrad in der Landespolizei MV beobachten. Dieser spiegelt sich auch in einem Rückgang der Anzahl der (bekannt gewordenen) unberechtigten Abfragen wider. Doch solange unberechtigte Datenabfragen stattfinden, werden diese konsequent durch den LfDI MV verfolgt. Angesichts der Änderungen, die aufgrund des Beschlusses des Oberlandesgerichts Rostock vorgenommen wurden sowie der Verfahrensänderungen in der Bearbeitung, ist von einer weiter zunehmenden Verhängung von Bußgeldern durch unsere Behörde auszugehen.

1 Vgl. 17. Bericht, 2021 und 8. Bericht über die Umsetzung des IFG 2020/2021 S. 33
URL: https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Taetigkeitsberichte/lfdmvtb17.pdf [abgerufen am 03.04.2024]

9.5 Novellierungsbedarfe des SÜG M-V und des LVerfSchG M-V

SÜG M-V

Soweit Personen mit einer sicherheitsempfindlichen Tätigkeit betraut werden sollen, wie beispielsweise dem Umgang mit Verschlusssachen ab VS-Vertraulich, regelt das Sicherheitsüberprüfungsgesetz M-V (SÜG M-V) die Voraussetzungen und das Verfahren zur Überprüfung einer Person. Dabei ist es Zweck des personellen Geheimschutzes, im öffentlichen Interesse geheimhaltungsbedürftige Angelegenheiten dadurch zu schützen, dass der Zugang von Personen verhindert wird, bei denen ein Sicherheitsrisiko vorliegt oder nicht ausgeschlossen werden kann. Je nach Art der jeweils durchgeführten Sicherheitsüberprüfung werden in entsprechendem Umfang auch überaus sensitive personenbezogenen Daten der zu überprüfenden Personen verarbeitet. An diese Verarbeitungen sind demnach entsprechend hohe datenschutzrechtliche Anforderungen zu stellen. Da uns nach § 19 Abs. 1 DSG M-V die datenschutzrechtliche Aufsicht obliegt, wenn eine Datenverarbeitung weder der DS-GVO noch der JI-RL unterfällt, kommen grundsätzlich auch Prüfungen/Kontrollen des LfDI MV der Einhaltung dieser Anforderungen mit Blick auf Sicherheitsüberprüfungen in Betracht.

Aufgrund der hohen Sensitivität der verarbeiteten personenbezogenen Daten wurde betroffenen Personen nach alter Rechtslage in § 24 Abs. 2 Satz 4, Abs. 6 BDSG a.F. ein Widerspruchsrecht gegen die Einsicht in die Akten über die Sicherheitsüberprüfung durch die Datenschutzaufsichtsbehörde eingeräumt. Im Berichtszeitraum erreichten uns hierzu Anfragen, die sich darauf bezogen, wo das Widerspruchsrecht nunmehr geregelt sei, weil es der aktuellen Fassung des BDSG nicht mehr zu entnehmen ist. Hierauf mussten wir jeweils antworten, dass das Widerspruchsrecht mit der Neuordnung des Datenschutzrechts in § 36a Abs. 2 des SÜG des Bundes überführt wurde, welches für Mecklenburg-Vorpommern jedoch nicht anwendbar ist. Es fehlt an einer vergleichbaren Regelung im SÜG M-V, sodass die rechtliche Lage mit Blick auf ein Widerspruchsrecht derzeit ungeklärt ist.

In Bezug auf das SÜG M-V bestehen außerdem weitere datenschutzrechtliche Änderungsbedarfe. Wir nahmen diesbezüglich bereits den Kontakt mit dem zuständigen Ressort der Landesregierung auf.

LVerfSchG M-V

Das Landesverfassungsschutzgesetz M-V (LVerfSchG M-V) wurde zuletzt 2022 geändert. Schon im Rahmen dieser Novelle wiesen wir auf weitere datenschutzrechtliche Änderungsbedarfe hin. Es wurde bereits in der Gesetzesbegründung zu dieser Änderung erwähnt, dass sich eine umfassende Novelle des LVerfSchG in der Vorbereitung befinde, die einen allgemeinen datenschutzrechtlichen Anpassungsbedarf aufgreifen sowie insbesondere notwendige Änderungen, die sich aus dem Urteil des Bundesverfassungsgerichtes vom 26.04.2022 (1 BvR 1619/17) ergeben, umsetzen werde.[1] An diesen dringenden Änderungen fehlt es immer noch, sodass auch zu diesen Novellierungsbedarfen Kontakt zu dem zuständigen Ressort der Landesregierung aufgenommen wurde.

1 Vgl. Landtag M-V, Drs. 8/756, S. 4

10. Justiz

Der LfDI MV erhielt mehrere Eingaben gegen Organe der Justiz im Land. Wir nahmen einen Hinweis zum Anlass, Gerichtsvollzieher:innen zur sicheren Nutzung von E-Mail Konten zu sensibilisieren und auf die einschlägige Orientierungshilfe der DSK hinzuweisen (siehe Punkt 10.1.). Ein besonders schwerwiegender Vorfall im Bereich der Justiz betraf einen USB-Stick, der auf dem Postweg verloren ging und unverschlüsselte Dateien u. a. mit Missbrauchsmaterial aus einem laufenden Strafverfahren enthielt (siehe Punkt 10.2.). Dieses noch laufende Verfahren illustriert zum einen die zentrale Rolle von TOMs für den Schutz der Rechte und Freiheiten von betroffenen Personen, sowie zum anderen die Notwendigkeit, die Zuständigkeit einer Datenschutzaufsicht bei Gerichten konkret zu regeln.

10.1. Unsichere E-Mail-Konten bei Gerichtsvollzieher:innen

Der LfDI MV nahm einen Hinweis eines Bürgers zum Anlass und verschickte an alle Gerichtsvollzieher:innen in Mecklenburg-Vorpommern eine Information zur datenschutzkonformen und sicheren Gestaltung der E-Mail-Kommunikation. Die Vorteile der Kommunikation mittels E-Mail sind unbestritten. Die Handlungsfähigkeit der Gerichtsvollzieher:innen hängt in hohem Maße von der Funktionalität des E-Mail-Systems ab. Auf Basis dieses Wissens sind E-Mail-Systeme jedoch häufig ein Ziel von Angriffen, um durch Ausspähen von E-Mails an Informationen zu gelangen oder dessen Verfügbarkeit zu beeinträchtigen und somit Gerichtsverfahren zu verlangsamen. Zusätzlich werden mit Schadsoftware infizierte E-Mails als Angriffsvektoren für Cyber-Angriffe benutzt. Die Sicherung dieses essenziellen Kommunikationskanals muss deshalb für alle Gerichtsvollzieher:innen eine hohe Priorität haben. Wir empfehlen daher, für den sicheren Empfang von E-Mail-Nachrichten einen verschlüsselten Kanal zu schaffen. Das bedeutet, dass der Empfangsserver mindestens den Aufbau von TLS-Verbindungen[1] (direkt per SMTPS- Simple Mail Transfer Protocol oder nach Erhalt eines STARTTLS-Befehls über SMTP) ermöglichen muss. Durch eine obligatorische Transportverschlüsselung soll eine unverschlüsselte Übermittlung der Nachrichten ausgeschlossen werden. Beim Versand einer E-Mail-Nachricht sollte zusätzlich sichergestellt werden, dass nur Personen die Nachricht zur Kenntnis nehmen, denen gegenüber eine Offenlegung der Nachricht gestattet ist, z. B. durch eine Ende-zu-Ende-Verschlüsselung mit den Verfahren S/MIME und OpenPGP. Außerdem kann mit folgenden grundsätzlichen Sicherheitsfunktionen der Datenschutz und die IT-Sicherheit erhöht werden:

» **Passwort-Manager** – er fungiert als geräteübergreifender Schlüsselbund, mit dem Konten und Zugangsdaten vor Hackern und Datenlecks geschützt werden können.

» **Virenschutz-Software** – sie schützt vor Trojanern, Phishing sowie anderer Malware und blockt zum Beispiel unerwünschten Zugriff auf die Webcam.

» **Backup-Software** – diese bewahrt vor Datenverlust, indem sie Sicherungskopien der wichtigen Daten auf externen Datenträgern oder in einem Cloud-Speicher mit Zwei-Faktor-Authentifizierung anlegt.

1 Transport Layer Security (TLS): ein Protokoll, das E-Mail-Nachrichten aus Sicherheits- und Datenschutzgründen verschlüsselt

Die Orientierungshilfe der DSK zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail[1] erläutert ausführlich, wie Verfahren zum Versand und zur Entgegennahme von E-Mail-Nachrichten datenschutzkonform gestaltet werden können.

10.2. Verlorener USB-Stick mit Missbrauchsmaterial

Ein Gericht teilte uns mit, dass ein USB-Stick während der laufenden Hauptverhandlung einer großen Strafkammer wegen u. a. schweren sexuellen Missbrauchs eines Kindes und Herstellens von kinderpornographischen Schriften über das Internet auf dem Postweg abhandenkam. Dieser wurde vom Landgericht per Post an einen Sachverständigen in Berlin versandt. Auf dem USB-Stick waren Videos der Missbrauchshandlungen sowie der Videovernehmung des minderjährigen Geschädigten im Ermittlungsverfahren gespeichert. Weder der genutzte private USB-Stick noch die einzelnen Dateien waren verschlüsselt. Der Datenträger wurde auf Anordnung des Kammervorsitzenden von der Geschäftsstelle an den im Ermittlungsverfahren bestellten Sachverständigen versandt. Der Sachverständige teilte daraufhin mit, er habe nur den Umschlag mit dem Anschreiben erhalten, ein USB-Stick sei nicht enthalten gewesen, vielmehr habe der Umschlag ein Loch in der Folie des Adressfensters aufgewiesen. Infolgedessen baten wir um weitere Unterlagen, um den Sachverhalt datenschutzrechtlich bewerten zu können. Diese wurden uns jedoch verweigert, da wir nach Auffassung des Gerichts nicht zuständig seien. Das Gericht vertritt den Standpunkt, es handele sich hierbei um einen Vorfall im Rahmen einer justiziellen Tätigkeit. Im Übrigen teilte es lediglich mit, dass das Geschehen zum Anlass genommen worden sei, die Richter:innen sowie die Mitarbeitenden auf die Vorschriften der Sicherheitsrichtlinie für Anwender von IT-Systemen hinzuweisen, insbesondere auf die Pflicht, bei der Versendung von personenbezogenen Daten dienstlich bereitgestellte und verschlüsselte mobile Datenträger zu verwenden. Der Fall ist derzeit noch offen. Fest steht zunächst, dass beim Versand eines unverschlüsselten Sticks per Post jedenfalls keine angemessenen TOMs ergriffen worden sind, um den Schutz der höchst sensiblen Daten zu gewährleisten.

Im Zusammenhang mit dem Datenschutz bei Gerichten sind viele Fragen ungeklärt. Die Gerichte haben jedoch auch die DS-GVO zu beachten, etwa bei der Beweiserhebung.[2] Allerdings sind die Datenschutzaufsichtsbehörden nicht für die Gerichte im Rahmen ihrer justiziellen Tätigkeit zuständig (vgl. Art. 55 Abs. 3 DS-GVO). Hierfür sollen besondere Stellen geschaffen werden.

In der Literatur ist umstritten, ob im Bereich der Strafgerichte die DS-GVO oder die JI-RL Anwendung findet. In dem vorliegenden Fall wird auch die Reichweite des Begriffs „justizielle Tätigkeit" diskutiert. Unserer Erachtens nach ist jedenfalls die Erfüllung datenschutzrechtlicher Pflichten aus der DS-GVO, einen Verantwortlichen (i.d.R. nicht jedoch nicht einzelne Richter:innen) zu bestimmen. Somit wäre dies als ein Verwaltungshandeln und nicht als justizielle Tätigkeit zu qualifizieren.

1 DSK, Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail, Orientierungshilfe, Stand: 16.06.2021
URL: https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Broschueren/20210616_OH_E-Mail.pdf [abgerufen am 11.04.2024]

2 Vgl. EuGH Urteil vom 2.3.2023 – C-268/21

Die Vorgabe im Sinne einer TOM, dass entsprechende Datenträger nur mit Verschlüsselung zu versenden sind, kann getroffen werden, ohne die justizielle Unabhängigkeit zu beeinträchtigen. Die Festlegung von TOMs ist reiner Verwaltungsakt. Dies gilt jedoch unter Vorbehalt der Ausgestaltung der datenschutzrechtlichen Verantwortlichkeit. Somit ist ebenfalls noch ungeklärt, ob lediglich das Gericht, vertreten durch Direktor:in oder Präsident:in, oder auch der Spruchkörper datenschutzrechtlich verantwortlich sind und in welchem datenschutzrechtlichen Verhältnis beide zueinander stehen. Übrig bleibt schlussendlich zur Frage, welche besonderen Stellen für die Überwachung der Einhaltung des Datenschutzes im Rahmen der justiziellen Tätigkeit zuständig sein sollen.

Der vorliegende Fall zeigt ausdrücklich, mit welchen Risiken für betroffene Personen Datenschutzverstöße bei Gerichten verbunden sein können. Umso wichtiger ist es, dass Datenschutzaufsichtsbehörden, Gerichte, die zuständigen Ministerien, aber auch der Gesetzgeber, ihre Möglichkeiten nutzen, um schnellstmöglich für Klarheit zu sorgen.

11. Verkehr

Der LfDI MV trägt auch im Bereich „Verkehr" durch stete Beratung und Kontrolle dazu bei, dass Behörden, Unternehmen und private Personen in Mecklenburg-Vorpommern personenbezogene Daten ordnungsgemäß verarbeiten und so das Recht jeder einzelnen Person auf informationelle Selbstbestimmung gewahrt wird. Es folgen einige exemplarische Fälle aus diesem Arbeitsbereich.

11.1. Verkehrsanalyse und Hinweispflicht an der Warnowquerung

Im August 2022 erreichte uns eine Anfrage zu einer datenschutzrechtlichen Stellungnahme einer geplanten Videoanalyse des Fahrzeugaufkommens und des Verkehrsverhaltens an der Mautstelle des Warnowtunnels. Bereits im Jahr 2020 wurde durch die Betreibenden des Tunnels nach Stellungnahme des LfDI MV eine Videoanalyse durchgeführt.

Die hieraus abgeleiteten Maßnahmen wurden nun fast alle umgesetzt, so dass sich die Betreibenden des Tunnels veranlasst sahen, eine erneute Analyse durchzuführen, um die Ergebnisse transparent und abrechenbar darzustellen. So sollen in einem bestimmten Zeitraum zwei Videokameras je Fahrtrichtung angebracht und deren Aufnahmen ausgewertet werden. Die niedrigauflösenden Kameras sollen feststehend am Straßenrand in einer Höhe von drei bis sechs Metern und nur für die zeitlich begrenzte Nutzung installiert werden. Um eine mögliche Erfassung von personenbezogenen Daten auszuschließen, muss sichergestellt werden, dass neben einzelnen Personen auch Fahrzeuge nicht mehr identifiziert werden können.

Bei einer zu geringen Pixeldichte können Fahrzeuge mit beispielsweise einer besonders auffälligen Farbgebung, Beschriftung oder Ausstattung auch ohne unverhältnismäßigen Aufwand identifiziert werden.

Wir haben den Betreibenden vor der ersten Videoanalyse entsprechend mitgeteilt, dass in diesem Fall unterhalb einer Grenze von weniger als 40 mm/Pixel (entspricht dem Detektieren gem. DIN EN 62676-4) von einer Videoüberwachung ohne Personenbezug ausgegangen werden kann. Die aktuelle Videoanalyse der Betreibenden haben wir zum Anlass genommen, um auch die Durchführung der Videoüberwachung vor Ort zu begutachten. So wurden durch die Betreibenden die Videokameras demonstriert sowie die Erfassung und Speicherung der Daten vor Ort dargestellt. Das Erfassen und Speichern von personenbezogenen Daten bei der Videoanalyse konnte nicht festgestellt werden.

Neben den temporären Videokameras befinden sich jedoch noch weitere Kameras im Bereich des Warnowtunnels, die den störungsfreien Ablauf des Betriebes des Mauttunnels und damit die Sicherheit der Verkehrsteilnehmenden gewährleisten sollen. Bei der Überprüfung vor Ort wurde nun festgestellt, dass auf die Videoüberwachung mit einem Piktogramm hingewiesen wurde, jedoch ein vollständiger Hinweis gem. Art. 13 DS-GVO nicht erfolgte. So sind der Umstand der Beobachtung und der Name wie auch die Kontaktdaten des Verantwortlichen durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen. Zum frühestmöglichen Zeitpunkt bedeutet, dass vor dem Betreten videoüberwachter Bereiche auf die Datenverarbeitung hingewiesen wird, damit betroffene Personen ihr Verhalten entsprechend ausrichten und ggf. auf das Betreten dieses Bereiches verzichten können.

Da der Verkehrsbereich vor dem Tunneleingang ohnehin schon sehr beschildert ist, erscheint das Aufstellen der vollständigen, notwendigen Informationen nachvollziehbarerweise als etwas schwierig. Ein Schild mit Nennung des Verantwortlichen und der Rechtsgrundlage ist rechtlich zwar notwendig, in diesem Einzelfall jedoch nicht unbedingt praktikabel, da die Kraftfahrzeuge relativ schnell daran vorbeifahren. Würde ein Verkehrsteilnehmender dieses Schild dann lesen wollen, entstünde mit einer Störung des fließenden Verkehrs eine zusätzliche und unnötige Gefahrensituation.

Eine vergleichbare Problemstellung liegt bei der Videoüberwachung im öffentlichen Nahverkehr in Bussen und Bahnen vor. Beim Einsteigen in videoüberwachte Fahrzeuge müssten die Fahrgäste ebenfalls zuvor umfassend informiert werden. Dies würde auch dort zu unnötigen Gefahrensituationen führen. Im öffentlichen Nahverkehr wird es deshalb akzeptiert, dass symbolhafte Hinweisschilder an den Türen der Fahrzeuge angebracht sind, auf denen die Verantwortlichen genannt werden. Die vollständigen Informationen gem. Art. 12 ff. DS-GVO müssen die Fahrgäste dann spätestens in den Fahrzeugen einsehen können, bestenfalls jedoch bereits vorher in den Verkaufsstellen und Informationszentren des Verantwortlichen.

Auch im Falle der Mautstelle an der Warnowquerung kann dies ähnlich gelöst werden. Die Verkehrsteilnehmenden können im Zweifel davon ausgehen, dass der Tunnel mithilfe von Kameras überwacht wird. Daher müssen hier vor Erfassung durch die Kameras symbolhafte Hinweisschilder mit Nennung des Verantwortlichen aufgestellt werden. Die vollständigen Informationen gem. Art. 12 ff. DS-GVO müssen dann im Bereich der Kassenhäuschen angebracht werden. Zur Stauvermeidung können diese Informationen den Kund:innen auf Verlangen ausgehändigt werden.

11.2. Kennzeichenerfassung auf Parkplätzen

Die automatisierte Kennzeichenerfassung auf drei Parkplätzen war Thema einer Beschwerde. Hierzu ist festzustellen, dass die automatisierte Kennzeichenerfassung zur Parkraumüberwachung grundsätzlich in engen Grenzen zulässig ist. Die Funktionsweise solcher automatisierten Parkraumüberwachungen von kostenpflichtigen oder kostenlosen Parkplätzen läuft in der Regel immer gleich ab. Sobald ein Fahrzeug die Einfahrt eines mittels automatisierter Kennzeichenerfassung überwachten Parkplatzes durchfahren hat, wird das Kfz-Kennzeichen erfasst und intern mit Datum und Uhrzeit gespeichert.

Bei den überprüften Parkplätzen handelte es sich um kostenpflichtige Parkplätze. Die Ein- und Ausfahrten sind mit Schranken gesichert. Die Benutzer:innen fahren an die Schranke heran und wählen aus, ob mit Kfz-Kennzeichenerfassung oder klassisch mit Ticket geparkt werden soll. Wird die Kfz-Kennzeichenerfassung gewählt, werden die o. g. Daten erfasst. Will man das Parken beenden und den Parkplatz verlassen, muss man zu einem Terminal auf dem jeweiligen Parkplatz gehen. Hier wird das Nummernschild eingegeben, dann wird das Parkentgelt berechnet und muss bezahlt werden. Anschließend fährt man an die Ausfahrtschranke und das Kennzeichen wird nochmalig gescannt. Im Hintergrund läuft ein automatisierter Abgleich zwischen Kennzeichen und abgeschlossenem Bezahlvorgang. War dieser erfolgreich, öffnet sich die Schranke und man kann den Parkplatz verlassen. Im Rahmen dieser automatisierten Kennzeichenerfassung werden unbestritten personenbezogene Daten der Halter:innen der Fahrzeuge in Form von Kfz-Kennzeichen verarbeitet. Für eine solche Verarbeitung der Daten ist jedoch zwingend eine Rechtsgrundlage notwendig. Eine solche Rechtsgrundlage lässt sich in den meisten Fällen einer automatisierten Kennzeichenerfassung in Art. 6 Abs. 1 lit. f DS-GVO finden. Hierbei wird das berechtigte Interesse des Parkraumbewirtschaftenden an einer ordnungsgemäßen Nutzung des Parkplatzes höher bewertet, als die Rechte und Freiheiten der auf den Parkplatz fahrenden Besucher:innen, sofern gewisse Voraussetzungen gegeben sind und umgesetzt werden.

Im vorliegenden Fall bedeutet dies, dass nur solche Daten verarbeitet werden dürfen, die für den genannten Zweck erforderlich sind. Für eine Parkraumüberwachung ist also ausschließlich das Kfz-Kennzeichen erforderlich. Die Einstellungen der Kameras bzw. der Erfassungsgeräte müssen demnach so konzipiert sein, dass nur das Kennzeichen erfasst wird und eben nicht der Fahrzeuginnenbereich oder die darin sitzenden Personen. Ferner muss auf die Datenverarbeitung unter Beachtung der Art. 12 ff. DS-GVO hingewiesen werden. Dieser Hinweis muss bereits erfolgen, bevor in den überwachten Bereich eingefahren wird. Schlussendlich müssen die gespeicherten Daten nach erfolgtem Bezahlvorgang und nach Verlassen des Parkplatzes, jedoch spätestens mit Ablauf des Tages gelöscht werden, soweit diese keinen gesetzlichen Aufbewahrungspflichten unterliegen.

11.3. Nutzung von Dashcams in Kraftfahrzeugen

In letzter Zeit häutfen sich beim LfDI MV Anfragen zu datenschutzrechtlichen Bedenken zur Nutzung sogenannter Dashboard-Kameras, insbesondere bei PKWs der Marke Tesla. Diese (bei Tesla meist direkt im Fahrzeug verbauten) Kameras beobachten bzw. filmen permanent das Fahrzeugumfeld und speichern die entsprechenden Daten zum Zweck der Beweissicherung, beispielsweise bei Unfällen. Hierbei werden auch Personen und Kfz-Kennzeichen erfasst. Eine solche permanente und damit anlasslose Fertigung von Videoaufnahmen im öffentlichen Straßenverkehr ist grundsätzlich unzulässig. Das Sammeln von Beweismitteln für einen hypothetischen Unfall reicht als „berechtigtes Interesse" nach Art. 6 Abs. 1 lit. f DS-GVO für die Nutzung derartiger Kameras und das Verarbeiten personenbezogener Daten nicht aus. Dies ergibt sich aus einer Abwägung zwischen dem Beweissicherungsinteresse der einzelnen Person und dem informationellen Selbstbestimmungsrecht einer Vielzahl von Verkehrsteilnehmenden. Zulässig können nach Rechtsprechung des Bundesgerichtshofes (BGH)[1] deshalb allenfalls kurzzeitige und anlassbezogenen Aufzeichnungen sein.

Ein datenschutzkonformer Einsatz von Dashcams ist deshalb nur möglich, wenn ein technisches Ringspeichersystem die vorhandenen Daten unmittelbar überschreibt und damit löscht, solange kein Anlass für eine dauerhafte Speicherung, z. B. durch ein Unfallereignis, gegeben ist. Als zulässig erachten wir hierbei einen Speicherzyklus von etwa ein bis zwei Minuten, d. h. ca. dreißig Sekunden bis eine Minute vor einem Ereignis und ca. dreißig Sekunden bis eine Minute nach einem Ereignis. Diese Zeitspanne sollte für die Dokumentation eines Unfallhergangs ausreichend sein.

In Fahrzeugen der Marke Tesla werden neben der Dashcam serienmäßig weitere Kameras verbaut. Mit diesen Kameras kann das Umfeld des Fahrzeugs im sogenannten Wächtermodus oder Sentry Mode kontinuierlich erfasst werden.

Dabei wird unserer Kenntnis nach bei eingestecktem USB-Stick die Kamerafunktion und die Speicherung von Bildaufnahmen auch schon aktiviert, wenn eine Person zu nah an einem Kfz der Marke Tesla vorbeigeht oder das Tesla-Erkennungssystem eine sonstige, durch den „Wächter (Sentry) Modus" als relevant eingestufte Bewegung zu erkennen meint. Einerseits fehlt somit oftmals schon ein konkreter Anlass. Andererseits wird die Umgebung samt unbeteiligter Passant:innen und gegebenenfalls weiterer personenbezogener Daten (wie z. B. Kfz-Kennzeichen) ab Aktivierung für einen Zeitraum von mehreren Minuten mit per Video aufgezeichnet sowie die Aufzeichnungen gespeichert.

Deshalb ist die Kamerafunktion grundsätzlich zu deaktivieren. Dies kann insbesondere durch ein Nicht-Nutzen bzw. ein Entfernen des USB-Sticks, der für die Aktivierung sowohl der „Dashcam" als auch des „Wächter (Sentry) Modus" im Fahrzeuginneren eingesteckt wird, erfolgen. Die Kamerafunktion der Dashcam kann alternativ, (ggf. je nach Tesla-Modell und Software-Stand des Fahrzeuges) auch am Display ausgeschaltet werden.

1 Siehe dazu Urteil vom 15.05.2018, Az. VI ZR 233/17, Rn. 26

Soweit das Fahrzeug in einer nicht öffentlich zugänglichen Umgebung abgestellt wird und dabei eine Aufzeichnung personenbezogener Daten Unbeteiligter (Personen, Kfz-Kennzeichen usw.) ausgeschlossen ist, steht der vollumfänglichen Nutzung des „Wächter (Sentry) Modus" mit Kameranutzung nichts entgegen. Auch die Tatsache, dass von einigen Gerichten mithilfe von Dashcams erstellte Aufnahmen als Beweismittel in Ordnungswidrigkeitenverfahren zugelassen wurden, ändert nichts an der oben genannten datenschutzrechtlichen Einschätzung des BGH. Die Frage der datenschutzrechtlichen Zulässigkeit derartiger Aufnahmen und die Frage ihrer prozessualen Verwertbarkeit sind zwei getrennte Fragen. Es liegt allein im Ermessen des jeweiligen Gerichts, ob unzulässig angefertigte Beweismittel in der Verhandlung zugelassen werden oder nicht.

Für alle Dashcams gilt: eine Verwendung in datenschutzrechtlich unzulässiger Weise ist gemäß Art. 83 Abs. 5 DS-GVO bußgeldbewehrt. Auch das Hochladen solcher Videos auf Online-Plattformen wie YouTube, Facebook, etc. kann mit einem Bußgeld geahndet werden.

11.4. Videoüberwachung in öffentlichen Verkehrsmitteln

In einer vorgelegten Beschwerde wurde bemängelt, dass in einem öffentlichen Verkehrsmittel, welches vor allem touristischen Zwecken dient, Videokameras installiert seien. Auf eine Datenverarbeitung durch die Videoüberwachung wurde dabei nicht nach den Vorgaben der Art. 12 ff. DS-GVO hingewiesen.

Die Befragung des Verantwortlichen ergab, dass der hintere Bereich des Fahrzeuges beim Öffnen und Schließen der hinteren Türen nicht auf andere Weise vom Fahrpersonal eingesehen werden kann. Die Kameras wurden daher aus Sicherheitsgründen eingesetzt und dienten dem Fahrpersonal als eine Art verlängertes Auge. Aufenthaltsbereiche im Fahrzeug wurden nicht gefilmt und es fand auch keine Aufzeichnung statt. Auf die Videokameras wurde durch Piktogramme mit Kamerasymbol hingewiesen, die im Inneren der Fahrzeug-Anhänger angebracht waren.

Die Verarbeitung der personenbezogenen Daten durch die Videoaufnahmen ist gem. Art. 6 Abs. 1 lit. f DS-GVO rechtmäßig, wenn die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Im vorliegenden Fall wurden die Kameras aus Sicherheitsgründen zur Überwachung der Türen eingesetzt. Ein milderes Mittel wäre der Einsatz einer weiteren Person, die diesen Bereich überwacht, was jedoch mit weitaus höheren Kosten verbunden wäre. Die Daten wurden in einem sparsamen Rahmen erhoben, die Videokameras nur auf den sicherheitsrelevanten Bereich gerichtet und die Daten wurden nicht gespeichert. Eine Videoüberwachung war in diesem Falle daher grundsätzlich rechtmäßig. Auf die Videoüberwachung ist jedoch gem. Art. 12 ff. DS-GVO adressatengerecht hinzuweisen. Es müssen transparente und umfassende Informationen vor Betreten des Sichtbereiches bereitgestellt werden.

Dazu gehören gem. Art. 13 DS-GVO mindestens die Angaben zur Identität des Verantwortlichen, die Kontaktdaten des betrieblichen Datenschutzbeauftragten, die Verarbeitungszwecke und die Rechtsgrundlage, die Angabe des berechtigten Interesses, die Dauer der Speicherung sowie der Hinweis auf Zugang zu weiteren Pflichtinformationen.

Lediglich ein Piktogramm im Inneren des Fahrzeuges entspricht diesen Vorgaben gesetzmäßig nicht. Um im Sonderfall des öffentlichen Personennahverkehrs (ÖPNV) besonders umfangreiche Informationen an den Türen und somit die Stau- und Unfallgefahren der einsteigenden Personen zu vermeiden, ist es hier auch akzeptabel, wenn außen an den Türen durch symbolhafte Hinweisschilder einschließlich der Angabe des Verantwortlichen auf die Videoüberwachung hingewiesen wird. Der vollständigen Hinweispflicht muss dann an den Verkaufsstellen, Kundeninformationszentren und sonstigen zentralen Stellen des Verkehrsunternehmens nachgekommen werden.

12. Vereine

Neben der Aufsicht über verantwortliche Stellen aus dem öffentlichen Bereich und der Wirtschaft obliegt dem LfDI MV auch die datenschutzrechtliche Aufsicht über Vereine, unabhängig davon, ob es sich hierbei um eingetragene oder gemeinnützige Vereine handelt, die beispielsweise als Sport-, Umweltschutz-, Selbsthilfe- oder Fördervereine agieren. Der Datenschutz ist für Vereine ein wichtiges Thema, denn der Umgang mit Mitgliederdaten ist zum einen unvermeidbar, zum anderen besteht ein Interesse daran, die gespeicherten personenbezogenen Daten der Mitgliedschaft angemessen zu schützen. In dem nachfolgenden Unterkapitel wird das Thema Datenschutz im Kleingartenverein (siehe Punkt 12.1.) behandelt, da uns zunehmend Beschwerden aus dieser Sparte erreichen.

12.1. Datenschutz im Kleingartenverein

Augen auf bei der Parzellenwahl – absurde Diskussionen und Streitigkeiten in Kleingartenanlagen bedienen ein typisch deutsches Klischee. Zunehmend erhalten wir Beschwerden der (ehemaligen) Mitglieder von Kleingartenvereinen in Mecklenburg-Vorpommern. Auffällig hierbei ist, dass das Datenschutzrecht in einigen Fällen als Deckmantel dafür genutzt wird, seinen Frust über die Arbeit der Vereinsvorstände rauszulassen, den Nachbarn zur Weißglut zu treiben oder sonstige persönliche Konflikte auszutragen. Nicht selten schildern uns die Betroffenen neben dem mutmaßlich datenschutzrechtlich relevanten Sachverhalt, dass es in jüngster Vergangenheit Streitigkeiten während Mitgliederversammlungen oder in der vereinsinternen Chat-Gruppe gegeben hätten.

Im Mittelpunkt der zahlreichen Beschwerdeverfahren, die im Berichtszeitraum bei uns anhängig gemacht wurden, standen insbesondere Aushänge in Schaukästen oder am Schwarzen Brett, denn diese werden nicht selten als „Pranger" zweckentfremdet. Auch mündliche Aussagen in Form von Verunglimpfungen oder Lästereien sind Gegenstand einiger Beschwerden gewesen.

In diesen Fällen mussten wir den betroffenen Personen jedoch mitteilen, dass Regelungen der DS-GVO erst Anwendung finden, wenn personenbezogene Daten in einem Dateisystem gespeichert sind oder in einem solchen gespeichert werden sollen (Art. 2 Abs. 1 DS-GVO). Rein mündliche Aussagen können daher nicht den Gegenstand eines Beschwerdeverfahrens bilden.

In vielen Fällen, die die Verarbeitung von Mitgliederdaten in Kleingartenvereinen betrafen, konnten wir jedoch erfolgreich mittels Beratungen und der Erteilung (informeller) Hinweise auf einen datenschutzkonformen Umgang mit Mitgliederdaten hinwirken und die Vereinsvorstände als verantwortliche Personen diesbezüglich sensibilisieren.

Nichtsdestotrotz sollte an dieser Stelle darauf hingewiesen werden, dass Fairness und Transparenz nicht nur als datenschutzrechtliche Grundsätze für die Verarbeitung von personenbezogenen Daten wahrzunehmen sind, sondern auch für das friedliche Miteinander innerhalb des Vereinslebens gelten sollten.

13. Bußgeldstelle und Justiziariat

Im Rahmen unserer Aufsichtstätigkeit ergehen immer wieder Bescheide des LfDI MV, die von Beschwerdeführer:innen oder von Verantwortlichen nicht akzeptiert und in der Folge durch das VG überprüft werden. Der kommende Abschnitt gibt eine Übersicht zu den laufenden und abgeschlossenen Gerichtsverfahren vor dem VG im Berichtszeitraum – besonders die Frage, ab wann Beschwerden oder gar Klagen als exzessiv zu betrachten sind, ist gerichtlich zu klären (siehe Punkt 13.1.).

In der Bußgeldstelle unserer Behörde liegt der Schwerpunkt weiter auf der Ahndung von sogenannten Mitarbeiterexzessen (siehe Punkt 13.2.). Insbesondere bei der Verarbeitung von sensiblen Daten, wie bspw. im Krankenhaus oder bei der Landespolizei MV, müssen Bürger:innen auf den Schutz dieser Daten vertrauen können. In Fällen, in denen sich einzelne Mitarbeitende eigenmächtig über Weisungen oder Zugriffsbeschränkungen des Verantwortlichen hinwegsetzen, kann ein Bußgeld drohen.

13.1. Bei dem Verwaltungsgericht anhängige Verfahren

Wir führen Rechtstreitigkeiten vor dem Verwaltungsgericht: sind Beschwerdeführer:innen mit unserer Entscheidung nicht einverstanden, wird regelmäßig der Rechtsweg zu dem VG Schwerin eröffnet. Ebenso können Verantwortliche unser Maßnahmen im Rahmen der Anfechtungsklage richterlich überprüfen lassen. Regelmäßig enden unsere Verfahren demnach mit einem Bescheid, entweder an Beschwerdeführer:innen oder an Verantwortliche, der richterlich überprüft werden kann. Diese Rechtsschutzmöglichkeit ist in Art. 78 DS-GVO ausdrücklich normiert.

Bundesweit häufen sich jedoch die Verfahren, in denen zumindest der Verdacht besteht, dass es nicht mehr um die Klärung einer datenschutzrechtlichen Frage geht, sondern vielmehr darum, durch eine Häufung von Beschwerden und Klagen Verwaltung und Justiz lahm zu legen.

Die DS-GVO spricht hier von offenkundig unbegründeten oder exzessiven Beschwerden, in denen die Datenschutzaufsichtsbehörden nicht mehr zum Tätigwerden verpflichtet sind (vgl. Art. 57 Abs. 4 DS-GVO). Das VG Schwerin hat in einer Reihe von Klagen daher die Frage zu klären, wann Beschwerden als rechtsmissbräuchlich oder exzessiv zu bewerten sind. Interessant ist hierbei die Frage, wann Gerichte die Klagen selbst als rechtsmissbräuchlich abweisen können. Unlängst erging in diesem Zusammenhang eine Entscheidung in Hessen. Unter Bezugnahme auf die Rechtsprechung des Bundesverfassungsgerichts[1] machte das VG Hessen deutlich, dass die Rechtsschutzgarantie nicht den Anspruch umfasse, eine förmliche Entscheidung auf Eingaben zu erhalten, die offensichtlich missbräuchlich, offensichtlich wiederholend oder sinnlos vorgebracht werden. Das Gericht führte weiter aus, dass bei Nachweis des systematischen Missbrauchs prozessualer Rechte einer Person in einer Vielzahl von Fällen, die Vermutung dafür spreche, dass auch künftigen Eingaben dieser Person Rechtsmissbrauch zugrunde liege. Um der Verpflichtung zur Rechtsschutzgewährung nach Art. 19 Abs. 4 Grundgesetz in diesen Fällen zu genügen, sei nur noch formlos zu prüfen, ob der Person für neuerlich vorgebrachte Anliegen entgegen der bestehenden Missbrauchsvermutung ein Mindestmaß an berechtigtem Rechtsverfolgungsinteresse zur Seite stehe, so das Gericht[2] weiter. Die erstinstanzliche Entscheidung eines VG eines anderen Bundeslandes entfaltet grundsätzlich keinerlei Bindungswirkung für die Gerichte in Mecklenburg-Vorpommern. Es bleibt daher spannend, ob und wie sich diese Rechtsprechung auf Entscheidungen des VG in Schwerin auswirken wird.

Im Rahmen der Klagen von Beschwerdeführer:innen wird weiterhin zu klären sein, ob die Datenschutzaufsichtsbehörden verpflichtet sind, förmliche Maßnahmen nach Art. 58 Abs. 2 DS-GVO immer auch gegen öffentliche Stellen zu ergreifen, wenn ein Datenschutzverstoß zwar festgestellt, die Beseitigung dessen aber durch den Verantwortlichen bereits zugesichert wurde. Ebenfalls von genereller Bedeutung wird die Entscheidung über die Einstellung eines Verfahrens gegen einen Presseverantwortlichen sein. Der LfDI MV vertrat hier die Auffassung, gem. § 18a Landespressegesetz Mecklenburg-Vorpommern nicht zuständig zu sein. Die Regelung sichert nach unserer Auffassung die verfassungsrechtlich normierte Staatsferne und Unabhängigkeit der Presse. Der Beschwerdeführer und Kläger in dem Verfahren äußert hingegen Bedenken an der Europarechtskonformität der Regelung.

Bei den Klagen von Verantwortlichen geht es in den allermeisten Fällen um Anordnungen des LfDI MV im Zusammenhang mit Videoüberwachungsanlagen. In einem Fall ist dabei die Auslegung von Art. 5 Abs. 2 DS-GVO Thema, ob eine Videoüberwachung bereits dann untersagt werden kann, wenn der Nachweis der Rechtmäßigkeit der Videoüberwachung vom Verantwortlichen nicht erbracht werden kann. Der EuGH stellte in einer Entscheidung aus Mai 2023[3] klar, dass zwar nicht jeder Verstoß gegen die Dokumentationspflichten der DS-GVO eine Verarbeitung rechtswidrig macht, sehr wohl aber ein Verstoß gegen die Dokumentationspflichten aus Art. 5 Abs. 2 DS-GVO.

1 BVerfG, Beschluss vom 19.04.2021 – 1 BvR 2552/18

2 VG Wiesbaden, Beschluss vom 05.02.2024 – 6 K 1/24. WI

3 Vgl. EuGH, Urteil vom 4.5.2023 – C-60/22

Darüber hinaus verwarf das OVG Mecklenburg-Vorpommern in verschiedenen Verfahren Berufungen von Verantwortlichen und bestätigte damit die Zulässigkeit von Maßnahmen unserer Behörde endgültig. Das betrifft zunächst die Entscheidung des LfDI MV zur Untersagung des Portals „neutrale Schule" der AfD-Fraktion im Landtag Mecklenburg-Vorpommern. Diese hatte über das Portal „neutrale Schule" Schüler:innen, Lehrer:innen und Eltern aufgefordert, kritische Äußerungen im Schulkontext über die AfD zu melden. Der LfDI MV sah für die Verarbeitung der besonders geschützten politischen Meinungen von Lehrkräften und Schüler:innen aber keine Rechtsgrundlage und sprach ein Verbot der Datenverarbeitung aus. Interessant für andere Verantwortliche ist dabei die Auslegung des Gerichts zu Art. 9 Abs. 2 lit. f DS-GVO. Demnach könne eine Verarbeitung von besonderen Kategorien personenbezogener Daten, wie etwa politische Meinungen oder Gesundheitsdaten (vgl. Art. 9 Abs. 1 DS-GVO), nur dann auf Art. 9 Abs. 2 lit. f DS-GVO gestützt werden, wenn eine rechtliche Auseinandersetzung bereits bestehe. Die präventive Speicherung sensibler Daten zur Abwehr möglicherweise in Zukunft geltend gemachter Ansprüche sei hingegen nicht umfasst.

In einer weiteren Entscheidung bestätigte das OVG[1] die Auslegung des LfDI MV zur weiten Auslegung des Begriffs der personenbezogenen Daten und des Anspruchs auf Kopie nach Art. 15 Abs. 3 DS-GVO. In dem zu Grunde liegenden Verfahren war demnach ein Baugutachten vollständig als personenbezogenes Datum zu qualifizieren und damit eine vollständige Kopie des Gutachtens an den Beschwerdeführer herauszugeben.

13.2. Mitarbeiterexzesse weiterhin Schwerpunkt der Bußgeldstelle

Es gehört zu den Aufgaben des LfDI MV, Bußgeldverfahren durchzuführen.

Vor allem beschäftigen uns als Bußgeldstelle im Berichtszeitraum sogenannte Mitarbeiterexzesse, die durch die Verantwortlichen als Datenpannen (vgl. Art. 33 DS-GVO) gemeldet wurden. Insbesondere Verantwortliche aus den Bereichen Polizei und sonstige öffentliche Stellen sowie Krankenhäuser melden regelmäßig entsprechende Verstöße ihrer Mitarbeiter:innen, nachdem diese ohne dienstliche oder betriebliche Veranlassung auf personenbezogene Daten zugegriffen haben, beispielsweise aus Neugier oder um die Daten an Dritte weiterzugeben. Nach der DS-GVO sind grundsätzlich nur die Verantwortlichen, demzufolge in der Regel die juristischen Personen vertreten durch die jeweilige Leitung und die Auftragsverarbeiter, nicht aber die Beschäftigten, zur Einhaltung der Bestimmungen nach der DS-GVO verantwortlich. Die Leitungen müssen vielmehr durch Weisungen nach Art. 29 DS-GVO und entsprechende technische Beschränkungen dafür Sorge tragen, dass Beschäftigte personenbezogene Daten nur im Rahmen ihrer Aufgabenerfüllung verarbeiten. Falls es an diesen Weisungen fehlte oder es keine geeigneten und angemessenen technischen Maßnahmen gab, um den jeweiligen rechtswidrigen Zugriff von Beschäftigten zu verhindern, verstießen nicht die Beschäftigten, sondern die jeweiligen Verantwortlichen selbst gegen den Datenschutz.

1 OVG Greifswald, Beschluss vom 14.12.2023 – 1 LZ 413/21 OVG

Dennoch kommt es immer wieder vor, dass Beschäftigte Zugangsbeschränkungen umgehen oder, sofern diese nicht möglich sind, ohne die Aufgabenerfüllung zu gefährden, sich über Weisungen hinwegsetzen. In diesen Fällen bestimmen Beschäftigte eigenmächtig über die Zwecke und Mittel der Verarbeitung und schwingen sich somit eigenmächtig zum Verantwortlichen auf und können damit auch selbst in den Fokus unserer Ermittlungen geraten. In diesen Fällen erachten wir eine Sanktionierung für besonders wichtig, da es sich regelmäßig um besonders sensible Daten handelt, die von Bürger:innen auf einer gesetzlichen Grundlage verarbeitet werden. Diese vertrauen darauf, dass die Daten (beispielweise in der Landespolizei MV oder in Krankenhäusern) sicher und vor rechtswidrigen Zugriffen geschützt sind. Wir erließen daher mehrere Bußgeldbescheide gegen Polizist:innen, eine ehemalige Beschäftigte eines Gerichts und einen ehemaligen Pfleger.

In einem Verfahren ziehen sich die Ermittlungen sehr lange hin. Da der zuständige Arbeitgeber nicht unserer Zuständigkeit unterliegt, wir aber für die Verfolgung der Ordnungswidrigkeit des Beschäftigten zuständig sind, verweigert der Arbeitgeber, (eine öffentliche Stelle) für unser Verfahren notwendige Auskünfte. Wir vertreten hier die Auffassung, dass die Stelle gem. § 160 Strafgesetzbuch (StGB) verpflichtet ist, uns die Auskünfte zu erteilen. Diese weigert sich jedoch „wegen des Datenschutzes". Grundsätzlich begrüßen wir es, wenn Anforderungen von personenbezogenen Daten kritisch hinterfragt werden und sensibel mit Beschäftigtendaten umgegangen wird. Allerdings wiesen wir mehrfach auf die Rechtsgrundlagen für die Übermittlung hin und die für die angefragte Stelle zuständige Datenschutzaufsichtsbehörde äußert auch keine Bedenken an der Zulässigkeit der Übermittlung der angefragten Daten. Da diese öffentliche Stelle mit sensiblen Sozialdaten umgeht, bleiben wir hartnäckig.

Ein weiteres Bußgeld wurde wegen eines Aushangs eines Gerichtsurteils mit personenbezogenen Daten Dritter durch einen Vermieter verhängt.

Teilweise wurden gegen die Bescheide Einsprüche eingelegt, so dass nunmehr der Strafrichter entscheiden muss.

14. Begleitung von Rechtssetzungsvorhaben

Nach Art. 57 Abs. 1 lit. c DS-GVO ist es unsere Aufgabe u. a. sowohl den Landtag MV als auch die Landesregierung über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten zu beraten. Damit korrespondiert auch die Pflicht nach Art. 36 Abs. 4 DS-GVO zur Konsultation des LfDI MV bei der Ausarbeitung von Rechtssetzungsvorhaben, soweit diese Verarbeitungen personenbezogener Daten betreffen.

Vor diesem rechtlichen Hintergrund begleiteten wir im Berichtszeitraum eine Vielzahl von Rechtssetzungsvorhaben in der vorparlamentarischen und parlamentarischen Phase. In der vorparlamentarischen Phase wurde der LfDI MV durch die Landesregierung entweder im Rahmen von Ressort- oder Verbandsanhörungen beteiligt.

Diesbezüglich ist auf § 4 Abs. 3 Satz 8 der Gemeinsamen Geschäftsordnung II (GGO II, Richtlinien zum Erlass vor Rechtsvorschriften und weiteren Regelungen durch die Landesregierung MV) hinzuweisen, wonach der LfDI MV zu allen Rechtsvorschriften, die das Recht auf informationelle Selbstbestimmung berühren, bereits in der Ressortanhörung einzubeziehen ist. Diese Beteiligung in der Ressortanhörung ist auch wichtig, damit bei Rechtssetzungsvorhaben frühzeitig eine Prüfung auf Datenschutzrechtskonformität durch die Aufsichtsbehörde erfolgen kann, sodass etwaige Änderungsbedarfe bereits in eine Verbandsanhörung einfließen könnten. Überwiegend wurde durch die Koordinierungsstellen der jeweiligen Ressorts jedoch entsprechend der Vorgaben der GGO II beteiligt.

Gleichwohl im Rahmen der Beteiligung zu Rechtssetzungsvorhaben vereinzelt auch abweichende Ansichten vertreten wurden, war die Zusammenarbeit sowohl mit den jeweiligen federführenden Ressorts der Landesregierung als auch in den Ausschüssen des Landtages überaus konstruktiv und ausgesprochen gut. Für die jeweiligen Beteiligungen durch den Landtag MV und die Landesregierung einschließlich der Berücksichtigung von Änderungsanregungen bedanken wir uns.

Besonders herauszuheben sind im Berichtszeitraum zwei Rechtssetzungsvorhaben. Dies betrifft die Modernisierung des Kommunalverfassungsrechts (siehe Punkt 14.1.) und die Anpassung des SOG M-V nach dem Beschluss des Bundesverfassungsgerichts vom 09.12.2022 (1 BvR 1345/21), mit welchem die Verfassungswidrigkeit einzelner Normen zu Ermittlungsbefugnissen der Polizei festgestellt wurde (siehe Punkt 14.2.).

14.1. Novellierung der Kommunalverfassung M-V

Die Kommunalverfassung für das Land Mecklenburg-Vorpommern (KV M-V) ist für die Regelung des Lebens und die demokratische Teilhabe in den Kommunen von kaum zu überschätzender Bedeutung. Im Zusammenhang mit der Anwendung der KV M-V, besonders für kommunale Vertretungsorgane wie bspw. Gemeinde- oder Stadtvertretungen, erreichten uns immer wieder Beratungsanfragen zu datenschutzkonformen Umsetzungen. Die Rechtsunsicherheiten waren vor allem mit Blick auf Ton-/Bildaufzeichnungen und –übertragungen sowie der Anfertigung von Tonaufzeichnungen für Protokollierungen von Sitzungen kommunaler Vertretungsorgane (§ 29 Abs. 5 Satz 5, Abs. 8 KV M-V), dem Umgang mit Beratungs- und Beschlussvorlagen sowie der datenschutzrechtlichen Verantwortlichkeiten im Rahmen der Ämterstruktur (§§ 125 ff. KV M-V) zu vernehmen. Zu den jeweiligen Beratungsanfragen konnten zwar jeweils Empfehlungen ausgesprochen werden, aber alle Rechtsunsicherheiten konnten mitunter nicht gänzlich ausgeräumt werden.

Insoweit wurde es seitens des LfDI MV sehr begrüßt, dass im Berichtszeitraum durch die Landesregierung die Arbeit an einem Gesetzesentwurf zur Modernisierung des Kommunalverfassungsrechts aufgenommen wurde. Nach dem Entwurf zur Änderung der KV M-V war u. a. vorgesehen, dass kommunale Vertretungsorgane auch unabhängig von besonderen Ausnahmesituationen (wie z. B. der SARS-CoV-2-Pandemie) Sitzungen mittels Videokonferenztechnik durchführen und unter bestimmten Voraussetzungen auch Live- und On-Demand-Streams anbieten können.

Damit dürfte einerseits die Arbeit von ehrenamtlich tätigen Vertreter:innen der kommunalen Organe erheblich erleichtert und die Vereinbarkeit von Familie/Privatleben, Beruf und Ehrenamt verstärkt werden. Darüber hinaus dürfte damit auch auf ein geändertes Informations- und Kommunikationsverhalten von Bürger:innen reagiert werden, indem über Live- und On-Demand-Streams der Sitzungen kommunaler Vertretungsorgane eine breitere und gezielte Teilhabe an kommunalen Willensbildungs- und Entscheidungsprozessen sowie die Erhöhung der Transparenz demokratischer Prozesse im Sinne des Öffentlichkeitsgrundsatzes ermöglicht wird.

Dieses Vorhaben wurde unserseits eindringlich befürwortet, sofern eine datenschutzrechtskonforme Umsetzung erfolgt. Diese konnte während des Rechtssetzungsvorhabens auch realisiert werden, indem die erforderlichen datenschutzrechtlichen Regelungen eingebracht wurden. In der vorparlamentarischen Phase wurde unsere Behörde aufgrund der weitreichenden datenschutzrechtlicher Bezüge sowohl in der Ressort- als auch in der Verbandsanhörung beteiligt. Es wurden zwar nicht alle Änderungsanregungen des LfDI MV berücksichtigt, aber die Zusammenarbeit war mit dem federführenden Ressort stets konstruktiv. Nebst der Regelungen zur Teilnahme an den Sitzungen kommunaler Vertretungsorgane mittels moderner Partizipationsmöglichkeiten wurden ebenso bisherige Rechtsunsicherheiten aufgegriffen. So gingen u. a. auch Regelungen zur Anfertigung von Tonaufnahmen zu Protokollierungszwecken sowie zu den datenschutzrechtlichen Verantwortlichkeiten im Rahmen der Ämterstruktur in den Gesetzesentwurf ein. Ferner wurden auch weitere aus datenschutzrechtlicher Perspektive zu begrüßende Regelungen aufgenommen.

In der parlamentarischen Phase des Rechtssetzungsvorhabens konnte der LfDI MV dankbarerweise auf verbleibende Änderungsbedarfe in einer schriftlichen Stellungnahme gegenüber dem Ausschuss für Inneres, Bau und Digitalisierung des Landtages MV hinweisen. In der sich anschließenden öffentlichen Anhörung wurde sodann vermehrt Kritik dahingehend geäußert, dass insbesondere die datenschutzrechtlichen Regelungen zu (partiell) digitalen Sitzungen kommunaler Vertretungsorgane sowie deren Übertragung und die Bereitstellung von Aufzeichnungen zu kompliziert seien. Diese Einwände sind teilweise nachvollziehbar, dennoch waren die datenschutzrechtlichen Regelungen im Gesetzesentwurf erforderlich, um die Unionsrechtskonformität zu gewährleisten. Obwohl der LfDI MV in der vorparlamentarischen Phase in zwei Anhörungen beteiligt wurde, hätte diese Kritik möglicherweise aufgefangen werden können, wenn der LfDI MV bereits in der ab September 2022 eingesetzten Arbeitsgruppe zur Novellierung der KV M-V eingebunden worden wäre.

Mit der Verabschiedung des Gesetzesentwurfes durch den Landtag sollten die Kommunen, falls von den modernen Partizipationsmöglichkeiten Gebrauch gemacht werden soll, für eine einfache Handhabung und die Reduzierung des Umsetzungsaufwands, wie bereits im Vorfeld durch den LfDI MV angeregt, mit Mustersatzungen unterstützt werden. Im Weiteren sollte von der vorgesehenen Ermächtigung zum Erlass einer Verordnung über die organisatorischen und technischen Anforderungen an eine Teilnahme mittels Bild- und Tonübertragung auch Gebrauch gemacht werden.

Denn es würde das Gesetzesvorhaben konterkarieren, den Kommunen zunächst moderne und digitale Partizipationsmöglichkeiten zu ermöglichen, diese aber zugleich mit Rechtsunsicherheiten zu konfrontieren, woraufhin die neuen Möglichkeiten zur Teilhabe am kommunalen Entscheidungsprozessen kommunaler Vertretungsorgane ggf. gar nicht erst wahrgenommen werden. Der LfDI MV stellt sich für die Unterstützung bei der Erarbeitung entsprechender Regelungen in beratender Funktion zur Verfügung.

14.2. Anpassung des SOG M-V an die Vorgaben des Bundesverfassungsgerichts

Mit Beschluss vom 09.12.2022 entschied das BVerfG, dass mehrere Regelungen des SOG M-V zu Ermittlungsbefugnissen der Polizei im Bereich der Gefahrenabwehr verfassungswidrig sind (1 BvR 1345/21). Dies betraf insbesondere Regelungen zur Wohnraum- und Telekommunikationsüberwachung, zur Onlinedurchsuchung, zur Rasterfahndung und dem Einsatz von Vertrauenspersonen. Die betreffenden Normen erfüllten weitgehend nicht die in ständiger Rechtsprechung konkretisierten Anforderungen der Verhältnismäßigkeit im engeren Sinne an heimliche Überwachungsmaßnahmen der Polizei.

Mitunter waren die Eingriffsschwellen der betreffenden Normen nicht hinreichend. Es wurden teilweise Anforderungen an das Gebot der Normenklarheit nicht erfüllt und der Schutz des Kernbereichs privater Lebensgestaltung wurde nicht hinreichend gewährleistet. Somit wurden durch das BVerfG einerseits bestimmte Normen zu Ermittlungsbefugnissen nichtig erklärt, andererseits konnten bestimmte Regelungen, die nicht nichtig erklärt wurden, unter einschränkenden Maßgaben bis 31.12.2023 fortgelten.

Die in der Entscheidung des BVerfG betroffenen Normen sind eingriffsintensive Ermittlungsbefugnisse, die im Rahmen der Novellierung des SOG M-V im Jahr 2020 geregelt wurden. Zu diesem Gesetzesvorhaben hatten wir sowohl bereits in der vorparlamentarischen Phase gegenüber der Landesregierung massive Kritik geäußert als auch im parlamentarischen Gesetzgebungsverfahren auf Missstände aufmerksam gemacht. Berücksichtigt wurden längst nicht alle Änderungsanregungen des LfDI MV. Teilweise wurden jedoch Missstände, auf die unsere Behörde bereits im Gesetzgebungsverfahren aufmerksam machte, nunmehr vom BVerfG aufgegriffen. Im Hinblick auf die dringend erforderlichen Änderungen des SOG M-V, die mit der Entscheidung des BVerfG einhergingen, boten wir der Landesregierung in der Hoffnung, dass unsere Hinweise nunmehr Berücksichtigung finden, Unterstützung an. In der Folge wurde der LfDI MV zum Änderungsgesetz zur Anpassung des SOG M-V an bundesverfassungsgerichtliche Vorgaben intensiv und frühzeitig beteiligt. Die Zusammenarbeit mit der Landesregierung an dem Gesetzesänderungsvorhaben war durchgängig konstruktiv und unsere Änderungsanregungen wurden aufgenommen.

Neben einer Anpassung an die Vorgaben des BVerfG wurden im Kontext dieses Gesetzesänderungsvorhabens auch Änderungen mit Blick auf die aufsichtsbehördlichen Befugnisse des LfDI MV vorgenommen. So waren ehemals nach § 48b SOG M-V keine Anordnungen zur Löschung personenbezogener Daten durch den LfDI MV möglich.

Novellierung des SOG M-V Hinweise des LfDI MV, wie auch beim Änderungsgesetz 2023, tatsächlich von der Landesregierung erhört werden und die ausgesprochen gute Zusammenarbeit, wie sie bei den jüngeren Rechtssetzungsvorhaben im Berichtszeitraum bestand, fortgesetzt wird.

Dies entsprach jedoch nicht den Vorgaben aus Art. 47 Abs. 2 der Richtlinie 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). Aufgrund dieser europarechtswidrigen Einschränkung der Befugnisse der Datenschutzaufsichtsbehörde war ein Vertragsverletzungsverfahren vor der Europäischen Kommission anhängig. Mit der Änderung des SOG M-V sind nunmehr auch Anordnungen zur Löschung personenbezogener Daten durch den LfDI MV möglich.

Die Entscheidung des BVerfG zum SOG M-V und die damit einhergehend vorgenommenen Änderungen sind für die Wahrung der Grundrechte von Bürger:innen, vor allem dem Schutz des Kernbereichs privater Lebensgestaltung, von überragender Bedeutung. Aktuell wird durch die Landesregierung bereits eine Evaluierung zu den mit der Novelle im Jahr 2020 vorgenommenen Änderungen durchgeführt, zu der dem Landtag bis zum 31.12.2024 zu berichten ist. An dieser Evaluierung wird der LfDI MV bereits derzeit beteiligt. Es bleibt zu hoffen, dass zu einer sich der Evaluierung etwaig anschließenden Novellierung des SOG M-V Hinweise des LfDI MV, wie auch beim Änderungsgesetz 2023, tatsächlich von der Landesregierung erhört werden und die ausgesprochen gute Zusammenarbeit, wie sie bei den jüngeren Rechtssetzungsvorhaben im Berichtszeitraum bestand, fortgesetzt wird.

Teil B

9. Bericht über die Umsetzung des Informationsfreiheitsgesetzes Mecklenburg-Vorpommern

Berichtszeitraum: 1. Januar 2022 bis 31. Dezember 2023

1. Informationsfreiheit in Mecklenburg-Vorpommern – Bedeutung, Zahlen und Fakten

Das gestiegene Interesse an der Informationsfreiheit in Mecklenburg-Vorpommern (M-V) war auch in den Berichtsjahren 2022 und 2023 deutlich zu erkennen. Zurückzuführen war dies zu einem großen Teil auf die deutschlandweit agierende Plattform „FragDenStaat". Dabei handelt es sich um eine Website des Open Knowledge Foundation Deutschland e.V., welche es Bürger:innen ermöglicht, Anträge auf Informationszugang gemäß Informationsfreiheitsgesetz Mecklenburg-Vorpommern (IFG M-V) unkompliziert an sämtliche Behörden in M-V zu übermitteln. Die Mehrheit der Anfragen, die zum Thema Informationsfreiheit beim LfDI MV eingingen, erreichte uns über diese Plattform. Dass dies auch zu Problemen und rechtlichen Herausforderungen führte, werden wir in einigen der nachfolgenden Berichte noch weiter erläutern.

Mit der heranwachsenden Bedeutung der Informationsfreiheit stieg auch das Arbeitspensum des LfDI MV. Unter anderem deshalb wurde im Rahmen einer im Jahr 2022 in dem für die Informationsfreiheit zuständigen Referat durchgeführten Umorganisation unsere Tätigkeit als Kontrollstelle bzw. hinsichtlich der Bearbeitung von an uns gerichteten Anfragen so organisiert, dass sich zwei Mitarbeiter:innen (wenn auch nur mit einem gewissen Zeitanteil) mit diesem Thema beschäftigen.

Den Hauptteil unserer Arbeit gestaltete die außergerichtliche Vermittlung bei diversen IFG-Anträgen. So wurde der LfDI MV im Berichtsjahr 2022 37 Mal schriftlich um Vermittlung gebeten. Diese Zahl verdoppelte sich im Berichtsjahr 2023 fast, sodass hier 60 schriftliche Vermittlungsanträge zu verzeichnen waren. Deutlich mehr als die Hälfte der insgesamt 97 eingegangenen Bitten um Vermittlung, erfolgten über die bereits angesprochene Plattform „FragDenStaat". Hinzu kamen hierbei noch zahlreiche telefonische Beratungen von Bürger:innen sowie natürlich auch der auskunftspflichtigen Stellen. Einige dieser Problematiken ließen sich bereits am Telefon bilateral klären.

Thematisch nahmen die Anfragen zur Corona-Pandemie deutlich ab. Anfragen zu finanziellen Belastungen der Behörden in M-V sowie Anträge auf Herausgaben von Gutachten, Protokollen und Verträgen traten hier in den Vordergrund.

Der LfDI MV fällt als Behörde selbst natürlich auch unter den Anwendungsbereich des IFG M-V. Im Jahr 2022 gingen bei uns daher neun Anträge auf Informationszugang und im Jahr 2023 elf Anträge ein. Auch hier erreichten uns 70 % der Anfragen via „FragDenStaat". Mehrheitlich wurde die Herausgabe von Statistiken beantragt. Jedoch wurde auch vereinzelt um Akteneinsicht in Unterlagen des LfDI MV gebeten, weshalb in diesen Fällen aufwendige Drittbeteiligungsverfahren und Bewertungen durch uns durchgeführt werden mussten.

Im Berichtsjahr 2023 war der LfDI MV seit langem wieder in der Lage, Schulungen zum IFG M-V anzubieten. So wurden diese bspw. in Kommunalverwaltungen oder Bildungsinstituten durchgeführt. Lange Zeit war dies aus Kapazitätsgründen und dann pandemiebedingt nicht möglich. Oft wurde jedoch festgestellt, dass bei vielen öffentlichen Verwaltungen ein hoher Schulungsbedarf hinsichtlich der Informationsfreiheit besteht.

Nach Einschätzung des LfDI MV sind einige Regelungen des aktuell gültigen IFG M-V, im Gegensatz zu anderen modernen Transparenzgesetzen, nicht mehr zeitgemäß und damit antiquiert. Auch darauf werden wir in einigen der nachfolgenden Berichte genauer eingehen.

Im derzeitigen Koalitionsvertrag hat die Landesregierung M-V in Punkt 506 u. a. festgehalten, dass das IFG M-V evaluiert und weiterentwickelt werden soll. Wie bereits im letzten Tätigkeitsbericht festgehalten, sollte die immer noch ausstehende Umsetzung dieses Punktes in Richtung der Schaffung eines modernen Transparenzgesetzes, an dessen Erarbeitung wir aufgrund unserer langjährigen Erfahrung auf diesem Gebiet gerne mitwirken, erfolgen.

Wir bekräftigen daher die bereits im letzten Tätigkeitsbericht ausgesprochene Empfehlung, auch für Mecklenburg-Vorpommern ein Transparenzgesetz mit klar festgelegten und in einem Transparenzregister zu regelnden Veröffentlichungspflichten zu schaffen.

2. Bildungsministerium gibt Abituraufgaben der vergangenen Jahre heraus

Sowohl im 7. als auch im 8. Tätigkeitsbericht haben wir über die Kampagne „FragSieAbi“ sowie über das Nachfolgeprojekt „Verschlusssache Prüfung“ berichtet, die 2019 von der Plattform FragDenStaat gemeinsam mit Wikimedia Deutschland ins Leben gerufen wurden. Diese sollten interessierten Bürger:innen zunächst die Herausgabe von Abitur-Aufgaben und später auch den Zugang zu den Abschlussprüfungen für die Berufsreife und Mittlere Reife ermöglichen.

In den vergangenen Berichtszeiträumen mussten wir zumeist vermittelnd tätigt werden, da es an einer fristgerechten Bearbeitung seitens des zuständigen Ministeriums für Bildung und Kindertagesförderung des Landes Mecklenburg-Vorpommern scheiterte. Nach mehreren Kontaktaufnahmen wurde dieses über eine beabsichtigte Beanstandung nach § 14 Abs. 3 IFG M-V in Kenntnis gesetzt. Nach einer ausführlichen internen Prüfung beim Ministerium wurden daraufhin viele der noch offenen Anfragen beschieden und Informationszugänge entsprechend gewährt. Dieses traf aber nicht auf alle offenen Vorgänge zu.

Bereits zu Beginn des neuen Berichtszeitraums setzten wir uns erneut mit dem BM MV in Verbindung und vereinbarten einen persönlichen Gesprächstermin mit den zuständigen Mitarbeiter:innen. Im Verlauf dieses Gesprächs kristallisierte sich heraus, dass bezüglich des Umgangs mit Informationszugangsrechten seitens des Ministeriums noch Unklarheiten bestanden.

Neben einer Beratung haben wir den Mitarbeiter:innen des Ministeriums Vorschläge für ein standardisiertes Verfahren unterbreitet, um die zahlreichen Anfragen zukünftig einfacher und fristgerechter bearbeiten zu können. Weiterhin hat der LfDI MV angeregt, die bereits über den Bildungsserver des Landes Mecklenburg-Vorpommern verfügbaren Übungsaufgaben zu erweitern, wenn bei diesen urheberrechtliche Fragen explizit abgeprüft worden sind.

Im Ergebnis führte der Gesprächstermin dazu, dass Vermittlungsersuchen zu Prüfungsaufgaben im Berichtszeitraum schneller und innerhalb der vorgeschriebenen Frist bearbeitet wurden und der LfDI MV merklich seltener von den Antragsteller:innen eingeschaltet werden musste.

3. Der LfDI MV ist bei seiner Aufgabenerfüllung zu unterstützen

Es kommt leider immer noch vor, dass wir in der Ausübung unserer Kontrolltätigkeit nicht die hierfür notwendige Unterstützung durch alle auskunftspflichtigen Stellen erhalten. So mussten wir im Berichtszeitraum in einem Fall beispielweise dreimal eine ausstehende Stellungnahme zu einem nicht gewährten Informationszugang einfordern. Erst die Androhung einer Beanstandung führte letztendlich dazu, dass uns geantwortet und der Informationszugang gewährt wurde. Nach § 14 Abs. 4 IFG M-V sind öffentliche Stellen verpflichtet, den LfDI MV bei der Aufgabenerfüllung zu unterstützen und dabei unter anderem Auskunft zu unseren Fragen sowie Einsicht in alle Unterlagen zu gewähren, die im Zusammenhang mit dem Informationszugang stehen. Das diesem immer noch nicht in jedem Fall Folge geleistet wird, liegt unseres Erachtens nach zum einen daran, dass sich einige auskunftspflichtige Stellen trotz nunmehr 18 Jahren Informationszugangsrecht in M-V mit dem Gedanken der Transparenz schwer tun. Zum anderen sind nicht bei allen Behörden die Zuständigkeiten hinsichtlich der Bearbeitung von Anträgen auf Informationszugang so klar organisiert, dass behördenintern eine bearbeitende Person für die Anträge auf Informationszugang benannt und verantwortlich ist. So erleben wir, dass diese Aufgabe oft dezentral durch die Fachbereiche selbst verantwortet wird. Da diese dann wiederum oft noch keine bzw. wenig Erfahrung mit dem Informationszugangsrecht haben, kommt es mitunter (insbesondere in Bezug auf die fristgerechte Bearbeitung oder der gegenüber dem LfDI MV bestehenden Unterstützungspflicht) zu nicht gesetzeskonformen Handlungen. Allen auskunftspflichtigen Stellen kann daher nur empfohlen werden, auf dem Wege der Einrichtung einer zentralen Stelle mit geschultem Fachpersonal Anträge nach dem IFG M-V oder anderen Zugangsrechten zu bearbeiten.

4. Ein laufendes Klageverfahren kann einem Auskunftsanspruch entgegenstehen

Im hier zu berichtenden Fall begehrte ein Petent Informationen zum Themenbereich des öffentlichen Straßenverkehrs von einer Kommunalverwaltung in Mecklenburg-Vorpommern. Da nach Antragstellung rund 19 Monate ohne Rückmeldung der besagten Verwaltung verstrichen waren, bat der Antragsteller den LfDI MV um Vermittlung.

Gemäß § 11 Absatz 1 IFG M-V ist ein Antrag auf Informationszugang innerhalb eines Monats zu bescheiden. Fristverlängerungen sind in einzelnen Ausnahmesituationen möglich. Außerdem besteht bei den öffentlichen Stellen gegenüber dem LfDI MV gemäß § 14 Absatz 4 IFG M-V eine Mitwirkungspflicht. Da auch auf die Schreiben des LfDI MV lange Zeit keine Rückmeldung erfolgte, wurde eine Beanstandung im Sinne des § 14 Absatz 3 IFG M-V ausgesprochen.

Daraufhin fand schließlich eine Kommunikation mit der Behörde statt, welche uns erläuterte, dass die erbetenen Informationen Gegenstand eines anhängigen Verwaltungsgerichtsverfahrens wären. Insofern war hier der Ablehnungstatbestand nach § 5 Nr. 2 IFG M-V einschlägig.

Wird ein Informationszugang aufgrund § 5 Nr. 2 IFG M-V nicht gewährt, reicht der bloße Verweis auf ein „laufendes Verfahren" nicht aus. Vielmehr muss durch die Bekanntgabe der Information der Verfahrensablauf erheblich beeinträchtigt werden. Diese Erheblichkeit ist im Einzelfall detailliert und nachvollziehbar durch die Behörde zu begründen. Es muss deutlich werden, dass das Verfahren nicht nur unbedeutend behindert oder für geraume Zeit verzögert werden würde. Nach Durchsicht der Unterlagen, insbesondere der Klageschrift, konnte die erhebliche Beeinträchtigung in diesem Fall bejaht werden, sodass der Antrag auf Informationszugang rechtmäßig abgelehnt werden musste.

Unabhängig von dem geschilderten Fall ist bezogen auf die Frage der Zugänglichkeit von etwaigen Gerichtsakten zu beachten, dass sich der Anwendungsbereich nicht auf Gerichte erstreckt, soweit sie als Organe der Rechtspflege oder aufgrund besonderer Rechtsvorschriften in richterlicher Unabhängigkeit tätig werden. Daher schützt dieser Ausnahmetatbestand insoweit nur Informationen anderer Stellen, wie vorliegend etwa die der Ausgangsbehörde.

5. Transparenz setzt eine ordnungsgemäße Aktenführung voraus

Eine Fragstellung, welche dem LfDI MV im Rahmen seiner Vermittlungen in den Berichtsjahren häufiger begegnet ist, ist die nach dem Vorhandensein von Informationen. Ein konkreter Fall handelte bspw. von einem Antrag auf Informationszugang bei einer Amtsverwaltung in Mecklenburg-Vorpommern. Diese Informationen bezogen sich auf Akten aus dem Bereich der öffentlichen Sicherheit und Ordnung. Die beantragten Informationen waren innerhalb der Amtsverwaltung nicht in einer „klassischen Akte" zusammen getragen worden. Die verantwortlichen Mitarbeitenden konnten sich jedoch an den Vorfall erinnern, sodass eine Auskunft dennoch grob erteilt wurde. Diese konnte allerdings nicht wie vom Petenten erwünscht (§ 4 Absatz 1 IFG M-V) in Form einer Aktenkopie erfolgen, da keine schriftlichen Aufzeichnungen vorhanden waren. Ob dies im vorliegenden Fachgebiet essenziell gewesen wäre, entzieht sich dem Kontrollbereich des LfDI MV.

Die Zielstellung des IFG M-V ist zunächst der freie Zugang für Bürger:innen zu bei den Behörden vorhandenen Informationen. Viele Antragsteller:innen nutzen die Möglichkeiten des IFG M-V ebenfalls dazu, einen besseren Einblick in das Arbeiten der öffentlichen Verwaltungen zu erlangen. Dies setzt allerdings immer voraus, dass Behörden sich an den „Grundsatz der ordnungsgemäßen Aktenführung" halten. Dieser ist zwar nicht gesetzlich normiert, stützt sich aber im Wesentlichen auf das Rechtsstaatsprinzip nach Artikel 20 Absatz 3 des Grundgesetzes (GG). Jegliches Verwaltungshandeln aller Verwaltungen unterliegt diesem Grundsatz. Vor allem im Rahmen des IFG M-V spielt das eine bedeutende Rolle. Nur durch Unterlagen, die vollständig, wahrheitsgemäß und nachvollziehbar sind, kann das transparente Arbeiten öffentlicher Verwaltungen gewährleistet und der Zugang zu amtlichen Informationen ermöglicht werden.

Der hier besprochene Antrag auf Informationszugang hat vermutlich letztendlich nicht gänzlich zum Erfolg geführt. Trotzdem konnte zumindest die Amtsverwaltung auf eventuelle Missstände hinsichtlich ihrer Dokumentation aufmerksam gemacht werden. Auch das kann im Rahmen des IFG M-V aufgedeckt und als Erfolg verbucht werden. Im Sinne der Transparenz sollten daher alle Behörden stets den Grundsatz der ordnungsgemäßen Aktenführung umsetzen und alle entscheidungsrelevanten Informationen und Unterlagen eines Sachverhalts in einer Akte zusammentragen. Dabei ist es irrelevant, ob eine Verwaltung noch papierbasiert oder schon mit der elektronischen Akte arbeitet.

6. Die Angabe einer Adresse ist nicht immer erforderlich

Anträge auf Informationszugang nach dem IFG M-V müssen gemäß § 11 Abs. 1 IFG M-V beschieden werden. Viele Behörden gehen dabei davon aus, dass die Bescheidung zwingend über den Postweg erfolgen muss. Für diese Art der Bescheidung wäre in diesem Zusammenhang die Mitteilung der vollständigen Adresse der Antragssteller:innen notwendig. Weder aus den Vorschriften des IFG M-V noch aus den allgemeinen Verwaltungsverfahrensvorschriften ergibt sich die generelle Pflicht, bei Antragstellung die eigene Postanschrift anzugeben. Das IFG M-V sieht lediglich bei Entscheidungen mit Drittbeteiligungen eine Schriftform vor (vgl. § 9 Abs. 1 IFG M-V). Ebenso ist bei ablehnenden Entscheidungen eine schriftliche, postalische Zustellung und damit auch die Erfassung einer Anschrift verständlich, um ggf. ein anschließendes Widerspruchs- oder Klageverfahren rechtssicher durchführen zu können. Selbiges gilt bei Bescheiden und Auskünften, die mit Gebühren und/oder Auslagen verknüpft sind.

Handelt es sich jedoch um eine stattgebende Entscheidung und die Auskunft wird erteilt, steht der Übermittlung auf elektronischem Weg, sofern von der Antragsteller:in gewünscht, nichts entgegen.

Ein Verwaltungsakt kann gemäß § 37 Absatz 2 Satz 1 Verwaltungsverfahrensgesetz Mecklenburg-Vorpommern (VwVfG M-V) grundsätzlich auch elektronisch erlassen werden. Lediglich, wenn für einen Verwaltungsakt, für welchen durch Rechtsvorschrift die Schriftform angeordnet ist, die elektronische Form verwendet wird, muss dieser gemäß § 37 Absatz 3 Satz 2 VwVfG M-V eine qualifizierte elektronische Signatur enthalten.

Die Erhebung der Postanschrift ist in diesen Fällen demnach nicht erforderlich. Diese umfassende Problematik begegnet dem LfDI MV hauptsächlich bei Anfragen über die Plattform „FragDenStaat“, da die Antragstellenden hier oftmals die Kommunikation via Mail wünschen. Da stattgebende Bescheide in aller Regel sowieso nicht förmlich zugestellt werden, sieht der LfDI MV keine Komplikationen bei der Kommunikation und Übermittlung via E-Mail.

7. Das Schriftformerfordernis verlangt eine eigenhändige Unterschrift

Im Berichtsjahr 2022 und 2023 erreichten uns auffallend viele Vermittlungsanträge, bei welchen das Schriftformerfordernis des IFG M-V, insbesondere bei Anfragen über die Plattform „FragDenStaat", eine zentrale Rolle spielte.

Gemäß § 10 Absatz 1 Satz 2 IFG M-V ist ein Antrag auf Informationszugang schriftlich oder zur Niederschrift an die Behörde zu richten, bei der die begehrten Informationen vorhanden sind. Die Schriftform allgemein ist geregelt in § 126 BGB. Dabei besagt Absatz 1, dass sobald durch ein Gesetz eine schriftliche Form vorgeschrieben ist, die Urkunde (hier: der Antrag) von dem Aussteller eigenhändig durch Namensunterschrift zu versehen ist.

Die Eigenhändigkeit ist nur dann gewährleistet, wenn die Unterschrift von der antragstellenden Person selbst erbracht wird. Dadurch wird jede Form der mechanischen Vervielfältigung etwa durch Stempelaufdruck oder durch datenmäßige Vervielfältigung durch Computereinblendung ausgeschlossen (vgl. OLG Düsseldorf BeckRS 2018, 24411).

Oft nutzten Interessierte die Plattform „FragDenStaat" für ihre Anträge auf Informationszugang. Auf dieser ist es üblich, die eigene Unterschrift einmalig im Konto zu hinterlegen. Bei Anträgen an Behörden innerhalb Mecklenburg-Vorpommern wird dann die zuvor gespeicherte Unterschrift jeweils automatisch auf die Anträge gedruckt. Diese Anträge werden via Mail und parallel via Fax an die betroffene Behörde übermittelt.

Somit handelt es sich jedes Mal um eine Reproduktion der Unterschrift. Die Eigenhändigkeit ist damit nicht gewährleistet. Infolgedessen ist auch die im IFG M-V geforderte Schriftform nicht erfüllt.

Im Sinne der Transparenz sollte es Behörden dennoch, auch bei Nichtwahrung des Schriftformerfordernisses, möglich sein, einfache Auskünfte formlos zu erteilen. Zumindest dann, wenn es sich um unkritische Daten handelt.

Unserer Auffassung nach ist das im IFG M-V verankerte Schriftformerfordernis antiquiert und sollte dringend den zeitlichen Ansprüchen entsprechend angepasst werden.

Wir empfehlen der Landesregierung daher, schnellstmöglich die elektronische Antragstellung zuzulassen. Dieses würde sowohl das Antragsverfahren vereinfachen als auch die Transparenz der öffentlichen Verwaltung weiter stärken.

8. Protokolle nicht-öffentlicher Sitzungen sind nicht automatisch vertraulich

Ein ortsansässiger Bürger verlangte Unterlagen zum Verkauf eines Fußballplatzes. Das dafür zuständige Amt lehnte den Antrag ab und begründetet dies damit, dass der Beschluss über den Verkauf in einer nicht-öffentlichen Sitzung gefasst wurde. Weiterhin wurde dem Antragsteller mitgeteilt, dass der Beschluss, das Gutachten sowie der Kaufvertrag aus datenschutzrechtlichen Gründen nicht herausgegeben werden können.

Obwohl die Beantragung auf Herausgabe der Informationen explizit auf das IFG M-V gestützt wurde, nahm das Amt in seiner Ablehnung keinerlei Bezug auf dieses. Auch der Hinweis des Antragstellers, schützenswerte Daten vor der Herausgabe zu schwärzen, wurde seitens des Amtes ignoriert.

Der LfDI MV wandte sich an die zuständige Behörde und informierte diese zunächst darüber, dass ein Antrag nach §11 IFG M-V ordnungsgemäß zu bescheiden ist.

Weiterhin setzten wir das Amt darüber in Kenntnis, dass in einem ablehnenden Bescheid dem Antragsteller die möglichen Ablehnungsgründe der §§ 5 bis 8 IFG M-V mitgeteilt und dargelegt werden müssen. Der Verweis auf den Datenschutz ohne Benennung der entsprechenden Rechtsgrundlage und Begründung der Ablehnung reicht nicht aus.

Aufgrund unserer Hinweise erfolgte innerhalb kürzester Zeit die Bescheidung des Antrages. Der Zugang zu den gewünschten Informationen wurde aber weiterhin abgelehnt. Dieses begründetet das Amt u. a. damit, dass Protokolle zu vertraulichen Beratungen wie der nicht-öffentliche Teil einer Gemeindevertretersitzung gemäß § 6 Abs. 3 IFG M-V geschützt sind.

Der Antragsteller wandte sich erneut an uns und bat um Informationen zu den weiteren Möglichkeiten zur Zugänglichmachung der von ihm begehrten Informationen. Daraufhin haben wir sowohl den Petenten auf den Verwaltungsrechtsweg und die damit bestehende Möglichkeit des Widerspruchs hingewiesen als auch der betreffenden Verwaltung unsere rechtliche Bewertung mitgeteilt.

Hiernach sind nach § 6 Abs. 3 IFG M-V Protokolle vertraulicher Beratungen zwar vom Informationszugang ausgenommen, wobei hier aber die Vertraulichkeit gesehen auf den in Frage stehenden Sachverhalt zu prüfen ist. Nicht-öffentliche Beratungen wie z. B. Sitzungen der Gemeindevertretung sind nicht per se vertraulich. Der Ausschluss der Öffentlichkeit von Sitzungen der Gemeindevertretung dient dem Ziel, eine objektive und unbeeinflussbare Amtsausübung durch die Gewährleistung einer offenen Aussprache und des Schutzes von Persönlichkeitsrechten zu ermöglichen.

Die bloße Bezeichnung eines Protokolls als „vertraulich" oder eine entsprechende Vereinbarung unter den Teilnehmenden reicht zur Begründung einer Zugangsverweigerung nicht aus. Es braucht vielmehr einen Zusammenhang mit den vorgenannten Punkten, die eine Vertraulichkeit und damit die Geheimhaltung rechtfertigen würden. Darüber hinaus wäre auch zu prüfen gewesen, ob neben etwaigen vertraulichen auch offenbarungswürdige Informationen in den gewünschten Unterlagen vorhanden sind, die zumindest einen Teilzugang im Sinne des § 11 Abs. 3 IFG M-V gerechtfertigt hätten.

Nach der getroffenen Darlegung der Sach- und Rechtslage verzichtete der betr. Antragsteller auf ein weiteres Vorgehen unserer Behörde. Uns ist daher nicht bekannt, ob in diesem Fall der gewünschte Informationszugang erfolgt ist.

9. Die Geschäftsordnung einer Gemeindevertretung steht einem Anspruch auf Informationszugang nicht entgegen

Eine Gemeinde wurde unter Bezugnahme auf das IFG M-V um die Herausgabe der Niederschrift einer Gemeindevertretersitzung gebeten. Unter Hinweis auf die für die betreffende Gemeindevertretung geltende Geschäftsordnung wurde lediglich eine Einsichtnahme, aber nicht die Herausgabe der begehrten Sitzungsniederschrift in Aussicht gestellt.

Wir haben der Gemeinde über den voraussetzungslosen Rechtsanspruch auf die Herausgabe von Informationen nach dem IFG M-V und den einzuhaltenden Grundsatz des Gesetzesvorranges hingewiesen. Nach diesem Grundsatz (Art. 20 Abs. 3 GG) und des damit verbundenen Vorrangprinzips dürfen bspw. durch Regelungen der für eine Gemeindevertretung geltenden Geschäftsordnung nicht gesetzlich normierte Ansprüche ausgehebelt werden. Insofern wäre der Antrag auf Herausgabe von Informationen, der sich im vorliegenden Fall explizit auf das IFG M-V bezog, nach den betreffenden gesetzlichen Normen des IFG M-V zu behandeln gewesen. Gemäß § 4 Abs. 3 Satz 3 IFG M-V besteht darüber hinaus auch ein Herausgabeanspruch von Kopien.

Des Weiteren wiesen wir darauf hin, dass die Herausgabe des Protokolls über den öffentlichen Teil der Gemeindevertretersitzung bezüglich der Frage möglicher geheimhaltungswürdiger Informationen aus unserer Sicht unproblematisch sein dürfte. Sofern es um die Herausgabe der Niederschrift für den nicht-öffentlichen Teil geht, wären die Bestimmungen des § 6 Abs. 3 i.V.m. Abs. 5 sowie des § 11 Abs. 3 IFG M-V zu beachten.

Auf unseren Hinweis hin erließ die auskunftspflichtige Stelle einen Abhilfebescheid und übersandte eine Kopie des in Frage stehenden Sitzungsprotokolls.

10. Ablehnung des Informationszugangs kann rechtmäßig sein

Hin und wieder kommt es vor, dass der LfDI MV um Vermittlung gebeten wird, wir uns nach Prüfung des Sachverhaltes aber nicht an die angefragte Behörde wenden, sondern den Antragsteller:innen mitteilen, dass die ergangenen Bescheide rechtmäßig sind.

In einem dieser Fälle begehrte ein Petent die für eine Gemeinde erstellten Brandschutzbedarfspläne. Die Herausgabe wurde abgelehnt, da die Pläne von der Gemeindevertretung noch nicht verabschiedet worden waren und sich noch im Entwurfsstadium befanden.

Der Antragsteller konnte die Begründung nicht nachvollziehen, da nach seiner Auffassung die Brandschutzbedarfspläne von Fachkundigen erstellt werden und von den Gemeinden nicht geändert werden können.

Von der angefragten Behörde wurde dem Antragsteller sehr ausführlich dargelegt, dass Brandschutzbedarfspläne von der Feuerwehr sowie der Verwaltung erstellt werden. Das Verfahren gemäß Brandschutz- und Hilfeleistungsgesetz M-V wurde ihm ebenfalls ausführlich erläutert. Es wurde weiterhin aufgezeigt, dass die Ablehnung sich auf § 6 Abs. 6 IFG M-V stützt und eine Veröffentlichung des Entwurfs der Brandschutzbedarfsplanung die rechtsstaatliche Durchführung des durch Verwaltungsvorschrift vorgegebenen Verwaltungsverfahrens erheblich beeinträchtigt und damit die kommunale Entscheidung gefährden würde.

Wir haben dem Antragsteller erörtert, dass wir die Ablehnung der Einsichtnahme als rechtmäßig erachten und bezüglich des Ablehnungsbescheids nicht vermittelnd tätig werden können.

11. Bei einem Drittbeteiligungsverfahren kann sich der Informationszugang verzögern

In einem weiteren Fall begehrte eine Umweltinitiative von einer größeren Stadt Informationen zu den mit den ansässigen Landwirt:innen geschlossenen Pachtverträgen.

Zunächst erhielt die Antragstellerin nach Ablauf von einem Monat nur eine schriftliche Eingangsbestätigung. Wochen später wurde die Antragstellerin aufgrund einer telefonischen Nachfrage darüber in Kenntnis gesetzt, dass den Pächter:innen im Rahmen eines Drittbeteiligungsverfahrens eine Frist zur Anhörung gegeben wurde. Nach einem weiteren Monat erhielt die Umweltinitiative telefonisch die Information, dass sich die Bearbeitung weiterhin verzögern würde, da einige Pächter:innen ihre Geschäftsgeheimisse nicht gewahrt sehen.

Nach einem Zeitraum von insgesamt fünf Monaten ab Antragstellung lagen somit weder die gewünschten Informationen noch ein Bescheid vor. Aus diesem Grund wandte sich ein Mitglied der Umweltinitiative an uns und bat um Vermittlung.

Zunächst haben wir die zuständige Stadt auf die Einhaltung der gesetzlichen Fristen nach § 11 IFG M-V hingewiesen. Nach dieser Vorschrift ist die Antragstellerin, wenn die Verlängerung aufgrund der Beteiligung von Dritten oder aufgrund Umfang oder Komplexität der begehrten Informationen als notwendig erachtet ist, über die Abweichung von der Standard-Frist schriftlich zu informieren.

Weiterhin haben wir um eine unverzügliche Bescheidung des Antrages gebeten und dabei auf § 10 Abs. 5 IFG M-V hingewiesen. Danach besteht Anspruch auf Zugang zu den übrigen Informationen, sollten Ausschlussgründe gegen eine vollumfängliche Herausgabe der gewünschten Information vorliegen. Dieses kann beispielsweise in Form von Schwärzung der schutzwürdigen Daten erfolgen.

Als Reaktion auf unser Stellungnahmeersuchen legte die Stadt dar, dass ein teilweiser Anspruch auf Herausgabe der Vertragskopien festgestellt wurde. In allen Pachtverträgen sollen Inhalte, die sich auf mögliche Betriebs- oder Geschäftsgeheimnisse beziehen, sowie in einem Fall die personenbezogenen Daten der Unterpächter:innen geschwärzt werden. Ein entsprechender Bescheid - zunächst ohne Herausgabe der gewünschten Informationen - wurde an die antragstellende Person verschickt.

Diese wandte sich erneut an uns und war mit der weiteren Verzögerung nicht einverstanden. Wir erläuterten ihr deshalb ausführlich das Drittbeteiligungsverfahren nach dem IFG M-V.

Die Stellungnahmen der betroffenen Dritten zu möglicherweise vorliegenden Betriebs- oder Geschäftsgeheimnissen sind zunächst von der Stadtverwaltung zu prüfen. Diese können bei der Entscheidung über die Herausgabe der Pachtverträge berücksichtigt werden, letztendlich entscheidet die auskunftspflichtige Stelle aber selbst. Da die Entscheidung der Behörde vom Willen der Pächter:innen abweichen kann, müssen die Pächter:innen nach § 9 Abs. 2 IFG M-V vorab über die getroffene Entscheidung informiert werden.

Natürlich könnte es sein, dass einer der Pächter:innen bereits in der Stellungnahme die Herausgabe des Pachtvertrages unterbinden wollte und nun Widerspruch gegen die Entscheidung der Stadt einlegt. Das würde zu Verzögerungen führen, die sicherlich ärgerlich sind. Das IFG M-V ermöglicht sowohl die Herausgabe von amtlichen Informationen als auch den Schutz geheimhaltungswürdiger Interessen Dritter.

Sollte es zu keinem Widerspruch kommen, steht der Herausgabe der Informationen nichts mehr im Wege. Wir haben die antragstellende Person deshalb um Geduld bis zum Verstreichen der Widerspruchsfrist gebeten.

Schlussendlich wurde von keinem der Pächter:innen Widerspruch gegen den Bescheid eingelegt, so dass die Umweltinitiative die gewünschten Informationen erhalten konnte.

12. Strenge Voraussetzungen beim Zugang zu personenbezogenen Daten

Im Rahmen einer von einer Baugenehmigungsbehörde nach §§ 7 und 9 IFG M-V durchgeführten Drittbeteiligung wurde durch den Dritten keine Einwilligung zum Zugang zu personenbezogenen Daten gegeben. Trotzdem entschied die Behörde, den Zugang zu diesen Informationen zu gewähren und berief sich dabei auf § 7 Nr. 5 IFG M-V. Nach dieser Vorschrift ist der Zugang zu personenbezogenen Daten möglich, wenn seitens der antragstellenden Person ein rechtliches Interesse an der Kenntnis der begehrten Information geltend gemacht wurde und überwiegende schutzwürdige Belange der/des Betroffenen der Offenbarung nicht entgegenstehen.

Ein rechtliches Interesse liegt vor, wenn mit dem Antrag auf Informationszugang ein Anspruch verfolgt wird, der sich aus einer konkreten Rechtsbeziehung zur betroffenen Person ergibt bzw. ergeben kann. Dies kann beispielsweise eine vertragliche Vereinbarung sein. Außerdem wäre ein rechtliches Interesse dann gegeben, wenn der Informationszugang möglicherweise größere Klarheit über den Sach- und Streitstand vermittelt und aus Sicht eines verständigen Betrachters die weitere Rechtsverfolgung oder -verteidigung erleichtert wird. Ein „rechtliches Interesse“ ist aber klar von einem „berechtigten Interesse“ abzugrenzen. Konkret wurde sich in diesem Fall nur auf ein berechtigtes, nicht auf das gesetzlich vorgeschriebene rechtliche Interesse, berufen.

Hinzu kam weiterhin, dass vorliegend offensichtlich die Herausgabe sog. Hinweisgeberdaten begehrt wurde. Dabei ist zu beachten, dass die Identität von Hinweisgeber:innen und Informant:innen grundsätzlich vertraulich zu behandeln ist. Eine Herausgabe kann unter anderem (und so auch Intention des § 7 Nr. 5 IFG M-V) dann erfolgen, wenn sich die Hinweise beispielsweise als falsche Anschuldigungen, erweisen, denen mit erheblicher Wahrscheinlichkeit eine Beleidigungs- oder Schädigungsabsicht der hinweisgebenden Person zugrunde liegt. Ein solches Indiz lag hier jedoch nicht vor.

Da neben der Anrufung unserer Behörde im betreffenden Fall auch durch den Betroffenen Widerspruch gegen die avisierte Offenlegung der personenbezogenen Daten erhoben wurde und die auskunftspflichtige Stelle unseren Empfehlungen auf Geheimhaltung der Daten gefolgt ist, konnte eine rechtswidrige Offenbarung verhindert werden.

Teil C

Ergänzungen

1. Empfehlungen | Zusammenfassung

Wir sprechen die folgenden bereichsspezifischen Empfehlungen aus:

Technik und Organisation

Thema: Einsatz von Künstlicher Intelligenz

Wir empfehlen der Landesregierung, bereits bei den Planungen zum **Einsatz von KI-Systemen** die damit verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen sorgfältig zu analysieren und die **Risiken beim Betrieb** derartiger Systeme durch technische und organisatorische Maßnahmen auf ein verantwortbares Maß zu reduzieren. Gleichzeitig empfehlen wir der Landesregierung, in einer **IT-Strategie darzulegen**, wie der zukünftige **Einsatz von KI in der Landesregierung** ausgestaltet sein sollte. Hierzu bedarf es mit Blick auf den Einsatz und das **Training von KI-Modellen** auch flankierender rechtlicher Rahmenbedingungen, in denen auch geregelt wird, wo die **Grenzen einer Nutzung** liegen.

Thema: Cybersicherheit

Wir empfehlen der Landesregierung, sich weiterhin für eine **Stärkung der IT-Sicherheit** einzusetzen und vorhandene Strukturen und Unterstützungsleistungen auszuweiten, insbesondere mit Blick auf den **kommunalen Raum**. Zudem empfehlen wir eine Stärkung des **CERT MV** sowie dessen Befugnissen.

Thema: Sicherheit bei der Übertragung von E-Mails beim LfDI MV

Wir empfehlen der Landesregierung, die eigenen Maßnahmen **zum Schutz personenbezogener Daten** bei der Übermittlung per E-Mail zu prüfen und die angesprochenen Techniken ebenfalls zu implementieren.

Thema: Einsatz von Videokonferenzsystemen

Wir empfehlen der Landesregierung, dass derzeitig eingesetzte Videokonferenzsysteme schnellstmöglich **gegen eine datenschutzkonforme Lösung** auf Basis von Open-Source zu ersetzen.

Thema: Auftragsdatenverarbeitung und Digitalisierung im Bereich Schule

Wir empfehlen der Landesregierung, hinreichend zu prüfen, ob im Zuge der zentralen Beschaffung und Bereitstellung von digitalen Lösungen eine **Neuausrichtung der datenschutzrechtlichen Verantwortung von Schulleitungen** hin zu zentraler datenschutzrechtlicher Verantwortlichkeit denkbar ist.

Thema: Integriertes Schulmanagementsystem ISY MV

Wir empfehlen dem Ministerium für Bildung und Kindertagesförderung des Landes Mecklenburg-Vorpommern, den Austausch mit unserer Behörde zum Projekt ISY MV **weiter fortzuführen**.

Thema: Arbeitsgruppe Microsoft- Onlinedienste

Vor dem Hintergrund der Festlegung der **DSK** empfehlen wir allen Verantwortlichen in Mecklenburg-Vorpommern aus dem öffentlichen sowie aus dem nicht-öffentlichen Bereich, die bereits Onlinedienste von Microsoft (z. B. Microsoft 365 mit Word, Excel, PowerPoint) im Rahmen der Auftragsverarbeitung einsetzen oder deren Einsatz planen, zu prüfen, ob sie in der Lage sind, diese Produkte **datenschutzgerecht** einzusetzen. Prüfmaßstab ist aus aufsichtsbehördlicher Sicht die **Festlegung der 104. DSK zu Microsoft 365** und der Abschlussbericht der Arbeitsgruppe. Insbesondere mit Blick auf die **digitale Souveränität** empfehlen wir den Verantwortlichen, den Einsatz alternativer Produkte zu prüfen, vorwiegend aus dem Open Source Bereich.

Thema: Orientierungshilfe für Anbietende von Telemedien

Wir empfehlen den Anbietenden von Telemedien aus dem öffentlichen und nicht-öffentlichen Bereich, sich mit der neuen Version der **Orientierungshilfe für Anbietende von Telemedien** vertraut zu machen und ihre Telemediendienste auf Datenschutzkonformität sowie bezüglich des Einsatzes von **Cookies** nach dem TTDSG zu prüfen. Darauf aufbauend sollte geprüft werden, 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.

Datenschutz und Bildung

Thema: Medienguides MV – Eltern.Medien.Kompetent

Wir empfehlen der Landesregierung dringend, (außerschulische) Projekte der Medienbildung, die sich konkret an **Eltern und Familien** richten, stärker in den Fokus der bildungspolitischen Agenda zu nehmen. Die Vermittlung von Medienkompetenz und Medienerziehung kann nicht allein von Akteur:innen des Bildungssystems geleistet werden und muss in der **Familie** beginnen. Im Sinne der Erziehungs- und Bildungspartnerschaft zwischen Bildungseinrichtungen und Eltern muss es **mehr Angebote** für Eltern und Familien geben, um Medienkompetenz zu erlangen und so besser und vor allem gemeinsam auf die lebensweltlichen Anforderungen der Kinder und Jugendlichen reagieren zu können.

Thema: TEO – Tage ethischer Orientierung: protect privacy – Mein Klick, meine Verantwortung

Wir empfehlen der Landesregierung den Austausch mit unserer Behörde sowie mit der Nordkirche bezüglich der TEO-Projekte, deren **zukünftige Weiterführung** aufgrund auslaufender Fördermöglichkeiten über den Europäischen Sozialfond (ESF) unklar ist. Einen möglichen **Wegfall** des Formates TEO PP sehen wir **äußerst kritisch**, da es kein vergleichbares Bildungsangebot zur ethischen/politischen Orientierung für Kinder und Jugendliche dieser Altersgruppe im Land gibt. Bei gleichzeitiger Reduzierung dieser nicht fest in den Lehrplänen verankerten Themen zur Medienkompetenz befürchten wir eine starke Beeinträchtigung der **ethischen/politischen Bildung junger Menschen** in unserem Land.

Thema: Qualifizierungskurs „Spielen, Zappen, Klicken" – Medienerziehung in Kita und Familie

Aufgrund der unsicheren Finanzierung der modularen Fortbildungsreihe „Spielen, Zappen, Klicken" durch den vdek e.V. fordert unsere Behörde seit Beginn des Weiterbildungsangebotes für pädagogische Fachkräfte in 2016 eine Verstetigung dessen **Finanzierung auf Landesebene**. Wir empfehlen der Landesregierung deshalb dringend, die Etablierung dieses Weiterbildungsangebotes zu prüfen und die Durchführung dauerhaft der LAKOST zu übertragen.

Thema: EU-Projekt #Digitale Vorbilder – Familien gehen online.

Wir raten der Landesregierung dringend an, **eine Weiterführung** des Projektes *#Digitale Vorbilder – Familien gehen online.* beim LfDI MV durch die Bereitstellung von Ressourcen zu unterstützen, damit ein niedrigschwelliger Zugang zu umfassenden Themen der **Medienerziehung für Familien** in Mecklenburg-Vorpommern weiterhin möglich ist. Der LfDI MV steht der Landesregierung jederzeit zur Verfügung, um inhaltlich und strategisch über die Projektergebnisse und deren **weitere Verwendungsmöglichkeiten** zu beraten, so dass auch weiterhin eine größtmögliche Zahl interessierter Familien in M-V vom gesammelten Expert:innenwissen profitieren können.

Thema: Medienaktiv M-V

Wir fordern die Landesregierung das zu auf, den LfDI MV mit den Kooperationspartnern soweit **zu unterstützen**, dass eine **flächendeckende Vernetzung** der Akteur:innen der Medienbildung **verbindlich umgesetzt** werden kann.

Beschäftigtendatenschutz

Thema: EuGH-Urteil vom 30. März 2023 Rs. C-34/21 zu den Anforderungen an gesetzliche Regelungen zum Beschäftigtendatenschutz

Wir empfehlen daher auch der Landesregierung, die bestehenden Regelungen **zur Verarbeitung von Beschäftigtendaten** im Landesdatenschutzgesetz und im Landesbeamtengesetz zu prüfen.

Behörden, Gesundheit und Soziales

Thema: Stellung und Aufgaben der behördlichen Datenschutzbeauftragten

Wir appellieren an alle öffentlichen Stellen sowohl auf Kommunal- als auch Landesebene – aber auch Verantwortliche darüber hinaus – den (b)DSBs im Einklang Art. 38 Abs. 2 DS-GVO die erforderlichen Ressourcen, insbesondere entsprechende **Zeitkontingente**, für die **Aufgabenerfüllung** zur Verfügung zu stellen, die (b)DSBs in alle mit dem Schutz personenbezogener Daten zusammenhängenden Frage einzubinden und die (b)DSBs bei der **Erfüllung ihrer Aufgaben** zu unterstützen.

Informationsfreiheit – IFG M-V

Thema: Bedeutung, Zahlen und Fakten

Wir bekräftigen daher die bereits im letzten Tätigkeitsbericht ausgesprochene Empfehlung, auch für Mecklenburg-Vorpommern ein **Transparenzgesetz** mit klar festgelegten und in einem Transparenzregister zu regelnden Veröffentlichungspflichten zu schaffen.

Thema: Schriftformerfordernis verlangt eigenhändige Unterschrift

Wir empfehlen der Landesregierung daher, schnellstmöglich die **elektronische Antragstellung** zuzulassen. Dieses würde sowohl das Antragsverfahren vereinfachen als auch die Transparenz der öffentlichen Verwaltung weiter stärken.

2. Abkürzungsverzeichnis

Das Abkürzungsverzeichnis wird alphabetisch geführt.

AEUV	Vertrages über die Arbeitsweise der Europäischen Union
AG	Arbeitsgruppe
AK Technik	Arbeitskreis „Technische und organisatorische Datenschutzfragen“
Art.	Artikel
bDSB	behördliche Datenschutzbeauftragte
BDSG	Das Bundesdatenschutzgesetz
BfDI	Der Bundesbeauftragte für Datenschutz und Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BIKO MV	Bildungskonzeption der 0 bis10 Jährigen in Mecklenburg-Vorpommern
BKAG	Bundeskriminalamtgesetz
BM MV	Ministerium für Bildung und Kindertagesförderung des Landes Mecklenburg-Vorpommern
BSI	Bundesamtes für Sicherheit in der Informationstechnik
BtMG	Betäubungsmittelgesetz
BUND MV	Bund für Umwelt und Naturschutz Mecklenburg-Vorpommern
BVerfG	Bundesverfassungsgericht
CDN	Content Delivery Networks
CERV-2021-DATA	EU-Programm “Citizens, Equality, Rights and Values-2021-DATA”
CERT MV	Computer Emergency Response Team Mecklenburg-Vorpommern
CNIL	Commission Nationale de l’Informatique et des Libertés
CSG	ComputerSpielSchule Greifswald (Projekt des Medienzentrums Greifswald e.V.)
D.E.A.P.	Data, Education, Awarness, Protection
DIZ	Digitales Innovationszentrum Schwerin
DKIM	DomainKeys Identified Mail
DMARC	Domain-based Message Authentication, Reporting, and Conformance
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DPA	Data Protection Addendum
DSFA	Datenschutz-Folgenabschätzung
DSG M-V	Landesdatenschutzgesetz Mecklenburg-Vorpommern
DS-GVO	Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
DVZ	Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH
EDSA	Europäischer Datenschutzausschuss
eGo MV	Zweckverband elektronische Verwaltung Mecklenburg-Vorpommern
ESF	Europäischer Sozialfond
ESG	Expert Subgroup

EU	Europäische Union
EuGH	Europäischer Gerichtshof
EVA	elektronischen Vorgangsassistent der Polizei
gem.	gemäß
GGO II	Gemeinsamen Geschäftsordnung II
GRCh	Charta der Grundrechte der Europäischen Union
HBG	Hessisches Beamtengesetz
HDSIG	Hessisches Datenschutz- und Informationsfreiheitsgesetz
IBAN	International Bank Account Number/Kontoverbindung
IMI	Binnenmarktinformationssystem, Englisch: Internal Market Information System
IFG	Informationsfreiheitsgesetz
IfSG	Infektionsschutzgesetz
IQ MV	Institut für Qualitätsentwicklung Mecklenburg-Vorpommern
ISY MV	Integriertes Schulmanagementsystem Mecklenburg-Vorpommern
JI-RL	Richtlinie für Justiz und Inneres
KI	Künstliche Intelligenz
KiFöG M-V	Kindertagsförderungsgesetz Mecklenburg-Vorpommern
KMK	Kultusministerkonferenz
KV M-V	Kommunalverfassung für das Land Mecklenburg-Vorpommern
LAKOST MV	Landeskoordinierungsstelle für Suchtthemen Mecklenburg-Vorpommern
LBG M-V	Landesbeamtengesetzes Mecklenburg-Vorpommern
LfDI MV	Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern
LfDI RLP	Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz
LHO MV	Landeshaushaltsordnung Mecklenburg-Vorpommern
LJR MV	Landesjugendring Mecklenburg-Vorpommern e.V.
LKA M-V	Landeskriminalamt Mecklenburg-Vorpommern
LLM	Large Language Models
LVerfSchG M-V	Landesverfassungsschutzgesetz M-V
LWaldG	Landeswaldgesetz Mecklenburg-Vorpommern
MII	Medizininformatik-Initiative
MMV	Landesmedienanstalt Mecklenburg-Vorpommern
MTA-STS	Mail Transfer Agent Strict Transport Security
NIPT	nicht-invasiver Pränataltest
OVG	Oberverwaltungsgericht
OST	Online Services Terms
PGP	Pretty Good Privacy
SDM	Standard-Datenschutzmodell
SGB	Sozialgesetzbuch
SOG M-V	Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommern
StGB	Strafgesetzbuch

StPO	Strafprozessordnung
SÜG M-V	Sicherheitsüberprüfungsgesetz M-V
TEO – PP	Tage ethischer Orientierung – protect privacy
TIDE	Bürger:innensender und Ausbildungskanal TIDE
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
VG	Verwaltungsgericht
VwVfG M-V	Verwaltungsverfahrensgesetz Mecklenburg-Vorpommern
WKM MV	Wissenschaft, Kultur, Bundes- und Europaangelegenheiten Mecklenburg-Vorpommern
ZDMV	Landesamt Zentrum für Digitalisierung Mecklenburg-Vorpommern
ZDMVG	Gesetz zur Errichtung des Landesamtes Zentrum für Digitalisierung Mecklenburg-Vorpommern

3. Stichwortverzeichnis

Symbole

§ 25 TTDSG 28

#Digitale Vorbilder 38

„Spielen, Zappen, Klicken" 35

A

Abitur-Aufgaben 99

Adresse 102

AK Technik 13

Aktenkopie 101

Angemessenheitsbeschluss 46

Anonymisierung 13

Anschrift 102

App 13

Art. 57 Abs. 1 lit. b) 40

Artikel 57 Abs. 1 lit. b DS-GVO 30

Auftragsverarbeitung 24

Auskunft 74, 76

Auskunftsrecht 44, 74, 76

B

Baugutachten 91

Beanstandung 100

behördliche Datenschutzbeauftragte 66

Beschäftigtendatenschutz 49, 50, 51

Betriebs- oder Geschäftsgeheimnisse 107

Bildungskonzeption der 0-10 Jährigen in MV 35

Bildungskonzeption für 0-10 Jährige in Mecklenburg-Vorpommern 35

Bildungsserver 99

Biometrie 15

BSI 17, 20

Bundesamt für Sicherheit in der Informationstechnik 14

Bundesverfassungsgericht 72

Bußgeld 54

Bußgelder 79, 92

C

Callcenter 49

CERT MV 18

CERV-2021-DATA 38

China 44
Cloud 14
Clouddienst 27
Content Delivery Network 14
Cyberkriminalität 17

D

Dashcams 86
Dataport 24
Datenpanne 13, 17
Datenschutzbeauftragte 66
Datenschutzbewusstsein 39
Datenschutz-Folgenabschätzung 20
Datenschutzkonferenz 13
Datenschutzkonferenz des Bundes und der Länder 36
Datenschutzthemen 40
Datenschutz und Schule 24, 26
digitale Signaturen 21
digitale Souveränität 19, 23, 27
Digitalpakt Schule 25
Dokumentation 102
Double-Opt-In-Verfahren 29
Drittbeteiligung 108
Drittbeteiligungsverfahren 98, 106
Dritte 63
Drittland 46
Drittlandsübermittlung 45

E

eGo MV 26
E-Learning 26
eingriffsintensive Maßnahmen 72
eingriffsintensive Maßnahmen der Polizei 95
elektronische Antragstellung 103
E-Mail 13, 21, 60, 81
Empfehlung 99
Ende-zu-Ende Verschlüsselung 21
Entwurfsstadium 106
Erwägungsgrund 53
Erwägungsgrund 132 30
EU-Projekt 40
Europäischer Datenschutzausschuss 43, 47

Europäische Zusammenarbeit 42, 43
EU-US Data Privacy Framework 46
Expert Subgroups 43, 47
exzessiv 63, 90

F

Familien 38
Festlegung der DSK 27
Fördermittelverfahren 64
Forschung 46
FragDenStaat 98, 99, 102, 103
freiwilligen gegenseitigen Amtshilfe 15

G

Gefahrenabwehr 58, 72, 95
Gemeindevertretersitzung 105
Gemeindevertretung 59, 106
Gemeindevertretungen 60, 94
Gericht 82
Geschäftsordnung 105
Gesetzesvorrang 105
Gesichtserkennung 14
Gesundheitsanwendung 14
Gesundheitsdaten 44
Grenzüberschreitende Fälle 43, 47

H

Hauptsitz 50
Hinweisgeberdaten 108

I

Integriertes Schulmanagementsystem ISY MV 24, 26
IMI (Internal Market Information System) 42, 47
Informationsfreiheit 98
Interessenkonflikt 67
IT-Grundschutz 20
IT-Sicherheit 17

J

Jugendamt 63
Jugendportal 36

K

Kennzeichenerfassung 85
Kernbereich privater Lebensgestaltung 95
Kinder 38

Kindertagsförderungsgesetz MV 35
Kleingartenverein 88
Klingelkameras 53
Koalitionsvertrag 99
Kommunalverwaltung 100
Kommunen 57
Kontrolle 49, 50, 72
Kooperationsverfahren 43
Kopie 62, 70, 91
Künstliche Intelligenz 25

L

LAKOST MV 35
Landesförderinstitut 64
Landespolizei MV 71, 76, 78
Löschung 15

M

Medien 38
Medienaktiv MV 30
Medienbildung 30, 34, 36, 39
Medienerziehung 40, 112
Medienguides MV 30, 32, 33
Medienscouts MV 31, 32, 33
Microsoft 27
Microsoft 365 27
Microsoft-Onlinedienste 27
Mini-Solaranlage 64
Ministeriums für Bildung und Kindertagesförderung MV 30
Mitarbeiterexzess 78, 91
Mitwirkungspflicht 100
mobiles Arbeiten 23

N

nachbarschaftlichen 12
Newsletter 29
Novellierungsbedarfe 80

O

öffentliche Stellen 50
Open-Source 19, 23
Orientierungshilfe 13

P

Projekt ISY MV 26

Pachtverträge 106
Partei 55
Patientenakte 70
Personalausweis 64
personenbezogene Daten 91
personenbezogenen Daten 108
Piktogramme 87
politische Meinungen 91
Polizeiliche Informationssysteme 74
Postweg 102
Privacy-by-Default 19
Privacy-by-Design 19
Protokoll 105
Protokolle 104
Pseudonymisierung 13

R

rechtliches Interesse 108
Rechtsgrundlage 51
rechtsmissbräuchlich 90
Rechtssetzungsvorhaben 92, 93
Rechtsstaatsprinzip 101
Ringspeichersystem 86

S

Schaukasten 88
Schriftform 102
Schriftformerfordernis 103
Schule 24, 26
Schulleitung 25
schützenswerte Daten 104
Schwachstelle 13
SEPA-Lastschriftverfahren 65
Sicherheitsüberprüfungen 80
Speicherzyklus 86
Standard-Datenschutzmodell 13, 20

T

Telemedien 28
TTDSG 28
Tage ethischer Orientierung 33
Tesla 86
TikTok 39, 48

TOMMI 37
Transparenz 103
Transparenzgesetz 99
Transparenzregister 99

U

Unberechtigte Datenabfragen 78
Unterschrift 103
Unterstützungspflicht 100
USB-Stick 82

V

Verantwortlicher 53
Vereine 88
Verkehr 83
Verkehrsanalyse 83
verlängertes Auge 87
Verschlüsselung 14, 81
Vertraulichkeit 104
Verwaltungsrechtsweg 104
Videokamera 57
Videokonferenzsystem 23
Videosequenzen 57
Videoüberwachung 57, 90

W

Wächtermodus 86
Webseiten 28
Widerspruch 29, 107

Z

Zahlungsvorgänge 65
ZDMV 19

19. Tätigkeitsbericht zum Datenschutz

Berichtszeitraum: 1. Januar 2022 bis 31. Dezember 2023

und

9. Bericht über die Umsetzung des Informationsfreiheitsgesetzes M-V

Berichtszeitraum: 1. Januar 2022 bis 31. Dezember 2023

Postanschrift
Schloss Schwerin
Lennéstraße 1
19053 Schwerin

Dienststelle
Werderstraße 74a
19055 Schwerin

Kontakt
Telefon: 0385 59494-0
E-Mail: info@datenschutz-mv.de

www.**datenschutz-mv**.de
www.**informationsfreiheit-mv**.de