LANDTAG MECKLENBURG-VORPOMMERN **Drucksache 7/5046**
7. Wahlperiode **04.06.2020**

UNTERRICHTUNG

durch den Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern

Fünfzehnter Tätigkeitsbericht gemäß Artikel 59 der Europäischen Datenschutz-Grundverordnung (DS-GVO)

Berichtszeitraum: 1. Januar 2019 bis 31. Dezember 2019

Siebenter Tätigkeitsbericht nach dem Informationsfreiheitsgesetz Mecklenburg-Vorpommern (IFG M-V)

Berichtszeitraum: 1. Januar 2018 bis 31. Dezember 2019

Vorwort

Mit den nachfolgenden Ausführungen lege ich den gemäß Art. 59 Europäische Datenschutz-Grundverordnung (DS-GVO) geforderten Jahresbericht dem Landtag Mecklenburg-Vorpommern, der Landesregierung Mecklenburg-Vorpommern und der Öffentlichkeit vor. Der Berichtszeitraum umfasst das Kalenderjahr 2019.

Gleichzeitig lege ich meinen Tätigkeitsbericht als Landesbeauftragter für Informationsfreiheit Mecklenburg-Vorpommern für den Berichtszeitraum 2018/2019 vor.

Heinz Müller
Landesbeauftragter für Datenschutz und Informationsfreiheit
Mecklenburg-Vorpommern

Inhaltsverzeichnis ..... Seite

1 Empfehlungen 6
1.1 Zusammenfassung aller Empfehlungen 6
1.2 Umsetzung der Empfehlungen des Vierzehnten Tätigkeitsberichtes 8

2 Zahlen und Fakten 10

3 Entwicklung der Behörde 12

4 Zusammenarbeit auf europäischer Ebene 13
4.1 Europäischer Datenschutzausschuss (EDSA) 13
4.2 Enforcement Subgroup 13
4.3 Technology Subgroup 14
4.4 Das europäische Binnenmarkt-Informationssystem (IMI) 15
4.5 Einzelfälle der europäischen Zusammenarbeit 16

5 Zusammenarbeit auf deutscher Ebene 17
5.1 Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) 17
5.2 AK Technik 20
5.3 IT-Planungsrat 21
5.3.1 Turnusmäßige Sitzungen 21
5.3.2 Registermodernisierung 22

6 Datenschutz und Bildung 23
6.1 Medienbildung 23
6.1.1 Datenschutz als Bildungsaufgabe 24
6.1.2 Projekte „Medienscouts MV“ und „TEO -Tage ethischer Orientierung“ 25
6.1.3 Netzwerk Medienaktiv M-V 27
6.1.4 „klicken, spielen, zappen“ - Modulare Fortbildungsreihe für Erzieherinnen und Erzieher 28
6.1.5 Jugend hackt & Hello World 29
6.1.6 Freiwilliges Soziales Jahr „Demokratie/Politik“ - ein Erfahrungsbericht 30

7 Technik und Organisation 31
7.1 Neue Technologien 31
7.1.1 Positionspapier Biometrische Analyse 31
7.1.2 Windows 10 33
7.1.3 Datenschutzaspekte Künstlicher Intelligenz 34
7.1.4 Microsoft Office 365 35
7.1.5 Standard-Datenschutzmodell (SDM) 36
7.1.6 MV-Serviceportal - das Tor zur digitalen Verwaltung 37
7.1.7 Elektronische Akte (eAkte) 39
7.1.8 Wenn kein sicheres Passwort verwendet wird 40
7.1.9 Meldung einer Datenpanne 41
7.2 Zertifizierung nach der DS-GVO 42
7.3 Kommunikation/Neue Medien 44
7.3.1 Messenger-Dienste im Krankenhaus 44
7.3.2 Neue Regeln für Webseitenanbieter 45

Seite

8	Datenschutz in verschiedenen Rechtsgebieten	47
8.1	Rechtswesen	47
8.1.1	Informationsportal „Neutrale Schule“ - AfD stellt Lehrer an den Pranger	47
8.1.2	Nachbarschaftslisten - nur mit Einwilligung	48
8.1.3	Auskunftsersuchen - Grenzen des Auskunftsverweigerungsrechts	49
8.1.4	Betroffenenrechte nach der Datenschutz-Grundverordnung - eine Herausforderung für Unternehmen und Behörden	50
8.1.5	Videoüberwachung im privaten und nachbarschaftlichen Bereich	52
8.1.6	Stetiger Meldedatenabgleich für den Rundfunkbeitrag	53
8.2	Polizei/Ordnungswesen	54
8.2.1	Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommern (SOG M-V)	54
8.2.2	Videoüberwachung Marienplatz	56
8.2.3	Einsatz von Bodycams bei der Polizei	59
8.2.4	Bußgeldverfahren gegen Polizisten	59
8.3	Justiz	60
8.3.1	Justizvollzugsdatenschutzgesetz	60
8.3.2	Kopie der Prüfungsakte des Landesjustizprüfungsamtes	60
8.4	Gesundheitswesen	61
8.4.1	Digitale Anwendungen und datenschutzrechtliche Verantwortlichkeiten	61
8.4.2	Projekt „Umgang mit Patientendaten in den Krankenhäusern Mecklenburg-Vorpommerns (UPDK)"	62
8.5	Neue Zuständigkeiten im Finanzbereich	63
8.6	Zensus 2021	64
8.7	Schule/Bildung	65
8.7.1	Integriertes-Schulmanagement-System (ISY)	65
8.7.2	Bring Your Own Device (BYOD) im Schulbereich	66
8.8	Datenverarbeitung in Vereinen	67
8.8.1	Rechtsgrundlagen	67
8.8.2	Einwilligung	68
8.8.3	Herausgabe von Mitgliederlisten an die Vereinsmitglieder	68
8.8.4	Leitfaden für Vereine	69
8.9	Kommunales	69
8.9.1	Speicherung Daten Verstorbener in einem Bestattungsportal	69
8.9.2	Verweigerung von Auskunftsansprüchen	70
8.9.3	Nutzung von Drohnen zu behördlichen Zwecken	70
8.9.4	Entwendung einer Festplatte aus einem Hortraum	71
8.9.5	Vertraulichkeit bei Übermittlungen von E-Mails	72

Seite

9 Informationsfreiheitsgesetz Mecklenburg-Vorpommern - IFG M-V 73
9.1 Informationsfreiheit in Mecklenburg-Vorpommern - Bedeutung, Zahlen und Fakten 73
9.2 Stellungnahme zum Entwurf eines Beteiligtentransparenzdokumentationsgesetzes (BeteildokG M-V) 74
9.3 Vertragsunterlagen zur Betreibung der Erstaufnahmeeinrichtungen für Asylbewerber als öffentliche Information? 75
9.4 Ist Sponsoring durch die Sparkasse Parchim-Lübz ein Betriebs- und Geschäftsgeheimnis? 76
9.5 Unvermuteter IFG-Kostenbescheid bei vorherigem kostenlosen Informationszugang 78
9.6 Keine Zuständigkeit des Landesbeauftragten für Informationsfreiheit bei Informationen nach dem Verbraucherinformationsgesetz (VIG) 79
9.7 Abschreckende Kosten bei hohem Verwaltungsaufwand? 80
9.8 Müssen städtische Aktiengesellschaften selbst Auskunft geben? 82
9.9 Sind die Datenschutzfolgen-Abschätzung sowie ein Datenschutz- und Informationssicherheitskonzept zur Videoüberwachung öffentliche Informationen? 82
9.10 Herausgabe von Abituraufgaben der vergangenen Jahrgänge über das Portal FragDenStaat 84
9.11 Ablehnung der Herausgabe der Ablösesumme für Stellplätze unzulässig 85
9.12 Bereitstellung von Informationen durch reine Addition gleichartiger Informationen ist kein Ausschlusskriterium 86
9.13 Herausgabeanspruch durch Auslegung eines Antrags auf Akteneinsicht als Antrag nach dem IFG M-V durchgesetzt 88
9.14 Einsichtnahme in einen Nutzungsvertrag zwischen einer Stadt und einer OHG 88

10 Abkürzungsverzeichnis 90

11 Stichwortverzeichnis 93

1 Empfehlungen

1.1 Zusammenfassung aller Empfehlungen

1. Das neue Bundesdatenschutzgesetz (BDSG) sieht vor, dass der Bundesrat als Stellvertreter einen Leiter der Aufsichtsbehörde eines Landes wählt. Das ist bislang jedoch nicht geschehen. Wir empfehlen der Landesregierung, sich dafür einzusetzen, dass dies schnellstmöglich nachgeholt wird, siehe Punkt 4.1.
2. Wir empfehlen der Landesregierung, sich dafür einzusetzen, dass bei der Modernisierung der Verwaltungsregister der verfassungskonforme Architekturansatz bereichsspezifischer Identifier in Anlehnung an das österreichische Stammzahlensystem umgesetzt wird und keine einheitlichen und verwaltungsübergreifenden Personenkennzeichen gebildet werden, siehe Punkt 5.3.2.
3. Wir empfehlen Verantwortlichen in Wirtschaft und Verwaltung, vor dem Einsatz von Verfahren zur Verarbeitung biometrischer Daten zu prüfen, ob die Verarbeitung die Zulässigkeitsvoraussetzungen des Art. 6 DS-GVO erfüllt und ob die zusätzlichen, strengeren Voraussetzungen des Art. 9 DS-GVO eingehalten werden können, und dabei die Empfehlungen des Positionspapiers „Biometrische Analyse“ zu berücksichtigen, siehe Punkt 7.1.1.
4. Wir empfehlen den Verantwortlichen, genau zu prüfen, ob sie die beim Einsatz von Windows 10 entstehenden Risiken beherrschen können. Falls nicht, sollten andere Betriebssysteme, insbesondere aus dem Open Source Bereich, in Betracht gezogen werden, siehe Punkt 7.1.2.
5. 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, siehe Punkt 7.1.3.
6. Wir empfehlen den Verantwortlichen in Wirtschaft und Verwaltung, entweder die Einführung von Microsoft Office365 solange zurückzustellen, bis die rechtlichen Rahmenbedingungen geklärt sind, oder den Einsatz anderer Produkte, insbesondere aus dem Open Source Bereich, zu prüfen, siehe Punkt 7.1.4.
7. Wir wiederholen unsere Empfehlung an die Landesregierung aus dem Vierzehnten Tätigkeitsbericht, bei der Einrichtung und beim Betrieb von personenbezogenen Verarbeitungstätigkeiten die im Standard-Datenschutzmodell (SDM) beschriebene Vorgehensweise anzuwenden und das dort beschriebene Datenschutzmanagement-System einzurichten, siehe Punkt 7.1.5.
8. Wir wiederholen unsere Empfehlung aus dem Vierzehnten Tätigkeitsbericht, die erforderlichen Rechtsgrundlagen für die Einrichtung und Registrierung von Nutzerkonten zu schaffen und die datenschutzrechtlichen Verantwortlichkeiten zwischen den am Verfahren Beteiligten zu klären. Bis zum Inkrafttreten des Zweiten Gesetzes zur Änderung des E-Government-Gesetzes und dem Erlassen der vorgesehenen Rechtsverordnung empfehlen wir eine Übergangsregelung, etwa einen Kabinettsbeschluss, siehe Punkt 7.1.6.
9. Wir empfehlen Verantwortlichen in Wirtschaft und Verwaltung, ein geeignetes Passwortmanagement aufzubauen und es einem regelmäßigen Revisionsprozess zu unterwerfen. Bei bereits vorhandenem Passwortmanagement sollte geprüft werden, ob es dem Stand der Technik entspricht, siehe Punkt 7.1.8.

10. Wir empfehlen Verantwortlichen, sich frühzeitig mit dem Thema Zertifizierung vertraut zu machen. Zertifikate bieten das Potenzial, sich bei Verarbeitungsvorgängen (etwa bei Auftragsverarbeitung oder Cloudstrukturen) Klarheit darüber zu verschaffen, ob die gesetzlichen Datenschutzanforderungen eingehalten werden, siehe Punkt 7.2.
11. Wir empfehlen den Verantwortlichen in Krankenhäusern, bei Planungen und beim Betrieb von Messenger-Diensten die Anregungen des Whitepapers „Technische Anforderungen an Messenger-Dienste im Krankenhaus“ zu berücksichtigen und sich an der Diskussion zur Weiterentwicklung des Papiers zu beteiligen, siehe Punkt 7.3.1.
12. Wir empfehlen den Webseitenanbietern in unserem Bundesland, ihre Webseiten an die vorgenannten neuen Regeln anzupassen. Dies gilt insbesondere für das Einbinden von Dritt-Inhalten und gilt auch für Tracking-Mechanismen. Wer Funktionen nutzt, die eine informierte Einwilligung erfordern, muss entweder eine informierte Einwilligung einholen oder die Funktion entfernen, siehe Punkt 7.3.2.
13. Wir empfehlen Verantwortlichen, einen festen Prozess zu etablieren und Beschäftigte entsprechend zu schulen, wie mit Betroffenenrechten umzugehen ist, siehe Punkt 8.1.4.
14. Wir empfehlen der Landesregierung, sich dafür einzusetzen, dass die Planungen zum stetigen Meldedatenabgleich für den Rundfunkbeitrag eingestellt werden, siehe Punkt 8.1.6.
15. Wir empfehlen dem Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern, den sehr produktiven Meinungsaustausch mit uns beizubehalten, die Abstände der Gespräche zwischen beiden Häusern im Jahr 2020 jedoch deutlich zu verkürzen, siehe Punkt 8.8.1.
16. Wir empfehlen der Landesregierung erneut, das Informationsfreiheitsgesetz Mecklenburg-Vorpommern hin zu einem modernen Transparenzgesetz fortzuentwickeln, siehe Punkt 9.1.

1.2 Umsetzung der Empfehlungen des Vierzehnten Tätigkeitsberichtes

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt im 14. TB
1	Wir empfehlen der Landesregierung, sich dafür einzusetzen, dass schnellstmöglich durch den Bundesrat ein Stellvertreter für den Europäischen Datenschutzausschuss (EDSA) gewählt wird.	Mit Ablauf des Berichtszeitraumes war der Stellvertreter noch immer nicht gewählt.	4.1
2	Wir empfehlen der Landesregierung, die Vernetzung aller medienpädagogisch Arbeitenden in MV aktiv zu unterstützen und politische Rahmenbedingungen für die Akteure zu schaffen. Die Vermittlung von Datenschutzbewusstsein und Medienkompetenz gehört nach unserer Auffassung zum staatlichen Bildungsauftrag. Im Einklang mit unserer gesetzlichen Aufgabe nach Art. 57 Abs. 1 Ziffer b DS-GVO übernehmen wir einen großen Bereich der Medienbildungsangebote im Land und initiierten ein umfangreiches Angebot in Kooperation mit zahlreichen außerschulischen Partnern.	Die Kooperationsvereinbarung zur Förderung von Medienkompetenz in Mecklenburg-Vorpommern wird nach Kabinettsbeschluss neu geschrieben. Das ist sehr zu begrüßen. Doch die Akteure und Umsetzer in den Institutionen und Einrichtungen vor Ort werden nicht mehr in die Erarbeitung eingebunden. Den gesamtgesellschaftlichen Dialog und den vernetzenden Grundgedanken sehen wir weiterhin nicht umgesetzt. Stattdessen soll ein Landesmedienkompetenzzentrum aufgebaut werden, welches die Gefahr von Parallelstrukturen birgt, da die Akteure des bestehenden Netzwerkes nicht eingebunden sind.	6.1
3	Wir empfehlen der Landesregierung, die datenschutzrechtlichen Verantwortlichkeiten zwischen den am Verfahren Beteiligten zu klären und die erforderlichen Rechtsgrundlagen für die Einrichtung und Registrierung von Nutzerkonten zu schaffen.	Die Landesregierung hat in Aussicht gestellt, dass mit der Verabschiedung des novellierten E-Government-Gesetzes des Landes im Mai 2020 eine tragfähige Rechtsgrundlage für die Einrichtung und Registrierung von Nutzerkonten geschaffen werden soll. Bis dahin läuft das Verfahren weiterhin auf Basis der Einwilligung der Betroffenen und damit auf einer äußerst fragwürdigen Rechtsgrundlage. Auch die Arbeiten zur Klärung der gemeinsamen Verantwortlichkeiten waren zum Ende des Berichtszeitraumes nicht abgeschlossen, sodass auch in diesem Bereich die rechtlichen Voraussetzungen für den Betrieb des Verfahrens nach wie vor nicht gegeben sind.	7.1.3

Lfd. Nr.	Empfehlung	Umsetzungsstand	Gliederungspunkt im 14. TB
4	Wir empfehlen der Landesregierung, bei der Planung, bei der Einrichtung und beim Betrieb von Verfahren zur Verarbeitung personenbezogener Daten die im Standard-Datenschutzmodell (SDM) beschriebene Vorgehensweise anzuwenden und uns über die Erfahrungen beim Umgang mit diesem Werkzeug zu berichten, um dadurch die Weiterentwicklung des Standard-Datenschutzmodells zu unterstützen.	Das Standard-Datenschutzmodell (SDM) spielt bei den Verfahrensplanungen der Landesverwaltung inzwischen eine wichtige Rolle. Der Landesdienstleister DVZ M-V GmbH hat mit uns gemeinsam ein Dokument erarbeitet, mit dem die Schutzbedarfsfeststellung nach BSI-Grundschutz, die Risikobewertung nach DS-GVO und die Schwellwertanalyse für die Datenschutzfolgen-Abschätzung (DSFA) nach der Systematik des SDM durchgeführt werden. Die Planung und Einführung wichtiger IT-Vorhaben etwa in den Bereichen Polizei, Bildung, Statistik oder Finanzwirtschaft erfolgt in zunehmendem Maße nach den Prinzipien der SDM-Systematik.	7.1.5
5	Wir erwarten, dass das Ministerium für Inneres und Europa Mecklenburg-Vorpommern die Erfahrungen des Einsatzes von Bodycams ergebnisoffen auswertet und vor allem auf Grundlage dieser Erfahrungen dann über das weitere Ob und Wie von Bodycams entscheidet und deren Einsatz grundrechtskonform im SOG M-V regelt.	Am 15. Oktober 2019 hat der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern eine Besprechung mit dem Ministerium für Inneres und Europa Mecklenburg-Vorpommern zur Evaluation des Pilotprojektes „Einsatz körpernah getragener Aufnahmegeräte durch die Polizei (Bodycams)“ geführt. Im Ergebnis der Besprechung wurde Einvernehmen im Sinne der der mit der Landesregierung vereinbarten Evaluation zum Pilotprojekt hergestellt. Die Auswertung des Pilotprojektes hat ergeben, dass in Mecklenburg-Vorpommern der Einsatzwert der Bodycam zum Schutz von Leib und Leben der Polizeivollzugsbeamten gegeben ist. Zugesichert wurde, dass mit der Einführung der Bodycam in der Landespolizei alle erforderlichen Aspekte des Datenschutzes eingehalten werden.	9.1.2
6	Wir empfehlen der Landesregierung, die entsprechenden Regelungen im KiföG M-V zu ändern.	Am 1. Januar 2020 wurde das neu KiföG M-V in Kraft gesetzt und im Zuge dessen ebenfalls zum 2. Januar 2020 die Verordnung über die inhaltliche Ausgestaltung und Durchführung der alltagsintegrierten Beobachtung und Dokumentation in der Kindertagesförderung (BeDoVo M-V). Durch die Abstimmung mit dem zuständigen Ressort konnten unsere Anregungen umgesetzt werden.	9.4.5

2 Zahlen und Fakten

Im Zusammenhang mit dem Wirksamwerden der Europäischen Datenschutz-Grundverordnung (DS-GVO) im Mai 2018 war der Arbeitsumfang in meiner Behörde massiv nach oben geschnellt. Dies wurde von außen teilweise dahingehend bewertet, dass es sich um eine „Blase“ handelt, ein kurzfristiges, heftiges Aufblähen also, das aber bald wieder in sich zusammenfallen würde. Die Entwicklungen des Jahres 2019 zeigen jedoch sehr eindrucksvoll, dass diese Annahme falsch war. Das Arbeitsvolumen ist im Jahr 2019 gegenüber dem Jahr 2018 insgesamt weiter massiv angestiegen.

Vor diesem Hintergrund mussten wir die Zahl der Veranstaltungen, die ja im Wesentlichen der Information und der Sensibilisierung dienen, bewusst reduzieren. Während wir in den letzten vier Monaten des Jahres 2018 noch 70 Veranstaltungen durchgeführt haben, was für ein Gesamtjahr auf eine Zahl von 210 schließen lässt, fanden im Jahr 2019 nur noch 175 Veranstaltungen mit ca. 3 500 Teilnehmerinnen und Teilnehmern statt.

Bei der Zahl der europäischen Verfahren, insbesondere der Kohärenzverfahren nach Art. 63 DS-GVO, lässt sich allerdings tatsächlich ein gewisser Rückgang feststellen. Da diese europäischen Instrumente stärker zur Routine geworden sind, wird folgerichtig nicht mehr zu schnell nach dem europäischen Verfahren gerufen. Gab es in den letzten vier Monaten 2018 noch 433 europäische Verfahren, an denen wir beteiligt wurden, so waren es im gesamten Jahr 2019 noch 1.069.

Bei allen anderen Aufgabenarten und allen Kennzahlen, die wir statistisch erfasst haben, ist es bei den extrem hohen Fallzahlen des Vorjahres geblieben oder es war sogar eine weitere Steigerung festzustellen. Während wir in den letzten vier Monaten 2018 nur von einer aufsichtsrechtlichen Maßnahme nach Art. 58 Abs. 2 DS-GVO Gebrauch gemacht haben, waren es im Jahr 2019 bereits 82. Die häufigste dabei ergriffene Maßnahme war die förmliche Warnung, mit der Verantwortliche auf voraussichtliche Datenschutzverstöße hingewiesen werden. Wenn der Verantwortliche auf eine solche Warnung reagiert und die Datenverarbeitung einstellt oder sie den rechtlichen Vorgaben anpasst, sehen wir regelmäßig von einem weiteren förmlichen Verfahren ab. Im Gegensatz zur Warnung stellen die anderen förmlichen Abhilfemaßnahmen Verwaltungsakte dar, vor deren Erlass wir dem Verantwortlichen Gelegenheit zur Stellungnahme geben. Insgesamt haben wir im Jahr 2019 94 Anhörungen zu förmlichen Maßnahmen durchgeführt.

Im Berichtszeitraum mussten wir fünf Bußgelder verhängen. Rechtsgrundlage hierfür war immer § 22 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V). Als deutlich wirksameres Mittel zur Durchsetzung von Datenschutzrecht hat sich aber die Androhung von Zwangsgeldern erwiesen. Hierzu haben wir im Berichtsjahr acht Mal gegriffen. Nachdem wir in den letzten vier Monaten des Jahres 2018 231 Stellungnahmen, Empfehlungen und Beratungen abgegeben haben, ist diese Zahl im Jahr 2019 auf 793 angestiegen. Hier ist deutlich erkennbar, wie hoch der Bedarf nach Kenntnis unserer Rechtseinschätzung ist.

Die Zahl der Meldungen gemäß Art. 33 DS-GVO, mit denen uns Verantwortliche Datenpannen mitteilen, ist nahezu konstant geblieben. Nach 36 Meldungen in den letzten vier Monaten des Jahres 2018 waren es im Jahr 2019 108 Fälle. Gestiegen ist hingegen die Zahl der Eingaben und Beschwerden. Im Berichtszeitraum registrierten wir 533 Fälle. Das Parlament und die Regierung forderten unsere Beratung in 54 Fällen an. Auch hier ist also eine Steigerung gegenüber dem Vorjahr zu verzeichnen. Wir haben 67 anlassbezogene Prüfungen durchgeführt. Die Zahl der anlassunabhängigen Prüfungen, die für die Durchsetzung des Datenschutzrechts von besonderer Bedeutung sind, verharrt mit drei Fällen auf einem extrem niedrigen Niveau. Diese Zahl verdeutlicht, dass wir hier unserer Aufgabe, der Durchsetzung der DS-GVO, nicht ansatzweise gerecht werden. Insgesamt ist festzuhalten, dass wir sehr stark reaktiv arbeiten müssen und nicht in der Lage sind, aus unserer Sicht heraus pro-aktiv tätig zu werden. Im reaktiven Handeln ist festzuhalten, dass dieses häufig ohne förmliche Sanktionen ausgekommen ist und oft im Gespräch die Probleme gelöst werden konnten.

Angesichts der andauernden Arbeitsüberlastung bleibt es nicht aus, dass einzelne Anliegen nicht in einer vertretbaren Frist bearbeitet werden können. Folgerichtig häufen sich bei uns die Beschwerden von Bürgerinnen und Bürgern, die ihr verfassungsmäßiges Recht auf Anrufung des Landesdatenschutzbeauftragten nach Art. 37 unserer Landesverfassung wahrnehmen und deren Anliegen von uns nicht in angemessener Zeit bearbeitet werden. Dabei schreibt uns Art. 78 DS-GVO vor, förmliche Beschwerden von Bürgerinnen und Bürgern innerhalb von drei Monaten zu bearbeiten, wenn auch nicht zwingend abschließend. Andernfalls können sich die Beschwerdeführer an das Verwaltungsgericht wenden. Damit genießen aber solche Anfragen Vorrang vor anderen Aufgaben, etwa vor Beratungen. Auch deshalb haben wir, wie oben erwähnt, eine Reihe von Wünschen nach Beratung, Vorträgen oder ähnlichem bereits ablehnen müssen.

Eine Ursache für das in der Summe weiter ansteigende Arbeitsvolumen ist sicherlich in der DS-GVO zu suchen, die den Aufsichtsbehörden zusätzliche Aufgaben gibt. Hier sind wir auch noch nicht am Ende der Entwicklung; in einigen Bereichen, etwa bei der Zertifizierung, beginnen die Aufsichtsbehörden gerade erst, sich diesen Feldern zu widmen. Eine weitere Ursache liegt in der rasanten technischen Entwicklung der Datenverarbeitung und der immer stärkeren Durchdringung nahezu aller Lebensbereiche. Dem steht ein geschärftes gesellschaftliches Bewusstsein für die Probleme einer nahezu allumfassenden Datenverarbeitung gegenüber. Und zuletzt: Neben den bekannten und erkannten Verstößen im Datenschutzbereich vermuten wir ein gigantisches Dunkelfeld von Rechtsbrüchen, die niemand bemerkt oder als solche erkennt. Die Aufgaben der Datenschutzaufsichtsbehörden werden also weiter wachsen.

3 Entwicklung der Behörde

Als einzige Datenschutzaufsichtsbehörde in Deutschland arbeitet der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern mit der gleichen Personalausstattung wie vor der Europäischen Datenschutz-Grundverordnung (DS-GVO). Zwar wurden bereits vor dem Berichtszeitraum fünf neue Stellen geschaffen, dieses jedoch mit einer Reduzierung der finanziellen Mittel für diesen Bereich erkauft. Im Ergebnis erhielten fünf Mitarbeiterinnen und Mitarbeiter, die bis dahin mit sogenannten Beschäftigungsentgelten an Vertretungs- und Aushilfskräfte bezahlt und mit befristeten Verträgen beschäftigt wurden, unbefristete Stellen. Eine Vermehrung der tatsächlichen Kräfte fand jedoch nicht statt.

Vergleicht man diese Tatsache mit der Entwicklung anderer Datenschutzaufsichtsbehörden, muss dies verwundern. Beispielhaft sei hier auf den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) hingewiesen, der übrigens mit Ausnahme von bundesweit tätigen Telekommunikationsunternehmen nicht für die Wirtschaft zuständig ist. Die Stellenzahl seiner Behörde stieg von 87 im Jahr 2014 auf 320 im Jahr 2020. Hier wurde also der Personalbestand nahezu vervierfacht. Auch ein Blick in die Länder zeigt die Ausnahmesituation von Mecklenburg-Vorpommern. Interessant ist, dass im Freistaat Bayern nicht nur der Landtag die Datenschutzaufsichtsbehörden (in Bayern gibt es eine Behörde für den öffentlichen und eine für den nicht-öffentlichen Bereich) besser ausstatten wollte. Auch das bayerische Innenministerium kam zu dem Ergebnis, dass das für den nicht-öffentlichen Bereich zuständige Landesamt für Datenschutzaufsicht mit seinem derzeitigen Stellenbestand, der vom Landtag bereits deutlich erhöht worden war, seine Aufgaben nicht erfüllen kann, und stellte dem Landesamt aus dem eigenen Bestand weitere Stellen zur Verfügung.

In Mecklenburg-Vorpommern wurden hingegen unsere detailliert begründeten Anträge auf bessere Stellenausstattung unterschiedslos in der Weise bearbeitet, dass man alle Stellen zwar in den Haushalt einstellte, sie aber gleichzeitig sperrte. Dieses gilt auch für notwendige Höherstufungen, wobei diese zum erheblichen Teil gar nicht aus der DS-GVO begründet werden, sondern mit anderen Entwicklungen in der Behörde zu tun haben. Auch hier wurde ohne Prüfung einzelner Anträge alles, was „vom Datenschutz“ kommt, auf Vorschlag der Landesregierung vom Parlament gesperrt.

Die bewährte innere Struktur unserer Behörde haben wir im Berichtszeitraum beibehalten. Die in der Vergangenheit vom Landesrechnungshof gemachten Anregungen zur Hebung von Einsparpotenzialen wurden, soweit dies möglich und sinnvoll war, umgesetzt.

Mit dem am Ende des Berichtszeitraumes beschlossenen Doppelhaushalt 2020/2021 hat der Landtag auf Vorschlag der Landesregierung auch erhebliche Teile der Mittel für die Bewirtschaftung unserer Dienststelle mit einem Sperrvermerk versehen. Somit stehen für das laufende Jahr noch keine ausreichenden Mittel für Strom, Reinigung, Müllabfuhr und Bewachung zur Verfügung. Es bleibt zu hoffen, dass die Aufhebung dieses Sperrvermerks im Laufe des Jahres 2020 gelingt, weil anderenfalls die Behörde im Laufe des Jahres komplett handlungsunfähig wird.

4 Zusammenarbeit auf europäischer Ebene

4.1 Europäischer Datenschutzausschuss (EDSA)

Der Europäische Datenschutzausschuss (EDSA) besteht aus dem Leiter einer Aufsichtsbehörde jedes Mitgliedstaats und dem Europäischen Datenschutzbeauftragten oder ihren jeweiligen Vertretern. Deutschland wird im EDSA durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vertreten. Das neue Bundesdatenschutzgesetz (BDSG) sieht vor, dass der Bundesrat als Stellvertreter einen Leiter der Aufsichtsbehörde eines Landes wählt. Das ist bislang jedoch nicht geschehen. Wir empfehlen der Landesregierung, sich dafür einzusetzen, dass dies schnellstmöglich nachgeholt wird.

Der EDSA ist eine Einrichtung der Europäischen Union mit eigener Rechtspersönlichkeit. Er hat die Aufgabe, die einheitliche Anwendung der Europäischen Datenschutz-Grundverordnung (DS-GVO) sicherzustellen. Bei Meinungsverschiedenheiten zwischen nationalen Aufsichtsbehörden ist der EDSA dazu befugt, durch Mehrheitsentscheidung innerhalb kurzer Fristen verbindliche Beschlüsse zu treffen. Außerdem hat er Leitlinien und Empfehlungen zur Auslegung einzelner Vorschriften der DS-GVO zu erstellen. Im Berichtszeitraum hat der EDSA unter https://edpb.europa.eu/edpb_de Leitlinien zu den Themen

- Verhaltensregeln und Überwachungsstellen
- Verarbeitung personenbezogener Daten nach Art. 6 Abs. 1 lit. b DS-GVO im Zusammenhang mit der Erbringung von Online-Diensten
- Verarbeitung personenbezogener Daten mit Hilfe von Videogeräten
- Datenschutz durch Design und datenschutzfreundliche Voreinstellung
- Voraussetzungen des Rechts auf Vergessenwerden in den Suchmaschinenfällen

veröffentlicht. Die Vorbereitung dieser Leitlinien erfolgt in Arbeitsgruppen, sogenannten Subgroups, die aus Mitarbeiterinnen und Mitarbeitern der Aufsichtsbehörden der Mitgliedstaaten bestehen. Soweit es uns zeitlich möglich ist, beteiligen wir uns an der Erarbeitung solcher Leitlinien. Zudem sind wir als ständiger Vertreter der deutschen Landesdatenschutzbeauftragten Mitglied der Technology Subgroup und entsenden bei Bedarf ein stellvertretendes Mitglied in die Enforcement Subgroup.

4.2 Enforcement Subgroup

Die Enforcement Subgroup, eine Arbeitsgruppe des Europäischen Datenschutzausschusses (EDSA), befasst sich mit praktischen Fragen der Durchsetzung der Europäischen Datenschutz-Grundverordnung (DS-GVO). Die Vertretung der Landesdatenschutzbeauftragten in der Enforcement Subgroup nehmen die Kollegen der Landesbeauftragten für Datenschutz und Informationsfreiheit Niedersachsen wahr, im Vertretungsfalle wir. Die Sitzungen der Enforcement Subgroup finden etwa alle zwei Monate in Brüssel statt.

Inhaltlich etabliert sich die Enforcement Subgroup als Forum für den Erfahrungsaustausch und die Klärung von Rechtsfragen anhand von Fallbeispielen aus der Praxis. Auch wurde in der Enforcement Subgroup die Richtlinie über die Voraussetzungen des Rechts auf Vergessenwerden in den Suchmaschinenfällen erarbeitet.

Während einige Mitgliedstaaten sich mit jeder nicht offenkundig unbegründeten Beschwerde befassen, behalten sich andere das Recht vor, nur solche Beschwerden zu bearbeiten, die ihrer Ansicht nach relevante Themen aufgreifen. Die Mitglieder der Enforcement Subgroup haben daher den Auftrag erhalten, ein gemeinsames Verständnis der „angemessenen“ Untersuchung einer Beschwerde im Sinne der DS-GVO zu erarbeiten.

Im Berichtszeitraum ist zum ersten Mal ein Streitbeilegungsverfahren vor dem EDSA eingeleitet worden. Der Enforcement Subgroup kommt in diesem Verfahren die Aufgabe zu, die Stellungnahme des EDSA vorzubereiten. Dazu kam es in diesem Fall jedoch nicht mehr, da die federführende Aufsichtsbehörde ihren Antrag nach der eingehenden Diskussion des Falles in der Enforcement Subgroup zurückzog.

Am Ende des Berichtszeitraumes stand das Strategiepapier „Coordinated Enforcement Framework“ kurz vor der Fertigstellung. Damit soll ein konkreter Rahmen für jährlich stattfindende koordinierte Aufsichtsmaßnahmen geschaffen werden.

4.3 Technology Subgroup

Die Technology Subgroup ist ein offizielles Gremium (Expert-Group) des Europäischen Datenschutzausschusses (EDSA), siehe Punkt 4.1, in dem die Aktivitäten aller europäischen Datenschutzaufsichtsbehörden koordiniert werden.

Ähnlich dem Arbeitskreis „Technische und organisatorische Datenschutzfragen“ auf nationaler Ebene (AK Technik, siehe Punkt 5.2) dient die „Technology Subgroup“ im internationalen Kontext dabei als ein Beratungs- und Unterstützungsgremium des EDSA.

Um die sich oft überschneidenden Themen der Technology Subgroup und des AK Technik zu koordinieren und die sich daraus ergebenden Synergieeffekte sinnvoll zu nutzen, sind wir als ständiger Vertreter der deutschen Landesdatenschutzbeauftragten Mitglied der Technology Subgroup. So ist es uns einerseits möglich, den AK Technik über die laufenden Entwicklungen im europäischen Rahmen zu informieren, und andererseits erlaubt uns die Mitgliedschaft, wichtige nationale Themen und Standpunkte des AK Technik auf internationaler Ebene einzubringen bzw. zu vertreten.

Mit dem Inkrafttreten der Europäischen Datenschutz-Grundverordnung (DS-GVO) hat sich die Bedeutung der Technology Subgroup deutlich erhöht. Denn eine europaweit einheitliche Auslegung der DS-GVO kann nur durch einen regelmäßigen Meinungsaustausch und durch eine gemeinsame Meinungsbildung zwischen den europäischen Mitgliedstaaten gewährleistet werden. Hierzu wurden im Berichtszeitraum beispielsweise auch die verbindlichen Listen von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DS-GVO[1], für die eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen ist, europaweit einheitlich abgestimmt.

[1] https://www.datenschutz-mv.de/static/DS/Dateien/DS-GVO/HilfsmittelzurUmsetzung/ListevonVerarbeitungsvorgaengennachArt35Abs4DS-GVO/DE_DSFA_Muss-Liste.pdf

Die Mitglieder der Subgroup bearbeiteten zudem die wichtigen Themen „Videoüberwachung“ und „Data Protection by Design and by Default“. Zu beiden Themen hat die Technology Subgroup entsprechende Leitlinien[2],[3] verabschiedet.

4.4 Das europäische Binnenmarkt-Informationssystem (IMI)

In Mecklenburg-Vorpommern ist grundsätzlich der Landesbeauftragte für Datenschutz und Informationsfreiheit für die Erfüllung der Aufgaben und die Ausübung der Befugnisse, die ihm durch die Europäische Datenschutz-Grundverordnung (DS-GVO) übertragen wurden, zuständig. Bei grenzüberschreitenden Verarbeitungen ist jedoch die Aufsichtsbehörde der Hauptniederlassung oder der einzigen Niederlassung des Verantwortlichen in der Europäischen Union federführend.

Das bedeutet, dass wir weiterhin für die Entgegennahme von Beschwerden über eine angeblich rechtswidrige Datenverarbeitung, beispielsweise durch Facebook, zuständig sind. Federführend bei der Entscheidung in der Sache sind jedoch die Kollegen von der irischen „Data Protection Commission“. Sie legen einen Entscheidungsentwurf vor. Wenn wir als betroffene Aufsichtsbehörde mit dieser Entscheidung nicht einverstanden sind, können wir dagegen Einspruch einlegen. Schließen sich die Iren diesem Einspruch nicht an, haben sie das sogenannte Kohärenzverfahren einzuleiten, das in einem verbindlichen Beschluss des Europäischen Datenschutzausschusses (EDSA) mündet.

Jeder einzelne der für die Zusammenarbeit der europäischen Datenschutzaufsichtsbehörden erforderlichen Verfahrensschritte ist im Binnenmarkt-Informationssystem (IMI) abgebildet. Dabei handelt es sich um ein mehrsprachiges Online-Tool, das die Behörden bei der grenzüberschreitenden Verwaltungszusammenarbeit in mehreren Politikbereichen des Binnenmarkts, nicht nur im Bereich des Datenschutzes, unterstützt.

Seit dem 25. Mai 2018 fand in 1.346 Fällen über IMI eine Verständigung über die federführende Aufsichtsbehörde statt. 807 Fälle grenzüberschreitender Datenverarbeitungen wurden im IMI-Fallregister eingetragen. Davon gingen 575 auf eine Beschwerde zurück. Die übrigen Verfahren wurden von Amts wegen eingeleitet, etwa auf der Grundlage eigener Ermittlungen oder wegen eines Medienberichts. 142 Entscheidungsentwürfe haben die federführenden Aufsichtsbehörden über IMI an die betroffenen Aufsichtsbehörden verteilt. Daraus sind bislang 79 endgültige Entscheidungen hervorgegangen. Wir haben insgesamt bei neun Beschwerden über grenzüberschreitende Verarbeitungen ein IMI-Verfahren eingeleitet.

[2] https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-32019-processing-personal-data-through-video_en

[3] https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en

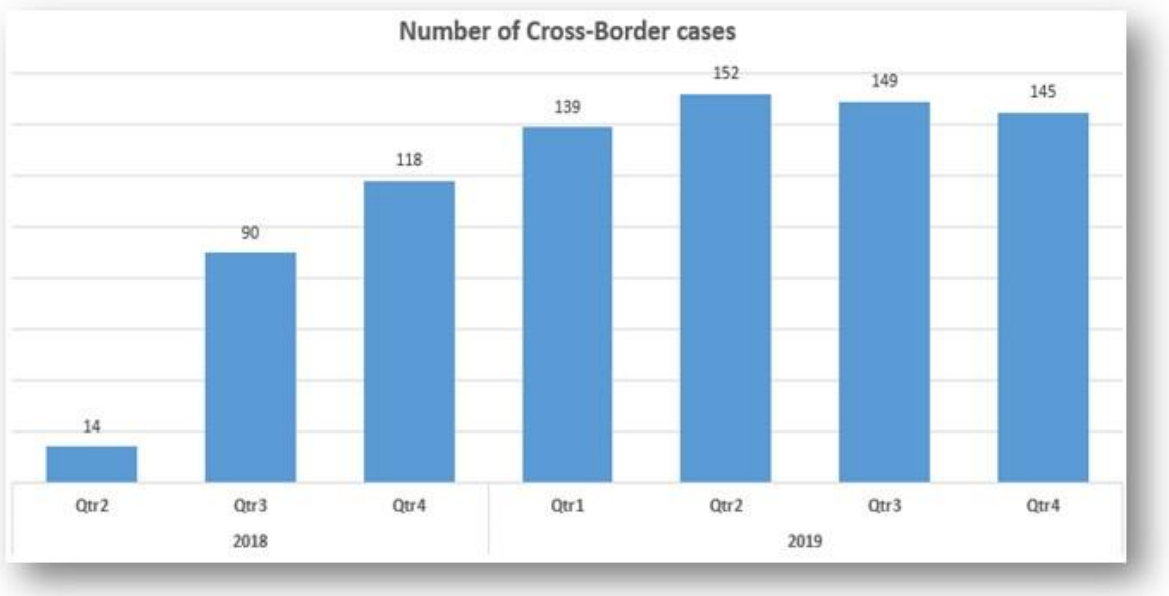

Abb. 1: Anzahl der Fälle grenzüberschreitender Datenverarbeitungen, die im IMI-Fallregister eingetragen wurden (Quelle: EDSA)

4.5 Einzelfälle der europäischen Zusammenarbeit

Der Europäische Datenschutzausschuss (EDSA) hat im Berichtszeitraum Leitlinien über die Verarbeitung personenbezogener Daten nach Art. 6 Abs. 1 lit. b Europäische Datenschutz-Grundverordnung (DS-GVO) im Zusammenhang mit der Erbringung von Online-Diensten herausgegeben. Nach Art. 6 Abs. 1 lit. b DS-GVO ist eine Verarbeitung personenbezogener Daten zulässig, wenn sie für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, erforderlich ist. Die Erbringer von Online-Diensten verarbeiten häufig personenbezogene Daten, um Kundenprofile aufzubauen und ihren Kunden auf diese Weise ein „personalisiertes Benutzererlebnis“ zu bieten. Wir sind der Meinung, dass sich dies nicht auf Art. 6 Abs. 1 lit. b DS-GVO stützen lässt, und haben uns dafür eingesetzt, dass der EDSA dies in den Leitlinien klarstellt. Das ist weitgehend gelungen. Selbst wenn die Verarbeitung von Kundenprofilen in den Vertragsbedingungen etwa eines Online-Verkäufers geregelt ist, wird sie, so die Leitlinien, deshalb nicht „erforderlich“ im Sinne des Art. 6 Abs. 1 lit. b DS-GVO.

Beim EDSA sind zudem Leitlinien über das Targeting von Social-Media-Nutzern in Arbeit. Unter Targeting wird die gezielte Ansprache einer bestimmten Gruppe von Personen verstanden mit dem Ziel, dieser zu kommerziellen, politischen oder sonstigen Zwecken spezifische Botschaften zu übermitteln. In dem Entwurf für die Leitlinien wird geprüft, ob sich die zu diesem Zweck erfolgende Verarbeitung personenbezogener Daten auf Art. 6 Abs. 1 lit. f DS-GVO stützen lässt. Wir haben deutlich gemacht, dass bei der in diesem Zusammenhang erforderlichen Interessenabwägung unter anderem der Umfang der verarbeiteten Daten eine Rolle spielen muss. In Fällen, in denen mehr oder weniger detaillierte Persönlichkeitsprofile der betroffenen Personen erstellt werden, überwiegen nach der Rechtsprechung des Europäischen Gerichtshofs (EuGH) in der Regel die Interessen der betroffenen Personen. Das muss aus unserer Sicht in den Leitlinien berücksichtigt werden. Die Arbeit an den Leitlinien dauert noch an.

„Jedes Mal, wenn eine verhaltensorientierte Werbeanzeige an eine Person gerichtet wird, die eine Website besucht, sendet das System, das die Werbeanzeige auswählt, persönliche Daten an Hunderte oder Tausende von Unternehmen.“ So beginnt der Bericht von Jonny Ryan zum Thema „Verhaltensbasierte Werbung und personenbezogene Daten“[4], den zwölf Menschenrechts- und Digitalrechtsorganisationen Mitte des Jahres zum Anlass nahmen, in neun EU-Ländern Beschwerden[5] bei den jeweiligen Datenschutzbehörden einzureichen, unter anderem bei uns. Die Beschwerdeführer gehen davon aus, dass es beim Platzieren von Online-Werbung über das Verfahren des „Real Time Biding“, der Echtzeit-Auktion, zu massiven Datenschutzverstößen kommt. Jede Auktion bringe die Übertragung zahlloser Informationen über Einzelpersonen mit sich. Das Ausmaß gehe weit darüber hinaus, was für die Bereitstellung einer Online-Anzeige erforderlich sei. Die schiere Anzahl der Empfänger führe dazu, dass die Sender weder die unbefugte Weiterverarbeitung der Daten verhindern noch die betroffenen Personen über die Empfänger der Daten ordnungsgemäß informieren können. Seien die Daten einmal weitergegeben, könne ihre rechtskonforme Verarbeitung nicht mehr gewährleistet werden. Nun liegt es an den europäischen Datenschutzaufsichtsbehörden, die #stopspyingonus-Beschwerden in einem angemessenen Umfang zu untersuchen.

5 Zusammenarbeit auf deutscher Ebene

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

Im Berichtszeitraum fanden zwei turnusmäßige Konferenzen, in diesem Jahr unter Vorsitz des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, statt. Der Konferenzvorsitzende hatte das Thema „Datenschutzrelevante Aspekte Künstlicher Intelligenz“ als Arbeitsschwerpunkt für das Jahr 2019 gewählt. Daneben war auch in diesem Berichtszeitraum die Umsetzung der Europäischen Datenschutz-Grundverordnung (DS-GVO) wieder ein Schwerpunkt der Beratungen in den Konferenzen.

Die 97. Datenschutzkonferenz fand im April 2019 auf geschichtsträchtigem Terrain statt. Tagungsort war das Hambacher Schloss, das wegen des 1832 dort ausgerichteten Hambacher Festes neben der Frankfurter Paulskirche als wichtigstes Symbol der deutschen Demokratiebewegung gilt. In seiner Begrüßung würdigte Landtagspräsident Hering die Entscheidung des Konferenzvorsitzenden, einen für die deutsche Demokratiegeschichte so bedeutsamen Ort für die Frühjahrskonferenz gewählt zu haben. Demokratie, Freiheit und Selbstbestimmung seien keine Selbstverständlichkeiten, sondern müssten in jeder Generation neu errungen werden. Dem komme gerade auch in einer digitalen Lebenswelt besondere Bedeutung zu, und unabhängige Datenschutzbeauftragte seien dabei unverzichtbar, gerade auch als kompetente Berater der Parlamente.

[4] https://digitalegesellschaft.de/wp-content/uploads/2019/06/Report_verhaltensbasierteWerbung_Dr_Ryan-DE.pdf

[5] https://www.netzwerk-datenschutzexpertise.de/sites/default/files/beschw_2019_personalisiertewerbung3.pdf

Mit dem Thema „Künstliche Intelligenz (KI)“ berieten die Konferenzmitglieder über einen besonders zukunftsträchtigen Aspekt dieser künftigen digitalen Lebenswelt. Im Ergebnis verabschiedete die Konferenz die „Hambacher Erklärung zur Künstlichen Intelligenz“[6]. Sie stellt klar, dass auch für KI-Systeme die Grundsätze der DS-GVO für die Verarbeitung personenbezogener Daten gelten. In sieben Thesen werden datenschutzrechtliche Anforderungen formuliert, die bei der Entwicklung und dem Einsatz von KI-Systemen zu beachten sind, siehe auch Punkt 7.1.3.

Die digitale Lebenswelt wird in zunehmendem Maße auch durch die Erhebung und Auswertung biometrischer Daten geprägt sein. Daher hat die Konferenz das Positionspapier „Biometrische Analyse“[7] verabschiedet, in dem Empfehlungen zur datenschutzkonformen Gestaltung von biometrischen Verfahren gegeben werden, siehe Punkt 7.1.1.

Nach wie vor gilt es, die Zusammenarbeit der deutschen Datenschutzaufsichtsbehörden untereinander und mit den Aufsichtsbehörden der anderen Mitgliedstaaten zu optimieren. Auf dem Hambacher Schloss war auch dies ein zentrales Thema. Die Konferenz fasste eine Reihe von Beschlüssen zur Arbeitsweise ihrer Arbeitskreise und deren Zusammenarbeit mit den Gremien des Europäischen Datenschutzausschusses (EDSA).

In der 98. Datenschutzkonferenz im November 2019 in Trier wurde das Jahresthema „Künstliche Intelligenz“ erneut aufgegriffen. Die im Frühjahr verabschiedeten Thesen zur KI wurden mit einem ausführlichen Positionspapier[8] zum Thema untersetzt, siehe Punkt 7.1.3. In der Entschließung[9] zu diesem Papier bietet die Konferenz den Dialog mit den relevanten Akteuren aus Politik, Wirtschaft, Wissenschaft und Gesellschaft wie den Verbraucher-vereinigungen an, um die Entwicklung und den Einsatz von KI auch unter Nutzung personenbezogener Daten konstruktiv zu begleiten.

Ein weiterer Schwerpunkt der Herbstkonferenz war der Gesundheitsbereich. Angesichts der fortschreitenden Digitalisierung des Gesundheitswesens fordert die Datenschutzkonferenz in einer Entschließung[10], dass, unabhängig von der Größe medizinischer Einrichtungen, Patientendaten nach dem Stand der Technik geschützt werden. In einer weiteren Entschließung[11] fordert die Konferenz, dass Gesundheitswebseiten und -Apps die Erwartungen ihrer Nutzerinnen und Nutzer an Vertraulichkeit gewährleisten und bei der Weitergabe personenbezogener Daten datenschutzrechtliche Anforderungen einhalten.

6 https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/97-Ent-Hambacher_Erklärung_KI.pdf

7 https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Broschueren/Positionspapier_Biometrie.pdf

8 https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/20191106_Positionspapier_TOM_KI_Systeme.pdf

9 https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/20191106Ent_Gestaltung-KI_Systeme.pdf

10 https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/20191106_Ent_Gesundheitseinrichtungen_Patientendaten.pdf

11 https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/20191106_Ent_GesApps_Datenweitergabe_an_Dritte.pdf

Für den Einsatz von Messenger-Diensten im Krankenhausbereich wurden in einem „Whitepaper“[12] technische Anforderungen zusammengestellt, die als Grundlage weiterer Diskussionen dienen sollen, siehe Punkt 7.3.1.

Schließlich verabschiedete die Konferenz eine neue, nun vollständig an die DS-GVO angepasste Version des Standard-Datenschutzmodells (SDM)[13]. In ihrer Pressemitteilung[14] empfiehlt die Konferenz den Verantwortlichen in Wirtschaft und Verwaltung, das SDM bei Planung, Einführung und Betrieb von personenbezogenen Verarbeitungen anzuwenden, siehe Punkt 7.1.5.

Ein weiteres Konferenzdokument soll Verantwortliche bei der datenschutzkonformen Ausgestaltung der eigenen IT-Landschaft unterstützen. Die Konferenz verabschiedete in ihrer 98. Sitzung ein Prüfschema[15] zum Betriebssystem Windows 10. Das Prüfschema gibt Verantwortlichen die Möglichkeit, die datenschutzrelevanten Fragen im Zusammenhang mit dem Einsatz der Software, der Übertragung von Telemetriedaten sowie der Update-Konfiguration zu bewerten, siehe Punkt 7.1.2.

Wie schon in den vergangenen Jahren reichte die Zeit in den turnusmäßigen Datenschutzkonferenzen nicht aus, die Vielzahl der aktuellen datenschutzrelevanten Themen in Wirtschaft und Verwaltung zu besprechen. Daher war es auch in diesem Berichtsjahr erforderlich, Zwischenkonferenzen durchzuführen. Diese Konferenzen fanden im Januar in Berlin und im Juni und September in Mainz statt. In diesen Zwischenkonferenzen wurden vorwiegend verschiedene Aspekte der Umsetzung der DS-GVO beraten. So war beispielsweise zu klären, wie die Zusammenarbeit der Datenschutzkonferenz mit den spezifischen Aufsichtsbehörden etwa aus dem Bereich der Kirchen oder des öffentlich-rechtlichen Rundfunks zu organisieren ist. Weiterhin war ein Weg zu finden, wie die Datenschutzkonferenz die Europäische Kommission unterstützt, die bis zum 25. Mai 2020 dem Europäischen Parlament und dem Rat einen Bericht über die Bewertung und Überprüfung der DS-GVO vorlegen muss. Auch die Frage der Festlegung angemessener Bußgelder beschäftigte die Konferenz. Unter Federführung des Arbeitskreises Sanktionen wurde ein Bußgeldkonzept erarbeitet. Mit der Veröffentlichung dieses Konzeptes[16] zur Bemessung von Geldbußen soll ein Beitrag zur Transparenz im Hinblick auf die Durchsetzung des Datenschutzrechts geleistet werden. Es soll Verantwortliche und Auftragsverarbeiter in die Lage versetzen, die Entscheidungen der Aufsichtsbehörden nachzuvollziehen.

[12] https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/20191106_WP_%20Messenger_in_KrankenHaeusern.pdf
[13] https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V2.0a.pdf
[14] https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/20191106_PM_SDM.pdf
[15] https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/20191106_Bes_Win10_-Pruefschema.pdf
[16] https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf

5.2 AK Technik

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) hat den Arbeitskreis „Technische und organisatorische Datenschutzfragen“ (AK Technik) bereits 1981 gegründet, um Aktivitäten im technischen Bereich zu koordinieren. Die Datenschutzaufsichtsbehörden entsenden dorthin Spezialistinnen und Spezialisten aus der Informatik und angrenzenden Fachgebieten. Unserer Behörde schenkt die Datenschutzkonferenz bereits seit 1993 das Vertrauen, diesen Arbeitskreis zu leiten; wir berichteten zuletzt im Vierzehnten Tätigkeitsbericht unter Punkt 5.3. Auch im Berichtszeitraum 2019 bildete diese Aufgabe wieder einen Schwerpunkt unserer Tätigkeit.

Die bewährte halbjährliche Tagungsfrequenz haben wir beibehalten, sind jedoch ab der 73. Sitzung wegen des gestiegenen Diskussionsbedarfs bei technischen Themen zu einer Tagungsdauer von eineinhalb Tagen übergegangen. Beibehalten haben wir auch die Zusammenarbeit mit anderen Datenschutzaufsichtsbehörden aus dem deutschsprachigen Ausland und aus den großen Kirchen. Auf der 73. Sitzung waren erstmals die Rundfunkdatenschutzbeauftragten vertreten. Die Mitglieder und Gäste des AK Technik schätzen diesen Erfahrungsaustausch.

Die 72. Sitzung fand im Frühjahr 2019 in Saarbrücken beim Deutschen Forschungszentrum für Künstliche Intelligenz (DFKI) statt. Mit Vorträgen und Diskussionen von Forschern des DFKI konnten die Mitglieder Erkenntnisse zum Thema „Künstliche Intelligenz“ (KI) gewinnen, die sie in die Entschließung „Hambacher Erklärung zur Künstlichen Intelligenz“ und das „Positionspapier der Datenschutzkonferenz zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen“, siehe Punkt 7.1.3, eingebracht haben. Weitere Schwerpunkte der Sitzung bildeten die Themen E-Mail-Verschlüsselung, Windows 10, siehe Punkt 7.1.2, und Messenger-Dienste im Krankenhausbereich, siehe Punkt 7.3.1.

Zur 73. Sitzung im Herbst 2019 hatte der Landesbeauftragte für Datenschutz und Informationsfreiheit Sachsen-Anhalt nach Magdeburg eingeladen. Für Fachvorträge wurden diesmal Gäste aus Unternehmen und Bildungseinrichtungen in Sachsen-Anhalt eingeladen. So wurde über Methoden der Computer-Forensik informiert. Kenntnisse in diesen Bereichen helfen den Mitarbeiterinnen und Mitarbeitern der Datenschutzaufsichtsbehörden, bei Datenschutzverstößen sachgemäß Beweismittel sichern und auswerten zu können. In weiteren Vorträgen ging es um Datenschutzfragen beim Einsatz von Produkten zum Schutz von Computern vor Schadsoftware wie Computerviren und um Software zum Datenschutzmanagement. Anforderungen an die Verschlüsselung von E-Mails wurden erneut diskutiert. Da E-Mails in außerordentlich vielen verschiedenen Einsatzszenarien eingesetzt werden, konnte der AK Technik die Systematisierung der Anforderungen noch nicht abschließen. Zu Windows 10 konnten die Diskussionen fortgeführt und im Nachgang zur Sitzung vorläufig abgeschlossen werden, sodass die Datenschutzkonferenz in ihrer turnusmäßigen Herbstsitzung ein Prüfschema, siehe Punkt 7.1.2, beschließen und veröffentlichen konnte.

Zu den Anforderungen des Datenschutzes an Messenger-Dienste im Krankenhaus konnte ebenfalls eine gemeinsame Position gefunden werden, siehe Punkt 7.3.1. Besonders hervorzuheben ist jedoch der Abschluss der Arbeiten zur Version 2.0 des Standard-Datenschutzmodells (SDM), siehe Punkt 7.1.5. Die Datenschutzkonferenz hat die Ergebnisdokumente zu den beiden letztgenannten Punkten im Herbst 2019 angenommen und veröffentlicht.

5.3 IT-Planungsrat

Über den IT-Planungsrat (IT-PLR) und unsere Rolle als Vertreter der Landesdatenschutzbeauftragten in diesem wichtigen Gremium haben wir in den Tätigkeitsberichten der letzten Jahre regelmäßig berichtet, zuletzt im Vierzehnten Tätigkeitsbericht unter Punkt 5.4. Die Beratung des IT-PLR zu Datenschutzfragen hat weiter an Bedeutung gewonnen, da die Umsetzung des Digitalisierungsprogramms für die öffentliche Verwaltung von Bund, Ländern und Kommunen an Fahrt aufgenommen hat und erhebliche Herausforderungen für die Wahrung der Rechte und Freiheiten der von der Digitalisierung betroffenen Bürgerinnen und Bürger mit sich bringt. Nur durch frühzeitige Berücksichtigung datenschutzrechtlicher Anforderungen wird es möglich sein, die wichtigen Prinzipien des „Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ (Art. 25 DS-GVO) angemessen zu berücksichtigen.

5.3.1 Turnusmäßige Sitzungen

Im Berichtszeitraum haben wir an den drei turnusmäßigen Sitzungen des IT-PLR teilgenommen. Auch in den vorbereitenden Sitzungen auf der Ebene der Abteilungsleiter waren wir vertreten, übrigens regelmäßig durch Nutzung unserer Videokonferenzanlage. Unterstützt werden wir bei unserer Arbeit im IT-PLR durch weitere Kolleginnen und Kollegen anderer Datenschutzaufsichtsbehörden, die in verschiedenen nachgeordneten Gremien aktiv sind, siehe Punkt 5.3.2. Ein Schwerpunkt der Arbeiten des IT-PLR betrifft nach wie vor die Umsetzung des Online-Zugangsgesetzes (OZG) und das daraus resultierende Digitalisierungsprogramm. Um alle Verwaltungsleistungen in der vorgegebenen Zeit digital bereitstellen zu können, werden sie arbeitsteilig in 14 Themenfeldern von Bund, Ländern und Kommunen gemeinsam geplant und bearbeitet. Jedes Themenfeld wird dabei von jeweils einem fachlich zuständigen Bundesressort und mindestens einem Bundesland federführend bearbeitet. Wir berichten darüber regelmäßig in der Datenschutzkonferenz, damit die jeweils zuständigen Datenschutzaufsichtsbehörden die Bearbeitung der Themenfelder in ihrem Zuständigkeitsbereich aufmerksam beobachten und gegebenenfalls begleiten können.

5.3.2 Registermodernisierung

In ihrer Jahreskonferenz im Oktober 2018 haben die Regierungschefinnen und Regierungschefs der Länder den Beschluss gefasst, die Registermodernisierung unter Beteiligung der Länder umgehend zu starten und dabei den im Herbst 2017 vom Normenkontrollrat mit seinem Gutachten gesetzten Impuls zur Registermodernisierung aufzunehmen, um die bereits identifizierten Hindernisse für den Datenaustausch kurzfristig zu beseitigen (siehe dazu auch Vierzehnter Tätigkeitsbericht, Punkt 5.4). Die Ständige Konferenz der Innenminister und -senatoren der Länder (IMK) hat im November 2018 einen Beschluss gefasst, in dem das Bundesinnenministerium gebeten wird, unter Beteiligung des IT-Planungsrates eine geeignete Arbeitsstruktur unter Einbeziehung der Vorsitzenden des AK I und des AK II zum Thema verfahrensübergreifendes Identitätsmanagement als Teil der Registermodernisierung einzurichten. Daraufhin hat der IT-PLR in seiner 28. Sitzung im März 2019 das Koordinierungsprojekt „Registermodernisierung“ eingerichtet. Die Datenschutzkonferenz hat eine Kontaktgruppe aus Mitgliedern ihrer Arbeitskreise Grundsatz, Verwaltung und Technik eingerichtet, die das Koordinierungsprojekt beratend begleiten soll.

In diesem Projekt sollen Wege gefunden werden, wie die in der Verwaltung geführten Register modernisiert werden können und wie der Zugriff auf die dort gespeicherten personenbezogenen Daten vereinfacht werden kann. Eine zentrale Rolle spielen dabei sogenannte einheitliche, personenbezogene Identifikatoren. Die Datenschutzkonferenz hat in ihrer Entschließung vom September 2019[17] auf die Risiken und verfassungsrechtlichen Schranken einheitlicher und verwaltungsübergreifender Personenkennzeichen bzw. Identifikatoren hingewiesen. Sie lehnt derartige Personenkennzeichen zur direkten Identifizierung von Bürgerinnen und Bürgern ab und fordert alternative Methoden zur eindeutigen Identifizierung, etwa sektorspezifische Identifikatoren, die eine eindeutige Identifizierung zwar erlauben, einseitigen staatlichen Abgleich von Daten jedoch verhindern.

Im Koordinierungsprojekt „Registermodernisierung“ werden zurzeit noch zwei verschiedene Architekturmodelle des Zugriffs auf die in staatlichen Registern gespeicherten personenbezogenen Daten diskutiert: Der Architekturansatz „Einheitlicher Identifier“ und der Architekturansatz „Bereichsspezifischer Identifier“, der an das Prinzip des österreichischen Stammzahlensystems angelehnt ist. Unsere Aufgabe als Datenschutzaufsichtsbehörden ist es, darauf hinzuwirken, dass nur datenschutzgerechte und verfassungskonforme Architekturansätze ausgewählt und in die Praxis umgesetzt werden. Einheitliche, verwaltungsübergreifende Identifikatoren können diese Anforderungen jedenfalls nicht erfüllen.

Wir empfehlen der Landesregierung, sich dafür einzusetzen, dass bei der Modernisierung der Verwaltungsregister der verfassungskonforme Architekturansatz bereichsspezifischer Identifier in Anlehnung an das österreichische Stammzahlensystem umgesetzt wird und keine einheitlichen und verwaltungsübergreifenden Personenkennzeichen gebildet werden.

[17] https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/20190912_Ent_Digitalisierung_der_Verwaltung.pdf

6 Datenschutz und Bildung

6.1 Medienbildung

Seit nunmehr dem Elften Tätigkeitsbericht berichten wir über unsere unterschiedlichen Aktivitäten im Bereich der Medienbildung und Medienkompetenzförderung sowie der Sensibilisierung aller Altersgruppen zum datenschutzbewussten Umgang mit persönlichen Daten. Neben der Weiterführung aller Projekte[18] wurden weitere Initiativen gestartet[19].

Die Europäische Datenschutz-Grundverordnung (DS-GVO) weist unserer Behörde mit Art. 57 Abs. 1 lit. b verpflichtend die Aufgabe zu, die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung zu sensibilisieren und sie darüber aufzuklären. Ein besonderes Augenmerk soll dabei auf spezifische Angebote für Kinder und Jugendliche gelegt werden.

Medienkompetenz, verstanden als Lebenskompetenz, zu vermitteln ist auch weiterhin eine gesamtgesellschaftliche Aufgabe, die sich durch alle Bereiche unserer Bevölkerung zieht. Eine gelungene Medienbildung ermöglicht gesellschaftliche Teilhabe, trägt zur Demokratiebildung und Chancengleichheit bei. Die digitalisierte und mediatisierte Entwicklung durchdringt mehr und mehr alle Bereiche unserer Gesellschaft. Das umfasst nicht nur den Bereich Schule, sondern Medienkompetenz bedeutet „lebenslanges Lernen“, da die rasante Entwicklung von digitalen Geräten und Anwendungen in unserer medial geprägten Gesellschaft dies nötig macht. Die stetige Auseinandersetzung mit den Vor- und Nachteilen der digitalen Kultur ist Voraussetzung für eine aktive und selbstbestimmte Rolle in unserer Gesellschaft, und das in jedem Alter. Dabei ist es wichtig, Kindern und Jugendlichen Kompetenzen zu vermitteln, die einen selbstbestimmten und reflektierten Umgang mit Medien ermöglichen. In einer digital geprägten Kultur ist Medienkompetenz/Digitale Kompetenz eine erforderliche Voraussetzung für eine gelingende Persönlichkeitsentwicklung und die Entwicklung der Ausbildungs- und Erwerbsfähigkeit.

Positiv werten wir die zunehmende Sensibilisierung für das Thema der Förderung von Medienkompetenz/Digitaler Kompetenz. Allein durch die Verabschiedung der Strategie der Kultusministerkonferenz „Bildung in der digitalen Welt“ im Dezember 2017 hat das Thema der Vermittlung dieser Kompetenzen seit dem Berichtszeitraum 2018 einen höheren Stellenwert eingenommen; dies hat sich im Jahr 2019 fortgesetzt. Wir begrüßen diese Entwicklung. Mit Blick in die Zukunft wünschen wir uns ein weitgreifendes Verständnis für die Wichtigkeit der Förderung von Medienkompetenz/Digitaler Kompetenz.

Nach unserer Auffassung ist die Vermittlung von Datenschutzbewusstsein und Medienkompetenz/Digitaler Kompetenz weiterhin eine notwendige Zukunftsaufgabe unseres Landes. Im Einklang mit unserer gesetzlichen Aufgabe nach Art. 57 Abs. 1 lit. b DS-GVO übernehmen wir einen großen Bereich der Medienbildungsangebote im Land und initiierten ein umfangreiches Angebot in Kooperation mit zahlreichen außerschulischen Partnern.

---

[18] Tage ethischer Orientierung (TEO) - protect privacy: Dein Klick - Deine Verantwortung; Medienscouts MV; Medienaktiv M-V; Kooperationsvereinbarung zur Förderung von Medienkompetenz in M-V und die dazugehörigen AG’S „Frühkindliche Medienbildung“ und „Digitale Schule“

[19] „klicken-spielen-zappen“ modulare Fortbildungsreihe für Erzieher/innen;“ Jugend hackt“ in MV;

6.1.1 Datenschutz als Bildungsaufgabe

Unsere Angebote und Projekte werden weiterhin mit großer Nachfrage dankend von Kindertagespflege, Kindertageseinrichtungen, Schulen, der beruflichen Bildung bis hin zu den Universitäten und in Form von Weiterbildungen für pädagogisch Tätige im Land angenommen.

Die Verabschiedung der KMK-Strategie „Bildung in der digitalen Welt“ sowie die Zusage der Bundesförderung von Schulen und Schuleinrichtungen (der sogenannte Digi-Pakt), aber auch die verstärkten Bemühungen um Vermittlung von Medienkompetenz im frühkindlichen Bereich haben dazu geführt, dass die Nachfrage nach Schulungen deutlich zugenommen hat. Pädagogisch Tätige wollen in zunehmendem Maße die Anwendungsbeispiele und didaktischen Mittel erlernen, um mediale und digitale Kompetenzen an Kinder und Jugendliche weitergeben zu können. Das führte zu einer erhöhten Nachfrage von Schulen nach schulinternen Lehrerfortbildungen (SchiLF) und Fortbildungen für Erzieherinnen und Erzieher. Wir führen solche Fortbildungen schulartunabhängig durch und stellen den Pädagoginnen und Pädagogen mediendidaktisches Wissen und praktische Arbeitshilfen bereit, um sie in die Lage zu versetzen, Datenschutzbewusstsein zu vermitteln. Die SchiLF-Tage veranstalten wir landesweit.

Der Grundstein für einen alters- und zeitangemessenen Medienkonsum sowie ein Grundverständnis für die Funktionsweise von Medien werden im Kindesalter gelegt. Deshalb ist es wichtig, hier bereits Angebote zu schaffen und Kindern und Jugendlichen Kompetenzen zu vermitteln, die einen selbstbestimmten und reflektierten Umgang mit Medien ermöglichen. In einer digital geprägten Kultur ist Medienbildung eine erforderliche Voraussetzung für eine gelingende Persönlichkeitsentwicklung, für das Demokratieverständnis, für die gesellschaftliche Teilhabe und für die Entwicklung von Ausbildungs- und Erwerbsfähigkeit. Wir führten daher auch in diesem Berichtszeitraum Projekttage schulart- und altersunabhängig landesweit durch.

An den Universitäten Rostock und Greifswald hielten wir Vorlesungen, um angehenden pädagogischen Fachkräften mediendidaktisches Wissen und praktische Arbeitshilfen zur Umsetzung der KMK-Strategie „Bildung in der digitalen Welt“ zu vermitteln.

Den wachsenden Bedarf an Schulungsangeboten können wir zurzeit nicht decken, da unsere personellen Kapazitäten nicht ausreichen. Daher führen wir eine „Warteliste“. Die Wartezeit auf Schulungen beträgt derzeit mehr als sechs bis acht Monate. Wir decken derzeit in unserer Behörde den überwiegenden Teil dieser Veranstaltungen mit einer Mitarbeiterin ab. Sie ist zudem zuständig für die Organisation und tragende Rolle im landesweiten Netzwerk der Medienbildung Medienaktiv M-V, für das Medienscouts MV-Projekt sowie weitere Gemeinschaftsprojekte, siehe Punkte 6.1.4 ff.

Bei unseren Schulungen und Sensibilisierungen werden wir vor Ort vor allem unterstützt von der Landeskoordinierungsstelle für Suchtthemen Mecklenburg-Vorpommern (LAKOST MV), der Medienanstalt Mecklenburg-Vorpommern (MMV) mit den Medientreckern und Offenen Kanälen, dem Kompetenzzentrum und der Beratungsstelle für exzessive Mediennutzung und Medienabhängigkeit Schwerin der Evangelischen Suchtkrankenhilfe Mecklenburg-Vorpommern, dem Landeskriminalamt Mecklenburg-Vorpommern (LKA M-V) sowie von der ComputerSpielSchule Greifswald/Medienzentrum Greifswald e. V. Ohne die ganz wesentliche Vernetzung im Medienaktiv M-V wären eine so weitreichende Sensibilisierung und Schulung in unserem Bundesland nicht möglich.

Das Feedback der Teilnehmenden erlaubt ein positives Fazit unserer Schulungen. In den Datenschutz-Veranstaltungen geht es um die Gefahren im Netz, den Umgang mit den unterschiedlichen Medien sowie um die technischen und rechtlichen Rahmenbedingungen (DS-GVO, Persönlichkeitsrecht, Urheberrecht, Recht am eigenen Bild). Dabei verfolgen wir nicht den Ansatz der Reglementierung, sondern der gemeinsamen Exploration von Chancen und Risiken im Internet in Kombination mit den rechtlichen Vorgaben. Das Ziel unserer gemeinsamen Anstrengungen bleibt dabei grundsätzlich das Erlernen eines selbstbestimmten Umgangs mit digitalen Medien. Denn nur wer die damit einhergehenden Gefahren kennt, kann diesen kompetent begegnen. Nur wer die damit verbundenen Chancen kennt, kann diese zielsicher und unter Berücksichtigung der Belange Dritter nutzen. Da wir nach wie vor Unwissenheit über die technische, rechtliche und didaktische Vermittlung von Medienkompetenz und Datenschutzbewusstsein vorfinden, liegt in diesem Schulungsbereich der Schwerpunkt auf pädagogischen Implikationen und technisch relevantem Basiswissen. Alle anfragenden Einrichtungen sind nach eigenen Angaben froh über die Möglichkeit, auf das Expertenwissen unserer Behörde zugreifen zu können, und freuen sich über die niederschwellige Vermittlung von Wissen.

Neben den oben genannten Veranstaltungen führen wir auch regelmäßig Elternabende durch. Die Elternarbeit ist ein wichtiger Baustein für eine gelingende Medienbildung der Kinder und Jugendlichen. Um die Zielgruppe der Familien in den Blick zu nehmen, werden wir ab dem Jahr 2020 ein Projekt speziell für Eltern auflegen. Es soll ebenfalls durch die Nutzung des peer-to-peer-Ansatzes unter den Eltern für die notwendige Aufklärung sorgen.

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

Medienscouts MV

Das Medienscouts MV-Projekt (www.medienscouts-mv.de) startete bereits im Juni 2012 und wird seither unterstützt von der Landeskoordinierungsstelle für Suchtthemen Mecklenburg-Vorpommern (LAKOST MV), dem Landesjugendring Mecklenburg-Vorpommern e. V. (LJR M-V), dem Landeskriminalamt Mecklenburg-Vorpommern (LKA M-V), der Landesmedienanstalt Mecklenburg-Vorpommern (MMV) und deren Online-Selbsthilfe-plattform juuuport sowie der ComputerSpielSchule Greifswald (CSG). Die Konzeptidee liegt auf dem peer-to-peer-Ansatz. Jugendliche können mit dieser Methode ihr Wissen unmittelbar an andere Jugendliche (und bisweilen auch an Lehrer oder an Eltern) weitergeben. Im Rahmen dieses Projektes werden die Jugendlichen (8. - 10. Klasse) von Freitag bis Sonntag im konstruktiv-kritischen Umgang mit digitalen Medien fit gemacht. Im Berichtszeitraum fanden diese Ausbildungswochenenden in Greifswald und Schwerin statt. Die angehenden Medienscouts lernten dort eine Auswahl an methodischen Konzepten zur Umsetzung von Workshops, Vorträgen und Projekttagen kennen und konnten sich darin sofort üben. Das Expertenteam steht ihnen auch nach der Ausbildung dauerhaft zur Verfügung, um Hilfe und Unterstützung zu leisten. Einmal jährlich werden alle bereits ausgebildeten Medienscouts MV zu einem Update-Treffen eingeladen, um sich auszutauschen, neue Themen zu besprechen und Trends zu diskutieren.

Seit 2012 wurden in 15 Ausbildungswochenenden etwa 500 Medienscouts landesweit ausgebildet. Durch den peer-to-peer-Ansatz ist es dem Gemeinschaftsprojekt möglich, das Wissen zu multiplizieren. Jährlich erreichen die Medienscouts MV rund 4 000 Schülerinnen und Schüler.

Dieses bundesweit beachtete Projekt wird nur dann dauerhaft erfolgreich sein, wenn die strukturelle, organisatorische und wirtschaftliche Basis für diese außerschulische Kooperation mindestens erhalten bleibt. Das in unserem Land praktizierte Kooperationsmodell mit vielen sehr unterschiedlichen und vor allem außerschulischen Kooperationspartnern genießt nach wie vor eine bundesweite Aufmerksamkeit. Das Projekt wird durch Mittel sowohl des Landes als auch des Landeskriminalamtes Mecklenburg-Vorpommern und der Medienanstalt Mecklenburg-Vorpommern finanziert. Die finanzielle Ausstattung des Projektes Medienscouts MV ist seit 2012 gleichbleibend. Jeder Schülerin und jedem Schüler wird eine kostenfreie Teilnahme garantiert. Auf diese Weise können auch Jugendliche aus finanzschwächeren Familien teilnehmen.

Auch das Interesse Erwachsener (Lehrkräfte, Schulsozialarbeiterinnen bzw. Schulsozialarbeiter) an unseren Veranstaltungen nimmt ständig zu. Nach den Ausbildungswochenenden entstehen dadurch insbesondere im Rahmen von Ganztagsangeboten an den Schulen Arbeitsgemeinschaften, sogenannte Medienscouts MV-AGs, in denen sich Jugendliche und Erwachsene regelmäßig treffen und Projekttage planen. Der zusätzliche Aufwand für beide Gruppen ist nicht zu unterschätzen. Wir würden uns sehr wünschen, dass dem ehrenamtlichen Engagement der Jugendlichen und betreuenden Erwachsenen angemessen Beachtung geschenkt wird.

Die gleichbleibend hohen Teilnehmerzahlen zeigen ein ungebrochenes Interesse an dem Projekt. Seit dem Jahr 2018 werden pro Durchgang bereits zehn Teilnehmende mehr als früher ausgebildet. Dennoch gibt es Wartelisten, und interessierte Jugendliche müssen auf den nächst folgenden Ausbildungslehrgang vertröstet werden. Mit der derzeitigen Teilnehmerzahl hat das Projekt die Grenze des Möglichen erreicht. Weder wir noch unsere Kooperationspartner verfügen über die strukturellen und finanziellen Voraussetzungen, um beispielsweise die Zahl der Ausbildungsdurchgänge zu erhöhen oder zielgruppenspezifisch (etwa für Berufsschülerinnen und Berufsschüler) anzupassen.

Um den Informationsaustausch zwischen allen Beteiligten des Medienscouts MV-Projektes zu optimieren, möchten wir eine datenschutzgerechte Kommunikationsplattform (Medienscout App) bereitstellen (siehe auch Dreizehnter Tätigkeitsbericht, Punkt 4.1.1). Durch die Bereitstellung von Geldern aus dem Strategiefond Mecklenburg-Vorpommern waren wir im Berichtszeitraum in der Lage, die hierfür erforderliche Ausschreibung zu erstellen. Im Laufe des Jahres 2020 sollen der Zuschlag erteilt werden und die Programmierung beginnen.

TEO - Tage ethischer Orientierung: Das Modul „protect privacy - Mein Klick, meine Verantwortung!?“

„Tage ethischer Orientierung“ (www.teo.nordkirche.de) ist ein schulkooperatives Modell der Nordkirche, das in Kooperation mit unserer Behörde durchgeführt wird. Das Format ist speziell für die 5. und 6. Klassen konzipiert. Es handelt sich hier ebenfalls nach „unserer Tradition“ um ein Gemeinschaftsprojekt. Wir werden unterstützt von überregional bekannten Referenten der LAKOST MV, dem Kompetenzzentrum und Beratungsstelle für exzessive Mediennutzung und Medienabhängigkeit Schwerin der Evangelischen Suchtkrankenhilfe Mecklenburg-Vorpommern sowie der ComputerSpielSchule Greifswald. Seit 2013 wurden rund 500 Schülerinnen und Schüler der 5. und 6. Klassen sowie Lehrerinnen und Lehrer in Mecklenburg-Vorpommern geschult. Dieses 4-tägige Modul ist konzipiert, um Inhalte der Handlungsfelder „Datenspuren im Netz, soziale Netzwerke, Cybermobbing, Apps, Smartphones, Handys und Computerspiele“ zu vermitteln und gemeinsam mit den Teilnehmenden die Möglichkeiten verantwortlicher Nutzung digitaler Medien zu erarbeiten.

Alle genannten Projekte sollen fortgeführt werden. Auch die außerschulischen Partner benötigen dafür verlässliche finanzielle und personelle Rahmenbedingungen.

6.1.3 Netzwerk Medienaktiv M-V

Das landesweite Netzwerk für Medienbildung in Mecklenburg-Vorpommern Medienaktiv M-V wird vom Landesjugendring Mecklenburg-Vorpommern e. V., der Landeskoordinierungsstelle für Suchtthemen Mecklenburg-Vorpommern, dem Landeskriminalamt Mecklenburg-Vorpommern, dem Kompetenzzentrum und Beratungsstelle für exzessive Mediennutzung und Medienabhängigkeit Schwerin der Evangelischen Suchtkrankenhilfe Mecklenburg-Vorpommern, der Landesmedienanstalt Mecklenburg-Vorpommern und unserer Behörde organisiert. Mittlerweile ist dieses Netzwerk bundesweit beispielgebend, da sich hier Sucht-hilfe, Jugendhilfe, Medienpädagogik, Polizei, Schule und Datenschutzbeauftragter gemeinsam und auf Augenhöhe engagieren. Nach unseren Erkenntnissen aus bundesweiten Arbeitsgruppen haben sich jedoch auch die anderen Bundesländer auf dem Weg gemacht, sich institutions-übergreifend zu vernetzen, und treiben Konzepte zur Medienkompetenzvermittlung aktiv voran. Möchte das Land Mecklenburg-Vorpommern weiterhin seine bundesweite Vorreiter-rolle behalten, bedarf es entsprechender Maßnahmen der Landesregierung.

Das Netzwerk Medienaktiv M-V ist offen gegenüber neuen Mitgliedern. Grundsätzlich sind alle Mitglieder im Netzwerk kooperationsfördernd gleichberechtigt und bringen ihre Kompetenzen in die Netzwerkarbeit ein. Medienaktiv M-V soll helfen, Partner für neue und vorhandene Projekte, Angebote, Ideen und gemeinsames Auftreten in der Öffentlichkeit zu den Themen des Netzwerkes zu finden. Das Netzwerk wird von vielen außerschulischen Partnern der Medienarbeit in Mecklenburg-Vorpommern unterstützt. Dazu gehören beispielsweise Medienwerkstätten, freie Medienpädagoginnen und Medienpädagogen, der LAG Medien e.V. sowie der Rat für Kriminalitätsvorbeugung Mecklenburg-Vorpommern, die Eltern- und Schülervertretungen des Landes sowie Vereine und Verbände, wie der Unternehmerverband Mecklenburg-Vorpommern.

Um auch weiterhin den politischen Diskurs zu begleiten, fand im Jahr 2019 die Frühjahrstagung des Netzwerkes im Landtag Mecklenburg-Vorpommern statt. Als Netzwerk wollen wir auch hier den Weg des Landes Mecklenburg-Vorpommern medienpolitisch begleiten. Nach Einschätzung der Partner und Akteure des Netzwerkes Medienaktiv M-V könnte eine vierte Fortschreibung der „Kooperationsvereinbarung zur Förderung der Medienkompetenz in Mecklenburg-Vorpommern“, ergänzend zur Digitalen Agenda, als Gesamtstrategie des Landes hochwertig durch das Netzwerk begleitet werden.

Die Herbsttagung des Netzwerkes stand unter dem Schwerpunkt der Beruflichen Bildung. Unter dem Titel „Bereit für die digitalisierte (Arbeits)Welt?“ fand die Tagung im Regionalen Beruflichen Bildungszentrum Müritz in Kooperation mit dem Unternehmerverband Mecklenburg-Vorpommern statt. Die angebotenen Workshops hatten das Ziel, Medienkompetenz/Digitale Kompetenz als Unterrichtsinhalte in der Beruflichen Bildung zu vermitteln. Sie waren für Berufsschullehrerinnen und Berufsschullehrer didaktisch aufbereitet.

Das Netzwerk macht die Vielfalt der Medienangebote unseres Bundeslandes besser wahrnehmbar, und es ist für weitere Partner aus dem Bereich der Medienbildung und der Vermittlung von digitalen Kompetenzen stets offen. Auf diese Weise vergrößern wir die Chance, mit unseren Medienthemen relevante Zielgruppen zu erreichen. Das Netzwerk ist ein Wissenspool, der es ermöglicht, uns gegenseitig zu qualifizieren und auf dem Laufenden zu halten. Die Akteure des landesweiten Netzwerkes Medienaktiv M-V brachten ihre Erfahrungen und ihr Know-How in den Erfahrungsbericht zur „Kooperationsvereinbarung zur Förderung von Medienkompetenz in Mecklenburg-Vorpommern“ ein. Wir haben uns bei dem Erfahrungsbericht zur Kooperationsvereinbarung aktiv eingebracht und begleiten die Neuschreibung.

Um das Netzwerk einheitlich zu präsentieren, wurde im Jahr 2019 die Website www.medienaktiv-mv.de überarbeitet.

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

Aus der Kampagne „Medien-Familie-Verantwortung“ (siehe Dreizehnter Tätigkeitsbericht, Punkt 4.1.4), die bereits im Herbst 2016 mit der Plakatkampagne „Heute schon mit Ihrem Kind gesprochen?“ gestartet war, ist ein modularer Fortbildungskurs entstanden. Das gesamte Projekt wird von der Landeskoordinierungsstelle für Suchtthemen Mecklenburg-Vorpommern (LAKOST MV) koordiniert. Gemeinsam wurden zwei Plakatmotive sowie eine City Card entworfen und landesweit verteilt. Die Plakate haben seit Erscheinen eine so große Nachfrage deutschlandweit, dass diese Plakate inzwischen auch in anderen Bundesländern gedruckt werden. Die Plakatmotive aus Mecklenburg-Vorpommern sind somit deutschlandweit bekannt.

Im weiteren Verlauf des Projektes wurde es mit Unterstützung des Verbandes der Ersatzkassen e. V. (vdek) möglich, eine Fortbildungsreihe für Erzieherinnen und Erzieher zu konzipieren, die im Januar 2018 startete und für die Jahre 2018, 2019 und 2020 durch die Finanzierung des vdek gesichert werden konnte. Wir sind intensiv an der Vorbereitung und Durchführung der modularen Fortbildung beteiligt. Auch hier liegt die Projektleitung beziehungsweise Koordination in den Händen der LAKOST MV. Projektpartner sind unsere Behörde, das Kompetenzzentrum und Beratungsstelle für exzessiven Mediengebrauch und Medienabhängigkeit, das Medienzentrum Greifswald e. V., die Medienwerkstatt raabatz der RAA Waren und die Bildungsstätte Schabernack, Zentrum für Praxis und Theorie der Jugendhilfe, Güstrow.

In acht Modulen werden unter anderem Themen wie Einflüsse der Medienaneignung, Mediennutzung in den Familien, Aufgreifen von Medienerlebnissen in der Kita sowie motivierende Elterngespräche behandelt und medienpädagogische Angebote entwickelt. Im Jahr 2019 wurde das Projekt durch den vdek evaluiert. Obwohl die Vermittlung von Medienkompetenz im frühkindlichen Bereich mit dem neuen Kindertagesförderungsgesetz Mecklenburg-Vorpommern (KiföG M-V) verpflichtend geregelt wurde, ist noch nicht absehbar, ob das Projekt auch über das Jahr 2020 hinaus weitergeführt werden kann.

Im Dreizehnten Tätigkeitsbericht haben wir unter Punkt 4.1.3 über die Arbeitsgemeinschaft „Frühkindliche Medienbildung“ berichtet. In diesem Berichtszeitraum haben wir den Text der 3. Säule eines Kapitels zur Vermittlung von Medienbildung und -erziehung abschließend erarbeitet. Dieses Kapitel wird die Bildungskonzeption der 0-10-Jährigen in Mecklenburg-Vorpommern ergänzen und wird im Jahr 2020 veröffentlicht.

6.1.5 Jugend hackt & Hello World

Bereits im Jahr 2018 fand das erste „Jugend hackt“-Event in Schwerin statt.[20] Das Projekt wurde vom Landesjugendring Mecklenburg-Vorpommern e. V. (LJR M-V) initiiert und von Beginn an von uns personell und finanziell unterstützt. Im Jahr 2019 wurde „Jugend hackt“ in Rostock durchgeführt.[21] Erstmals haben wir parallel auch „Hello World“ als die Einsteigervariante angeboten. Dies konnten sowohl interessierte Medienscouts MV als auch andere interessierte Kinder und Jugendliche ab 10 Jahren nutzen.

Die Idee von Jugend hackt ist es, jungen Menschen Fähigkeiten im Bereich der Informationstechnik zu vermitteln und sie dabei zu unterstützen, sich mit ihren Ideen als Teil der modernen Gesellschaft zu erleben. Das Programm „Hello World“ ermöglicht Kindern und Jugendlichen die ersten Schritte bei der Mitgestaltung ihrer digitalen Lebenswelt. An dem Wochenende ging es für die „Hello World“-Teilnehmer um niedrigschwellige und kreative Zugänge zu Themenfeldern rund um Technik, Robotik und Coding.[22]

[20] https://jugendhackt.org/event-rueckblick/schwerin-2018/
[21] https://jugendhackt.org/event-rueckblick/rostock-2019/
[22] https://www.hellohelloworld.org/chapters/mecklenburg-vorpommern

Wir haben auch dieses Wochenende aktiv begleitet und die Kooperation zu den Medienscouts MV sowie dem Hackspace in Rostock und dem Hacklabor Schwerin hergestellt. Die finanzielle und personelle Absicherung der Projekte „Jugend hackt“ und „Hello World“ ist jedoch nicht gesichert. Aus diesem Grund ist es fraglich, inwieweit wir diese technisch orientierten Programme in Mecklenburg-Vorpommern fortführen können.

Wir teilen die Auffassung des Europäischen Parlaments und des Rates, dass die digitale Kompetenz als eine der acht Schlüsselkompetenzen für das lebenslange Lernen notwendig ist.[23] Diese Kompetenz besteht im sicheren und kritischen Umgang mit den gesamten digitalen Technologien, die für die Information, Kommunikation und die Problemlösungsstrategien in allen Lebensbereichen genutzt werden. Die digitale Kompetenz ist als eine übergreifende Kompetenz anzunehmen. Sie hilft dabei, andere Kompetenzen zu meistern, wie beispielsweise Kommunikation, Demokratiebildung und Sprachkenntnisse. Um das Wesentliche dieser Kompetenz besser zu verstehen, hat die Europäische Kommission den Europäischen Referenzrahmen für digitale Kompetenzen (DigComp 2.0: The Digital Competence Framework for Citizens) entwickelt.[24]

Im Zeitalter der Digitalisierung ist es sicher wichtig, dass alle Bürgerinnen und Bürger ein Grundverständnis und Wissen zur Programmierung erlernen und weiterentwickeln. Dabei ist aber nicht davon auszugehen, dass alle Menschen komplexe Programme schreiben können müssen. Menschen sollten jedoch grundsätzlich verstehen, wie Programmierung funktioniert. Auch aus diesem Blickwinkel ist es wünschenswert, dass dieses Projekt weitergeführt wird.

6.1.6 Freiwilliges Soziales Jahr „Demokratie/Politik“ - ein Erfahrungsbericht

Seit einiger Zeit bieten wir jungen Leuten an, ein Freiwilliges Soziales Jahr „Demokratie/Politik“ in unserer Dienststelle zu absolvieren (siehe dazu auch Vierzehnter Tätigkeitsbericht, Punkt 6.14). Wir haben „unserem FSJler“ auch in diesem Jahr die Möglichkeit gegeben, mit dem folgenden Text über seine Arbeit im aktuellen Tätigkeitsbericht zu informieren:

Meine Aufgaben beim Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern sind sowohl Verwaltungstätigkeiten, wie das Schreiben und Beantworten von E-Mails, das Führen von Telefonaten, das Pflegen von Listen, als auch die Recherche zu relevanten Themen. Insbesondere gehört auch die Begleitung des Projektes „Medienscouts MV“ dazu.

Seit einiger Zeit stellen die Projektkoordinierenden des „Medienscouts MV“-Projektes fest, dass die Kommunikationswege mit den ausgebildeten Medienscouts verbessert werden müssen. Es ist schwierig, die Jugendlichen nach dem Ausbildungswochenende über E-Mail zu erreichen, da dies nicht ihrem Kommunikationsverhalten entspricht.

[23] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32006H0962&from=EN
[24] https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/digcomp-20-digital-competence-framework-citizens-update-phase-1-conceptual-reference-model

Um bei diesem Problem Abhilfe zu schaffen, wurden dem Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern zusätzliche finanzielle Mittel zur Verfügung gestellt, um eine App entwickeln zu lassen. In die Recherche und die Arbeitsgespräche zu der Entwicklung dieser App war ich ebenfalls involviert. Nach Vorgesprächen mit Firmen aus Mecklenburg-Vorpommern und dem Abwägen der Vor- und Nachteile haben wir uns jedoch entschieden, keine native App entwickeln zu lassen, sondern eine progressive Web-App. Eine solche Web-App ist vorteilhaft, weil sie kostengünstiger ist, die Wartung einfacher ist und weil sie auf allen aktuellen und zukünftigen Betriebssystemen läuft.

Auch die Vorbereitung und Durchführung von Projekten über Informatische Grundbildung von Schülerinnen und Schülern der 4. – 6. Klasse gehört zu meinen Aufgaben. Hierfür überlege ich mir interessante Möglichkeiten, jüngeren Kindern mit dem Calliope mini, einem Einplatinen-Computer für pädagogische Zwecke, erste Kenntnisse des Programmierens beizubringen. Außerdem beschäftige ich mich mit dem Raspberry Pi, einem komplexeren Einplatinen-Computer, um etwas älteren Schülern informatische Kenntnisse, explizit erste Linux-Kenntnisse, beizubringen.

Bei Veranstaltungen, wie Tagungen, Planungstreffen, Ausschüssen des Landtags und Arbeitsgesprächen, bin ich dabei und unterstütze, wenn möglich, bei der Organisation und Vorbereitung. Dadurch habe ich viele Einblicke in die Verwaltung und Politik des Landes Mecklenburg-Vorpommern erhalten. Des Weiteren habe ich durch Gespräche mit Kollegen aus der IT-Abteilung viele neue IT-Kenntnisse erwerben können.

7 Technik und Organisation

7.1 Neue Technologien

7.1.1 Positionspapier Biometrische Analyse

Im Berichtszeitraum hat die Datenschutzkonferenz das Positionspapier „Biometrische Analyse“ verabschiedet[25]. Dieses Papier wurde von einer Arbeitsgruppe der Datenschutzkonferenz erarbeitet, die wir leiten, siehe Vierzehnter Tätigkeitsbericht, Punkt 7.1.2. Im Positionspapier erläutern die Datenschutzaufsichtsbehörden, unter welchen Voraussetzungen bestimmte Verfahren zur Verarbeitung biometrischer Daten datenschutzkonform betrieben werden können.

Das Papier konzentriert sich auf solche Verfahren, die in der Praxis und in der Datenschutzkontrolle besonders relevant sind. Betrachtet werden unter anderem Anwendungen von Fingerabdrucklesern zur Bezahlung und zur Zugangskontrolle, biometrische Gesichtserkennung für Werbezwecke oder Videoüberwachungsanlagen. Zur korrekten Beschreibung und Einordnung der biometrischen Systeme sowie deren Teile und Funktionen greift das Papier auf die Begriffe und Ansätze der internationalen Norm ISO/IEC 2382-37 („Information Technology - Vocabulary - Part 37: Biometrics“) zurück.

[25] https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Broschueren/Positionspapier_Biometrie.pdf

Das Positionspapier zeigt, dass sich die bereits im Vierzehnten Tätigkeitsbericht skizzierte Rechtsansicht durchgesetzt hat: Sowohl biometrische Samples als auch biometrische Merkmale sind als biometrische Daten (Art. 4 Nr. 14 DS-GVO) einzustufen. Als biometrische Samples bezeichnet man die analogen oder digitalen Repräsentationen biometrischer Charakteristika vor der biometrischen Merkmalsextraktion. Dazu gehören Bilder von Gesichtern von Menschen auf Fotopapier oder in Bild- oder Videodateien oder Fingerabdrücke. Qualität und Auflösung dieser Daten müssen jedoch dazu ausreichen, die Identität einer Person ermitteln oder bestätigen zu können. Biometrische Merkmale hingegen sind die Zahlen oder markanten Kennzeichen, die aus einem biometrischen Sample extrahiert wurden und zum Vergleich verwendet werden können. Dies sind beispielsweise die aus dem Gesichtsbild gewonnenen Messwerte für den Abstand und die Lage der Augen oder die aus einem Abbild der Linienstrukturen eines Fingerabdruckes ermittelten Daten über die Lage von Endungen und Verzweigungen dieser Linien.

Bei der Verarbeitung jeglicher Art von personenbezogenen Daten ist stets Art. 6 DS-GVO zu beachten. Dies gilt auch für biometrische Daten. Wenn Verantwortliche jedoch biometrische Auswertungen zur Identifikation von Personen beabsichtigen und über die technischen Mittel dafür verfügen, sind zusätzlich die strengeren Voraussetzungen des Art. 9 DS-GVO einzuhalten. So ist der Betrieb einer Videoüberwachungsanlage ohne biometrische Funktionen zur Ausübung des Hausrechts nach Art. 6 DS-GVO zu beurteilen. Hingegen sind für eine Zugangskontrolleinrichtung mit Fingerabdrucklesern die Artikel 6 und 9 DS-GVO einschlägig.

Zu beachten ist in jedem Fall, dass von einer Verarbeitung biometrischer Daten spezielle Risiken für die betroffenen Personen ausgehen können. Zielt eine biometrische Auswertung beispielsweise lediglich auf eine Geschlechts- oder Altersklassifikation ohne Identifikation ab, so besteht grundsätzlich das Risiko, dass eine Identifikationsfunktion missbräuchlich zum System hinzugefügt oder darin aktiviert wird. Solche Risiken können zur Unzulässigkeit der Verarbeitung führen. Dies ist im privaten Bereich der Fall, wenn die Interessen der betroffenen Person die des Verantwortlichen oder Dritten, in dessen Interesse die Verarbeitung liegt, überwiegen (Art. 6 Abs. 1 lit. f DS-GVO). Im öffentlichen und privaten Bereich sind die genannten Risiken bei der Auswahl und Umsetzung von technischen und organisatorischen Datenschutzmaßnahmen nach Art. 32 DS-GVO zu berücksichtigen. Können die Risiken nicht hinreichend eingedämmt werden, ist die Verarbeitung unzulässig.

Auch der Europäische Datenschutzausschuss (EDSA) hat sich im Berichtszeitraum mit diesen Fragen beschäftigt. Er kommt in den „Guidelines 3/2019 on processing of personal data through video devices“ (in englischer Sprache[26]) zu den gleichen Ergebnissen (siehe dort Abschnitt 5).

Wir empfehlen Verantwortlichen in Wirtschaft und Verwaltung, vor dem Einsatz von Verfahren zur Verarbeitung biometrischer Daten zu prüfen, ob die Verarbeitung die Zulässigkeitsvoraussetzungen des Art. 6 DS-GVO erfüllt und ob die zusätzlichen, strengeren Voraussetzungen des Art. 9 DS-GVO eingehalten werden können, und dabei die Empfehlungen des Positionspapiers „Biometrische Analyse“ zu berücksichtigen.

[26] https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-32019-processing-personal-data-through-video_en

7.1.2 Windows 10

Kurz nach Ende des Berichtszeitraumes läuft der reguläre Support von Microsoft für das Betriebssystem Windows 7 aus. Microsoft positioniert Windows 10 als Nachfolger von Windows 7. Für die Anwenderschaft stellte und stellt sich jedoch die Frage, ob sie Windows 10 datenschutzgerecht einsetzen kann. Hierbei sind die Datenübermittlungen von Windows 10 an Microsoft von besonderer Bedeutung. Deshalb hat die Datenschutzkonferenz auf ihrer Herbstsitzung 2019 ein Prüfschema zu Windows 10 herausgegeben, anhand dessen Anwenderinnen und Anwender die Datenschutzkonformität ihres konkreten Einsatzfalls beurteilen können[27]. Der Hauptteil des Prüfschemas enthält rechtliche Hinweise, technische Fragen werden im Anhang[28] behandelt.

Die Frage, ob Windows 10 datenschutzkonform ist, kann nicht pauschal beantwortet werden. Windows 10 ist eine Produktfamilie, bei der das eigentliche Betriebssystem nur noch einen Teil der Funktionalität ausmacht. Beispielsweise sind der Sprachassistent Cortana und die Anti-Virus-Software Windows Defender im Lieferumfang enthalten. Durch Updates können neue Funktionen hinzukommen.

Windows-10-Installationen übermitteln zu verschiedenen Gelegenheiten Daten an Microsoft. Hierunter befinden sich insbesondere Daten, welche von Microsoft als Telemetrie- oder Diagnosedaten bezeichnet werden. Welche Daten genau übermittelt werden, hängt von der eingesetzten Edition, den Konfigurationseinstellungen, den genutzten Funktionen und der Einsatzumgebung ab. Allein durch Änderung der Konfiguration lässt sich die Datenübermittlung an Microsoft nicht komplett abschalten. Außerdem kann sich auch das Kommunikationsverhalten von Windows 10 mit jedem Update ändern.

Um prüfen zu können, ob Windows 10 im konkreten Anwendungsfall datenschutzgerecht eingesetzt werden kann, muss eine Aufstellung darüber vorliegen, welche Verarbeitungstätigkeiten unter Nutzung von Windows 10 durchgeführt werden und welche personenbezogenen Daten dort in welchem Umfang verarbeitet werden. Außerdem müssen Erkenntnisse darüber vorliegen, welche personenbezogenen Daten für welche Zwecke an Microsoft übermittelt werden. Dies wird in dem vorliegenden Prüfschema näher erläutert.

Es zeigt sich, dass der Einsatz von Windows 10 mit rechtlichen Risiken verbunden ist, die man nur durch aufwändige technische Maßnahmen in den Griff bekommen kann. Der Einsatz von Bordmitteln reicht dazu in den meisten Fällen nicht aus.

Das Prüfschema betrifft nur Windows 10 Enterprise, wobei der Telemetrie-Level auf die Stufe „Security“, den geringstmöglichen Datentransfer zu Microsoft, gesetzt wird. Die Stufe „Security“ ist jedoch nur bei Windows 10 Enterprise verfügbar. Andere Editionen übermitteln deutlich mehr Daten an Microsoft, was das Problem für die Anwender verschärft.

[27] https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/20191106_Bes_Win10_-Pruefschema.pdf

[28] https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/20191106_Bes_Win_10_-Pr%C3%BCfschema_Anlage.pdf

Die Datenschutzaufsichtsbehörden aus Bund und Ländern stehen weiter mit Microsoft im Dialog, um ihre Bewertung der Windows-10-Produktfamilie abschließen zu können.

Vorläufig empfehlen wir den Verantwortlichen, genau zu prüfen, ob sie die beim Einsatz von Windows 10 entstehenden Risiken beherrschen können. Falls nicht, sollten andere Betriebssysteme in Betracht gezogen werden. Zu möglichen Alternativen gehört auch, Windows 7 mit zusätzlich verlängertem Support von Microsoft zu nutzen. Diese Option bietet Microsoft kostenpflichtig für ausgewählte Editionen bis Anfang Januar 2023 an. Sie beinhaltet die Auslieferung von als kritisch oder wichtig eingestuften Sicherheits-Updates. Spätestens dann stellt sich auch für die Kunden, die diese Option gewählt haben, die Frage nach der Zulässigkeit des Einsatzes von Windows 10 erneut.

Wir empfehlen den Verantwortlichen, genau zu prüfen, ob sie die beim Einsatz von Windows 10 entstehenden Risiken beherrschen können. Falls nicht, sollten andere Betriebssysteme, insbesondere aus dem Open Source Bereich, in Betracht gezogen werden.

7.1.3 Datenschutzaspekte Künstlicher Intelligenz

Der Vorsitzende der Datenschutzkonferenz hatte das Thema „Datenschutzrelevante Aspekte Künstlicher Intelligenz“ als Arbeitsschwerpunkt für das Jahr 2019 gewählt, siehe Punkt 5.1. Die Konferenz rief im Frühjahr 2019 eine Taskforce ins Leben, die sich mit den speziellen Anforderungen Künstlicher Intelligenz (KI) befassen sollte. Wir waren als Vorsitzender des AK Technik, siehe Punkt 5.2, in die Taskforce berufen worden, weil vorrangig technische und organisatorische Maßnahmen erarbeitet werden sollten, die bei der Entwicklung und dem Betrieb von KI-Systemen erforderlich sind.

Ein erstes Zwischenergebnis legte die Taskforce der 97. Datenschutzkonferenz im Frühjahr 2019 vor. Auf der Basis dieses Zwischenergebnisses verabschiedete die Konferenz die „Hambacher Erklärung zur Künstlichen Intelligenz“, siehe Punkt 5.1. Diese Erklärung verdeutlicht, dass Entwicklungen und Anwendungen von KI in demokratisch-rechtsstaatlicher Weise den Grundrechten entsprechen müssen und dass auch für KI-Systeme die Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 DS-GVO) gelten. In sieben Thesen fordert die Konferenz, dass KI

- Menschen nicht zum Objekt machen darf,
- nur für verfassungsrechtlich legitimierte Zwecke eingesetzt werden und das Zweckbindungsgebot nicht aufheben darf,
- transparent, nachvollziehbar und erklärbar sein muss,
- Diskriminierungen vermeiden muss,
- dem Grundsatz der Datenminimierung folgen muss,
- Verantwortlichkeit braucht und
- technische und organisatorische Standards benötigt.

Im Laufe des Jahres 2019 war die Taskforce gefordert, das Thesenpapier zu einem aussagekräftigen Positionspapier weiterzuentwickeln. Zur 98. Datenschutzkonferenz im Herbst 2019 legte die Taskforce das Arbeitsergebnis vor und die Konferenz verabschiedete das „Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen“[29].

[29] https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/20191106_Positionspapier-_TOM_KI_Systeme.pdf

In diesem Positionspapier werden die Lebenszyklen Design, Veredelung der Rohdaten zu Trainingsdaten, Training, Validierung der Daten, Einsatz und Nutzung sowie Rückkopplung von Ergebnissen und Selbstveränderung von KI-Systemen betrachtet, um die Risiken für die Rechte und Freiheiten der von KI-Verfahren betroffenen natürlichen Personen zu identifizieren. Diese Risiken hängen maßgeblich vom Einsatz-Szenario sowie von den verwendeten KI-Komponenten ab. Problematisch aus datenschutzrechtlicher Sicht ist die Tatsache, dass KI-Systeme in vielfältiger und teils nur schwer erkennbarer, vorhersehbarer oder beweisbarer Art und Weise derartige Risiken darstellen können. Dennoch gilt auch hier der Grundsatz, dass nachvollziehbar sein muss, welche Daten verarbeitet wurden, welche Programme und Systeme zum Einsatz kommen und wie diese organisatorisch in die Verarbeitungstätigkeit eingebunden sind. Die speziellen Funktionsweisen der unterschiedlichen KI-Komponenten müssen erklärt werden können.

Im Hauptteil des Positionspapiers werden technische und organisatorische Anforderungen definiert, orientiert an den oben genannten Lebenszyklen von KI-Systemen. Zur Strukturierung der Anforderungen der jeweiligen Lebenszyklen dienen die Gewährleistungsziele des Standard-Datenschutzmodells, siehe Punkt 7.1.5.

In ihrer Entschließung „Empfehlungen für eine datenschutzkonforme Gestaltung von KI-Systemen“[30] erläutert die Datenschutzkonferenz, dass mit dem Positionspapier den Verantwortlichen im Umfeld von KI ein Handlungsrahmen für die datenschutzrechtlichen Vorgaben an die Hand gegeben wird, an dem sie sich bei der Planung und dem Betrieb von KI-Systemen orientieren können. Die Konferenz legt dieses Positionspapier auch vor, um den Dialog mit den relevanten Akteuren aus Politik, Wirtschaft, Wissenschaft und Gesellschaft wie den Verbrauchervereinigungen auf dieser Grundlage weiter zu intensivieren.

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.

7.1.4 Microsoft Office 365

Bereits im Vierzehnten Tätigkeitsbericht haben wir unter Punkt 7.1.4 über die neuen Entwicklungen bei Microsoft berichtet. Microsoft hatte den Betrieb der Deutschland-Cloud eingestellt und ab dem 1. September 2018 keine Neuverträge mehr zu diesem Modell abgeschlossen. Damit hatten sich die vertraglichen Grundlagen so grundlegend geändert, dass der Arbeitskreis Verwaltungsmodernisierung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder nicht umhin kam, die neuen Vertragsunterlagen zu prüfen. In der dafür eingerichteten Unterarbeitsgruppe arbeiten wir aktiv mit.

[30] https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/20191106_Ent_Gestaltung_KI_Systeme.pdf

Der inhaltliche Ausgangspunkt der Unterarbeitsgruppe war die Prüfung der Unterlagen zur Auftragsverarbeitung, die Microsoft zur Verfügung gestellt hatte. Das Modell der Auftragsverarbeitung ist in der Europäischen Datenschutz-Grundverordnung (DS-GVO) normiert. Die Unterarbeitsgruppe betrachtete die Konstellation, dass öffentliche Stellen in ihrer Eigenschaft als Verantwortliche im Sinne der DS-GVO als Auftraggeber und Microsoft als Auftragsverarbeiter handeln. Nach dem Austausch von verschiedenen Schriftsätzen und nach Gesprächen mit Microsoft Deutschland über die Vertragsunterlagen wurde deutlich, dass die Differenzen der datenschutzrechtlichen Bewertungen hinsichtlich der Verarbeitung sowohl der sogenannten Telemetriedaten als auch der Inhaltsdaten nicht ausgeräumt waren. Es zeichnete sich ab, dass eine Lösung für die unterschiedlichen Probleme kurzfristig nicht zu finden war.

Für die Unterarbeitsgruppe sehr überraschend kündigte die Microsoft Corporation (Redmond, USA) im November 2019 an, die Vertragsunterlagen zur Auftragsverarbeitung umzugestalten. Microsoft Corporation gab öffentlich bekannt, dass sie in Zukunft selbst als Verantwortlicher für die Datenverarbeitung bezüglich einiger Teilaspekte in der Auftragsbearbeitung auftreten will. Aufgabe der Unterarbeitsgruppe wird es daher sein, die nun abermals neuen Vertragsunterlagen datenschutzrechtlich zu prüfen und hinsichtlich der Geeignetheit des Einsatzes von Microsoft Office365 für den öffentlichen Bereich zu bewerten. Angesichts der Komplexität und des Umfangs der Unterlagen muss davon ausgegangen werden, dass die Prüfung einen längeren Zeitraum erfordern wird.

Wir empfehlen den Verantwortlichen in Wirtschaft und Verwaltung, entweder die Einführung von Microsoft Office365 solange zurückzustellen, bis die rechtlichen Rahmenbedingungen geklärt sind, oder den Einsatz anderer Produkte, insbesondere aus dem Open Source Bereich, zu prüfen.

7.1.5 Standard-Datenschutzmodell (SDM)

Im Vierzehnten Tätigkeitsbericht haben wir unter Punkt 7.1.5 über die Version 1.1 des Standard-Datenschutzmodells (SDM) berichtet und die Weiterentwicklung in Aussicht gestellt. Schon damals war zu erkennen, dass eine noch engere Bindung an die Europäische Datenschutz-Grundverordnung (DS-GVO) erforderlich sein wird. Folgerichtig hat die 95. Datenschutzkonferenz im April 2018 eine Arbeitsgruppe des AK Technik beauftragt, das SDM weiterzuentwickeln. Im September legte die Arbeitsgruppe das Ergebnis der Überarbeitung zunächst dem AK Technik vor, der den Entwurf des vollständig überarbeiteten SDM einstimmig verabschiedete. Im November 2019 verabschiedete die 98. Datenschutzkonferenz dann einstimmig die Version 2.0 des Standard-Datenschutzmodells[31] mit der vollständigen Bezeichnung „Das Standard- Datenschutzmodell - Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele (Version 2.0)“. In der Pressemitteilung zum SDM[32] empfiehlt die Datenschutzkonferenz den Verantwortlichen in Wirtschaft und Verwaltung, das SDM bei Planung, Einführung und Betrieb von personenbezogenen Verarbeitungen anzuwenden. Anwenderinnen und Anwender werden gebeten, den Datenschutzaufsichtsbehörden ihre Erfahrungen bei der Nutzung des SDM mitzuteilen, um zu einer stetigen Verbesserung des Modells beizutragen.

[31] https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V2.0a.pdf
[32] https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/20191106_PM_SDM.pdf

Die Version 2.0 des SDM hat eine völlig neue Gliederung erhalten. Im Teil A wird das SDM beschrieben, Teil B enthält die Anforderungen der DS-GVO, die mit dem SDM umgesetzt werden können, Teil C systematisiert die Anforderungen der DS-GVO durch die Gewährleistungsziele, Teil D gibt Hinweise zur Umsetzung des SDM in der Praxis und Teil E beschreibt einige organisatorische Rahmenbedingungen der Anwendung des SDM.

Eine neue Qualität hat das SDM unter anderem dadurch bekommen, dass im Abschnitt B die zentralen datenschutzrechtlichen Anforderungen der DS-GVO zusammengetragen und im Teil C den einzelnen Gewährleistungszielen zugeordnet wurden. Zur neuen Qualität trägt auch der vollständig überarbeitete Teil D bei, der neben den schon bekannten und weiter vervollständigten generischen Maßnahmen ausführliche Erläuterungen zum Risikobegriff enthält und das Verhältnis der Begriffe Risiko und Schutzbedarf klärt. Zudem wurde in den Teil D ein neues Kapitel zum Datenschutzmanagement aufgenommen, in dem eine Methode erläutert wird, mit der systematisch alle Anforderungen des Datenschutzrechts in einer Organisation umgesetzt werden können. Ergänzt wurde das SDM schließlich um ein Kapitel im Teil E, in dem das Zusammenwirken von SDM und BSI-Grundschutz erläutert wird.

Die Überarbeitung des SDM hat die Kapazitäten der kleinen Arbeitsgruppe des AK Technik über eine lange Zeit vollständig gebunden, sodass die Weiterentwicklung des Referenzmaßnahmen-Katalogs zunächst zurückgestellt werden musste. Während des Berichtszeitraumes konnten daher noch keine neuen Bausteine des Katalogs entwickelt werden. Für die Anwendung des SDM in der Praxis stellt das jedoch kein unüberwindbares Hindernis dar, weil mit dem Katalog der generischen Maßnahmen ein niederschwelliger Einstieg in das SDM ermöglicht wird, vergleichbar mit der Basisabsicherung des BSI-Grundschutzes. Inzwischen hat die SDM-Arbeitsgruppe des AK Technik die Erarbeitung des Referenzmaßnahmen-Katalogs wieder aufgenommen. Im Frühjahr 2020 sollen weitere Bausteine veröffentlicht werden.

Wir wiederholen unsere Empfehlung an die Landesregierung aus dem Vierzehnten Tätigkeitsbericht, bei der Einrichtung und beim Betrieb von personenbezogenen Verarbeitungstätigkeiten die im Standard-Datenschutzmodell (SDM) beschriebene Vorgehensweise anzuwenden und das dort beschriebene Datenschutzmanagement-System einzurichten.

7.1.6 MV-Serviceportal - das Tor zur digitalen Verwaltung

„Bund und Länder sind verpflichtet, bis spätestens zum Ablauf des fünften auf die Verkündung dieses Gesetzes folgenden Kalenderjahres ihre Verwaltungsleistungen auch elektronisch über Verwaltungsportale anzubieten.“ So lautet der erste Satz des Online-Zugangsgesetzes (OZG). Damit hat der Bundesgesetzgeber auch das Land Mecklenburg-Vorpommern vor die anspruchsvolle Aufgabe gestellt, seine Verwaltungsdienstleistungen zu digitalisieren. Den elektronischen Zugang zu diesen Dienstleistungen soll das MV-Serviceportal ermöglichen. In die Planungen zu diesem Portal sind wir seit Mitte 2018 einbezogen (siehe Vierzehnter Tätigkeitsbericht, Punkt 7.1.3).

Wiederholt haben wir auf das Erfordernis einer tragfähigen Rechtsgrundlage als Voraussetzung für den Betrieb des Portals durch das Ministerium für Energie, Infrastruktur und Digitalisierung Mecklenburg-Vorpommern hingewiesen.

Erst am Tag der Freischaltung des MV-Serviceportals im Juni 2019 informierte uns das Ministerium über den Start des Wirkbetriebs des Portals. Diese Information hat uns überrascht, denn die Beratungen zum Projekt waren noch nicht abgeschlossen und zahlreiche rechtliche und technische Grundsatzfragen noch ungeklärt. Nach wie vor waren die Passagen des OZG nicht umgesetzt, durch die das Ministerium als diejenige öffentliche Stelle bestimmt wird, die den Nutzern die Einrichtung eines Nutzerkontos anbietet und die die Registrierung von Nutzerkonten vornehmen darf (§ 7 Abs. 1 und 2 OZG). Auch lagen zum Zeitpunkt des Freischaltens weder das Verzeichnis der Verarbeitungstätigkeiten noch das Datenschutz- und IT-Sicherheitskonzept, die Vereinbarungen zu gemeinsamen Verantwortlichkeiten oder eine Datenschutz-Folgenabschätzung (DSFA) vor. Zudem war die im Portal online bereitgestellte Datenschutzerklärung fehlerhaft und führte unter anderem dazu, dass die von den Nutzern eingeholten Einwilligungen nicht den Anforderungen der Europäischen Datenschutz-Grundverordnung (DS-GVO) genügten und somit unwirksam waren.

Wir haben das Ministerium auf diese gravierenden Mängel hingewiesen und um Mitteilung gebeten, welche kurzfristigen Schritte unternommen werden, um einen datenschutzkonformen Betrieb des MV-Serviceportals zu gewährleisten. Zudem haben wir gefordert, die bereits online verfügbare Datenschutzerklärung und die Einwilligungserklärung für das Nutzerkonto-MV unverzüglich zu überarbeiten.

Nachdem das Ministerium innerhalb der folgenden acht Wochen nicht auf unsere Hinweise reagiert hatte, sahen wir uns gezwungen, von unseren aufsichtsrechtlichen Befugnissen nach Art. 58 DS-GVO Gebrauch zu machen. Wir haben das Ministerium gemäß Art. 58 Abs. 1 lit. a DS-GVO formell angewiesen, uns die angeforderten Unterlagen bereitzustellen und eine Reihe von Fragen zu beantworten. Erst nach der Androhung, den Betrieb des Portals gemäß Art. 58 Abs. 2 lit. f DS-GVO zu untersagen und nach formeller Anhörung nach § 28 Verwaltungsverfahrensgesetz Mecklenburg-Vorpommern (VwVfG M-V) reagierte das Ministerium, stellte einen Teil der angeforderten Unterlagen zur Verfügung und bat um einen Gesprächstermin.

Bis zu diesem Gesprächstermin war zwar die Datenschutzerklärung im Portal überarbeitet worden. Die rechtlichen Rahmenbedingungen für den Betrieb des Portals waren aber nach wie vor strittig. Das Ministerium war der Auffassung, das Portal auch ohne Umsetzung des OZG betreiben zu dürfen und dies auf die Einwilligung der Nutzer zu stützen. Wir hielten es jedoch für erforderlich, die vom OZG geforderte Rechtsgrundlage zu schaffen.

Inzwischen liegt der Entwurf zum Zweiten Gesetz zur Änderung des E-Government-Gesetzes Mecklenburg-Vorpommern vor. Er enthält die erforderliche Regelung zum OZG, einschließlich einer Bestimmung, wonach die Landesregierung ein Verwaltungsportal mit bestimmten Komponenten als kostenlosen E-Government-Basisdienst anbieten darf. Das Gesetz sieht nämlich eine Verordnungsermächtigung vor, in der die Einrichtung und Registrierung von Nutzerkonten im Portal geregelt werden sollen. Der Zeitplan zur Behandlung des Gesetzentwurfs im Kabinett und im Parlament verdeutlicht jedoch, dass mit dem Inkrafttreten nicht vor April 2020 zu rechnen ist. Wann mit der angekündigten Verordnung zu rechnen ist, bleibt offen. Damit wird das MV-Serviceportal auch weiterhin auf einer sehr fragwürdigen Rechtsgrundlage betrieben. Denn nach unserer Auffassung sollte es nicht sein, dass eine vorhandene Rechtsvorschrift, hier das OZG, zumindest zeitweise umgangen wird, indem die Verarbeitung personenbezogener Daten im Portal lediglich auf die Einwilligung der Betroffenen gestützt wird.

Wir wiederholen unsere Empfehlung aus dem Vierzehnten Tätigkeitsbericht, die erforderlichen Rechtsgrundlagen für die Einrichtung und Registrierung von Nutzerkonten zu schaffen und die datenschutzrechtlichen Verantwortlichkeiten zwischen den am Verfahren Beteiligten zu klären. Bis zum Inkrafttreten des Zweiten Gesetzes zur Änderung des E-Government-Gesetzes und dem Erlassen der vorgesehenen Rechtsverordnung empfehlen wir eine Übergangsregelung, etwa einen Kabinettsbeschluss.

7.1.7 Elektronische Akte (eAkte)

Bereits seit dem Jahr 2016 begleiten wir beratend die Einführung der elektronischen Akte (eAkte) in den Behörden Mecklenburg-Vorpommerns, siehe dazu auch Dreizehnter Tätigkeitsbericht, Punkt 5.1.5.

Der rechtliche Rahmen wurde hierfür bereits im April 2016 mit dem „Gesetz zur Förderung der elektronischen Verwaltungstätigkeit in Mecklenburg-Vorpommern“ (E-Government-Gesetz Mecklenburg-Vorpommern - EGovG M-V) geschaffen. Das Gesetz hatte zunächst alle Landesbehörden verpflichtet, ihre Akten ab dem 1. Januar 2020 elektronisch zu führen, soweit nicht wichtige Gründe entgegenstehen. Offensichtlich war die Komplexität des Projektes jedoch unterschätzt worden. Der recht ambitionierte Termin war nicht zu halten. Der Entwurf eines Zweiten Gesetzes zur Änderung des Gesetzes zur Förderung der elektronischen Verwaltungstätigkeit in Mecklenburg-Vorpommern (EGovG M-V) sieht nun vor, dass die elektronische Aktenführung in den Landesbehörden ab dem 1. Januar 2023 mit einem einheitlichen informationstechnischen System erfolgen soll.

Die eAkte sollte dabei auf den Erfahrungen aufbauen, die es im Umgang mit dem elektronischen Dokumentenmanagement- und Vorgangsbearbeitungssystem „DOMEA®“ in den Ministerien und der Staatskanzlei bereits seit vielen Jahren gibt, siehe dazu auch Zehnter Tätigkeitsbericht, Punkt 4.3.2. Die Planungen sahen vor, einen Anforderungskatalog zu erarbeiten, welcher die wesentlichen Bedarfe der künftigen Nutzerinnen und Nutzer aus den unterschiedlichen Behörden berücksichtigt. Außer Frage steht, dass mit einem umfassenden eAkte-System auch zahlreiche personenbezogene Daten verarbeitet werden, sowohl von den Bürgerinnen und Bürgern als auch von den Anwendern und Betreibern des Systems selbst.

Dies erfordert umfassende technische und organisatorische Maßnahmen gemäß Art. 24 Abs. 1 Europäische Datenschutz-Grundverordnung (DS-GVO), die ebenfalls im Anforderungskatalog berücksichtigt werden müssen. Wir haben schon zum Projektbeginn im Jahr 2016 auf diese Anforderungen der DS-GVO hingewiesen, da absehbar war, dass diese Verordnung beim Start des neuen Systems anzuwenden ist.

Im Verlauf der Planungsphase kam es aus unterschiedlichsten Gründen immer wieder zu Verzögerungen und Änderungen im Anforderungskatalog, die letztendlich darin mündeten, dass bis Ende 2019 noch immer kein einheitliches eAkte-System gefunden wurde. Dies führt neben der oben erwähnten Terminverschiebung dazu, dass das eigentlich zu ersetzende Dokumentenmanagement- und Vorgangsbearbeitungssystem DOMEA® nun über die ursprünglich geplante Zeit hinaus betrieben wird und bei der Landespolizei und in einigen weiteren Behörden übergangsweise sogar neu eingeführt werden muss, ehe ein geeigneter Nachfolger gefunden ist. Dabei sind Änderungen im bestehenden DOMEA®-System unausweichlich, um den geänderten Rechtsgrundlagen und neuen Anforderungen, die sich aus der fortschreitenden Digitalisierung der öffentlichen Verwaltung ergeben (siehe hierzu auch Punkt 7.1.5), Rechnung zu tragen.

Sowohl bei der Planung und Einführung des neuen eAkte-Systems als auch bei der „Neueinführung“ der eAkte in Form von DOMEA®, beispielsweise in den nachgeordneten Polizeibehörden des Landes Mecklenburg-Vorpommern, stehen wir auch weiterhin beratend zur Seite.

7.1.8 Wenn kein sicheres Passwort verwendet wird

Regelmäßig weisen wir darauf hin, dass im digitalen Zeitalter die Wahl eines sicheren Passwortes unabdingbar ist. Denn wer sich bei einem Onlinedienst unberechtigt für einen anderen Nutzer anmelden kann, nimmt auch dessen Identität an und handelt in seinem Namen. Sämtliche Fehlhandlungen werden in der Regel dann zuerst dem eigentlichen Accountinhaber angerechnet.

Wir erhielten den Hinweis eines Bürgers, dass er sich bei einem Onlineportal, in dem die für einen Dienst in Anspruch genommenen Leistungen eingesehen werden können, ohne größeren Aufwand auch für andere Kunden anmelden konnte. Der Auslöser war hierbei das vom Betreiber des Onlineportals vergebene Standardpasswort „password“, welches bei der ersten Anmeldung am Portal auch nicht geändert werden musste. Zudem haben viele Nutzer zwar einen standardmäßigen Zugang zum Portal, eine Anmeldung jedoch nie vorgenommen. Dementsprechend wurden bei vielen Accounts auch keine Passwortänderungen durchgeführt.

Die Europäische Datenschutz-Grundverordnung (DS-GVO) fordert in Artikel 32 technische und organisatorische Maßnahmen, um die Sicherheit der Verarbeitung personenbezogener Daten zu gewährleisten. Die Vergabe eines derart schwachen Initialpasswortes, welches dann auch noch für alle Nutzer gleich ist, verstößt gegen diese Anforderungen. Ein dem Stand der Technik entsprechendes Passwortmanagement hätte an dieser Stelle ein individuelles und sicheres Initialpasswort vorgesehen.

Wir haben umgehend den Kontakt zu dem Betreiber des Portals aufgenommen, welcher uns daraufhin zugesagt hat, sein Passwortmanagement anzupassen. Zum Ende des Berichtszeitraumes waren im ersten Schritt alle Nutzer zu Fragen der Passwortsicherheit sensibilisiert und es begann parallel dazu die Überarbeitung des Passwortvergabeverfahrens. So sollen künftig individuelle und sichere Passwörter an die Kunden verteilt und die Möglichkeit, unsichere Passwörter verwenden zu können, ausgeschlossen werden.

Tipps zur sicheren Passwortgestaltung:
- je länger desto sicherer, mindestens acht, besser aber 10 bis 12 Zeichen oder mehr
- alle verfügbaren Zeichen, beispielsweise Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen (Leerzeichen, ?!%+…), verwenden
- Passwörter nicht mehrfach verwenden, sondern für jeden Dienst ein eigenes nutzen
- Passwörter niemals an andere weitergeben
- wenn möglich eine 2-Faktor-Authentifizierung nutzen, um die Sicherheit weiter zu erhöhen; neben dem Passwort ist hierfür ein weiteres Zugangsmerkmal wie eine SMS oder TAN erforderlich
- ggf. einen Passwortmanager nutzen, um die unterschiedlichen Passwörter zu verwalten

Wir empfehlen Verantwortlichen in Wirtschaft und Verwaltung, ein geeignetes Passwortmanagement aufzubauen und es einem regelmäßigen Revisionsprozess zu unterwerfen. Bei bereits vorhandenem Passwortmanagement sollte geprüft werden, ob es dem Stand der Technik entspricht.

7.1.9 Meldung einer Datenpanne

Im August des Berichtszeitraumes erreichte uns eine Meldung der Verletzung des Schutzes personenbezogener Daten nach Art. 33 Europäische Datenschutz-Grundverordnung (DS-GVO), besser bekannt als die Meldung einer Datenpanne.

Hierbei wurde uns von einem IT-Dienstleister mitgeteilt, dass die Daten eines Kunden aufgrund einer vorgenommenen Fehlkonfiguration über einen Zeitraum von ca. 5 Monaten hinweg von außen einsehbar waren. Unsere Ermittlungen ergaben, dass von dieser Datenpanne ca. 250 000 Nutzer betroffen waren. Zugänglich waren Datensätze wie Geburtsdatum und E-Mail-Adresse, teilweise auch Anschriften und Telefonnummern. Zu den betroffenen Daten gehörten zudem die Passwörter, die verschlüsselt hinterlegt waren. In 3 % der Fälle, also immerhin noch bei ca. 7.500 Nutzern, waren sie jedoch mit einem nicht dem Stand der Technik entsprechenden Verfahren verschlüsselt worden. Es musste daher davon ausgegangen werden, dass diese Passwörter entschlüsselt und für Angriffe gegen Nutzer verwendet werden können. Das Risiko für Betroffene war besonders hoch, wenn sie das Passwort mehrfach, also auch für andere Portale, verwendet haben. Der in diesem Fall sorglose Umgang mit Passwörtern unterstreicht einmal mehr, wie wichtig es ist, für unterschiedliche Dienste auch unterschiedliche Passwörter zu verwenden. Tipps zum Umgang und der richtigen Auswahl von Passwörtern geben wir auch unter Punkt 7.1.8.

Wir haben umgehend das von der Datenpanne betroffene Unternehmen kontaktiert und eine schnelle Unterrichtung der betroffenen Personen angeregt sowie weitere Abhilfemaßnahmen empfohlen. Außer Frage steht, dass die Sicherheit der Verarbeitung von personenbezogenen Daten nicht gemäß den Vorgaben von Art. 32 DS-GVO gewährleistet wurde. Erschwerend kam hinzu, dass uns sowohl von dem Unternehmen als Auftraggeber, also dem für die Datenverarbeitung Verantwortlichen (Art. 4 Nr. 7 DS-GVO), als auch von dem meldenden Dienstleister als Auftragsverarbeiter kein Auftragsverarbeitungsvertrag[33] nach Art. 28 Abs. 3 DS-GVO vorgelegt werden konnte, in dem die Rechte und Pflichten beider Parteien und damit die Umsetzungen der datenschutzrechtlichen Anforderungen geregelt sind.

Gemäß Art. 5 Abs. 2 DS-GVO liegt die Gesamtverantwortung für die Datenverarbeitung sowie die Nachweispflicht beim Verantwortlichen; sie umfasst auch die Verarbeitung durch den Auftragsverarbeiter. Da das betroffene Unternehmen seine Hauptniederlassung in Frankreich betreibt, lag die Zuständigkeit für die weiteren Untersuchungen und für die Einleitung eines möglichen Bußgeldverfahrens jedoch bei der französischen Aufsichtsbehörde, der Commission Nationale de l'Informatique et des Libertés (CNIL). Wir haben daher die erforderlichen Verfahrensschritte unternommen und die CNIL über das europäische Binnenmarkt-Informationssystem (IMI) unterrichtet, siehe dazu auch Vierzehnter Tätigkeitsbericht, Punkt 4.3. Zum Abschluss des Berichtszeitraumes lagen uns noch keine Erkenntnisse darüber vor, welche Maßnahmen die CNIL getroffen hat und ob gegebenenfalls ein Bußgeldverfahren eingeleitet wurde.

7.2 Zertifizierung nach der DS-GVO

In den Artikeln 42 und 43 Europäische Datenschutz-Grundverordnung (DS-GVO) werden einheitliche Akkreditierungs- und Zertifizierungsverfahren geregelt. Zertifikate können Verantwortlichen helfen, ihrer Rechenschaftspflicht in verschiedenen Konstellationen einfacher nachzukommen, siehe dazu auch das Kurzpapier Nr. 9 der Datenschutzkonferenz[34]. Das Vorliegen von DS-GVO-konformen Zertifikaten kann beispielsweise als Faktor herangezogen werden, um die Erfüllung der Pflichten des für die Verarbeitung Verantwortlichen nachzuweisen (Art. 24 Abs. 3 DS-GVO). Zudem können Verantwortliche Zertifikate nutzen, um im Zusammenhang mit Datenübermittlungen in ein Drittland nachzuweisen, dass dort geeignete Garantien zur Wahrung der Rechte und Freiheiten betroffener Personen vorhanden sind (Art. 46 Abs. 2 lit. f DS-GVO). Auch Auftragsverarbeiter können von der Einhaltung eines genehmigten Zertifizierungsverfahrens profitieren. Sie können Zertifikate nutzen, um etwa nachzuweisen, dass sie selbst und gegebenenfalls ihre Unterauftragsverarbeiter geeignete technische und organisatorische Maßnahmen durchführen (Art. 28 Abs. 5 DS-GVO).

[33] https://www.datenschutz-mv.de/static/DS/Dateien/DS-GVO/Kurzpapiere/Kurzpapier_Nr_13.pdf
[34] https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Kurzpapiere/Kurzpapier_Nr_9.pdf

Die Durchführung von datenschutzspezifischen Zertifizierungen ist ein mehrstufiges Verfahren. Gemäß Art. 43 DS-GVO erteilen sogenannte Zertifizierungsstellen die oben genannten Zertifikate. Das Bundesdatenschutzgesetz (BDSG) legt in § 39 fest, dass die jeweils zuständige Datenschutzaufsichtsbehörde von Bund oder Ländern die Befugnis erteilt, als Zertifizierungsstelle tätig zu werden. Diese Erlaubnis dürfen die Aufsichtsbehörden erst dann erteilen, wenn die Deutsche Akkreditierungsstelle (DAkkS) die künftige Zertifizierungsstelle, allerdings im Einvernehmen mit den Datenschutzaufsichtsbehörden, auf der Grundlage eines Konformitätsbewertungsprogramms akkreditiert hat. Dieser komplexe Vorgang erfordert eine intensive Zusammenarbeit zwischen den Aufsichtsbehörden und der DAkkS. Eine zwischen allen Datenschutzaufsichtsbehörden und der DAkkS geschlossene Kooperationsvereinbarung regelt die Bereitstellung von Fachpersonal durch die Aufsichtsbehörden.

Um das gesamte Verfahren gemeinsam mit der DAkkS zu planen und zu konzipieren, hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) bereits im Mai 2016 eine Arbeitsgruppe gegründet. Seit Juni 2016 tagt diese Arbeitsgruppe regelmäßig mit dem vorrangigen Ziel, die Erarbeitung des Akkreditierungsprozesses zu unterstützen.

Zu den wesentlichen Aufgaben der Aufsichtsbehörden im Akkreditierungs- und Zertifizierungsprozess gehören die Fachprüfung von Konformitätsbewertungsprogrammen und den entsprechenden Zertifizierungskriterien, die Fachbegutachtung der Zertifizierungsstellen, die Beteiligung an der Akkreditierung als Mitglied des Akkreditierungsausschusses (AKA) und die oben genannte Erteilung der Befugnis, als Zertifizierungsstelle im Rahmen des akkreditierten Programms tätig zu werden. Inzwischen hat die DAkkS die ersten Konformitätsbewertungsprogramme und die entsprechenden Zertifizierungskriterien an die Aufsichtsbehörden zur Fachprüfung übergeben.

Die gemeinsam mit der DAkkS erarbeiteten Akkreditierungskriterien wurden inzwischen von der Datenschutzkonferenz beschlossen. Sofern Zertifikate im Sinne einer einheitlichen Anwendung der DS-GVO in allen Mitgliedstaaten anerkannt werden sollen, ist eine internationale Abstimmung (Kohärenzverfahren nach Art. 63 DS-GVO) erforderlich. Diese Abstimmung auf europäischer Ebene wird demnächst in entsprechenden Stellungnahmeverfahren starten.

Wir empfehlen Verantwortlichen, sich frühzeitig mit dem Thema Zertifizierung vertraut zu machen. Zertifikate bieten das Potenzial, sich bei Verarbeitungsvorgängen (etwa bei Auftragsverarbeitung oder Cloudstrukturen) Klarheit darüber zu verschaffen, ob die gesetzlichen Datenschutzanforderungen eingehalten werden.

7.3 Kommunikation/Neue Medien

7.3.1 Messenger-Dienste im Krankenhaus

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) hat im Berichtszeitraum das Whitepaper „Technische Anforderungen an Messenger-Dienste im Krankenhaus“ verabschiedet. Das Papier soll als Grundlage für Gespräche mit Verbänden im Krankenhausbereich dienen. Es wurde federführend vom Unterarbeitskreis „Digitalisierung im Gesundheitswesen“ erarbeitet, der von den Arbeitskreisen „Gesundheit und Soziales“ und „Technik“ der Datenschutzkonferenz getragen wird.

Messenger-Dienste haben parallel zur Verbreitung von Smartphones in den letzten Jahren zentrale Bedeutung für den Austausch von Nachrichten erlangt. Sie haben andere Kommunikationsdienste wie E-Mail oder SMS vielfach ersetzt und zählen im privaten Alltag zu den beliebtesten Kommunikationsformen. Deshalb wird auf diese Messenger-Dienste auch im Gesundheitsbereich zunehmend zurückgegriffen, häufig verbunden mit der Nutzung eines privaten Endgerätes.

Der berufliche oder gewerbliche Einsatz von Messenger-Diensten unterliegt gesetzlichen Datenschutzvorgaben, denen gängige Messenger-Dienste bislang nicht oder nur bedingt entsprechen. Insbesondere der verbreitet genutzte Dienst WhatsApp führt bei einer geschäftlichen Nutzung zu einer Reihe von Problemen, die einen Einsatz im Krankenhaus weitgehend ausschließen. Ähnliches gilt für andere im privaten Bereich häufig genutzte Dienste.

Die im Papier beschriebenen Anforderungen beziehen sich vorrangig auf die eigentliche Messenger-Applikation, die Kommunikation zwischen den Teilnehmern, die genutzte Plattform sowie die eingesetzten Endgeräte. Der eigentliche Betrieb von Messenger-Diensten im Krankenhaus findet nur insoweit Berücksichtigung, als dass es sich um allgemeine Anforderungen handelt. Dies ist der Tatsache geschuldet, dass die Einsatzbedingungen in den Krankenhäusern erfahrungsgemäß sehr heterogen sind. Das Whitepaper geht insbesondere auf folgende Einzelaspekte ein:

Verlangt wird beispielsweise, dass man die Messenger-Applikation nur nach zusätzlicher Authentifikation nutzen kann. Es darf also nicht ausreichen, das Gerät lediglich zu entsperren. Die Kontaktdaten des Messengers müssen separat verwaltet werden; sie dürfen nicht mit denen anderer Apps vermischt sein.

Inhalts- und Verkehrsdaten müssen regelmäßig gelöscht werden. Insbesondere auf den Endgeräten muss dies automatisiert geschehen. Längerfristige Speicherungen von personenbezogenen Daten von Patienten sind nur auf den Servern des Krankenhauses oder seiner Auftragsverarbeiter zulässig.

Unbedingt erforderlich ist auch, dass der Messenger eine Ende-zu-Ende-Verschlüsselung unterstützt. Die Daten des Messengers müssen darüber hinaus auch auf dem verwendeten Endgerät verschlüsselt gespeichert werden. Es ist sicherzustellen, dass das Endgerät regelmäßig mit Sicherheits-Updates versorgt wird. Hierzu ist erforderlich, dass der Hersteller der Betriebssystemplattform die verwendete Version des Betriebssystems aktuell pflegt, dass der Gerätehersteller die vom Betriebssystemhersteller gelieferten Patches kurzfristig an das Gerät anpasst und ausliefert und dass die Anwenderinnen und Anwender diese Patches unverzüglich einspielen.

Wegen der besonderen Schutzbedürftigkeit der verarbeiteten Daten müssen die Endgeräte in ein Mobile Device Management (MDM) eingebunden sein. Mit einer solchen Lösung kann der für die Verarbeitung Verantwortliche überprüfen, ob das Endgerät den Sicherheitsvorgaben genügt. Kann das MDM die Einhaltung dieser Vorgaben nicht erzwingen, so löscht es bei Verstößen oder Verlust automatisch relevante Daten auf dem Endgerät.

Beim Einsatz eines MDM sind deshalb auch Fragen des Arbeitnehmerdatenschutzes zu beachten. Dies gilt insbesondere dann, wenn die Beschäftigten ihre privaten Endgeräte verwenden.

Der Unterarbeitskreis „Digitalisierung im Gesundheitswesen“ verfolgt das Ziel, über die in dem vorliegenden Papier beschriebenen Anforderungen möglichst einen Konsens mit den Fachverbänden im Krankenhausbereich zu erzielen. Gleichzeitig sind die Inhalte sinngemäß auch auf andere Branchen übertragbar, die sensible personenbezogene Daten im Sinne von Art. 9 DS-GVO verarbeiten. Hierzu gehören insbesondere Altenpflege und soziale Einrichtungen.

Wir empfehlen den Verantwortlichen in Krankenhäusern, bei Planungen und beim Betrieb von Messenger-Diensten die Anregungen des Whitepapers „Technische Anforderungen an Messenger-Dienste im Krankenhaus“ zu berücksichtigen und sich an der Diskussion zur Weiterentwicklung des Papiers zu beteiligen.

7.3.2 Neue Regeln für Webseitenanbieter

Im Vierzehnten Tätigkeitsbericht haben wir unter Punkt 7.2.4 bereits Hinweise zum Datenschutz auf Webseiten gegeben. Auch in diesem Berichtszeitraum haben sich Neuerungen bezüglich der datenschutzgerechten Gestaltung von Webseiten ergeben. Der Europäische Gerichtshof (EuGH) hat hierzu im Berichtsjahr 2019 zwei Urteile gefällt.

Ein Urteil bezieht sich auf die Einbindung von Social-Plugins auf Webseiten (EuGH, Urteil vom 29. Juli 2019 - C40/70 - „Fashion ID"). Social-Plugins sind kleine Schaltflächen auf Webseiten, über die personenbezogene Daten der Webseitenbesucher an die Anbieter der Social-Plugins übertragen werden können. Die Anbieter von Social-Plugins sind meist Social-Media-Netzwerke. Weil durch die Verwendung von Social-Plugins die Reichweite von Webseiteninhalten in den sozialen Netzwerken erhöht wird, ist die Verwendung von Social-Plugins durch Webseitenbetreiber weit verbreitet.

Der Hinweis auf die Webseiteninhalte wird umgangssprachlich zum Beispiel „teilen“ oder „liken“ genannt und erscheint dann im Nutzerprofil des Webseitenbesuchers des Anbieters des Social-Plugins. In der Praxis findet sich oft das Problem, dass beim Webseitenaufruf die Social-Plugins bereits direkt durch die Browser der Webseitenbesucher aus dem Internet nachgeladen und angezeigt werden. Dadurch erfolgt eine Übermittlung von personenbezogenen Daten an den Anbieter des Social-Plugins. Der EuGH befasste sich in seinem Urteil unter anderem mit der Frage, wer für das Einbinden des Social-Plugins auf der Webseite datenschutzrechtlich verantwortlich ist. Ebenso sollte geklärt werden, welche Rechtsgrundlage für die Übermittlung der personenbezogenen Daten des Webseitenbesuchers an den Anbieter des Social-Plugins einschlägig ist.

In einem weiteren Urteil befasste sich der EuGH mit der datenschutzrechtlichen Einwilligung in Form eines vorausgefüllten Ankreuzkästchens beim Einbinden von Cookies auf Webseiten (EuGH, Urteil vom 1. Oktober 2019 - C-673/17 - „Planet49“). Cookies sind kleine Textdateien, die im Browser auf dem Endgerät des Webseitenbesuchers gespeichert und diesem somit zugeordnet werden. Bei zum Beispiel der Speicherung, beim Auslesen oder bei der Weitergabe der Inhalte von Cookies durch die Cookie-Anbieter werden personenbezogene Daten verarbeitet.

Auch wenn beide Urteile sich technisch mit unterschiedlichen Funktionen auseinandersetzten, lassen sich große Schnittmengen identifizieren. So hat der EuGH nochmals bekräftigt, dass der Webseitenbetreiber für das Einbinden von Drittinhalten (z. B. Social-Plugin) oder für das Veranlassen des Setzens eines Cookies eine datenschutzrechtliche Verantwortung trägt. Für das Einbinden von Social-Plugins gilt in Zukunft, dass sich der Webseitenbetreiber die gemäß der Europäischen Datenschutz-Grundverordnung (DS-GVO) hierfür nötige informierte Einwilligung vom Webseitenbesucher einholen muss. Das Setzen von Cookies, welche rein technisch für das Bereitstellen der Webseite nicht erforderlich sind (z. B. für den Warenkorb), benötigt künftig auch die informierte Einwilligung. Ebenfalls wurde höchstrichterlich bekräftigt, dass vorausgefüllte Ankreuzkästchen zum Einholen einer informierten Einwilligung datenschutzrechtlich nicht zulässig sind. Ein sogenannter Cookie-Banner, der von der Annahme ausgeht, dass ein Weitersurfen auf der Website eine informierte Einwilligung bedeuten soll, ist somit unzureichend. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) hat in der Orientierungshilfe für Telemedienanbieter[35] die genannten Auffassungen bereits zuvor vertreten.

Wir empfehlen den Webseitenanbietern in unserem Bundesland, ihre Webseiten an die vorgenannten neuen Regeln anzupassen. Dies gilt insbesondere für das Einbinden von Dritt-Inhalten und gilt auch für Tracking-Mechanismen. Wer Funktionen nutzt, die eine informierte Einwilligung erfordern, muss entweder eine informierte Einwilligung einholen oder die Funktion entfernen.

[35] https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Broschueren/OH_TMG.pdf

8 Datenschutz in verschiedenen Rechtsgebieten

8.1 Rechtswesen

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

Ende August 2019 hat der Landesverband der Partei „Alternative für Deutschland“ (Verantwortlicher) auf seiner Homepage ein sogenanntes Informationsportal „Neutrale Schule“ freigeschaltet. Nach Prüfung des Portals haben wir die Datenerhebung über das Portal untersagt und die sofortige Vollziehung dieses Verbotes angeordnet. Der Verantwortliche ist diesem Verbot fristgemäß nachgekommen. Er hat aber gegen das Verbot Anfechtungsklage erhoben und ist auch im einstweiligen Rechtsschutzverfahren gegen die Anordnung der sofortigen Vollziehung des Verbotes vorgegangen. Im einstweiligen Rechtsschutzverfahren konnte der Verantwortliche nicht erfolgreich gegen unser Verbot vorgehen. Eine Entscheidung im Hauptsacheverfahren steht noch aus.

Das Portal richtete sich sowohl an Erwachsene als auch an Schülerinnen und Schüler. Das Portal war so gestaltet, dass sowohl von den Personen, die das Portal zur Meldung nutzen, als auch von den Personen, die über das Portal zum Gegenstand einer Meldung gemacht worden sind, politische Meinungen erfasst wurden. Politische Meinungen sind, genau wie beispielsweise medizinische Daten, nach der Europäischen Datenschutz-Grundverordnung (DS-GVO) besonders geschützte Daten, sogenannte besondere Kategorien personenbezogener Daten. Nur in streng geregelten Ausnahmen ist die Verarbeitung solcher Daten zulässig. In der Regel ist die Verarbeitung dieser Daten aber verboten. Zulässig ist es etwa, wenn eine betroffene Person in die Verarbeitung dieser Daten einwilligt. Für eine wirksame Einwilligung ist aber erforderlich, dass die Person über die Risiken dieser Datenverarbeitung informiert wird. Auch ist es zulässig, wenn eine Partei die politische Meinung ihrer Mitglieder verarbeitet oder ein Verlag oder Fernsehsender politische Meinungen veröffentlicht, die Personen selbst öffentlich gemacht haben. Wichtig ist hierbei aber, dass die betroffene Person bewusst und gewollt ihre Äußerungen für einen unbestimmten Personenkreis zugänglich machen wollte. Eine weitere in der DS-GVO geregelte Ausnahme ist die Nutzung dieser sensiblen Daten, wenn diese erforderlich sind, um eigene Rechte durchzusetzen. Wichtig für diese Ausnahme ist aber, dass sich ein entsprechender Rechtsanspruch bereits konkretisieren lässt, dass man also etwa weiß, welchen Sachverhalt genau man überprüfen lassen möchte.

Keine dieser Ausnahmen war vorliegend einschlägig, um ausnahmsweise über das Portal politische Meinungen zu erfassen. Da die Datenerhebung über das Portal somit nach den Vorgaben der DS-GVO verboten war, war das Verbot der Datenerhebung die einzig mögliche Maßnahme, um einen datenschutzkonformen Zustand wieder herzustellen. Dies hat auch das Verwaltungsgericht Schwerin im einstweiligen Rechtsschutzverfahren bestätigt und sich dabei insbesondere mit der möglichen Ausnahme, dass die Datenverarbeitung zur Rechtsdurchsetzung erforderlich sein könnte, auseinandergesetzt.

Nach Angaben der Partei „Alternative für Deutschland“ auf der Homepage selbst sollte das Portal dem Zweck dienen, einen neutralen Schulunterricht zu gewährleisten. Der Verantwortliche gab also vor, insoweit die Rechte der Schülerinnen und Schüler zu vertreten. Im Gerichtsverfahren berief sich der Verantwortliche dann aber auch auf sein eigenes Recht als Partei, wonach er durch staatliche Organe nicht in der Chancengleichheit beeinträchtigt werden dürfe. Im Schulgesetz für das Land Mecklenburg-Vorpommern (SchulG M-V) ist aber gerade nicht geregelt, dass Schulunterricht völlig neutral zu erfolgen hat, sondern dass vielmehr die Lehrerinnen und Lehrer im Unterricht den Werten des Grundgesetzes und der Landesverfassung verpflichtet sind und Grundrechte, wie insbesondere das Recht auf freie Meinungsäußerung, ihren Schülerinnen und Schülern auch vorleben müssen. Auch nach der Auffassung des Verwaltungsgerichts Schwerin müssen sich Lehrerinnen und Lehrer im Unterricht kritisch mit Positionen von politischen Parteien auseinandersetzen können, ohne befürchten zu müssen, durch diese Parteien dann an den Pranger gestellt zu werden. Diese Auseinandersetzung verletzt politische Parteien daher auch nicht in ihrem Recht auf Chancengleichheit. Soweit sich Schülerinnen und Schüler durch politische Äußerungen von Lehrerinnen und Lehrern überrumpelt, angegriffen oder sogar diskriminiert fühlen, können sie sich selbstverständlich an geeignete Stellen, wie etwa Vertrauenslehrer, die Schule oder die Schulbehörde wenden, um sich beraten zu lassen. Die Datenerhebung über das Portal war damit nicht erforderlich, um rechtliche Ansprüche der Schülerinnen und Schüler oder der Partei „Alternative für Deutschland“ sicherzustellen.

8.1.2 Nachbarschaftslisten - nur mit Einwilligung

Im vorliegenden Fall legte ein Rentner eine Liste über seine Nachbarn in einer Reihenhaus- und Einfamilienhaussiedlung an. Diese Nachbarschaftsliste enthielt neben der Adresse mit Hausnummer und Familienname auch die Vornamen der Bewohner sowie die Namen derer Kinder. Nachdem Kopien der Listen in der Nachbarschaft durch den Rentner verteilt wurden, waren mindestens vier Haushalte über diese Datenerhebung und -verbreitung extrem irritiert.

Auf Nachfrage dieser Bewohner beim verantwortlichen Rentner zum Sinn und Zweck der Listen und zur Herkunft der Daten, insbesondere der Namen der Kinder, machte dieser nur lapidare Ausführungen, wie, die Daten habe er erlangt durch Gespräche mit anderen Nachbarn und er benötige diese Daten für die Anmeldung des jährlich von ihm organisierten Osterfeuers in der Siedlung. Die Beschwerdeführer hatten allerdings in der Vergangenheit noch nie an dieser nachbarschaftlichen Veranstaltung teilgenommen und hatten dies künftig auch nicht vor und verlangten die Löschung ihrer Daten. Da die Auskunft des Rentners zur Datenherkunft ungenügend und er selbst auch uneinsichtig war, beschwerten sie sich beim Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern. Eine Recherche unsererseits ergab des Weiteren, dass für die Anmeldung von Brauchtumsfeuern (Osterfeuer) keine „Teilnehmerliste“ erforderlich ist. Es werden nur die Daten desjenigen benötigt, der das Feuer bei der Stadt anmeldet.

Unproblematisch wäre die Erstellung dieser Liste gewesen, wenn der Rentner von Nachbar zu Nachbar gegangen wäre und die Daten bei diesen persönlich mit deren Einwilligung erhoben hätte. Da er dies nicht getan hat, sondern die Daten über Dritte unter Verletzung des Direkterhebungsgrundsatzes, unter Verletzung seiner Informationspflichten und letztendlich ohne Rechtsgrundlage erhoben und verarbeitet hat, leiteten wir daraufhin ein Ordnungswidrigkeitenverfahren ein und erließen einen Bußgeldbescheid in Höhe von 500,00 Euro.

Der Bußgeldbescheid wurde in der Sache vom Amtsgericht Schwerin bestätigt, allerdings das Bußgeld auf 200,00 Euro heruntergesetzt.

8.1.3 Auskunftsersuchen - Grenzen des Auskunftsverweigerungsrechts

Im vorliegenden Fall wurde angezeigt, dass an einer Lagerhalle Videokameras installiert wurden, die über die Umzäunung hinaus den öffentlichen Raum mitüberwachen. Der Verantwortliche wurde angeschrieben und zur Auskunft aufgefordert. In diesem Zusammenhang werden die Verantwortlichen über ihr Auskunftsverweigerungsrecht informiert. Dieses besteht, wenn sich der Verantwortliche selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der Zivilprozessordnung (ZPO) bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten (OWiG) aussetzen würde. Die Inanspruchnahme des Auskunftsverweigerungsrechts ist zu erklären und grundsätzlich nachvollziehbar zu begründen.

Der Verantwortliche berief sich nicht auf sein Auskunftsverweigerungsrecht, sondern teilte mit, dass es sich bei den von ihm installierten Kameras um Attrappen handele. Den geforderten Nachweis hierfür erbrachte er allerdings nicht. Es stellte sich vielmehr im weiteren Verfahren heraus, dass es sich um funktionsfähige Kameras handelte, die auch aufzeichneten.

Um die Kameras datenschutzrechtlich bewerten zu können, wurde der Verantwortliche mit einem Auskunftsheranziehungsbescheid verpflichtet, Auskunft zu den installierten Kameras zu erteilen, unseren Fragenkatalog zu beantworten und Videosequenzen der Kameras zu übersenden. Der Verantwortliche verweigerte die Auskunft zu seiner Videoüberwachungsanlage mit der Begründung, dass er von seinem Auskunftsverweigerungsrecht Gebrauch mache, weil er sich durch seine falsche Auskunftserteilung der Gefahr eines Ordnungswidrigkeitenverfahrens ausgesetzt sah.

Gegen unseren Bescheid reichte er Klage beim Verwaltungsgericht ein und beantragte die Aufhebung des Heranziehungsbescheides.

Die Klage wurde durch das Verwaltungsgericht abgewiesen.

Das Verwaltungsgericht erklärte, dass die Aufsichtsbehörde im Rahmen ihres Ermessens den Verantwortlichen dazu verpflichten kann, Auskunft zu erteilen. Die Aufsichtsbehörde kann Auskunft zu sämtlichen Fragen beanspruchen, deren Klärung geeignet und erforderlich ist, um die Beachtung der datenschutzrechtlichen Bestimmungen zu gewährleisten. Es obliegt dem Ermessen der Aufsichtsbehörde, auf welche Art und Weise sie die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte einholt. Hierzu kann auch ein Fragenkatalog übersendet werden, der von der zur Auskunft verpflichteten Stelle zu beantworten ist.

Zum Auskunftsverweigerungsrecht erklärte das Gericht, dass es den Auskunftspflichtigen zwar davor schützen soll, sich selbst zu belasten, dies allerdings nicht solche Straftaten oder Ordnungswidrigkeiten betrifft, derer er sich durch sein bisheriges Verhalten in dem Auskunftseinholungsverfahren verdächtig gemacht hat. Sofern der Verantwortliche im Verwaltungsverfahren zunächst eine falsche Angabe gemacht und somit den Tatbestand einer Ordnungswidrigkeit verwirklicht haben könnte, hat er dabei ohne Zwang und in pflichtwidriger Weise in Kenntnis der möglichen Verwirklichung einer Ordnungswidrigkeit gehandelt. Ein solches Verhalten kann ihn nicht von seiner Verpflichtung zur Auskunftserteilung befreien, denn ansonsten hätte es der Auskunftspflichtige immer selber in der Hand, das Verwaltungsverfahren zu steuern und nachträglich die Rechtswidrigkeit einer Heranziehungsverfügung herbeizuführen, was nicht Sinn und Zweck der Regelung ist.

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

In einem erheblichen Teil der in unserer Behörde eingegangenen förmlichen Beschwerden kritisieren Bürgerinnen und Bürger, dass Betroffenenrechte, die sie gegenüber einem Unternehmen, dem Hausarzt, einem Verein oder einer Behörde geltend gemacht haben, schlicht ignoriert oder nur unzureichend erfüllt werden.

Nach der Wertung der Europäischen Datenschutz-Grundverordnung (DS-GVO) spielt die betroffene Person bei der Kontrolle der Rechtmäßigkeit der Verarbeitung ihrer Daten eine ganz entscheidende Rolle. Mit den Betroffenenrechten stellt die DS-GVO sicher, dass die betroffene Person auch über die Werkzeuge verfügt, um diese Kontrolle auszuüben. So muss die betroffene Person grundsätzlich darüber informiert werden, dass über sie personenbezogene Daten verarbeitet werden. Eine heimliche Datenverarbeitung ist in aller Regel unzulässig. Mit einem sogenannten Auskunftsrecht nach Art. 15 DS-GVO kann die betroffene Person überprüfen, ob ein Verantwortlicher personenbezogene Daten über sie verarbeitet, ob diese Daten richtig sind und ob die Datenverarbeitung entsprechend der erteilten Information erfolgt. Sind die Daten falsch, hat die betroffene Person nach Art. 16 DS-GVO ein Recht auf Berichtigung. Liegen die Voraussetzungen für die Datenverarbeitung nicht mehr vor, regelt Art. 17 DS-GVO ein Recht auf Löschung. Ist unklar, ob die Daten rechtmäßig verarbeitet werden oder richtig sind, kann die betroffene Person gemäß Art. 18 DS-GVO ein Recht auf Einschränkung der Verarbeitung geltend machen, solange die Angaben geprüft werden. Art. 19 DS-GVO bestimmt, dass ein Verantwortlicher die Empfänger, denen er personenbezogene Daten übermittelt hat, darüber unterrichten muss, wenn Betroffenenrechte ausgeübt wurden. Art. 20 DS-GVO sieht in bestimmten Fällen das Recht auf Datenübertragbarkeit vor. Das bedeutet, dass die betroffene Person unter bestimmten Voraussetzungen ein Recht hat, dass ihr digital verarbeitete Daten in einem maschinenlesbaren Format zur Verfügung gestellt werden. Schließlich besteht nach Art. 21 DS-GVO unter bestimmten Voraussetzungen die Möglichkeit, einer Datenverarbeitung zu widersprechen.

Die Betroffenenrechte sind entweder an bestimmte Voraussetzungen geknüpft oder durch andere Gesetze eingeschränkt, die von dem Verantwortlichen geprüft werden müssen. So können Ärztinnen und Ärzte einem Anspruch auf Löschung von Patientendaten regelmäßig nur nach Ablauf ihrer gesetzlichen Aufbewahrungsfristen aus § 630 f BGB nachkommen. Anwältinnen und Anwälte können unter Berufung auf ihr Berufsgeheimnis der gegnerischen Partei die Auskunft zumindest teilweise verwehren. Verarbeitet ein Gesundheitsamt Gesundheitsdaten von Bürgerinnen und Bürgern auf Grundlage eines Gesetzes, wird ein Widerspruch gegen diese Datenverarbeitung regelmäßig vergeblich sein.

All diesen Betroffenenrechten ist aber gemein, dass sie unverzüglich, spätestens jedoch innerhalb von vier Wochen, zu bearbeiten sind. Nur unter engen Voraussetzungen kann diese Frist verlängert werden. In jedem Fall muss aber innerhalb dieser vier Wochen reagiert werden. Der Verantwortliche muss also innerhalb dieser vier Wochen entweder das Betroffenenrecht erfüllen und dies der betroffenen Person mitteilen, oder aber die betroffene Person unter Nennung der Gründe über eine Fristverlängerung informieren. Lehnt der Verantwortliche ein Betroffenenrecht ab, muss er diese Ablehnung innerhalb der Frist begründen und die betroffene Person auf Rechtsschutzmöglichkeiten, also insbesondere die Beschwerde beim Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, hinweisen. Auch wenn der Verantwortliche überhaupt keine personenbezogenen Daten der betroffenen Person verarbeitet, muss er dies der betroffenen Person mitteilen.

Die Frist beginnt mit Eingang des Antrages. Lässt sich die Identität der betroffenen Person mit Eingang des Antrages nicht hinreichend klären und besteht Anlass zu Nachfragen, müssen diese Nachfragen zwar unverzüglich erfolgen, die Frist beginnt dann aber erst mit Eingang der zusätzlich angefragten Informationen.

Die Bearbeitung von Betroffenenrechten muss für die betroffene Person grundsätzlich kostenfrei erfolgen. Nur in Fällen rechtsmissbräuchlicher Antragstellung, also insbesondere bei grundloser häufiger Wiederholung des gleichen Antrages, kann die Erfüllung von einem Entgelt abhängig gemacht oder sogar vollständig versagt werden.

Bereits die Nichtbearbeitung eines Betroffenenrechts innerhalb der in Art. 12 Abs. 3 und 4 DS-GVO geregelten Frist stellt, unabhängig davon, ob das Betroffenenrecht selbst tatsächlich erfüllt werden müsste oder nicht, einen Datenschutzverstoß dar, der mit einem Bußgeld sanktioniert werden kann.

Zudem kann die Datenschutzaufsichtsbehörde auch im Verwaltungsverfahren ganz konkret anordnen, dass Betroffenenrechte zu erfüllen sind. Wird eine entsprechende Anordnung nicht erfüllt und auch nicht vor Gericht angefochten, kann für diese Weigerung ebenfalls ein Bußgeld verhängt werden. Zudem kann die Datenschutzaufsichtsbehörde Zwangsgelder verhängen, bis das Betroffenenrecht erfüllt ist.

Wir raten Verantwortlichen, einen festen Prozess zu etablieren und Beschäftigte entsprechend zu schulen, wie mit Betroffenenrechten umzugehen ist. Es empfiehlt sich, einen Beschäftigten zu benennen, der für die Bearbeitung von Betroffenenrechten zuständig ist. Allen anderen Beschäftigten muss aber klar sein, dass ihnen gegenüber geltend gemachte Betroffenenrechte unverzüglich an die zuständige Mitarbeiterin oder den zuständigen Mitarbeiter weiterzuleiten sind. Sind mehrere Stellen gemeinsam für eine Datenverarbeitung verantwortlich oder verarbeitet eine Stelle im Auftrag einer anderen personenbezogene Daten, dürfen betroffene Personen auch nicht einfach an die andere Stelle verwiesen werden. In diesen Konstellationen muss die Stelle, bei der das Betroffenenrecht zunächst geltend gemacht worden ist, das Gesuch umgehend an die Stelle weiterleiten, die über die Erfüllung des Betroffenenrechts entscheiden kann.

Besonders umstritten ist das Recht auf Erhalt einer Kopie der über die betroffene Person verarbeiteten personenbezogenen Daten nach Art. 15 Abs. 3 DS-GVO. Der Anspruch setzt nach unserer Auffassung zunächst voraus, dass die betroffene Person diese Kopie ausdrücklich beantragt. Insoweit ist auch der tatsächliche Wille der betroffenen Person zu erforschen. Insbesondere sind Akteneinsichtsgesuche hiervon abzugrenzen. Das Recht auf Akteneinsicht geht regelmäßig über das Recht auf Erhalt einer Kopie hinaus, kann aber in der Regel auch von einem Entgelt abhängig gemacht werden.

Der Anspruch auf Erhalt einer Kopie erstreckt sich auf alle Seiten einer Akte oder eines Vorgangs, die personenbezogene Daten enthalten. Dabei ist der Begriff der personenbezogenen Daten weit auszulegen. Gemeint sind hier insbesondere nicht nur Name und Kontaktdaten. Eine Patientenakte wird daher regelmäßig vollständig kopiert werden müssen, bei einem Verwaltungsvorgang müssen allgemeine Rechtsgutachten, die sich nicht konkret auf die betroffene Person beziehen, nicht mit übersandt werden. Zudem können dem Recht auf Erhalt einer Kopie Rechte Dritter entgegenstehen. Der Verantwortliche muss gegenüber der betroffenen Person aber nachweisen, dass eine solche Kollisionslage besteht. Zudem darf die Kopie nicht vollständig verweigert werden. In Verwaltungsvorgängen können beispielsweise die Namen unbeteiligter Dritter geschwärzt und der betroffenen Person im Übrigen die Kopie überlassen werden.

Vor dem Verwaltungsgericht Schwerin ist derzeit ein Verfahren anhängig, bei dem der Verantwortliche behauptet, dass Urheberrechte als Rechte Dritter der Übersendung einer Kopie entgegenstehen. Eine Entscheidung in diesem Verfahren steht noch aus. In diesem Fall haben wir die Übersendung der Kopie trotz des Hinweises auf das Urheberrecht angeordnet, da das Bestehen von entgegengesetzten Urheberrechten weder nachgewiesen noch plausibel gemacht worden ist.

8.1.5 Videoüberwachung im privaten und nachbarschaftlichen Bereich

Dem Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern werden immer wieder Beschwerden zu Videoüberwachungsanlagen oder Videokameras im privaten und nachbarschaftlichen Bereich vorgelegt. Die Europäische Datenschutz-Grundverordnung (DS-GVO) gilt allerdings nicht für die Verarbeitung von personenbezogenen Daten, 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).

Das eigene private Grundstück kann somit grundsätzlich überwacht werden.

Unzulässig ist es, wenn der Verantwortliche ein privates Nachbargrundstück mit überwacht. In diesem Fall kann der mögliche Eingriff des Nachbarn in die Persönlichkeitsrechte des Betroffenen durch den Betroffenen zivilgerichtlich geltend gemacht werden und im Rahmen von zivilgerichtlichen Abwehr- und Unterlassungsansprüchen abgestellt werden lassen (§§ 823, 1004 BGB). Hierzu kann auch auf die einschlägige Rechtsprechung vor Inkrafttreten der DS-GVO, das heißt vor dem 25. Mai 2018, zurückgegriffen werden, da sich an der rechtlichen Bewertung von Videoüberwachungsanlagen und Videokameras grundsätzlich nichts geändert hat.

Der persönliche oder familiäre Anwendungsbereich einer Videoüberwachungsanlage oder Videokamera wird grundsätzlich immer verlassen, wenn über die Grundstücksgrenze hinaus öffentlicher Raum, wie der öffentliche Gehweg oder die öffentliche Straße, mit überwacht werden. Dies ist grundsätzlich immer unzulässig, wobei die Erfassung eines schmalen Streifens entlang der Hauswand unter bestimmten Umständen nach der Rechtsprechung ausnahmsweise zulässig sein kann.

8.1.6 Stetiger Meldedatenabgleich für den Rundfunkbeitrag

Der Rundfunkstaatsvertrag (RStV) enthält die grundlegenden Regelungen für den öffentlich-rechtlichen und den privaten Rundfunk in dem dualen Rundfunksystem der Länder Deutschlands. Mit Inkrafttreten der 15. Änderung des Rundfunkstaatsvertrages am 1. Januar 2013 wurde ein vollständiger Meldedatenabgleich durchgeführt, um den Wechsel von einer gerätebezogenen Abgabe zu einem wohnungs- bzw. betriebsbezogenen Beitrag zur Finanzierung des öffentlich-rechtlichen Rundfunks zu ermöglichen. Dazu wurden die Daten des Beitragsservices der bisher Beitragspflichtigen mit den Daten aller volljährigen Personen, die bei den Einwohnermeldeämtern in Deutschland gemeldet sind, verglichen. Wie bereits im Zwölften Tätigkeitsbericht unter Punkt 5.4.10 beschrieben, hatte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) ihre damalige Kritik zu diesem Vorhaben (siehe Beschluss vom 11. Oktober 2010[36]) zurückgestellt, weil die Rundfunkanstalten nachweisen konnten, dass ein solcher Eingriff in das Recht auf informationelle Selbstbestimmung der betroffenen Beitragspflichtigen erforderlich war. Wie zu befürchten stand, wurde bei der 19. Änderung des Rundfunkstaatsvertrages ein nochmaliger vollständiger Meldedatenabgleich aller meldepflichtigen Personen in Deutschland vorgenommen. Dieser erneute Meldedatenabgleich war nach unserer Auffassung nicht erforderlich. Die Rundfunkanstalten konnten nicht zufriedenstellend aufzeigen, wie hoch der jährliche Beitragsverlust etwa durch Umzüge, Scheidungen oder durch den Tod von Beitragspflichtigen tatsächlich ist. Aus unserer Sicht war somit der Eingriff in das Recht auf informationelle Selbstbestimmung der betroffenen Beitragspflichtigen nicht hinreichend legitimiert.

Im aktuellen Entwurf zum 23. Rundfunkänderungsstaatsvertrag ist nun ein stetiger Meldedatenabgleich für alle vier Jahre ab dem Jahr 2020 vorgesehen. In ihrem Beschluss vom 26. April 2019[37] kritisierte die Datenschutzkonferenz dieses erneute Vorhaben. Auch wir haben unsere Bedenken der Landesregierung mitgeteilt. Denn der verstetigte Meldedatenabgleich ist ein unverhältnismäßiger Eingriff in das Recht auf informationelle Selbstbestimmung der Beitragspflichtigen und steht in Konflikt mit den Grundsätzen der Datenminimierung und der Erforderlichkeit aus der Europäischen Datenschutz-Grundverordnung (DS-GVO). Das geplante Vorhaben, den Meldedatenabgleich unter den Vorbehalt der Kommission zur Ermittlung des Finanzbedarfs der Rundfunkanstalten zu stellen, führt nicht zu einer anderen Bewertung. Auch ist kritisch zu hinterfragen, warum beim geplanten Meldedatenabgleich mehr personenbezogene Daten abgerufen werden sollen als die Beitragspflichtigen bei der Anmeldung für den Rundfunkbeitrag mitteilen müssen (z. B. Doktorgrad, Familienstand).

[36] https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/rundfunk.pdf
[37] https://www.datenschutzkonferenz-online.de/media/dskb/20190426_dsk-beschluss_rfbeitrag.pdf

Der geplante stetige Meldedatenabgleich würde zur abwegigen Situation führen, dass mehr personenbezogene Daten an die Rundfunkanstalten übermittelt werden als diese selbst zur Beitragserhebung abfragen.

Wir empfehlen der Landesregierung, sich dafür einzusetzen, dass die Planungen zum stetigen Meldedatenabgleich für den Rundfunkbeitrag eingestellt werden.

8.2 Polizei/Ordnungswesen

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

Zum Entwurf des Sicherheits- und Ordnungsgesetzes Mecklenburg-Vorpommern (SOG M-V) haben wir eine umfangreiche schriftliche Stellungnahme abgegeben, die sehr genau bei den jeweiligen Gesetzesnormen die Anforderungen der Datenschutzrichtlinie für Polizei und Strafjustiz (EU) 2016/680 und des Urteils des Bundesverfassungsgerichts zum Bundeskriminalamtsgesetz sowie Defizite des SOG M-V-Gesetzentwurfs im Einzelnen beleuchtet. Diese liegt als Ausschussdrucksache zu der Landtagsdrucksache 7/3694 vor.

Zunächst haben wir darauf hingewiesen, dass es bei einem so eingriffsintensiven Gesetz wie dem SOG M-V, welches sich an einen breiten Kreis von Adressaten unterschiedlicher Qualifikationsniveaus richtet, bedeutsam ist, durchgängig die sprachliche Verständlichkeit besonders in den Blick zu nehmen. Es ist hier schlicht ein Gebot der Rechtsstaatlichkeit, dass das Gesetz gut verständlich, lesbar und anwenderfreundlich ist. Nicht zuletzt soll und muss dieses Gesetz aufgrund der Eingriffsintensität der geregelten Maßnahmen nicht nur den Rechtsanwendern absolute Rechtsklarheit verschaffen, sondern auch die betroffenen Bürgerinnen und Bürger in die Lage versetzen, die Rechtmäßigkeit der gegen sie ergriffenen Maßnahmen einzuschätzen. Für uns steht es vor diesem Hintergrund außer Frage, dass dieses Gesetz vor allem leicht verständliche, klare und präzise Regelungen enthalten muss.

Leider ist zu konstatieren, dass dieses Gesetz diesen Anforderungen nicht gerecht wird. Das SOG M-V macht es den Anwendern kaum möglich, rechtsfehlerfrei ihre Aufgaben zu erfüllen. Die Vorschrift § 25 SOG M-V ist ein Negativbeispiel. Diese Regelung bereitet sowohl in rechtlicher als auch in sprachlicher Hinsicht große Schwierigkeiten, und es stellt sich die Frage, ob diese Regelung für Adressaten und Anwender aus der Polizei, den Ordnungsbehörden und den Gerichten in dieser Form verständlich vollziehbar ist. Dabei ist für uns ausschlaggebend, ob die Norm aus sich heraus für die Adressaten und Anwender verständlich ist oder nicht, und es ist nicht maßgeblich, dass der Sinn der Vorschrift unter Berücksichtigung der Gesetzesbegründung geklärt werden könnte. Nach diesen Maßstäben halten wir die genannte Regelung nicht für so verständlich, dass sie von den Anwendern sicher genutzt werden kann.

Dass ein Gesetz wie das SOG M-V die Materie auch verständlich regeln kann, zeigt ein Ländervergleich: Das Bayerische Polizeiaufgabengesetz ist (unabhängig von den zum Teil verfassungsrechtlich kritischen Grenzziehungen) sprachlich in weiten Teilen sehr gut verständlich.

Weiter sind die Regelungen der Befugnisse der Datenschutzaufsichtsbehörde nach unserer Auffassung im SOG M-V europarechtswidrig. Wie die aufsichtsbehördlichen Kompetenzen zu regeln sind, ergibt sich aus der JI-Richtlinie. Dort werden die Standards, die bei der Ausgestaltung dieser Befugnisse einzuhalten sind, vorgegeben, und in der JI-Richtlinie ist auch festgelegt, dass für die Aufsichtsbehörde wirksame Abhilfebefugnisse geschaffen werden müssen. Dies sind beispielsweise Warnungen, Anweisungen und die Verhängung einer vorübergehenden oder endgültigen Beschränkung der Verarbeitung, einschließlich eines Verbotes. Und bei verständiger Interpretation der JI-Richtlinie gehört dazu auch, dass für die Aufsichtsbehörde die Möglichkeit geschaffen werden muss, gegebenenfalls auch die Löschung von Daten anordnen zu können. Solche aufsichtsbehördlichen Befugnisse sind im SOG M-V aber nur unzureichend vorgesehen. Die Regelung von Warnungen und die Beratung durch die Aufsichtsbehörde werden überhaupt nicht im SOG M-V selbst geregelt. Hier wird systemwidrig auf die Europäische Datenschutz-Grundverordnung (DS-GVO) verwiesen, obwohl eine konkrete Regelung im SOG M-V zu treffen gewesen wäre. Darüber hinaus ist in § 48b Abs. 2 Satz 2 SOG M-V sogar die Anordnung der Löschung oder eines Verbots durch die Aufsichtsbehörde ausdrücklich ausgeschlossen. Diese Einschränkungen der aufsichtsbehördlichen Befugnisse im SOG M-V überschreiten den Spielraum, den die JI-Richtlinie vorgibt, und sind europarechtswidrig.

Weiter stellt die in § 33 c SOG M-V neu eingeführte Online-Durchsuchung einen äußerst schwerwiegenden Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) dar. Entsprechend hohe Anforderungen stellt das Bundesverfassungsgericht an die Rechtfertigung eines solchen Eingriffs. Zwar sieht § 33 c SOG M-V in Abs. 2 Satz 3 vor, dass, soweit möglich, technisch sicherzustellen ist, dass Daten, die kernbereichsrelevante Informationen betreffen, nicht erhoben werden. Es fehlt aber an verfassungsrechtlich hinreichenden Vorkehrungen auf der Ebene des nachgelagerten Kernbereichsschutzes. Die Vorschrift des § 26 Abs. 5 SOG M-V, nach der die erhobenen Daten der oder dem behördlichen Datenschutzbeauftragten zur Auswertung und Entscheidung über die Rechtmäßigkeit dieser Datenerhebung vorzulegen sind, beinhaltet keine hinreichend unabhängige Kontrolle. Laut Bundesverfassungsgericht (BVerfG) dient die verfassungsrechtlich gebotene Sichtung durch eine unabhängige Stelle neben der Rechtmäßigkeitskontrolle maßgeblich dem Ziel, kernbereichsrelevante Daten so frühzeitig herauszufiltern, dass sie den Sicherheitsbehörden nach Möglichkeit nicht offenbar werden. Dies setzt voraus, dass die Kontrolle im Wesentlichen von externen, nicht mit Sicherheitsaufgaben betrauten Personen wahrgenommen wird. Das ist hier jedoch nicht der Fall. Die vorliegende Regelung überlässt die Sichtung einer oder einem Bediensteten der Behörde. Dass diese oder dieser als behördeninterne Datenschutzbeauftragte oder behördeninterner Datenschutzbeauftragter weisungsfrei ist, reicht für eine unabhängige Kontrolle nicht aus. Die Gewährleistung einer wirksamen aufsichtlichen Kontrolle setzt nach den Ausführungen des Bundesverfassungsgerichts zunächst eine mit wirksamen Befugnissen ausgestattete Stelle voraus. Außerdem ist erforderlich, dass die Datenerhebungen vollständig protokolliert werden. Es muss durch technische und organisatorische Maßnahmen sichergestellt werden, dass die Daten den Datenschutzbeauftragten in praktikabel auswertbarer Weise zur Verfügung stehen und die Protokollierung hinreichende Angaben zu dem zu kontrollierenden Vorgang enthält.

Ein weiteres Beispiel einer aus unserer Sicht neu geschaffenen verfassungswidrigen Norm ist die Regelung der automatisierten Kennzeichenerfassung in § 43 a Abs. 1 Nr. 6 SOG M-V. Hier ist die Bezeichnung des Gebiets „von der Bundesgrenze bis einschließlich der Bundesautobahn A 20“ zu unbestimmt und genügt nicht verfassungsrechtlichen Vorgaben. Angezeigt wäre eine kilometermäßige Begrenzung. Dies gilt insbesondere mit Blick auf die Entscheidung des Bundesverfassungsgerichts vom 18. Dezember 2018 (Pressemitteilung Nr. 8/2019 des Bundesverfassungsgerichts vom 5. Februar 2019). Das Gericht hat ausgeführt, dass es verfassungsrechtlich unbedenklich ist, Kennzeichenkontrollen in einem Grenzgebiet bis zu einer Tiefe von 30 km durchzuführen. In der Entscheidung ist ausdrücklich benannt, dass die Befugnis zu Kennzeichenkontrollen hinreichend bestimmt und begrenzt sein sowie einen klaren Grenzbezug aufweisen muss. Diesen Anforderungen genügt die Formulierung im SOG M-V „bis einschließlich der Bundesautobahn A 20“ nicht. Die A 20 zieht sich vom Grenzgebiet im Stettiner Raum hoch nach Greifswald und dann quer durch Mecklenburg-Vorpommern in Richtung Lübeck. Auf dieser gesamten Strecke sind nach dem Wortlaut des § 43 a Abs. 1 Nr. 6 SOG M-V Kennzeichenkontrollen möglich. Diese Regelung steht damit im klaren Widerspruch zu den vom Bundesverfassungsgericht festgelegten Vorgaben für die Zulässigkeit einer Kennzeichenkontrolle und ist unzulässig.

Bei der Anhörung im Landtag Mecklenburg-Vorpommern am 12. September 2019 haben wir diese und weitere Kritikpunkte wiederholt und erläutert. Die Zweite Lesung durch den Landtag steht noch aus.

8.2.2 Videoüberwachung Marienplatz

Bereits seit dem Jahr 2016 plante das Ministerium für Inneres und Europa Mecklenburg-Vorpommern, auf dem Marienplatz in Schwerin eine Videoüberwachungsanlage zu installieren. Wir haben diesen Prozess seit November 2016 beratend begleitet. Aufgrund technischer Probleme zögerte sich die Umsetzung des Projektes bis Ende 2018 hinaus. Im Laufe des Planungsprozesses hat sich die für die Videoüberwachung relevante Rechtslage geändert. Seit dem 25. Mai 2018 war nun auch für die Videoüberwachungsanlage auf dem Marienplatz die Europäische Datenschutz-Grundverordnung (DS-GVO) anzuwenden. Dies ergibt sich aus einer Festlegung des Landesdatenschutzgesetzes Mecklenburg-Vorpommern (DSG M-V), wonach die DS-GVO auch für polizeiliche Maßnahmen Geltung findet, bis speziellere Regelungen, insbesondere das Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommern (SOG M-V), an die neue Rechtslage angepasst worden sind. Diese Anpassung ist derzeit noch nicht verabschiedet.

Nach der DS-GVO musste bei der Videoüberwachung auf dem Marienplatz sichergestellt sein, dass insbesondere auch technische Komponenten den Schutz personenbezogener Daten bei der Datenverarbeitung gewährleisten. Zudem muss vor der Inbetriebnahme der Videoüberwachungsanlage eine sogenannte Datenschutz-Folgenabschätzung (DSFA) überprüfen, ob der Schutz personenbezogener Daten bei der Datenverarbeitung gewährleistet wird.

Mitte Februar 2018 erhielten wir vom Polizeipräsidium Rostock Unterlagen zum Videoüberwachungsprojekt, unter anderem auch die förmliche Freigabe des gesamten Verfahrens. Da wir in diesen Unterlagen das erforderliche Datenschutz- und Sicherheitskonzept vermissten, baten wir um Bereitstellung dieses Dokuments, um das gesamte Verfahren datenschutzrechtlich beurteilen zu können. Das Konzept existierte zu diesem Zeitpunkt offensichtlich noch nicht. Wir erhielten jedoch eine detaillierte Schutzbedarfsfeststellung, die zum Ergebnis kam, dass hinsichtlich der Gewährleistungsziele Vertraulichkeit, Integrität und Verfügbarkeit hoher Schutzbedarf bestünde. Folgerichtig wurde schon in den ersten vorbereitenden Dokumenten für das Sicherheitskonzept festgehalten, dass die drahtlose Datenübertragung von den Videokameras bis zum Videoserver der Polizei durchgehend zu verschlüsseln ist (Ende-zu-Ende-Verschlüsselung).

In den folgenden Monaten zeigte sich jedoch, dass die Polizei erhebliche technische Probleme hatte, die erforderlichen Maßnahmen für eine vollständige Verschlüsselung des Datenstroms umzusetzen. Der Starttermin des Wirkbetriebs wurde verschoben und dem bislang beauftragten technischen Dienstleister wurde der Auftrag entzogen. Aber auch im Laufe der nächsten Monate gelang es dem Polizeipräsidium im Rahmen des Testbetriebs der Anlage nicht, die eigenen Anforderungen an eine sichere Datenübertragung zu erfüllen.

Im Dezember 2018 wurde uns mitgeteilt, dass eine Verschlüsselung aller Teilstrecken der Funkübertragung nicht realisiert werden kann. Weder die ursprünglich geplante Ende-zu-Ende-Verschlüsselung noch die vollständige, abschnittsweise Verschlüsselung der verwendeten Richtfunkstrecken konnte realisiert werden. Dennoch sollte der zunächst zeitlich befristete, vorläufige Wirkbetrieb des Verfahrens zum Ende des Jahres aufgenommen werden. Daraufhin sprachen wir dem Polizeipräsidium eine förmliche Warnung gemäß Art. 58 Abs. 2 lit. a DS-GVO aus, in der wir darauf hinwiesen, dass der Start des vorläufigen Wirkbetriebes der Anlage voraussichtlich gegen die Bestimmungen der DS-GVO verstoßen würde. Diese Warnung wurde vom Polizeipräsidium missachtet und der Wirkbetrieb wurde wie geplant aufgenommen.

Vor diesem Hintergrund sahen wir uns gezwungen, von weiteren aufsichtsrechtlichen Befugnissen Gebrauch zu machen. Wir wiesen die Polizeiinspektion Schwerin und das Polizeipräsidium Rostock gemäß Art. 58 Abs. 1 lit. a DS-GVO zunächst an, bislang fehlende Dokumente bereitzustellen. Das betraf insbesondere die Vereinbarung zur gemeinsamen Verantwortlichkeit der beiden Beteiligten, das Datenschutz- und Informationssicherheitskonzept und die Dokumentation zur Datenschutz-Folgenabschätzung. Unabhängig davon plante das Polizeipräsidium, den vorläufigen Wirkbetrieb über die geplante Befristung hinaus fortzusetzen, ohne dass die Anforderungen an die Verschlüsselung der Funkstrecke erfüllt waren. Daher wiesen wir nunmehr gemäß Art. 58 Abs. 2 lit. d DS-GVO an, vor einer Verlängerung des vorläufigen Wirkbetriebes eine Ende-zu-Ende-Verschlüsselung sicherzustellen. Wir machten deutlich, dass wir als Übergangslösung auch eine abschnittsweise Verschlüsselung für den gesamten Übertragungsweg der Bilddaten akzeptieren würden, sofern die Übertragungsgeräte (Relaisstellen) mit geeigneten mechanischen Vorrichtungen vor dem Zugriff unberechtigter Dritter geschützt werden würden.

Auch diese Anweisung führte weder dazu, dass eine ordnungsgemäße Verschlüsselung realisiert wurde, noch dass der Testbetrieb der Videoüberwachung bis zur Behebung der Mängel eingestellt wurde. Folgerichtig blieb uns Anfang Februar 2019 keine andere Möglichkeit, als durch eine Anordnung nach Art. 58 Abs. 2 lit. f DS-GVO die unverschlüsselte Datenübertragung beim Betrieb der Videoüberwachungsanlage vorläufig zu untersagen. Da trotz dieses Verbotes die Videoüberwachungsanlage weiterbetrieben wurde und die personenbezogenen Daten weiterhin unverschlüsselt übertragen wurden, haben wir juristische Maßnahmen zur Durchsetzung unseres Verbotes geprüft. In Betracht kam insoweit, eine sogenannte Leistungsklage beim Verwaltungsgericht Schwerin zu erheben. Da aus unserer Sicht akuter Handlungsbedarf bestand, haben wir weiterhin Eilmaßnahmen im einstweiligen Rechtsschutzverfahren geprüft. Hier kam die Beantragung einer einstweiligen Anordnung beim Verwaltungsgericht Schwerin in Betracht. Einen entsprechenden Antrag haben wir am 8. Februar 2019 beim Verwaltungsgericht Schwerin gestellt.

Das Verwaltungsgericht Schwerin hat in der Folge beide Parteien zu einer Güteverhandlung eingeladen. In diesem Gütetermin haben wir uns mit dem Ministerium für Inneres und Europa darauf verständigt, dass die Übertragung der personenbezogenen Daten bei einer derartigen Videoüberwachung stets verschlüsselt zu erfolgen hat. Dieses Ergebnis wurde durch das Verwaltungsgericht Schwerin protokolliert. Die Videoüberwachung auf dem Marienplatz sollte entsprechend nachgerüstet werden. Für ähnliche Projekte wurde für die Zukunft festgehalten, dass auch hier die Videoüberwachung nur datenschutzrechtlich zulässig ist, wenn eine verschlüsselte Übertragung sichergestellt werden kann.

Die vom Verwaltungsgericht Schwerin initiierte Verständigung war aus unserer Sicht in jeder Hinsicht erfolgreich. Es bestand daher keine Veranlassung, ein förmliches Gerichtsverfahren weiter zu betreiben.

Das Ministerium für Inneres und Europa ist den Vereinbarungen aus dem Gütetermin gefolgt. Im Ergebnis der Güteverhandlung wurden einige Komponenten der Richtfunkstrecken ausgetauscht. Die neuen Komponenten ermöglichten es nun, den Videodatenstrom bei der Übertragung von den Kameras bis zu den Servern der Polizei auf allen Teilabschnitten zu verschlüsseln. Bei einer Besichtigung der verwendeten Relaisstellen konnten wir die geforderten mechanischen Vorrichtungen zum Schutz vor dem Zugriff unberechtigter Dritter begutachten und noch einige Hinweise zur weiteren Verbesserung dieser Vorkehrungen geben.

Unter Bezug auf die Vereinbarung im Gütetermin am Verwaltungsgericht Schwerin hat das Ministerium für Inneres und Europa uns im Oktober 2019 einen „Erfahrungsbericht der Polizeiinspektion Schwerin zum Projekt Bildüberwachung und -speicherung auf dem Marienplatz in Schwerin“ übermittelt und im persönlichen Gespräch erläutert. Dabei wurde auch erörtert, dass Beschwerden aus der Bevölkerung derzeit nicht zu verzeichnen sind. Allerdings wurde auch deutlich, dass die Erwartung, mit der Einrichtung der Bildüberwachung am Marienplatz würden Personen von strafbaren Handlungen abgehalten werden können, sich nicht erfüllt hat. Gerade Personen, die in Zusammenhang mit polizeilich relevanten Sachverhalten am Marienplatz angetroffen und befragt werden, verweisen bei der Sachverhaltsaufklärung häufig auf die Bildüberwachung und fordern deren Auswertung. Das Ministerium für Inneres und Europa hat uns im Oktober 2019 aber auch eine Tabelle mit dem Straftatenaufkommen und der Aufklärungsquote übermittelt, aus der sich ergibt, dass die Aufklärungsquote von Januar bis September 2019 deutlich gesteigert werden konnte.

Die Rechtsgrundlage für den Einsatz technischer Mittel zur offenen Bild- und Tonaufzeichnung im SOG M-V wird derzeit überarbeitet und in Kürze in Kraft treten. Wir werden uns fortlaufend über die Entwicklung informieren und in den Blick nehmen, welche Auswirkungen durch die Bildüberwachung auf dem Marienplatz auf das Straftatenaufkommen und die Aufklärungsquote tatsächlich zu verzeichnen sind.

8.2.3 Einsatz von Bodycams bei der Polizei

Die gesetzliche Grundlage für den Einsatz von Bodycams bei der Polizei Mecklenburg-Vorpommern hatte der Landtag Mecklenburg-Vorpommern bereits im Jahr 2018 auf den Weg gebracht. In diesem Gesetzgebungsverfahren hatten wir uns insbesondere zu der rechtlichen Grundlage des sogenannten Pre-Recordings und zum Einsatz der Bodycam in Wohn- und Geschäftsräumen kritisch geäußert. Wir haben bereits im Vierzehnten Tätigkeitsbericht darüber berichtet, siehe dort Punkt 9.1.2.

Das Ministerium für Inneres und Europa Mecklenburg-Vorpommern hat nach der Verabschiedung des Gesetzes das Pilotprojekt Bodycam gestartet und uns im Oktober 2019 die Auswertung dieses Projektes der Polizei Mecklenburg-Vorpommern vorgestellt. In seinem Bericht erläuterte das Ministerium, der Einsatz der Bodycam wirke bei dem polizeilichen Gegenüber deeskalierend. Darüber hinaus habe die Praxis gezeigt, dass die gesetzliche Regelung des Pre-Recording sinnvoll ist und auch die Regelung zum Einsatz der Bodycam in Wohn- und Geschäftsräumen sowie befriedetem Besitztum erforderlich sei. Das Ministerium hat entsprechende Zahlen vorgelegt, die diese Einschätzung untermauern.

Gleichwohl wird die Situation von der Polizei so eingeschätzt, dass eine zeitnahe, flächendeckende Einführung von Bodycams in Mecklenburg-Vorpommern derzeit nicht angezeigt ist. Vielmehr hat das Ministerium Schwerpunktdienststellen der Landespolizei ausgewählt, die schrittweise mit Bodycams ausgestattet werden.

Wir haben den Bericht des Ministeriums über das Pilotprojekt Bodycam zur Kenntnis genommen und der sukzessiven Einführung von Bodycams in der Landespolizei Mecklenburg-Vorpommern zugestimmt und werden die Umsetzung dieser Maßnahme weiter begleiten.

8.2.4 Bußgeldverfahren gegen Polizisten

Regelmäßig müssen wir Bußgeldverfahren gegen Polizisten wegen der Nutzung des Informationszugangs für private Zwecke führen. Aus den unterschiedlichsten privaten Gründen nutzen Polizeibeamtinnen und -beamte ihre dienstlichen Möglichkeiten zur Recherche in den Informationssystemen der Polizei. Besonders gravierende Fälle haben wir schon im Vierzehnten Tätigkeitsbericht dargelegt, siehe dort Punkt 9.1.4.

Im jetzigen Berichtszeitraum ist vor allem die Anzahl der Fälle zu erwähnen: Insgesamt wurden und werden bei uns bislang 16 Verfahren geführt. Wir betrachten diese Zahlen allerdings nur als die Spitze des Eisberges. Die konsequente Eröffnung von Bußgeldverfahren in den uns bekanntgewordenen Fällen zielt auch darauf ab, die Sensibilisierung für diesen Datenschutzbereich zu erhöhen und das Bewusstsein dafür zu schärfen, dass für Polizisten zu privaten Zwecken die Recherche in den Informationssystemen der Polizei tabu ist.

8.3 Justiz

8.3.1 Justizvollzugsdatenschutzgesetz

Das Justizvollzugsdatenschutzgesetz soll den Datenschutz in den Justizvollzugsanstalten in Mecklenburg-Vorpommern regeln. Dieses Gesetz haben wir von Beginn an begleitet. Das Justizministerium Mecklenburg-Vorpommern hat uns frühzeitig über dieses Gesetzesvorhaben informiert und uns die Gelegenheit zur Beteiligung gegeben. In diesem Verfahren wurden einige unserer datenschutzrechtlichen Hinweise aufgegriffen und umgesetzt. Insgesamt ist festzustellen, dass der Gesetzentwurf ersichtlich von dem Bestreben getragen ist, sowohl die Richtlinie (EU) 2016/680 (JI-RL) umzusetzen als auch die jüngste Rechtsprechung des Bundesverfassungsgerichts (BVerfG) zu berücksichtigen.

Den Gesetzentwurf beurteilen wir aus datenschutzrechtlicher Sicht insgesamt als sehr gut gelungen. Wir haben allerdings auch auf verschiedene Punkte hingewiesen, die bis jetzt keine Berücksichtigung gefunden haben.

Besonders kritisch sehen wir nach wie vor, dass unsere Befugnisse gegenüber der JI-RL zu stark eingeschränkt werden. Die in Art. 47 Abs. 2 JI-RL vorgesehenen Befugnisse der Datenschutzaufsichtsbehörde werden durch den Gesetzentwurf nicht so umgesetzt, wie es in Art. 47 Abs. 2 JI-RL vorgesehen ist. Dieser verlangt, dass der Datenschutzaufsichtsbehörde wirksame Befugnisse eingeräumt werden, mit denen der Verantwortliche angewiesen werden kann, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums mit den nach dieser Richtlinie erlassenen Vorschriften in Einklang zu bringen, insbesondere durch die Anordnung der Berichtigung oder Löschung personenbezogener Daten oder Einschränkung der Verarbeitung. Ebenso muss die Datenschutzaufsichtsbehörde eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, verhängen können.

Der Gesetzentwurf wird in Kürze den parlamentarischen Raum erreichen, wo wir weiter darauf hinweisen werden, was aus unserer Sicht in diesem Gesetzesvorhaben zu berücksichtigen ist, denn wir werden dieses Gesetzgebungsverfahren auch im parlamentarischen Raum weiter begleiten.

8.3.2 Kopie der Prüfungsakte des Landesjustizprüfungsamtes

Ein Absolvent der ersten juristischen Staatsprüfung hatte sich mit einer Beschwerde an uns gewandt, weil das Landesjustizprüfungsamt ihm keine Ablichtung seiner Prüfungsakte übersenden wollte. Wir haben angeordnet, dass das Landesjustizprüfungsamt dem Betroffenen eine vollständige Kopie seiner Prüfungsakte erstellen und übersenden muss.

Die schriftlichen Lösungen eines Prüflings und etwaige Anmerkungen der Prüfer zu diesen Lösungen sind personenbezogene Daten, die in einem Dateisystem gespeichert werden. Nach Art. 15 Abs. 3 Europäische Datenschutz-Grundverordnung (DS-GVO) besteht ein Anspruch auf Übermittlung einer Kopie dieser personenbezogenen Daten.

Zwar gibt es Grenzen für das Recht auf Übersendung einer Datenkopie. Hier ist eine solche Grenze aber nicht erreicht. Insbesondere darf dem Prüfling nicht entgegengehalten werden, die Erstellung der Kopie stelle einen zu großen Aufwand für das Landesjustizprüfungsamt dar.

Das Landesjustizprüfungsamt ist unserer Anordnung gefolgt und hat dem Betroffenen eine vollständige Kopie der Prüfungsakte übersandt.

8.4 Gesundheitswesen

8.4.1 Digitale Anwendungen und datenschutzrechtliche Verantwortlichkeiten

Die elektronische Patientenakte, digital verfügbare Notfalldaten, ein elektronischer Medikationsplan und der sichere Datenaustausch und E-Mail-Verkehr zwischen Angehörigen von Gesundheitsberufen - das sind die ambitionierten Ziele des Ende 2015 in Kraft getretenen E-Health-Gesetzes. Dafür braucht es vor allem eines: ein sicheres Kommunikationsnetzwerk. Diese Telematikinfrastruktur soll die Gematik sicherstellen. Die Gematik ist ein Unternehmen, deren Gesellschafter das Bundesministerium für Gesundheit (BMG), die Bundesärztekammer (BÄK), die Bundeszahnärztekammer (BZÄK), der Deutsche Apothekerverband (DAV), die Deutsche Krankenhausgesellschaft (DKG), der Spitzenverband der Gesetzlichen Krankenversicherungen (GKV-SV), die Kassenärztliche Bundesvereinigung (KBV) und die Kassenzahnärztliche Bundesvereinigung (KZBV) sind.

Patientinnen und Patienten können zumindest bei einzelnen Anwendungen selbst entscheiden, ob sie diese nutzen oder nicht. Die Pflichtanwendungen sind für alle Mitglieder der gesetzlichen Krankenkassen verbindlich. Dazu zählen der Online-Abgleich der Versichertenstammdaten auf der elektronischen Gesundheitskarte, das elektronische Empfangen und Einlösen einer Verordnung (eVerordnung) mit der Karte sowie die Verwendung der Europäischen Krankenversicherungskarte (EHIC) auf der Rückseite. Zu den freiwilligen Anwendungen gehören das Notfalldaten-Management, der elektronische Medikationsplan und das Datenmanagement zur Prüfung der Arzneimitteltherapiesicherheit, Anwendungen der Versicherten und die Elektronische Patientenakte. Angehörige von Gesundheitsberufen, wie Ärzte, Zahnärzte, Psychotherapeuten oder Apotheker, sind verpflichtet, sich an die Telematikinfrastruktur anzuschließen, sonst drohen Honorarabzüge. Hierzu müssen bestimmte zertifizierte Konnektoren beschafft und installiert werden.

Doch wer ist eigentlich datenschutzrechtlich verantwortlich für diese Anwendungen? Wer haftet, wenn trotz aller Sicherheitsvorkehrungen der Schutz der sensiblen Patientendaten verletzt wird? Wer ist dafür zuständig, die umfangreichen datenschutzrechtlichen Pflichten zu erfüllen? Also wer muss die Datenschutz-Folgenabschätzung (DSFA) für diese Anwendungen machen? Müssen Angehörige von Gesundheitsberufen jetzt nur wegen des Anschlusses an die Telematikinfrastruktur Datenschutzbeauftragte bestellen? Wie ist die Information der Patientinnen und Patienten über die Datenverarbeitung sicherzustellen?

Mit Fragen wie diesen wurden wir 2019 vielfach konfrontiert. Lange Zeit waren diese Fragen ungeklärt. Gemeinsam mit den Datenschutzaufsichtsbehörden anderer Bundesländer haben wir uns in verschiedenen Arbeitsgruppen der Datenschutzaufsichtsbehörden des Bundes und der Länder dafür eingesetzt, dass die alleinige Verantwortlichkeit keinesfalls bei den Angehörigen der Gesundheitsberufe liegen kann, sondern die Gematik für all das, was den Nutzern vorgeschrieben wird, die Verantwortung tragen muss. Unsere Bemühungen sind in einen Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) eingeflossen, der für alle Aufsichtsbehörden verbindlich ist. Danach ist die Gematik alleinverantwortlich für die sogenannte zentrale Zone, also insbesondere die TI-Plattform. Bei der sogenannten dezentralen Zone, also im Wesentlichen der Bereich des Anschlusses bei den Nutzern vor Ort, besteht eine sogenannte gemeinsame Verantwortlichkeit, die durch den Gesetzgeber weiter ausdifferenziert werden muss. In jedem Fall ist die Gematik verantwortlich für die von ihr vorgegebenen Spezifikationen und Konfigurationen für die Konnektoren, VPN-Zugangsdienste und Kartenterminals. Die Verantwortlichkeit bleibt insoweit bei den Anwendern, als dass diese sichere Rahmenbedingungen für den Anschluss an die Telematikinfrastruktur schaffen müssen, die aber ohnehin selbstverständlich sind.

Gemeint sind hier etwa bestimmte Konfigurationen der Praxis-Software oder eine Zugangskontrolle zu Datenverarbeitungsgeräten und Räumlichkeiten. Im Ergebnis sind Anwender nicht verpflichtet, eine Datenschutz-Folgenabschätzung (DSFA) für die Telematikinfrastruktur vorzunehmen. Folglich müssen auch keine Datenschutzbeauftragten bestellt werden, nur weil sich Anwender an die Telematikinfrastruktur anschließen lassen. Die Information der Patientinnen und Patienten zur Datenverarbeitung sollte aber um die Gematik bei den Empfängern personenbezogener Daten erweitert werden. Weitergehende Informationen zur Telematikinfrastruktur erhalten Patientinnen und Patienten dann auf der Homepage der Gematik: https://www.gematik.de/.

8.4.2 Projekt „Umgang mit Patientendaten in den Krankenhäusern Mecklenburg-Vorpommerns (UPDK)"

Projekt

Mit der Europäischen Datenschutz-Grundverordnung (DS-GVO) kamen auch auf die Krankenhäuser und Universitätskliniken in Mecklenburg-Vorpommern neue Aufgaben zu. Um hier bei den anstehenden Fragen zu unterstützen, hat der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern in Kooperation mit dem Datenschutzbeauftragten der Nordkirche im Jahr 2018 das Projekt „Umgang mit Patientendaten in den Krankenhäusern Mecklenburg-Vorpommerns (UPKD)“ initiiert, siehe auch Vierzehnter Tätigkeitsbericht, Punkt 6.3. Das Projekt ist im Berichtszeitraum fortgeführt und beendet worden.

Ziel des Projektes war es, einen Überblick über den Stand des Umgangs mit Patientendaten in ausgewählten Handlungsfeldern der Krankenhäuser und Universitätskliniken in Mecklenburg-Vorpommern zu erhalten. Gemeinsam mit den beteiligten Krankenhäusern und Universitätskliniken in Mecklenburg-Vorpommern wurden Aspekte des Datenschutzes in der täglichen Arbeit erörtert, wie Unsicherheiten im Hinblick auf die zahlreichen Beteiligten an den einzelnen Prozessen, auf die vorhandenen Informationsflüsse, auf die Umsetzung von Betroffenenrechten (insbesondere gemäß Art. 12, 13 DS-GVO).

Darüber hinaus wurden die Krankenhausinformationssysteme (*KIS*) einer weitergehenden Betrachtung unterzogen. Im Ergebnis konnten so mit den Krankenhäusern und Universitätskliniken Verfahrensweisen bewertet und Veränderungen erarbeitet werden.

Der Projektbericht ist zu finden unter: https://www.datenschutz-mv.de/datenschutz/Projekte/-UPDK/

Danken möchten wir allen Beteiligten an diesem Projekt - den Krankenhäusern und Universitätskliniken in Mecklenburg-Vorpommern, der Landeskrankenhausgesellschaft Mecklenburg-Vorpommern, dem Datenschutzbeauftragten der Nordkirche, Peter von Loeper. Ein besonderer Dank gilt unserer ehemaligen Mitarbeiterin Coretta Mauch, die für dieses Projekt befristet in der Behörde des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern eingestellt war und mit besonderem Engagement und großer Fachkenntnis maßgeblich zum Gelingen des Projektes beigetragen hat.

Datenschutz-Fachtagung „Datenschutz: Krankheit oder Therapie?

Ein Ergebnis des Projektes war die Datenschutz-Fachtagung zum Thema „Datenschutz: Krankheit oder Therapie?“, die aufgrund des erhöhten Informationsbedarfes zum Thema Datenschutz in Krankenhäusern und Universitätskliniken in Mecklenburg-Vorpommern am 28. Oktober 2019 im Bürgersaal in Waren (Müritz) durchgeführt wurde. Eingeladen waren Geschäftsführungen, Datenschutzbeauftragte, Ärztinnen und Ärzte, Mitarbeitende in den Verwaltungen sowie Pflegekräfte und weitere Fachkräfte der Krankenhäuser und Universitätskliniken in Mecklenburg-Vorpommern. Inhaltlicher Schwerpunkt dieser Fachtagung waren die Auswirkungen der Europäischen Datenschutz-Grundverordnung (DS-GVO) auf die Arbeit in den Krankenhäusern und Universitätskliniken des Landes. Im Rahmen der Datenschutz-Fachtagung wurde diskutiert, ob der Datenschutz eher als „Krankheit“ wirkt und den Versorgungsbetrieb stört oder ob der Datenschutz eher wie eine „Therapie“ wirkt und, richtig angewandt, unerwünschte Auswirkungen beseitigen kann. In vier bereichsspezifischen Diskussionsforen wurden Fragen der Teilnehmenden beantwortet und Lösungen aufgezeigt. Auch hier sei allen Beteiligten, insbesondere den Referentinnen und Referenten aus den Krankenhäusern und Universitätskliniken, herzlich gedankt.

Informationen zur Datenschutz-Fachtagung finden Sie unter: https://www.datenschutz-mv.de/-veranstaltungen/fachtagungen/Datenschutz_Krankheit_oder_Therapie

8.5 Neue Zuständigkeiten im Finanzbereich

Die Zuständigkeit für die datenschutzrechtliche Aufsicht im Steuerwesen ist seit dem 25. Mai 2018 neu geregelt. Bis dahin oblag die datenschutzrechtliche Aufsicht über die Finanzämter und über die kommunalen Steuerbehörden unserer Behörde. Durch § 32 h Abs. 1 Satz 1 Abgabenordnung (AO) wird die datenschutzrechtliche Aufsicht über die Finanzbehörden bei der Verarbeitung personenbezogener Daten im Anwendungsbereich der Abgabenordnung auf den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit übertragen.

Diese Neuregelung wird mit einem Interesse an einer bundesweit einheitlichen Anwendung der Abgabenordnung begründet, hat jedoch eine Zuständigkeitsteilung zwischen Bund und Ländern mit einigen Abgrenzungsschwierigkeiten zur Folge und bedarf daher einer kurzen Erläuterung.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ist zuständig für die Aufsicht in Bezug auf die Verwaltung bundesgesetzlich geregelter Steuern von den Finanzämtern (z. B. Einkommensteuer, Umsatzsteuer, Körperschaftssteuer, Schenkungssteuer, Erbschaftssteuer). Ebenso betrifft dies auch die Aufsicht bezüglich der Grund- und Gewerbesteuer (Realsteuern), wenn entweder das Finanzamt dafür zuständig ist (bundesgesetzlich geregelte Steuern) oder aber die Gemeinde, soweit sie die Realsteuern im Anwendungsbereich der Abgabenordnung erhebt und festsetzt.

Handeln die kommunalen Steuerämter dagegen im Rahmen der Vollstreckung von Realsteuern oder in außergerichtlichen Rechtsbehelfsverfahren nicht auf der Grundlage der Abgabenordnung, sondern aufgrund anderer Rechtsgrundlagen, wie der Verwaltungsgerichtsordnung (VwGO) oder landesrechtlicher Vorschriften, ist unsere Behörde weiterhin zuständig. Sobald Steuern von den Kommunen verwaltet und aufgrund landesrechtlicher beziehungsweise kommunaler Regelungen erhoben werden (z. B. Zweitwohnungssteuer und Hundesteuer), liegt die datenschutzrechtliche Aufsicht ebenfalls bei unserer Behörde.

Dies trifft ebenso für die Kirchensteuer zu, soweit deren Verwaltung durch die staatlichen Finanzbehörden auf dem Kirchensteuergesetz des Landes Mecklenburg-Vorpommern (KiStG M-V) beruht.

Des Weiteren unterliegen die Finanzämter, wie bisher auch, unserer datenschutzrechtlichen Aufsicht, wenn es um nicht-steuerbezogene Tätigkeiten geht. Dies betrifft vor allem den Beschäftigtendatenschutz, also die Frage, ob die Finanzämter mit den personenbezogenen Daten ihrer Mitarbeiterinnen und Mitarbeiter datenschutzgerecht umgehen.

8.6 Zensus 2021

Im Jahr 2021 findet in Deutschland wieder ein Zensus statt. Damit nimmt Deutschland an einer EU-weiten Zensusrunde teil, die seit 2011 alle zehn Jahre stattfindet.

Um verlässliche Basiszahlen für Planungen zu haben, ist eine regelmäßige Bestandsaufnahme der Einwohnerzahl notwendig. Mit einer solchen statistischen Erhebung wird ermittelt, wie viele Menschen in Deutschland leben, wie sie wohnen und arbeiten. Viele Entscheidungen in Bund, Ländern und Gemeinden beruhen auf Bevölkerungs- und Wohnungszahlen. Die amtliche Einwohnerzahl ist eine wichtige Grundlage für zahlreiche rechtliche Regelungen und für politische Planungen und andere Vorhaben (z. B. Einteilung der Wahlkreise, Festlegung der Stimmenverteilung der Länder im Bundesrat, Länderfinanzausgleich, Berechnungen für EU-Fördermittel, Planung von Schulen, Studienplätzen oder Altenheimen).

In Deutschland ist der Zensus 2021 eine registergestützte Bevölkerungszählung, die durch eine Haushaltebefragung auf Stichprobenbasis ergänzt und mit einer Gebäude- und Wohnungszählung sowie Erhebungen an Anschriften mit Sonderbereichen kombiniert wird.

In erster Linie werden also bereits vorhandene Daten aus Verwaltungsregistern, insbesondere Melderegisterdaten genutzt, sodass die Mehrheit der Bevölkerung keine Auskunft leisten muss. Ergänzende Erhebungen werden nur dann durchgeführt, wenn Verwaltungsdaten für bestimmte Merkmale nicht vorhanden oder aus statistischer Sicht nicht für die Auswertung geeignet sind.

Mit dem Zensusgesetz 2021 hat das Bundesministerium des Innern, für Bau und Heimat die rechtlichen Voraussetzungen zur Durchführung des Zensus geschaffen. Durchgeführt wird der Zensus vom Statistischen Bundesamt und den Statistischen Landesämtern. Das Statistische Amt Mecklenburg-Vorpommern richtet für die Vorbereitung und Durchführung der statistischen Erhebungen Erhebungsstellen ein, die von der restlichen Verwaltung organisatorisch, personell, technisch und räumlich getrennt sind. Zudem werden sogenannte Erhebungsbeauftragte bestellt, die stichprobenartige Befragungen bei Auskunftspflichtigen durchführen. Zur technischen Ausstattung der Laptops, die die Erhebungsbeauftragten nutzen, beraten wir das Statistische Amt. Dabei geht es beispielsweise um technische Maßnahmen zum Schutz der erhobenen Daten bei der Übermittlung vom Laptop zu den zentralen IT-Systemen oder um die Auswahl eines datenschutzkonformen Betriebssystems der Laptops, siehe dazu auch Punkt 7.1.2.

Das Statistische Amt informiert den Landesbeauftragten in bewährter Weise - wie bereits bei der letzten Volkszählung 2011 - über alle relevanten datenschutzrechtlichen Fragestellungen, damit offene Fragen frühestmöglich geklärt werden können.

8.7 Schule/Bildung

8.7.1 Integriertes-Schulmanagement-System (ISY)

Im Zuge der Digitalisierung im Schulbereich will das Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern eine einheitliche Schulverwaltungssoftware für die Schulen im Land bereitstellen. Das Projekt für ein Integriertes-Schulmanagement-System (ISY) konnten wir im Berichtszeitraum beratend begleiten. In zahlreichen Gesprächen mit dem Ministerium haben wir sowohl die datenschutzrechtlichen Anforderungen als auch die Herausforderungen bei der Planung sowie beim Einsatz einer einheitlichen Schulverwaltungssoftware erörtert. Die Zusammenarbeit mit dem Ministerium begrüßen wir ausdrücklich. Bereits im Dreizehnten Tätigkeitsbericht haben wir unter Punkt 6.8.1 darauf hingewiesen, dass bei der künftigen Planung einer einheitlichen Schulverwaltungssoftware die datenschutzrechtlichen Aspekte frühzeitig berücksichtigt werden sollten.

Wir empfehlen dem Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern, den sehr produktiven Meinungsaustausch mit uns beizubehalten, die Abstände der Gespräche zwischen beiden Häusern im Jahr 2020 jedoch deutlich zu verkürzen.

8.7.2 Bring Your Own Device (BYOD) im Schulbereich

Auch in diesem Berichtszeitraum erhielten wir Anfragen zum Thema „Bring Your Own Device“ (BYOD) im Umfeld von Schulen. Dort bedeutet der Begriff BYOD, dass Lehrkräfte ihre privaten Datenverarbeitungsanlagen (private Endgeräte wie Smartphone, Tablet, Notebook) der Schule für deren Aufgabenerfüllung zur Verfügung stellen. Nachfolgend möchten wir grundsätzliche Überlegungen zum BYOD-Modell anstellen und Hinweise hierzu geben.

Zunächst ist die grundsätzliche Frage zu stellen, warum Lehrkräfte (Bedienstete des Landes) den Schulen (verantwortliche Stellen) ihre privaten Datenverarbeitungsgeräte zur Verfügung stellen sollten, damit der Staat (die Schulen) seinem gesetzlich bestimmten Auftrag zur Bildung und Erziehung nachkommen kann. Den Lehrkräften wird nicht einfach zu vermitteln sein, warum Aufgaben des Staates unter Nutzung privater Technik erfüllt werden sollen.

Weiterhin wäre zu klären, wer die privaten Endgeräte im Namen des Verantwortlichen (Schule) technisch betreuen soll. Schulen verfügen weder über die dafür erforderliche Rechtsfähigkeit noch über die notwendigen finanziellen Mittel. Daher käme dafür zurzeit nur der Schulträger in Betracht. Datenschutzrechtlich sind Schulen und Schulträger jedoch jeweils eigenständige Verantwortliche mit unterschiedlichen Datenverarbeitungsbefugnissen. Aus dem Schulgesetz für das Land Mecklenburg-Vorpommern (SchulG M-V) ergibt sich, dass die Schulträger verpflichtet sind, die Schulen mit Technik auszustatten und diese zu administrieren. Sie sind hingegen nicht verpflichtet, die technische Administration privater Datenverarbeitungsanlagen der Lehrkräfte für den dienstlichen Gebrauch zu gewährleisten. Wenn ein Schulträger das BYOD-Modell technisch und finanziell unterstützt, muss er einen Vertrag zur Auftragsverarbeitung mit dem Verantwortlichen (Schule) abschließen, da der Schulträger keine eigene Datenverarbeitungsbefugnis für die beim BYOD-Modell anfallenden personenbezogenen Daten hat. Art. 28 Europäische Datenschutz-Grundverordnung (DS-GVO) ist dann vollumfänglich einzuhalten und schließt das neue Haftungsrisiko der DS-GVO für Auftragsverarbeiter ein. In diesem Zusammenhang muss daher die grundsätzliche Frage aufgeworfen werden, warum sich Schulträger über ihre gesetzlich normierten Aufgaben hinaus einem zusätzlichen finanziellen Risiko aussetzen sollten, wenn sie bereits die Schulen mit Technik ausstatten.

Sollte trotz aller Bedenken die Umsetzung des BYOD-Modelles geplant werden, sind folgende Hinweise zu berücksichtigen:
Das Zurverfügungstellen der privaten Datenverarbeitungsgeräte durch Lehrkräfte muss völlig freiwillig sein.

Die Schule muss als Verantwortlicher der Rechenschaftspflicht zur Einhaltung aller datenschutzrechtlichen Vorgaben gemäß Art. 5 Abs. 2 DS-GVO nachkommen. Beim BYOD-Modell kann die Schule rechtlich zunächst keine Ansprüche gegen die Lehrkraft durchsetzen, solange sie keine faktische Hoheit über das private Endgerät hat und ihr noch keine vertraglichen Nutzungs- und Administrationsrechte übertragen wurden. Dafür wären vertragliche Vereinbarungen zwischen der Schule und der Lehrkraft zu schließen, welche zwangsläufig umfänglich in das Recht der Nutzung des privaten Datenverarbeitungsgerätes der Lehrkraft eingreifen. Die Lehrkraft wäre dann zwar weiterhin Eigentümer des Gerätes, würde jedoch ihre eigenen Nutzungsrechte stark einschränken bzw. vollständig an die Schule abgeben.

- Der Schule ist ein Zutrittsrecht zur privaten Wohnung der Lehrkraft zu datenschutzrechtlichen Kontrollzwecken einzuräumen, damit sie ihrer Rechenschaftspflicht nachkommen kann.
- Für die Administration und Dokumentation unterschiedlicher privater Endgeräte von Lehrkräften sind unter anderem das Verzeichnis von Verarbeitungstätigkeiten, Datenschutz- und Sicherheitskonzepte (für eine Vielzahl von unterschiedlichen Geräten), die stetige Wartung der Geräte sowie die Umsetzung umfassender technischer und organisatorischer Maßnahmen erforderlich.

Vor einer weiteren Diskussion der datenschutzrechtlichen Aspekte von BYOD-Modellen sollten zudem folgende Fragen geklärt werden:

- Sind die Lehrkräfte bereit, ihre private Technik der Schule für deren Aufgabenerfüllung zur Verfügung zu stellen?
- Ist der Lehrer-Hauptpersonalrat als Gesamtvertretung für alle Lehrkräfte mit dem BYOD-Modell vertraut und würde er diesem zustimmen?
- Sind die Schulträger mit dem BYOD-Modell vertraut und insbesondere über die zusätzlichen, über die gesetzlichen Anforderungen hinausgehenden Verpflichtungen (Auftragsverarbeiter, Administration der privaten Datenverarbeitungsanlagen, finanzielles Risiko, Tragen der Kosten) informiert und stimmen sie diesen zu?

Die vorstehenden Überlegungen und Hinweise verdeutlichen, dass das BYOD-Modell allenfalls einen theoretischen Ansatz darstellt. Wir gehen davon aus, dass dieses Modell an der praktischen Umsetzbarkeit und an der fehlenden Akzeptanz der beteiligten Akteure scheitern wird.

8.8 Datenverarbeitung in Vereinen

8.8.1 Rechtsgrundlagen

Im Berichtszeitraum haben uns viele Anfragen von Vereinen zur Umsetzung der Europäischen Datenschutz-Grundverordnung (DS-GVO) erreicht, die für eine gewisse Unsicherheit beim Umgang mit Mitgliederdaten sprachen.

Grundsätzlich gilt, dass die Verarbeitung personenbezogener Daten im Verein nur dann zulässig ist, wenn sie für die Begründung und die Durchführung eines Vertragsverhältnisses (Buchhaltung, Mitgliederverwaltung oder Durchführung von Vereinsaktivitäten) erforderlich ist. Ein solches Vertragsverhältnis geht das Mitglied mit seinem Beitritt in den Verein ein. Verantwortlicher im Sinne der DS-GVO ist immer der Verein, also der Vorstand.

Die Rechtsgrundlagen für die Verarbeitung von Mitgliederdaten finden sich in Art. 6 DS-GVO. Unter diese Rechtsvorschrift fallen alle Verarbeitungen der Mitgliederdaten, die für die Verwaltung und Betreuung der Mitglieder und die Verfolgung der Vereinsziele erforderlich sind. Wenn also beispielsweise das Ziel des Vereins unter anderem darin besteht, seine Mitglieder untereinander in Kontakt zu bringen (z. B. bei Ehemaligenvereinen) sowie bei Vereinen, deren Ziel in der Vernetzung seiner Mitglieder besteht, ist die Zulässigkeit gemäß Art. 6 Abs. 1 lit. b DS-GVO leicht ersichtlich.

In diesem Fall wäre das Verteilen von Mitgliederlisten in der Regel durch diese Bestimmung gedeckt. Vereinsziele müssen aber in der Satzung definiert sein, damit sie als Rechtfertigungsgrund dienen können. Die einzelnen Verarbeitungen müssen hier mit ihrem konkreten Zweck transparent aufgeführt werden.

8.8.2 Einwilligung

Sollen personenbezogene Daten zu Zwecken verarbeitet werden, die in der Satzung nicht erwähnt sind, ist als gesetzliche Grundlage eine Einwilligung der Mitglieder erforderlich. Eine Einwilligung kann beispielsweise in Teilnahmeanträgen enthalten sein.

Die Einwilligung ist nicht zwingend schriftlich einzuholen. Auch mündliche Erklärungen sind wirksam. Da das Vorliegen von Einwilligungen im Zweifelsfall jedoch nachgewiesen werden muss, sind schriftliche Einwilligungen vorzuziehen, denn im Fall von Unstimmigkeiten führen sie für den Verein immer zu Rechtssicherheit.

Eine starre Altersgrenze in Bezug auf die Einwilligungsfähigkeit kennt die DS-GVO außerhalb des Art. 8 DS-GVO (hier 16 Jahre, diese Vorschrift gilt nur im Zusammenhang mit kindorientierten Telemedien, wie z. B. an Kinder gerichtete Onlineshops und -spiele) nicht. Bei Kindern unter 13 Jahren ist nach unserer Auffassung regelmäßig davon auszugehen, dass sie die Konsequenzen der Verwendung ihrer Daten noch nicht übersehen können. Ist die Einsichtsfähigkeit zu verneinen, ist die Verarbeitung der Daten nur mit Einwilligung der Personensorgeberechtigten zulässig.

8.8.3 Herausgabe von Mitgliederlisten an die Vereinsmitglieder

Bei Vereinsmitgliedern untereinander handelt es sich im Datenschutzrecht um Dritte. Vereinsmitglieder dürfen also nicht einfach auf die Daten der anderen Mitglieder zugreifen. Mitgliederlisten dürfen daher nicht ohne weiteres herausgegeben werden. Wie unter Punkt 8.9.1 ausgeführt, wäre die Weitergabe der Mitgliederliste durch Art. 6 Abs. 1 lit. b DS-GVO lediglich dann gedeckt, wenn das Ziel des Vereins darin besteht, seine Mitglieder untereinander in Kontakt zu bringen oder der Vernetzung seiner Mitglieder dient. Anderenfalls wäre die Einwilligung der Mitglieder einzuholen.

8.8.4 Leitfaden für Vereine

Da uns seit dem Inkrafttreten der DS-GVO viele Fragen zum Umgang mit Mitgliederdaten erreichten, haben wir den „Leitfaden Datenschutz - Orientierungshilfe für Vereine in Mecklenburg-Vorpommern“, der auf unserer Internetseite veröffentlicht ist[38], gemeinsam mit der Stiftung für Ehrenamt und bürgerschaftliches Engagement in Mecklenburg-Vorpommern erarbeitet. Dieser enthält auch Muster für eine Einwilligungserklärung für die Veröffentlichung von Mitgliederdaten im Internet (Seite 22) sowie ein Muster für die Erfüllung der Informationspflicht bei der Erhebung von personenbezogenen Daten gemäß Art. 13 DS-GVO (Seite 25 und 31). Auch auf der Internetseite des Landessportbundes Mecklenburg-Vorpommern e. V. gibt es unter der Überschrift „Datenschutz - Erste Hilfe zur Datenschutz-Grundverordnung für Sportvereine“ entsprechende Hinweise[39].

8.9 Kommunales

8.9.1 Speicherung Daten Verstorbener in einem Bestattungsportal

Wir wurden darüber informiert, dass ein städtischer Friedhof die Möglichkeit einräumen würde, online auf einem sogenannten Bestattungsportal nach Verstorbenen zu suchen sowie einen Trauerfeierkalender einzusehen. In dem uns zur Bewertung vorliegenden Fall gab der Petent an, dass er als Hinterbliebener keine Einwilligung zur Datenverarbeitung gegeben hat, und bat deshalb um rechtliche Prüfung.

Auch wenn es hierbei um Daten bereits Verstorbener und es sich somit um den sogenannten postmortalen Datenschutz handelt, ist zu beachten, dass personenbezogene Daten auch nach dem Tod geschützt sind und es somit einer Rechtsgrundlage bedarf.

Die betreffende Kommune gab an, dass es sich bei dem Bestattungsportal um eine städtische Serviceleistung handeln würde. Die Veröffentlichung und die damit einhergehende Datenverarbeitung wurde insbesondere damit gerechtfertigt, dass in dem Portal Daten enthalten seien, die regelmäßig bereits durch Traueranzeigen in der Zeitung bekanntgegeben werden. Außerdem seien Namen und Lebensdaten auf den Grabsteinen für jedermann sichtbar. Auch würde die Möglichkeit bestehen, bei der Beantragung von Bestattungsleistungen die Einwilligung zu versagen.

Dem Argument der Nutzung von personenbezogenen Daten, die bereits auf anderem Wege der Öffentlichkeit zugänglich gemacht wurden, hielten wir entgegen, dass dies unter Berücksichtigung der Bestimmungen zur DS-GVO keine Rechtmäßigkeit einer Datenverarbeitung impliziert. Lediglich das bis zum 25. Mai 2018 geltende Datenschutzrecht erlaubte in § 10 Abs. 3 Nr. 5 DSG M-V (alt) gegebenenfalls eine Nutzung personenbezogener Daten zu anderen Zwecken, soweit diese aus allgemein zugänglichen Quellen entnommen werden konnten und keine schutzwürdigen Interessen der Betroffenen dem entgegenstanden.

[38] https://www.datenschutz-mv.de/datenschutz/publikationen/Hilfe-f%C3%BCr-Vereine
[39] https://www.lsb-mv.de/service/datenschutz/

Auch den Hinweis, dass die Einwilligung versagt werden könnte, akzeptierten wir nicht, da dies eine Widerspruchslösung und keine wirksame Einwilligung darstellt. Deshalb haben wir die Empfehlung ausgesprochen, künftig nur noch Veröffentlichungen im Bestattungsportal durchzuführen, wenn hierfür die Einwilligung der Angehörigen vorliegt. Dieser Empfehlung ist die Stadtverwaltung gefolgt.

8.9.2 Verweigerung von Auskunftsansprüchen

Ein Petent informierte uns darüber, dass er bei einer Landkreisverwaltung das ihm nach Art. 15 DS-GVO zustehende Auskunftsrecht geltend gemacht hat. Dieser Antrag wurde zunächst abgelehnt, da dieser Inhalte aus einem Ordnungswidrigkeitenverfahren betraf und somit der Ablehnungstatbestand nach § 6 Abs. 2 Nr. 2 DSG M-V gegeben war. Erst nach Abschluss des OWiG-Verfahrens kam es zu der Beauskunftung. Im Zusammenhang mit der in § 6 DSG M-V enthaltenen beschränkenden Regelung, aufgrund dessen die Auskunft erst nach Verfahrensabschluss gewährt wurde, wies die Landkreisverwaltung darauf hin, dass es sich „bei dem Datenschutzgesetz des Landes Mecklenburg-Vorpommern um eine höherrangige Vorschrift handele und diese Vorrang vor einer EU-Verordnung habe“.

Diese Behauptung hat uns irritiert. Da die DS-GVO in all ihren Teilen verbindlich ist und unmittelbar in jedem Mitgliedstaat gilt, hat nicht das DSG M-V, sondern die DS-GVO Vorrang vor nationalem Recht. Somit haben die Gesetze nationaler Gesetzgeber die Vorgaben und Grundsätze der DS-GVO zu beachten. Für die Normenhierarchie gilt also, dass ganz oben die DS-GVO steht. Unter ihr stehen unionsrechtliche und mitgliedstaatliche Gesetze und Rechtsordnungen.

Aus unserer Sicht bedurfte es an dieser Stelle einer Klarstellung zu der vorgenannten Normenhierarchie, die durch das Innenministerium Mecklenburg-Vorpommern gegenüber der betreffenden Verwaltung auch vorgenommen wurde.

8.9.3 Nutzung von Drohnen zu behördlichen Zwecken

Eine Amtsverwaltung stellte an uns die Frage, ob der Einsatz einer Flugdrohne zu behördlichen Zwecken zulässig sei.

Flugdrohnen als sogenannte unbemannte Luftfahrtsysteme bzw. Flugmodelle unterliegen gemäß § 21 a der Luftverkehrsordnung (LuftVO) grundsätzlich einem Erlaubniserfordernis. Sofern diese Drohnen jedoch von Behörden zum Zwecke ihrer Aufgabenerfüllung genutzt werden, bedarf es einer solchen Erlaubnis nicht. Nichtdestotrotz müssen bei einem möglichen Einsatz insbesondere datenschutzrechtliche Aspekte berücksichtigt und eingehalten werden.

Durch die Aufnahme von Bildern mit Flugdrohnen werden personenbezogene Daten verarbeitet, da auch schon Bilder eines Grundstückes mit den dazugehörigen baulichen Anlagen Rückschluss auf die wirtschaftlichen Verhältnisse einer natürlichen Person erlauben. Eine derartige Datenverarbeitung ist unter anderem dann zulässig, wenn eine Rechtsgrundlage dieses erlaubt.

So ist beispielsweise vorstellbar, dass Flugdrohnen beim Brandschutz eingesetzt werden. Nach § 7 Abs. 3 BrSchG sind öffentliche Feuerwehren unter anderem befugt, Grundstücke, Anlagen und Gebäude zum Zwecke der Brandbekämpfung zu betreten. Gemäß dieser Vorschrift in Verbindung mit § 4 DSG M-V ist es durchaus vorstellbar, dass beispielsweise Flugdrohnen bei einer durchzuführenden Brandwache als „verlängertes Auge“ der Feuerwehr eingesetzt werden. Ein etwaiger Drohneneinsatz durch die Feuerwehren kann unter Berücksichtigung der jeweiligen Gefahrenlage somit gerechtfertigt sein.

In jedem Fall muss der Grundsatz der Verhältnismäßigkeit beachtet werden. Somit dürfen nur die für die Aufgabenerfüllung erforderlichen personenbezogenen Daten verarbeitet werden.

Folglich ist eine Datenverarbeitung nur dann zulässig, wenn die Aufgabe sonst nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllt werden kann. Auf eine bloße Nützlichkeit bestimmter Daten kommt es hierbei nicht an. Von daher sollte der Einsatz von Drohnen kritisch geprüft und restriktiv gehandhabt werden.

8.9.4 Entwendung einer Festplatte aus einem Hortraum

Aufgrund einer Datenpannenmeldung wurden wir darüber informiert, dass aus einem abgeschlossenen Hortraum eine externe (unverschlüsselte) Festplatte entwendet wurde, auf der auch personenbezogene Daten gespeichert waren.

Aus unserer Sicht waren schwerpunktlich zwei Punkte zu klären. Auf der Festplatte sollen Daten der letzten zehn Jahre vorhanden gewesen sein. Uns stellte sich die Frage, warum die Daten für einen derartig langen Zeitraum gespeichert wurden. Nach Art. 5 Abs. 1 lit. e DS-GVO dürfen personenbezogene Daten nur so lange gespeichert werden, solange diese für die Zwecke, für die sie verarbeitet werden, erforderlich sind. Offensichtlich wurde die Speicherdauer im vorliegenden Fall bislang noch nicht kritisch hinterfragt. Dieses soll nunmehr geschehen, sodass entsprechende Festlegungen sowie Dokumentationen (Löschkonzept) erarbeitet werden.

Neben den fehlenden Regelungen zur Speicherbegrenzung wurde auch weiteren Gewährleistungszielen (hier insbesondere die Integrität und Vertraulichkeit) nicht in einem angemessenen Umfang Rechnung getragen. Dies betrifft sowohl die Aufbewahrung derartiger Speichermedien als auch die Frage nach einer Festplattenverschlüsselung.

Unsere Hinweise führten dazu, dass die Speichermedien nunmehr verschlüsselt und verschlossen in dazu vorgesehenen Räumen aufbewahrt werden. Außerdem werden entsprechende Dienstvereinbarungen mit klaren Regelungen zum Umgang mit Datenträgern erarbeitet.

8.9.5 Vertraulichkeit bei Übermittlungen von E-Mails

Im Berichtszeitraum wurden wir einige Male mit der Frage der Vertraulichkeit bei der elektronischen Kommunikation konfrontiert. Hiervon betroffen waren unterschiedliche Bereiche der Verwaltung.

So wurden beispielsweise in einem Stellenbesetzungsverfahren Angaben zu den Bewerbern unverschlüsselt per E-Mail an Mitglieder eines beratenden Ausschusses übermittelt.

In einem weiteren Fall wandte sich eine Bürgerin an uns und beschwerte sich darüber, dass der Bürgermeister ihrer Wohnsitzgemeinde Informationen an Verwaltungsmitarbeiter sowie Mitglieder der Gemeindevertretung und Fachausschüssen so übermittelt hat, dass die Mailadressen aller Empfänger in das Feld „An“ eingetragen waren. Die Mailadressen konnten bestimmten betroffenen Personen zugeordnet werden, sodass es in der Folge zu ungewollten Kontaktaufnahmen kam.

Ähnlich stellte sich auch eine an uns gemeldete Datenpanne dar. Hier ging es darum, dass eine Landesbehörde eine Rundmail an Firmenkontakte, die sich zuvor auf dem digitalen Vergabemarktplatz mit diesen Kontaktdaten registriert hatten, versandt hatte. Hierbei wurde die Verteilerart CC statt BCC genutzt, wodurch ca. 900 E-Mail-Adressen für alle Kontakte sichtbar waren. Zu berücksichtigen war dabei auch, dass viele der Mailadressen konkrete Namensangaben enthielten. Neben der von der Landesbehörde direkt an uns gemeldeten Datenpanne wurden wir auch von betroffenen Firmeninhabern hiervon in Kenntnis gesetzt.

Allen drei Beispielen ist gemeinsam, dass die notwendige Sorgfalt beim Umgang mit elektronischer Kommunikation nicht gewahrt wurde. So darf beispielsweise bei unverschlüsseltem E-Mail-Verkehr nicht unberücksichtigt bleiben, dass Personen die jeweilige E-Mail unbefugt mitlesen können. Im Fall einer unverschlüsselten Kommunikation von Bewerberdaten wäre der Vertraulichkeit und Integrität (siehe Art. 5 Abs. 1 lit. f i. V. m. Art. 32 Abs. 1 DS-GVO) nicht Rechnung getragen. Die betreffende Verwaltung gestand den Fehler ein. Mit den betroffenen Mitarbeitern wurde der Vorfall durch den behördlichen Datenschutzbeauftragten ausgewertet und das künftige Verfahren, wonach datenschutzkonforme Kommunikationsformen gewählt werden sollen, besprochen.

Bei der Übermittlung von E-Mail-Adressen, die einer bestimmten natürlichen Person zugeordnet werden können, bedarf es entweder einer entsprechenden Rechtsgrundlage oder einer vorliegenden Einwilligung. Beides lag in den genannten Fällen jedoch nicht vor. Wir haben deshalb die Empfehlung ausgesprochen, künftig beim Versenden einer E-Mail das Feld BC (Blindkopie) zu nutzen. Hiermit würde die Nachricht alle Empfänger erreichen, ohne dass der jeweilige Empfänger sehen kann, welche andere Personen diese E-Mail noch erhalten haben.

9 Informationsfreiheitsgesetz Mecklenburg-Vorpommern - IFG M-V

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

Die Bedeutung der Informationsfreiheit ist leider wegen des großen Arbeitsanfalls im Bereich der Umsetzung der Europäischen Datenschutz-Grundverordnung (DS-GVO) etwas in den Hintergrund getreten. Zusätzliches Personal im Bereich der Informationsfreiheit hat es in den letzten Jahren nicht gegeben, obwohl sowohl die Anzahl als auch die Komplexität der Anträge nach dem Informationsfreiheitsgesetz (IFG M-V) zugenommen hat.

So hat sich die Anzahl der schriftlichen Vorgänge im Berichtszeitraum im Jahr 2018 von 63 auf 75 Vorgänge im Jahr 2019 erhöht. Das ist eine Steigerung um 16 %. Darüber hinaus finden durchschnittlich jeden zweiten Tag auch telefonische Beratungen gegenüber Behörden sowie Bürgerinnen und Bürgern statt. Auch die Komplexität der Eingaben hat sich erhöht; der Arbeitsaufwand ist im Einzelfall hoch, weil häufig bereits eine umfangreiche Korrespondenz zwischen der antragstellenden Person und der angefragten Behörde vorliegt, die vom Landesbeauftragten für Informationsfreiheit in seiner Rolle als Vermittler zu würdigen ist.

Daher geraten weitere Aufgaben unserer Behörde, wie beispielsweise die Schulung der Verwaltungen in Bezug auf den Umgang mit IFG-Anfragen ins Hintertreffen. In der täglichen Arbeit fällt jedoch auf, dass erheblicher Schulungsbedarf besteht. Im Berichtszeitraum wurde lediglich eine förmliche Beanstandung ausgesprochen. Auch das liegt darin, dass derartige Maßnahmen einen erhöhten Begründungsaufwand erfordern und daher im Vergleich zu anderen verpflichtenden Aufgaben eher selten ausgesprochen werden.

Insgesamt ist festzustellen, dass unser Informationsfreiheitsgesetz aus dem Jahr 2006 mit lediglich einer inhaltlichen Novellierung im Jahr 2011 im Vergleich zu anderen Transparenzgesetzen/Informationsfreiheitsgesetzen, wie in Bremen, Hamburg, Rheinland-Pfalz oder Thüringen, ziemlich veraltet ist. Bereits im letzten Tätigkeitsbericht hatten wir eine grundsätzliche Neuausrichtung unter Benennung zahlreicher Vorschläge unterbreitet, siehe Sechster Tätigkeitsbericht zum Informationsfreiheitsgesetz, Punkt 10.3. Leider wurden diese Vorschläge vom Gesetzgeber nicht aufgegriffen mit der Begründung, dass derzeit eine Novellierung nicht beabsichtigt sei, siehe Stellungnahme der Landesregierung zum Sechsten Tätigkeitsbericht nach dem Informationsfreiheitsgesetz (IFG M-V), Drucksache 7/3685, Seite 24, vom 3. Juni 2019.

Wir empfehlen der Landesregierung erneut, das Informationsfreiheitsgesetz Mecklenburg-Vorpommern hin zu einem modernen Transparenzgesetz fortzuentwickeln.

9.2 Stellungnahme zum Entwurf eines Beteiligtentransparenzdokumentationsgesetzes (BeteildokG M-V)

Der Rechtsausschuss des Landtages Mecklenburg-Vorpommern hat den Landesbeauftragten für Informationsfreiheit Mecklenburg-Vorpommern zu einer öffentlichen Anhörung zum Entwurf eines Gesetzes über die Errichtung einer Beteiligtentransparenzdokumentation beim Landtag (BeteildokG M-V) eingeladen. Mit diesem von einer Oppositionsfraktion eingebrachten Gesetzentwurf soll durch Einrichtung einer Dokumentationsplattform transparent gemacht werden, wer sich in welcher Form an parlamentarischen Prozessen inhaltlich beteiligt hat.

Der Landesbeauftragte für Informationsfreiheit Mecklenburg-Vorpommern begrüßt den Ansatz des vorliegenden Gesetzentwurfes, da er dazu beiträgt, für mehr Transparenz im Rahmen politischer Entscheidungsprozesse zu sorgen. Bürgerinnen und Bürger sollten wissen, wer im Laufe des Entstehungsprozesses an der Formulierung eines Gesetzentwurfes beteiligt war und wer in wessen Auftrag und mit welchen Mitteln auf politische Entscheidungen einzuwirken versucht. Verflechtungen, insbesondere zwischen Politik und Wirtschaft, sind erkennbar zu machen, damit verdeckte Einflussnahmen erschwert sowie eine öffentliche Kontrolle ermöglicht wird.

So bestehen bereits in einigen Staaten, wie den USA, in Kanada sowie auch in Österreich, dem Vereinigten Königreich und Irland, sogenannte verpflichtende Lobbyregister mit umfassenden Eintragungspflichten und Sanktionsmöglichkeiten. In den deutschen Bundesländern existieren bisher in Brandenburg, Rheinland-Pfalz und Sachsen-Anhalt Lobbyregister beziehungsweise ein Beteiligtentransparenzdokumentationsgesetz in Thüringen.

Auch aus Sicht der Informationsfreiheitsbeauftragten in Deutschland (https://www.daten-schutz-mv.de/informationsfreiheit/publikationen/entschließungen) ist es für ein demokratisches Gemeinwesen geboten, verpflichtend Register einzuführen, in die Informationen über Interessenvertretungen und deren Aktivitäten einzutragen sind. Darin sind mindestens die Namen der natürlichen und juristischen Personen unter Angabe ihrer Organisationsform, der Schwerpunkt der inhaltlichen oder beruflichen Tätigkeit und die Inhalte des Beitrags zum jeweiligen Gesetzgebungsverfahren zu veröffentlichen. Die damit hergestellte Transparenz stärkt das Vertrauen der Menschen in die Politik, ermöglicht demokratische Kontrolle und erhöht die Akzeptanz politischer - insbesondere gesetzgeberischer - Entscheidungen.

Der Landesbeauftragte für Informationsfreiheit Mecklenburg-Vorpommern hat zu einigen datenschutzrechtlichen Unklarheiten im Gesetzentwurf dem Rechtsausschuss Vorschläge zur Klarstellung unterbreitet. Unsere ausführliche Stellungnahme ist unter https://www.landtag-mv.de/landtag/ausschuesse/rechtsausschuss/oeffentliche-anhoerungen abrufbar.

9.3 Vertragsunterlagen zur Betreibung der Erstaufnahmeeinrichtungen für Asylbewerber als öffentliche Information?

Ein Journalist bat uns um Vermittlung hinsichtlich seines beim Landesamt für innere Verwaltung Mecklenburg-Vorpommern (LAiV M-V) gestellten Antrags nach dem Informationsfreiheitsgesetz Mecklenburg-Vorpommern (IFG M-V). Grundsätzlich war seinem Antrag auf Einsicht in die Vertragsunterlagen zur Betreibung der Erstaufnahmeeinrichtungen zwar entsprochen worden, jedoch nicht vollständig. So waren die Unterlagen teilweise umfangreich geschwärzt worden. Den Umfang der Schwärzungen (Anonymisierungen) wollte der Antragsteller durch den Landesbeauftragten für Informationsfreiheit Mecklenburg-Vorpommern überprüft haben.

Wir haben daraufhin die Originalvertragsunterlagen vor Ort eingesehen. In einem konstruktiven Gespräch erörterten wir mit der Behördenleitung die Gründe für die Schwärzungen im Einzelnen. Nach den Grundsätzen des IFG M-V sind amtliche Informationen herauszugeben, es sei denn, Ausschlussgründe der §§ 5 bis 8 IFG M-V greifen ein, wobei die Ausschlussgründe jeweils restriktiv auszulegen sind.

Anhand dieser Grundsätze haben wir den Vertrag geprüft und sind im Ergebnis zu einer Reduzierung der Schwärzungen gelangt. Im Wesentlichen handelt es sich dabei um die folgenden Punkte:

- Die Schwärzungen zu Adressdaten der Aufnahmeeinrichtungen werden aufgehoben. Die Schwärzung der Adresse zur Ausweichunterkunft in Parchim bleibt. Hier greift der Ausschlussgrund des § 5 Nr. 4 IFG M-V. Danach ist der Antrag auf Zugang zu Informationen abzulehnen, soweit und solange das Bekanntwerden der Informationen die öffentliche Sicherheit und Ordnung gefährden kann. Zu diesem Ausschlusstatbestand hat das LAiV M-V Gründe benannt.
- Die Informationen zu den Vertragslaufzeiten werden vollständig offengelegt.
- Die Quadratmeter-Größen der Liegenschaften werden offengelegt. Die Nummern der Gebäude blieben weiterhin zum Schutz der Flüchtlinge geschwärzt, vergleiche § 5 Nr. 4 IFG M-V.
- Die Schwärzung der Kostenpauschale bleibt. Hier handelt es sich um Bestandteile von Kalkulationen, die hochgerechnet werden könnten, somit mutmaßlich wettbewerbsrelevant wären und mithin ein Geschäftsgeheimnis im Sinne des § 8 IFG M-V darstellen.
- Vor- und Zuname und weitere Adressdaten von Auftraggeber und Auftragnehmer werden offengelegt. Für Funktionsträger einer Behörde gilt Folgendes: Eine öffentliche Stelle ist nur über ihre Mitarbeiter als natürliche Personen handlungsfähig. Soweit ein Vorgang in einem notwendigen Zusammenhang zu den dienstlichen Aufgaben steht, handelt es sich bei den Namen und Vornamen der Beschäftigten um Funktionsträgerdaten, die als solche nicht von der DS-GVO geschützt sind. Dies betrifft, wie im vorliegenden Fall, die Benennung der Vertreter einer Behörde in einem Vertrag. Vergleichbares gilt für den Geschäftsführer einer Gesellschaft mit beschränkter Haftung (GmbH). So sind Daten von juristischen Personen nicht nach den Datenschutzgesetzen geschützt. Das würde allenfalls bei einer „Ein-Mann-GmbH“ gelten, bei der der alleinige Inhaber mit dem Geschäftsführer personenidentisch ist. Bei den MW Malteser Werke gGmbH handelt es sich ersichtlich nicht um eine „Ein-Mann-GmbH“, sodass die Daten offenzulegen sind.

Wir haben hier im Wege der Vermittlung ein Ergebnis erreicht, mit dem auch der Antragsteller zufrieden war, sodass er seinen Widerspruch gegen den förmlichen Bescheid des LAiV M-V zurückgenommen hat.

9.4 Ist Sponsoring durch die Sparkasse Parchim-Lübz ein Betriebs- und Geschäftsgeheimnis?

Ein Antragsteller bat uns um Vermittlung hinsichtlich seines Antrags auf Auskunft über das Sponsoring des Wirtschaftsballs 2018 durch die Sparkasse Parchim-Lübz. Diese hatte dem Antragsteller die Auskunft verweigert. Sie vertrat die Auffassung, dass Sparkassen zwar in öffentlich-rechtlicher Form organisiert seien, aber rein privatrechtlich handeln. Nur die Behördentätigkeit im weiteren Sinn, also die Wahrnehmung von Verwaltungsaufgaben, führe zur Anwendbarkeit des Informationsfreiheitsgesetzes Mecklenburg-Vorpommern (IFG M-V).

Wir sind dieser Auffassung inhaltlich entgegengetreten. Trotzdem wollte die Sparkasse die Information nicht herausgeben. Wir sahen uns daraufhin gezwungen, eine förmliche Beanstandung auszusprechen. Unsere rechtliche Bewertung stellte sich wie folgt dar:

Zweck des IFG M-V ist es, den freien Zugang zu in den Behörden vorhandenen Informationen sowie die Verbreitung dieser Informationen zu gewährleisten, siehe § 1 Abs.1, 1. Halbsatz IFG M-V.

Das Gesetz soll zu einer besseren Information der Bürgerinnen und Bürger führen und der Transparenz der Verwaltung dienen. Gemäß § 3 Abs. 1 IFG M-V gelten die Vorschriften über den Zugang zu Informationen für Behörden des Landes, der Landkreise, der Ämter und Gemeinden, für die sonstigen Körperschaften, rechtsfähigen Anstalten und Stiftungen des öffentlichen Rechts sowie für den Landtag, soweit er Verwaltungsaufgaben wahrnimmt, auch, wenn diese Bundesrecht oder Recht der Europäischen Union ausführen.

Die Sparkasse Parchim-Lübz ist eine rechtsfähige Anstalt des öffentlichen Rechts. Auch materiell-rechtlich gesehen kommt die Sparkasse öffentlichen Aufgaben nach. Gemäß § 2 Abs.1 Sparkassengesetz (SpkG) sind die Sparkassen selbständige Wirtschaftsunternehmen in kommunaler Trägerschaft mit der Aufgabe, auf der Grundlage der Markt- und Wettbewerbserfordernisse für ihr Geschäftsgebiet den Wettbewerb zu stärken und die angemessene und ausreichende Versorgung aller Bevölkerungskreise und insbesondere des Mittelstandes mit geld- und kreditwirtschaftlichen Leistungen auch in der Fläche ihres Geschäftsbereichs sicherzustellen. Sie unterstützen die Aufgabenerfüllung der Kommunen im wirtschaftlichen, regionalpolitischen, sozialen und kulturellen Bereich. Zum kulturellen und wirtschaftlichen Bereich gehört nach allgemeinem Verständnis auch das Sponsoring eines Wirtschaftsballs.

Somit ist der Anwendungsbereich des IFG M-V eröffnet.

Grundsätzlich können sich die Sparkassen - dies ist höchstrichterlich geklärt, siehe BVerwG, Beschluss vom 23. Juni 2011, 20 F 21/10 juris - im Rahmen ihrer wirtschaftlichen Tätigkeit auf den Schutz von Betriebs- und Geschäftsgeheimnissen gegenüber Dritten berufen. Ein Verweigerungsgrund im Sinne des § 8 IFG M-V, die Informationen zum Sponsoring des Wirtschaftsballs der Unternehmerverbände Mecklenburg-Vorpommern nicht herauszugeben, liegt jedoch nicht vor.

Als Betriebs- und Geschäftsgeheimnis werden alle auf ein Unternehmen bezogenen Tatsachen, Umstände und Vorgänge verstanden, die nicht offenkundig, sondern nur einem begrenzten Personenkreis zugänglich sind und an deren Nichtverbreitung der Rechtsträger ein berechtigtes Interesse hat (so BVerfG, Beschluss vom 14. März 2006 - 1 BvR 2007, 2111/03). Ein solches Interesse fehlt, wenn die Offenlegung der Information nicht geeignet ist, exklusives technisches oder kaufmännisches Wissen den Marktkonkurrenten zugänglich zu machen und so die Wettbewerbsposition des Unternehmens nachteilig zu beeinflussen (so BVerwG 7 C 18.08, Beschluss vom 28. Mai 2009 und BVerwG 20 F 23.07, Beschluss vom 19. Januar 2009).

Geschäftsgeheimnisse (und nur die kommen hier in Betracht) umfassen zum Beispiel Informationen zu Umsätzen, Ertragslagen, Lieferanten und Kundenlisten, Bezugsquellen, Konditionen, Marktstrategien, Kalkulationen, Patentanmeldungen etc. eines Unternehmens.

Es ist seitens der Sparkasse nicht dargelegt worden, inwiefern Geschäftsgeheimnisse durch die Veröffentlichung der Sponsoringsumme in Bezug auf den Wirtschaftsball die Wettbewerbsposition der Sparkasse gegenüber anderen Marktteilnehmern nachteilig beeinflussen könnte. Es werden hier lediglich allgemeine Ausführungen getätigt, ohne zu benennen, warum durch die Veröffentlichung der Tatsache und der Höhe des Sponsorings des Wirtschaftsballs Wettbewerbsnachteile entstünden. Der Hinweis, Wettbewerber würden durch diese Informationen insbesondere in die Lage versetzt, ihre eigene Marktstrategie mit derjenigen der Sparkasse zu vergleichen, reicht nicht aus. Vielmehr müsste die Sparkasse darlegen, warum die Kenntnis von Sponsoring andere Kreditinstitute in die Lage versetzen würde, ihre Marktanteile zu erhöhen beziehungsweise dazu führen würde - und das ist entscheidend -, dass die Sparkasse Parchim-Lübz Marktanteile verliert.

Das Gegenteil dürfte jedoch der Fall sein. Die Gemeinwohlorientierung und das gesellschaftliche Engagement in Sachen Sponsoring führen dazu, dass die Sparkasse Marktanteile hält beziehungsweise ausbaut. Die Ostseesparkasse Rostock (OSPA) beispielsweise stellt sich in einem Auszug ihres Geschäftsberichts von 2017 wie folgt dar:

„Öffentlicher Auftrag“

Gemeinwohlorientierung und gesellschaftliches Engagement sind wesentliche Merkmale der OSPA. So hat die Sparkasse im Rahmen ihres öffentlichen Auftrags und jenseits von Finanzgeschäften auch im abgelaufenen Geschäftsjahr ihre Förderung von kulturellen, sozialen und sportlichen Projekten in der Region weitergeführt. Zu den besonders erfolgreichen Initiativen zählen die „Leuchtturmprojekte“ der OSPA-Stiftung im Bereich der Kulturförderung …

Insgesamt wurden 2017 rund 600 Projekte, Initiativen, Vereine und Institutionen im Geschäftsgebiet der OSPA mit knapp 2,0 Mio. EUR an Spenden-, Stiftungs- und Sponsoringgeldern unterstützt …“

Insofern ist jedenfalls seitens der Sparkasse Parchim-Lübz nicht dargelegt worden, dass eine Kenntnis der Mitbewerber über die Höhe des Sponsorings des Wirtschaftsballs die eigene Wettbewerbsposition verschlechtern würde. Daher ist festzustellen, dass der Verweigerungsgrund des § 8 IFG M-V nicht greift und mithin die Informationen an den Antragsteller herauszugeben sind.

Nach einem weiteren Gespräch zwischen Vertreterinnen des Finanzministeriums Mecklenburg-Vorpommern als zuständiger oberster Aufsichtsbehörde, dem Vorstandsvorsitzenden der Sparkasse Parchim-Lübz und Vertretern unserer Behörde war die Sparkasse bereit, dem Antragsteller die begehrte Information - die Höhe der Sponsoringsumme für den Wirtschaftsball 2018 - herauszugeben.

9.5 Unvermuteter IFG-Kostenbescheid bei vorherigem kostenlosen Informationszugang

Die Vorsitzende eines eingetragenen Vereins hatte sich gemäß § 14 Informationsfreiheitsgesetz Mecklenburg-Vorpommern (IFG M-V) an uns gewandt und um Vermittlung hinsichtlich eines an den Verein ergangenen Kostenbescheides gebeten. Sie hatte rechtzeitig Widerspruch gegen den Kostenbescheid eingelegt. Die Korrespondenz hierzu lag uns vor. Wir hatten die Behörde gebeten, das förmliche Verwaltungsverfahren solange ruhen zu lassen, bis wir zu einem Ergebnis in der Sache gekommen sind.

Die Antragstellerin war der Auffassung, dass der Kostenbescheid völlig unvermittelt erlassen wurde, da ihre Anfragen in der Vergangenheit immer kostenfrei gewesen seien und sie daher nicht mit derartigen Kosten hätte rechnen müssen. Sie hat uns gegenüber dargelegt, dass der Verein auch künftig auf kostenfreie Informationen angewiesen sei, um bestimmte Gebiete zu schützen, was Vereinszweck ist.

Der Landesbeauftragte für Informationsfreiheit Mecklenburg-Vorpommern hat sich gegenüber der Behörde dazu wie folgt geäußert:

In der Vergangenheit hat der Verein vergleichbare Anfragen gestellt, die schriftlich beantwortet wurden. Die Anfragen waren nicht ausdrücklich auf das IFG M-V gestützt. Insofern war nach dem Empfängerhorizont schon fraglich, ob der Vorsitzenden des Vereins bekannt war, dass möglicherweise auch Kosten aufgrund ihrer Anfrage entstehen könnten. Ein Indiz für die Wertung als IFG-Anfrage könnte der Umstand gewesen sein, dass die Behörde sich bei ihren Antworten auf die Anfragen aus den Jahren 2016, 2017 und 2018 jeweils am Ende ihrer Schreiben auf § 13 IFG M-V in Verbindung mit der Informationskostenverordnung Mecklenburg-Vorpommern (IFGKostVO M-V) bezogen und klargestellt hat, dass keine Kosten erhoben werden, da es sich um die Erteilung einer einfachen Auskunft handele.

Dagegen spricht allerdings, dass die Behörde frühere Anfragen in ihrer Beantwortung im Betreff und in der Form nie als IFG-Anfragen behandelt hat und diese immer kostenfrei beantwortet hat. Die Antragstellerin durfte daher auch bei der hier zu beurteilenden Anfrage davon ausgehen, dass diese aufgrund ständiger Übung kostenfrei bearbeitet werde. Insofern wäre es aus unserer Sicht auf jeden Fall erforderlich gewesen, dass die Behörde die anfragende Person vorher auf möglicherweise entstehende Kosten hinweist, auch wenn die Summe unterhalb des Betrages von 200,00 € liegt. Bei einem höheren Verwaltungsaufwand von mehr als 200,00 € ist die Behörde bekanntermaßen aufgrund des § 4 IFGKostVO M-V verpflichtet, eine vorläufige Kostenaufstellung vorzulegen. Zudem fällt auf, dass der Kostenbescheid einen Monat nach dem Bescheid über die Informationsgewährung erfolgt ist. Im Regelfall erfolgt ein Kostenbescheid zeitnah im Zusammenhang mit dem eigentlichen Bescheid. Mit einem derartigen Kostenbescheid in Höhe von 147,31 € musste die Anfragende jedenfalls aufgrund der in der Vergangenheit geübten Praxis nicht rechnen.

Zudem haben wir die Behörde auf § 2 IFGKostVO M-V hingewiesen. Danach kann von Gebühren und Auslagen aus Gründen der Billigkeit oder des öffentlichen Interesses ganz oder teilweise auf Antrag abgesehen werden. Unseres Erachtens bestand durchaus ein öffentliches Interesse an den begehrten Informationen.

Darüber hinaus bestand Grund zu der Annahme, dass es sich bei den Fragen im Zusammenhang mit dem Sandtagebau sogar um Umweltinformationen nach dem Umweltinformationsgesetz (UIG) handelt, da die betreffenden Informationen Auswirkungen auf die Umwelt haben, sodass ein öffentliches Interesse an den betreffenden Informationen besteht. Gemäß § 10 Abs. 1 UIG unterrichten informationspflichtige Stellen die Öffentlichkeit in angemessenem Umfang aktiv und systematisch über die Umwelt. In diesem Rahmen verbreiten sie Umweltinformationen, die für ihre Aufgaben von Bedeutung sind und über die sie verfügen. Zu den zu verbreitenden Informationen gehören nach Abs. 2 Nr. 4 UIG Daten oder Zusammenfassungen von Daten aus der Überwachung von Tätigkeiten, die sich auf die Umwelt auswirken, nach Abs. 2 Nr. 5 UIG Zulassungsentscheidungen, die erhebliche Auswirkungen auf die Umwelt haben, und Umweltvereinbarungen. Dass diese Voraussetzungen hier einschlägig waren, ergab sich aus den Darlegungen der Behörde.

Zusammengefasst bedeutet das, dass das UIG gegenüber dem IFG M-V als spezielleres Gesetz einschlägig gewesen sein dürfte, die IFGKostVO M-V gar nicht anwendbar wäre und im Ergebnis die vom Verein erfragten Informationen kostenfrei (§ 12 Abs. 1 S. 2 UIG) hätten zur Verfügung gestellt werden müssen, soweit die Informationen nicht bereits auf einer Internetseite (§ 10 Abs. 4 UIG) öffentlich gemacht worden sind.

Schlussendlich hat die Behörde den Kostenbescheid aufgehoben.

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

Uns erreichten in der letzten Zeit einige Anfragen mit der Bitte um Vermittlung gemäß § 14 Informationsfreiheitsgesetz Mecklenburg-Vorpommern (IFG M-V) über die Plattform FragDenStaat zu Verbraucherinformationen. Seit Anfang 2018 berichtet die Plattform auch über die Ergebnisse von Hygienekontrollen von Restaurants. Jede Person, die zum Beispiel über den Hygienezustand ihrer Lieblingspizzeria etwas wissen möchte, kann sich über die Plattform an die zuständigen Behörden wenden und Kontrollberichte anfordern.

Anspruchsgrundlage für den freien Zugang zu Kontrollberichten in Bezug auf lebensmittelrechtliche Betriebsprüfungen ist § 2 Abs. 1 i. V. m. § 4 Abs. 1 Gesetz zur Verbesserung der gesundheitsbezogenen Verbraucherinformation (VIG).

Der Landesbeauftragte für Informationsfreiheit Mecklenburg-Vorpommern ist jedoch für die Vermittlung bezüglich des VIG nicht zuständig. Gemäß § 14 Abs. 1 S. 1 IFG M-V wird das Recht auf Informationsfreiheit durch die oder den Landesbeauftragten für Informationsfreiheit (Kontrollstelle) gewahrt.

Eine Person, die der Ansicht ist, dass ihr Informationsersuchen zu Unrecht abgelehnt oder nicht beachtet worden ist, hat das Recht auf Anrufung der Kontrollstelle (§ 14 Abs. 2 S. 1 IFG M-V). Gemäß § 14 Abs. 3 S. 1 IFG M-V kontrolliert die Kontrollstelle die Einhaltung der Vorschriften dieses Gesetzes.

Uns fehlt daher die Kontrollzuständigkeit für Informationen nach dem VIG.

Oberste Aufsichtsbehörde für die Lebensmittelüberwachung ist das Ministerium für Landwirtschaft und Umwelt Mecklenburg-Vorpommern.

9.7 Abschreckende Kosten bei hohem Verwaltungsaufwand?

Eine Journalistin hat über ihre Rechtsvertreterin um Vermittlung hinsichtlich des IFG-Antrages, den sie bei einem Landkreis gestellt hat, gebeten. Sie beantragte Akteneinsicht in die beim Jugendamt des Landkreises vorhandenen Informationen zu mehreren Kindertagesstätten, von deren Gründung an bis dato, zu gewähren beziehungsweise Kopien dieser Informationen zu übermitteln. Darüber hinaus bat sie darum, Akteneinsicht über dort vorhandene Informationen zu bestimmten privaten Trägern zu gewähren beziehungsweise ihr die Informationen durch Übersendung entsprechender Kopien zur Verfügung zu stellen.

Der Landkreis stellte der Rechtsvertreterin in Aussicht, dass Akteneinsicht gewährt wird. Wegen des tatsächlich erheblichen Aufwands bezifferte der Landkreis die Gebühren vorläufig in Höhe von über 4 000,00 € und Auslagen in Höhe von mehr als 400,00 € und bezog sich dabei auf § 4 i. V. m. § 3 Verordnung über die Gebühren und Auslagen nach dem Informationsfreiheitsgesetz (Informationskostenverordnung – IFGKostVO).

Der Landesbeauftragte für Informationsfreiheit Mecklenburg-Vorpommern hat den Fall gegenüber dem Landkreis rechtlich wie folgt bewertet:

Nach § 3 IFGKostVO kann sich die Gebühr über die in den Tarifstellen 1.3, 2.2 und 3.2 des Gebühren- und Auslagenverzeichnisses vorgesehenen Gebühren im Einzelfall über die in diesen Tarifstellen festgelegten Rahmengebühren erhöhen, wenn die Amtshandlung nach dem Informationsfreiheitsgesetz einen höheren Verwaltungsaufwand erfordert.

Wir haben dem Landkreis zugestanden, dass das im vorliegenden Fall verfolgte Auskunfts-begehren/Akteneinsicht für die Verwaltung tatsächlich einen sehr hohen Verwaltungsaufwand darstellt. Trotzdem waren wir der Auffassung, dass ein über die Rahmengebühr hinausgehender erhöhter Verwaltungsaufwand im Sinne des § 3 IFGKostVO hier nicht geltend gemacht werden kann und zwar aus folgenden Gründen:

Zweck des Informationsfreiheitsgesetzes ist es, den freien Zugang zu in den Behörden vorhandenen Informationen sowie die Verbreitung dieser Informationen zu gewährleisten und die grundlegenden Voraussetzungen festzulegen, unter denen derartige Informationen zugänglich gemacht werden sollen (so § 1 Abs. 1 IFG M-V). Diesem Gesetzeszweck würde es zuwiderlaufen, wenn Gebühren derart hoch sind, dass der Informationszugang nicht wirksam in Anspruch genommen werden kann. In der Gesetzesbegründung - Drucksache 4/2117, vom 22. Juni 2006, S. 17 - heißt es wörtlich: „Die Höhe der Gebühren soll sich am Grundsatz der Kostendeckung orientieren, von dem Ausnahmen möglich sind. Zugleich soll dem Informationsbedürfnis und -anspruch Rechnung getragen werden."

Die hier vorläufig in Rechnung gestellten Kosten in Höhe von insgesamt mehr als 4 000,00 € sind für den Informationszugang objektiv gesehen abschreckend und unterlaufen den vom Gesetzgeber verfolgten Zweck, den Informationsanspruch wahrzunehmen und durchzusetzen. Zu dieser Thematik gibt es ein Urteil des OVG Berlin-Brandenburg - OVG 12 B 11.16 - vom 14. September 2017 zur Informationsgebührenverordnung (IFGGebV) des Bundes. Zwar ist diese Rechtsprechung nicht direkt auf die IFGKostVO M-V zu übertragen; die wesentlichen kostenrechtlichen Grundsätze sind es jedoch schon. In dem dieser Entscheidung zugrundeliegenden Fall sah es das Gericht bereits als rechtswidrig an, den Gebührenrahmen voll auszuschöpfen und 500,00 € in Rechnung zu stellen bei einem mit 2 100,00 € bezifferten tatsächlichen Verwaltungsaufwand. 500,00 € wurden hier von der Behörde als Kappungsgrenze angesehen. Das OVG führte aus, dass dieses Vorgehen nicht rechtmäßig sei. Vielmehr müsse gewährleistet werden, dass Antragsteller nicht durch erhebliche finanzielle Gebühren abgeschreckt werden und sich deshalb die Gebühren zwar am Verwaltungsaufwand orientieren (so auch die Gesetzesbegründung in Mecklenburg-Vorpommern, s. o.), jedoch nicht notwendig kostendeckend bemessen werden sollten, vgl. hierzu OVG Berlin-Brandenburg - OVG 12 B 11.16 - Rn. 20, zitiert nach juris.

Die IFGKostVO M-V geht durch die Formulierung des § 3 nochmals über den in der Tarifstelle 1.3 des Gebühren- und Auslagenverzeichnisses vorgesehenen Gebührenrahmen von 20,00 bis 500,00 € „im Einzelfall" hinaus. Der Gesetzgeber sah die Vorschrift des § 3 als Sonderregelung an, die nicht schematisch dann anzuwenden ist, wenn bei hohem Stundenaufkommen die festgeschriebene Rahmengebühr von 500,00 € überschritten wird. Kosten - Gebühren und Auslagen - in Höhe von mehr als 4 000,00 € wirken sich eindeutig abschreckend in Bezug auf die Durchsetzung des Informationszugangs aus. Der Informationszugang wird in derartigen Fällen nicht wahrgenommen werden.

Soweit ersichtlich gibt es in Mecklenburg-Vorpommern noch keine Rechtsprechung zu dieser Problematik. Insofern haben wir auf die gebührenrechtlichen Grundsätze des OVG Berlin-Brandenburg, wie oben dargestellt, verwiesen. Wir haben dem Landkreis dementsprechend empfohlen, die (vorläufige) Kostenaufstellung nochmals zu überprüfen und eine deutlich niedrigere Gebühr festzusetzen.

Der Landkreis ist unserer Argumentation gefolgt und hat die Gebühr auf 500,00 € plus Auslagen reduziert.

9.8 Müssen städtische Aktiengesellschaften selbst Auskunft geben?

Ein Antragsteller bat uns um Vermittlung hinsichtlich seiner Anfrage zu „internen Anweisungen zum Umgang mit Anfragen nach dem Informationsfreiheitsgesetz Mecklenburg-Vorpommern (IFG M-V)“ bei der Rostocker Straßenbahn AG (RSAG). Er hatte den Eindruck, dass seine Anfragen dort ignoriert werden.

Wir haben den Antragsteller auf Folgendes aufmerksam gemacht:

Die RSAG ist keine Behörde im Sinne des § 3 Abs. 1 IFG M-V. Danach gelten die Vorschriften über den Zugang zu Informationen für die Behörden des Landes, der Landkreise, der Ämter und Gemeinden, für die sonstigen Körperschaften, rechtsfähigen Anstalten und Stiftungen des öffentlichen Rechts sowie für den Landtag, soweit er Verwaltungsaufgaben wahrnimmt, auch, wenn diese Bundesrecht oder Recht der Europäischen Gemeinschaften ausführen.

Gemäß § 3 Abs. 3 IFG M-V steht einer Behörde im Sinne dieser Vorschrift eine natürliche oder juristische Person des Privatrechts gleich, soweit sie Aufgaben der öffentlichen Verwaltung wahrnimmt oder dieser Person die Erfüllung öffentlicher Aufgaben übertragen wurde oder an denen eine oder mehrere der in Absatz 1 genannten juristischen Personen des öffentlichen Rechts mit einer Mehrheit der Anteile oder Stimmen beteiligt sind. Der Rostocker Straßenbahn AG wurde zweifelsohne von der Stadt Rostock im Bereich Verkehr die Erfüllung öffentlicher Aufgaben übertragen.

In derartigen Fallgestaltungen ist gemäß § 10 Abs. 1 S. 2 IFG M-V der IFG-Antrag an die Behörde zu richten, die sich der natürlichen oder juristischen Person des Privatrechts zur Erfüllung ihrer öffentlich-rechtlichen Aufgaben bedient. Die RSAG wäre dann im Innenverhältnis gegenüber der Stadt Rostock zur Auskunft verpflichtet.

Wir haben daher dem Antragsteller empfohlen, seinen Antrag direkt an die Stadt Rostock zu richten.

9.9 Sind die Datenschutzfolgen-Abschätzung sowie ein Datenschutz- und Informationssicherheitskonzept zur Videoüberwachung öffentliche Informationen?

Ein Petent bat uns um Vermittlung hinsichtlich einer Anfrage zur Datenschutz-Folgenabschätzung sowie zum Datenschutz- und Informationssicherheitskonzept zur Videoüberwachung auf dem Schweriner Marienplatz gemäß § 14 Informationsfreiheitsgesetz Mecklenburg-Vorpommern (IFG M-V). Er hatte diesbezüglich einen ablehnenden Bescheid vom Polizeipräsidium (PP) Rostock erhalten. Zur Begründung hatte das PP Rostock die Ablehnung auf § 6 Abs. 6 IFG M-V sowie auf § 5 Nr. 4 IFG M-V gestützt.

Nach § 6 Abs. 6 IFG M-V ist der Antrag auf Informationszugang abzulehnen, wenn zu befürchten ist, dass durch das Bekanntwerden der Informationen der Erfolg behördlicher Maßnahmen, insbesondere von Überwachungs- und Aufsichtsmaßnahmen, von ordnungsbehördlichen Anordnungen oder Maßnahmen der Verwaltungsvollstreckung, gefährdet oder vereitelt sowie die ordnungsgemäße Erfüllung der Aufgaben der betroffenen Behörde erheblich beeinträchtigt würde.

Das Polizeipräsidium hatte argumentiert, dass die Geheimhaltung der von dem Antragsteller geforderten Datenschutz-Folgenabschätzung sowie der aktuellen Fassung des Datenschutz- und Informationssicherheitskonzeptes der Bildüberwachungsanlage auf dem Schweriner Marienplatz maßgebliche Voraussetzung für den Erfolg dieser Maßnahme sei. Bei Herausgabe der Dokumente, die spezifische Angaben zum Schutz der technischen Anlage sowie der verarbeiteten personenbezogenen Daten enthalten, wäre die ordnungsgemäße Aufgabenerfüllung gefährdet. Zudem sah das PP den Ablehnungsgrund des § 5 Nr. 4 IFG M-V als einschlägig an, ohne dies allerdings zu begründen.

Der Antragsteller hielt diese Argumentation für nicht tragfähig, weil auf Basis der angefragten Unterlagen der Schutz und die störungsfreie Durchführung der Polizeimaßnahmen geplant worden seien und deshalb ein befürchteter Eingriff oder eine Vereitelung der Überwachung gar nicht stattfinden könne.

Aus informationsfreiheitsrechtlicher Sicht haben wir den Sachverhalt wie folgt bewertet:

Die Begründung des PP Rostock zur Ablehnung der Herausgabe der Informationen, hier: Datenschutz-Folgenabschätzung und Sicherheitskonzept (Datenschutz- und Informationssicherheitskonzept) ist dürftig. Teilweise wird lediglich der Gesetzeswortlaut wiederholt.

Jedoch wäre dem Antragsteller nicht damit gedient gewesen, wenn wir das PP Rostock aufgefordert hätten, die Ablehnung der Herausgabe der Informationen besser zu begründen. Dessen Ziel, die Unterlagen zu erhalten, würde dadurch jedenfalls nicht erreicht. Im Ergebnis waren wir ebenfalls der Auffassung, dass letztlich Verweigerungsgründe nach dem IFG M-V einschlägig sind.

Nach § 6 Abs. 6 IFG M-V ist der Antrag auf Informationszugang abzulehnen, wenn zu befürchten ist, dass durch das Bekanntwerden der Informationen der Erfolg behördlicher Maßnahmen erheblich beeinträchtigt würde. Das ist vorliegend auch nach unserer Einschätzung der Fall. Datenschutzkonzepte, die technische und organisatorische Maßnahmen nach Art. 24, 25, 32 Europäische Datenschutz-Grundverordnung (DS-GVO) enthalten, oder auch eine Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DS-GVO beschreiben zunächst die Risiken der Verarbeitung und sollen dann Maßnahmen zur Eindämmung dieses Risikos festlegen. Damit sind in diesen Dokumenten aber regelmäßig auch die Schwachstellen einer Datenverarbeitung aufgelistet, mit deren Bekanntwerden Angriffe auf die jeweilige Datenverarbeitung gezielt vorbereitet werden könnten. Vor diesem Hintergrund sind auch nach der Wertung der DS-GVO diese Informationen gegenüber der betroffenen Person nicht zwingend transparent zu machen. Weder im Rahmen der Informationspflichten nach Art. 13, 14 DS-GVO noch bei Ausübung des Auskunftsrechts erstreckt sich der notwendige Inhalt der zu erteilenden Informationen auch auf die vom Antragsteller erbetenen Dokumente. Das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO, das regelmäßig ein Datenschutzkonzept als Anlage enthält, ist ebenfalls nicht öffentlich zugänglich. Das schließt natürlich nicht aus, dass Verantwortliche, also beispielsweise Unternehmen, Datenschutzkonzepte veröffentlichen, um auch mit der Sicherheit der jeweiligen Datenverarbeitung zu werben. Verpflichtet sind die Unternehmen dazu nicht.

Um betroffenen Personen dennoch hinreichend Möglichkeiten zu bieten, eine Datenverarbeitung auch auf ihre Sicherheit hin zu überprüfen beziehungsweise überprüfen zu lassen, besteht nach Art. 77 DS-GVO ein Beschwerderecht für Personen, die von einer Datenverarbeitung betroffen sind. Dieses verpflichtet die Datenschutzaufsichtsbehörde, in Mecklenburg-Vorpommern den Landesbeauftragten für Datenschutz und Informationsfreiheit, tätig zu werden. Die Datenschutzaufsichtsbehörde hat nach der DS-GVO sehr weitreichende Untersuchungs- und Abhilfebefugnisse und kann, beispielsweise im Rahmen der Bearbeitung einer Beschwerde, auch sensible Unterlagen, wie eine Datenschutz-Folgenabschätzung, von dem Verantwortlichen anfordern. Die betroffene Person, die die Beschwerde erhoben hat, würde dann zwar nicht über den Inhalt der Dokumente detailliert in Kenntnis gesetzt, aber über den Ausgang der Bearbeitung der Beschwerde informiert werden. Diese Information enthält dann regelmäßig auch eine Bewertung, ob die in Rede stehende Datenverarbeitung datenschutzkonform, also zulässig und sicher, ist.

9.10 Herausgabe von Abituraufgaben der vergangenen Jahrgänge über das Portal FragDenStaat

FragDenStaat startete im Februar zusammen mit Wikimedia Deutschland die Kampagne „FragSieAbi“ und ermöglichte damit allen interessierten Personen, Abituraufgaben vergangener Jahre mit Hilfe eines Formulars und unter Beachtung des jeweils geltenden Informationsfreiheitsgesetzes anzufragen.

Für Mecklenburg-Vorpommern verzeichnete die Plattform 65 Anfragen. Bei insgesamt 16 dieser Anfragen wurde der Landesbeauftragte für Informationsfreiheit Mecklenburg-Vorpommern im Laufe des Jahres 2019 um Vermittlung gemäß § 14 Informationsfreiheitsgesetz Mecklenburg-Vorpommern (IFG M-V) gebeten.

In allen Fällen haben wir uns an das Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern gewandt und auf die Fristen des § 11 IFG M-V hingewiesen. Wir haben das Ministerium ebenfalls darauf aufmerksam gemacht, dass, wenn es sich um umfangreiche oder komplexe Informationsherausgaben handeln sollte, die Antragsteller über eine Fristverlängerung und deren Gründe schriftlich zu informieren sind. Eine schnellstmögliche Bescheidung der Anträge ist dennoch ausgeblieben.

Eine weitere Erinnerung an die Bearbeitung des Antrages blieb ebenso erfolglos. Zwar erhielten wir eine Rückmeldung, mit der die Abarbeitung der Ersuchen angekündigt wurde, eine Herausgabe der Informationen erfolgte aber weiterhin nicht. Aus diesem Grund haben wir in einem weiteren Schreiben alle offenen Anfragen aufgelistet und unter letztmaliger Fristsetzung die Bescheidung der Anträge gefordert. Wir haben außerdem darauf hingewiesen, dass andernfalls mit einer förmlichen Beanstandung gemäß § 14 Abs. 3 IFG M-V zu rechnen ist.

In einer der 16 Anfragen hat uns der Antragsteller parallel dazu darüber informiert, dass er beim Verwaltungsgericht Untätigkeitsklage eingereicht hat.

Sowohl unser Schreiben mit dem Hinweis auf eine förmliche Beanstandung als auch das Gerichtsverfahren führten schlussendlich dazu, dass in allen Fällen die Herausgabe der gewünschten Abituraufgaben gewährt wurde.

9.11 Ablehnung der Herausgabe der Ablösesumme für Stellplätze unzulässig

Die Leiterin eines Bürgeramtes trat an den Landesbeauftragten für Informationsfreiheit Mecklenburg-Vorpommern heran und bat um die Beurteilung einer Sach- und Rechtslage eines Antrages.

Mit diesem Antrag begehrte ein Rechtsanwalt die Übermittlung der Vereinbarung zwischen einer Baugesellschaft und der Gemeinde über die Ablösung von Stellplätzen sowie den dazugehörigen Zahlungsnachweis. Es wurde ein Drittbeteiligungsverfahren nach § 9 Informationsfreiheitsgesetz Mecklenburg-Vorpommern (IFG M-V) durchgeführt und der Baugesellschaft die Möglichkeit zur Stellungnahme eingeräumt.

Nach der Rückmeldung durch die beauftragte Anwaltskanzlei des Bauunternehmens vertrat das Amt die Meinung, dass nach dem IFG M-V kein Anspruch auf Herausgabe der Vereinbarung besteht, da die Zustimmung seitens der Baugesellschaft versagt wurde. Weiterhin wurde an der formellen Rechtmäßigkeit gezweifelt, da der Antrag per Fax an den Landkreis und von dort per E-Mail an das zuständige Amt gesandt wurde. Zusätzlich wurde geltend gemacht, dass es sich bei der Ablösevereinbarung um einen Vertrag zwischen der Gemeinde und einem Dritten handelt, der nicht offenkundig sein darf, sodass der Antragsteller auch keinen Anspruch auf Teileinsicht hat.

Nach Überprüfung der Unterlagen teilten wir der Leiterin als erstes mit, dass das geforderte Schrifterfordernis gemäß § 10 Abs. 1 IFG M-V eingehalten wurde, da der Antrag per Fax gestellt wurde. Die Weiterleitung per E-Mail ist dabei nicht relevant.

Weiterhin haben wir die betreffende Stadt auf die Entschließung der 21. Konferenz der Informationsfreiheitsbeauftragten vom 13. Dezember 2010 hingewiesen, wonach Verträge mit der öffentlichen Hand grundsätzlich offenzulegen sind[40].

Da sich die von der Baugesellschaft beauftragte Rechtsanwaltskanzlei in ihrer Stellungnahme auf den absoluten Schutz der Betriebs- und Geschäftsgeheimnisse bezog, haben wir im weiteren Verlauf erläutert, dass ein Kriterium für das Vorliegen eines Geschäftsgeheimnisses ist, dass die Informationen nur einem begrenzten Personenkreis bekannt, also nicht offenkundig sein dürfen.

In diesem Fall sollte geprüft werden, in welchem Umfang die Ablöse von Stellplätzen in Form einer Satzung oder ähnlichem gesetzlich geregelt und somit bereits offenkundig ist.

Es war für uns nicht nachvollziehbar, inwiefern die Ablöse von Stellplätzen, der Zahlungsnachweis beziehungsweise die Zahlung der Ablösesumme ein solches Geschäftsgeheimnis darstellen soll. Weiterhin ist nicht dargelegt worden, inwiefern durch die Herausgabe dieser Informationen exklusives kaufmännisches Wissen Konkurrenten zugänglich gemacht wird und so die Wettbewerbsposition der Baugesellschaft nachteilig beeinflusst wird.

[40] PDF-Datei „Verträge zwischen Staat und Unternehmen offen legen“ unter: https://www.datenschutz-mv.de/-informationsfreiheit/publikationen/entschliessungen/

Die Rechtsanwaltskanzlei berief sich ebenfalls auf den Schutz von personenbezogenen Daten nach § 7 IFG M-V. Wir vermuteten, dass es sich beim Vertragspartner zur Ablöse der Stellplätze aber nicht um die Geschäftsführer der Baugesellschaft, sondern um die GmbH selbst und somit nicht um eine natürliche Person handelt. Der Schutz von personenbezogenen Daten kam für uns deshalb nicht als Ablehnungsgrund in Betracht.

Wir haben der Leiterin des Bürgeramtes eine erneute sorgfältige Prüfung angeraten und empfohlen, die Informationen, die dem Schutz von §§ 7 und 8 IFG M-V unterliegen, zu schwärzen und dem Antragsteller die übrigen begehrten Informationen zukommen zu lassen.

Nach einer weiteren Beratung, in der die beabsichtigten Schwärzungen durch uns geprüft wurden, sind dem Antragsteller die Vereinbarung über die Ablösung von Stellplätzen sowie der dazugehörige Zahlungsnachweis übermittelt worden.

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

Ein Petent beantragte beim Finanzamt Auskünfte zur Anzahl von erlassenen Haftungsbescheiden sowie Informationen darüber, gegen wie viele Einspruch eingelegt worden ist, bei wie vielen angefochtenen Haftungsbescheiden deshalb Verböserung angedroht wurde und wie viele Einsprüche aufgrund dieser Androhung zurückgenommen wurden.

Sein Antrag wurde nur teilweise bewilligt und beantwortet. Auch nach Aufforderung zur Beantwortung der verbliebenen Fragen wurde lediglich Auskunft darüber erteilt, dass Informationen zu den letzten beiden Fragen mangels entsprechender statistischer Anschreibungen nicht vorliegen. Im Übrigen wurde es abgelehnt, die Zahlen zu ermitteln.

Gegen diesen Bescheid legte der Antragsteller Widerspruch ein und wandte sich gleichzeitig an uns, da es ihm nicht glaubhaft erschien, dass das Finanzamt nicht in der Lage ist, die gewünschten Informationen zu elf vom Einspruch betroffenen Vorgängen bereitzustellen.

Im ersten Schritt haben wir die Behörde gebeten, dass Verwaltungsverfahren ruhen zu lassen, bis wir den Vorgang geprüft und uns zur Sache geäußert haben. Dieses blieb jedoch wirkungslos, da der Widerspruch des Petenten zwischenzeitlich bereits abschlägig beschieden wurde. Das Finanzamt vertritt weiterhin die Ansicht, dass die Mitteilung der gewünschten Zahlen nur mittels Schaffung von neuen Informationen möglich ist. Das Informationsfreiheitsgesetz Mecklenburg-Vorpommern (IFG M-V) sieht dieses aber nicht vor, da es sich ausdrücklich nur auf vorhandene Informationen bezieht.

Dem Antragsteller haben wir daraufhin mitgeteilt, dass wir uns trotz bereits abgeschlossenen Verwaltungsverfahrens an das Finanzamt wenden werden, um auf die Herausgabe der begehrten Informationen hinzuwirken. Sollte dieses nicht erfolgen, bliebe nur noch der Weg über das Verwaltungsgericht.

Gegenüber dem Finanzamt haben wir uns inhaltlich zum Sachverhalt geäußert. Zunächst haben wir bestätigt, dass eine Behörde keine Informationsbeschaffungspflicht hat. Sie ist auch nicht dazu verpflichtet, begehrte Informationen durch Untersuchungen erst zu generieren.

Liegen die Informationen jedoch in strukturierter Form vor und bedarf es zur Bereitstellung der Informationen lediglich einer „reinen Übertragungsleistung“, ändert die Notwendigkeit dieses Zwischenschritts nichts an dem vorausgesetzten Vorhandensein der Information.

Mit Urteil vom 27. November 2014 hat das Bundesverwaltungsgericht entschieden, dass „allein die Addition gleichartiger Informationen keine vom Informationsanspruch nicht umfasste inhaltliche Aufbereitung von Informationen ist“ (7 C 20/12). Wenn die vom Antragsteller gewünschten Informationen also in Datenbanken vorliegen und diese lediglich zusammengestellt oder addiert werden müssen, so wären die Informationen im Sinne des IFG M-V vorhanden.

Wir vermuteten, dass im vorliegenden Fall eine einfache Addition ausreichend gewesen wäre, und teilten dem Finanzamt mit, dass die Zurückweisung des Widerspruchs aufgrund fehlender Aufzeichnungen in der Behörde als nicht ausreichend begründet angesehen wird. Wir empfahlen, dem Petenten die begehrten Informationen trotz abgeschlossenen Verfahrens zur Verfügung zu stellen.

Das Finanzamt hielt dennoch an der bislang vertretenen Auffassung fest, sodass der Antragsteller Klage beim Verwaltungsgericht eingereicht hat. Dieses ist unserer Argumentation gefolgt und hat ein Urteil zugunsten des Petenten gefällt.

Das weitere Vorgehen des Finanzamtes erforderte erneut die Vermittlung durch den Landesbeauftragten für Informationsfreiheit Mecklenburg-Vorpommern. Zusammen mit der schriftlichen Beantwortung der offen gebliebenen Fragen erhielt der Antragsteller einen Gebührenbescheid über 264,00 Euro. Dieser Betrag erschien dem Petenten deutlich zu hoch.

Im weiteren Verlauf haben wir das Finanzamt darauf hingewiesen, dass Gebühren über 200,00 Euro nach § 4 Informationskostenverordnung (IFGKostVO M-V) eine vorläufige Kostenaufstellung erfordern. Dieser Mitteilungspflicht ist die Behörde aber nicht nachgekommen.

Darüber hinaus können dem Gebührenbescheid weder die Zusammensetzung des Betrages, der Arbeitsaufwand noch der zugrundeliegende Stundensatz entnommen werden.

Unserer Empfehlung, den Gebührenbescheid zurückzunehmen, ist das Finanzamt nicht nachgekommen. Im Rahmen eines Vergleiches bot es aber eine Reduzierung der Gebühren auf 200,00 Euro an.

Da die Kostenentscheidung erst nach Einlegung des Widerspruchs begründet wurde, die Gebühren für den dargelegten Aufwand dennoch überhöht erschienen, haben wir nach Rücksprache mit dem Petenten eine Herabsetzung der Gebühren auf 150,00 Euro vorgeschlagen.

Das Finanzamt ist unserer Bitte gefolgt und hat die Gebühr reduziert und einen angepassten Bescheid erstellt.

9.13 Herausgabeanspruch durch Auslegung eines Antrags auf Akteneinsicht als Antrag nach dem IFG M-V durchgesetzt

Ein Petent beantragte bei einem Abwasserzweckverband Akteneinsicht in die Dokumentation eines Projektes zur Regenwasserentsorgung. Die Akteneinsicht wurde von der zuständigen Stelle nicht gewährt. In der Begründung hieß es, dass dem Antrag kein berechtigtes persönliches oder öffentliches Interesse zu entnehmen sei. Daraufhin wandte sich der Petent an den Landesbeauftragten für Informationsfreiheit Mecklenburg-Vorpommern mit der Bitte um Klärung seines Anliegens.

In einer telefonischen Beratung des Antragstellers haben wir ihm vorgeschlagen, seinen Vortrag als Antrag auf Vermittlung nach dem IFG zu werten. Der Petent erklärte sich mit diesem Vorgehen einverstanden.

Dem Abwasserzweckverband haben wir schriftlich dargelegt, dass wir die Anfrage des Petenten als ein Auskunftsersuchen nach § 10 Informationsfreiheitsgesetz Mecklenburg-Vorpommern (IFG M-V) werten. Ein Antrag auf den freien Zugang zu in den Behörden vorhandenen Informationen muss sich nicht ausdrücklich auf das Informationsfreiheitsgesetz beziehen. Da sich der Antragsteller aber auf einen konkret benannten Vorgang bezieht, haben wir empfohlen, den Antrag des Petenten unter Beachtung des IFG M-V erneut zu prüfen.

Der Abwasserzweckverband ist unserer Empfehlung nachgekommen und hat die begehrte Akteneinsicht gewährt.

9.14 Einsichtnahme in einen Nutzungsvertrag zwischen einer Stadt und einer OHG

Ein Antragsteller beantragte bei seiner Stadt Information zu den Pacht- und Nutzungsverhältnissen des Stadthafens. Sein Antrag ist unter Hinweis auf das Vorliegen eines privatrechtlichen Vertrages zwischen der Stadt und einer OHG sowie bestehende Geschäftsgeheimnisse abgelehnt worden. Der Petent wandte sich an uns, da er mit Antragstellung bereits ausdrücklich um die Schwärzung schützenswerter Inhalte gebeten hatte und die Ablehnungsgründe für ihn nicht nachvollziehbar waren.

In unserem Stellungnahmeersuchen haben wir die betreffende Stadt eingangs ebenfalls auf die Entschließung der Konferenz der Informationsfreiheitsbeauftragten hingewiesen, siehe auch Punkt 9.11, wonach Verträge mit der öffentlichen Hand grundsätzlich offenzulegen sind.

Darüber hinaus haben wir angemerkt, dass der Ablehnungsbescheid keine ausreichende Begründung enthält. Da in einem Online-Artikel einer regionalen Tageszeitung neben der jährlichen Pachthöhe, die die Stadt an den Bund zahlt, auch das jährliche Nutzungsentgelt der OHG entnommen werden kann, erachten wir den Verweis auf den Schutz von Betriebs- und Geschäftsgeheimnissen als nicht ausreichend.

Wir haben der Stadt deshalb empfohlen, die Herausgabe des Vertrages unter Berücksichtigung unserer Hinweise zur Definition von Betriebs- und Geschäftsgeheimnissen erneut zu prüfen. Sie wurde ebenfalls darauf hingewiesen, dass, soweit Informationen gemäß § 10 Abs. 5 Informationsfreiheitsgesetz Mecklenburg-Vorpommern (IFG M-V) nicht zugänglich gemacht werden dürfen, Anspruch auf Zugang zu den übrigen Informationen besteht. Informationen, die nach der erneuten Überprüfung dem Schutz von §§ 5 bis 8 IFG M-V unterliegen, sollten unkenntlich gemacht werden und der Antragsteller die übrigen begehrten Informationen erhalten.

Als Reaktion auf unser Ersuchen legte die Stadt dar, dass sie an ihrer ursprünglichen Argumentation festhält. Der Schutz von Betriebs- und Geschäftsgeheimnissen wird trotz Veröffentlichung einiger Vertragsinhalte weiterhin als gegeben angesehen. Zusätzlich führte sie aus, dass der Antragsteller gemäß § 7 Abs. 5 IFG M-V kein rechtliches Interesse an der Kenntnis der begehrten Informationen geltend gemacht hat.

Im weiteren schriftlichen und telefonischen Kontakt mit der Stadt haben wir unter anderem erläutert, dass sich § 7 Abs. 5 IFG M-V nur auf den Schutz von personenbezogenen Daten bezieht, der Antragsteller aber bereits die Schwärzung dieser eingeräumt hat. Weiterhin haben wir dargelegt, dass das IFG M-V den freien Zugang zu in den Behörden vorhandenen Informationen gewährleisten soll, eine Begründung durch den Antragsteller aber nicht erforderlich ist. Darüber hinaus informierten wir die Stadt über die ordnungsgemäße Durchführung eines Drittbeteiligungsverfahrens nach § 9 IFG M-V. Dem Dritten soll damit die gesetzlich geforderte Gelegenheit zur Stellungnahme eingeräumt werden. Die Frage nach der Einwilligung in den Informationszugang kann und muss dabei nicht nur eindeutig mit „ja“ oder „nein“ beantwortet, sondern auch begründet werden. Die Ablehnung seitens der OHG ist aber ohne Begründung erfolgt. Wir haben deshalb empfohlen, sich erneut an die OHG zu wenden und eine Begründung für Ablehnung in die Einsichtnahme zu fordern. Diese Begründung muss anschließend von der Stadt geprüft werden. Denn die Entscheidung darüber, ob im konkreten Fall ein Betriebs- oder Geschäftsgeheimnis anzuerkennen ist, obliegt allein der mit dem Informationszugang befassten Behörde. Dabei ist eine sorgfältige Prüfung angezeigt, da die behördliche Entscheidung der vollen gerichtlichen Kontrolle unterliegt. Die Stadt darf sich deshalb nicht einfach nur auf die Aussage des betroffenen Unternehmens verlassen.

Schlussendlich hat die Stadt im Rahmen der Drittbeteiligung alle schützenswerten Betriebs- und Geschäftsgeheimnisse geschwärzt und den Informationszugang zu den restlichen Informationen gewährt.

10 Abkürzungsverzeichnis

AKA	Akkreditierungsausschuss
AK Technik	Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
AO	Abgabenordnung
BÄK	Bundesärztekammer
BDSG	Bundesdatenschutzgesetz
BeteildokG M-V	Beteiligtentransparenzdokumentationsgesetz Mecklenburg-Vorpommern
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BMG	Bundesministerium für Gesundheit
BMI	Bundesministerium des Innern
BrSchG	Brandschutz- und Hilfeleistungsgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
BYOD	Bring Your Own Device
BZÄK	Bundeszahnärztekammer
CNIL	Commission Nationale de l'Informatique et des Libertés
CSG	ComputerSpielSchule Greifswald
DAV	Deutscher Apothekerverband
DAkkS	Deutsche Akkreditierungsstelle
DFKI	Deutsches Forschungszentrum für Künstliche Intelligenz GmbH
DKG	Deutsche Krankenhausgesellschaft
DSFA	Datenschutz-Folgenabschätzung
DSG M-V	Landesdatenschutzgesetz Mecklenburg-Vorpommern
DS-GVO	Europäische Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
DVZ M-V GmbH	Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH
EDSA	Europäischer Datenschutzausschuss
EG	Europäische Gemeinschaft
eGo-MV	Zweckverband Elektronische Verwaltung in Mecklenburg-Vorpommern
EHIC	Europäische Krankenversicherungskarte
eID	Elektronischer Identitätsnachweis
EU	Europäische Union
EuGH	Europäischer Gerichtshof
GKV-SV	Spitzenverband der Gesetzlichen Krankenversicherungen
GmbH	Gesellschaft mit beschränkter Haftung
HTTP	Hypertext Transport Protocol
HTTPS	Hypertext Transport Protocol Secure
IFG M-V	Informationsfreiheitsgesetz Mecklenburg-Vorpommern
IFGGebV	Informationsgebührenverordnung
IFGKostVO M-V	Informationskostenverordnung Mecklenburg-Vorpommern
IMI	Europäisches Binnenmarkt-Informationssystem
IMK	Ständige Konferenz der Innenminister und -senatoren der Länder (Innenministerkonferenz)

IP	Internet Protocol
IPsec	Internet Protocol Security
JI-RL	Richtlinie (EU) 2016/680 (Justiz-Richtlinie)
KBV	Kassenärztliche Bundesvereinigung
KI	Künstliche Intelligenz
KiföG M-V	Kindertagesförderungsgesetz Mecklenburg-Vorpommern
KIS	Krankenhausinformationssystem
KiStG M-V	Kirchensteuergesetz Mecklenburg-Vorpommern
KMK	Ständige Konferenz der Kultusminister der Länder in der Bundesrepublik Deutschland (Kultusministerkonferenz)
KV M-V	Kassenärztliche Vereinigung Mecklenburg-Vorpommern
KZ BV	Kassenzahnärztliche Bundesvereinigung
LAiV M-V	Landesamt für innere Verwaltung Mecklenburg-Vorpommern
LAKOST MV	Landeskoordinierungsstelle für Suchtthemen Mecklenburg-Vorpommern
LJR M-V	Landesjugendring Mecklenburg-Vorpommern e. V.
LKA M-V	Landeskriminalamt Mecklenburg-Vorpommern
LT-Drs.	Landtags-Drucksache
LuftVO	Luftverkehrsordnung
MDM	Mobile Device Management
MMV	Medienanstalt Mecklenburg-Vorpommern
OHG	Offene Handelsgesellschaft
OSPA	Ostseesparkasse Rostock
OVG	Oberverwaltungsgericht
OWiG	Gesetz über Ordnungswidrigkeiten
OZG	Online-Zugangsgesetz
PDF	Portable Document Format - plattformunabhängiges Dateiformat für Dokumente
PP	Polizeipräsidium
RSAG	Rostocker Straßenbahn AG
SchiLF	Schulinterne Lehrerfortbildung
SchulDSVO M-V	Schuldatenschutzverordnung Mecklenburg-Vorpommern
SchulG M-V	Schulgesetz Mecklenburg-Vorpommern
SDM	Standard-Datenschutzmodell
SIP	Schulinformations- und Planungssystem
SOG M-V	Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommern
SpkG	Sparkassengesetz
SSL	Secure Sockets Layer
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TEO	Tage ethischer Orientierung
TLS	Transport Layer Security
TMG	Telemediengesetz
UIG	Umweltinformationsgesetz
UPDK	Umgang mit Patientendaten in den Krankenhäusern Mecklenburg-Vorpommerns

Vdek e.V.	Verband der Ersatzkassen e. V.
VIG	Gesetz zur Verbesserung der gesundheitsbezogenen Verbraucherinformation
VwGO	Verwaltungsgerichtsordnung
VwVfG M-V	Landesverwaltungsverfahrensgesetz Mecklenburg-Vorpommern
WWW	World Wide Web

11 Stichwortverzeichnis

Abgabenordnung 63
Abhilfebefugnis 55
Adressdaten 75
AK Technik 14, 34, 36
Akkreditierung 42
Akkreditierungsausschuss 43
Akkreditierungskriterien 43
Akteneinsicht 80
Altersklassifikation 32
anlassbezogene Prüfung 11
anlassunabhängige Prüfung 11
Anti-Virus-Software 33
Anweisung 55
Arbeitskreis Gesundheit und Soziales 44
Arbeitskreis Technik 20, 44
Arbeitskreis Technische und organisatorische Datenschutzfragen 20
Art. 33 Meldung 11
aufsichtsrechtliche Maßnahme 10
Auftragsverarbeiter 42
Auftragsverarbeitung 36, 42
Auskunftsrecht 70
Authentifikation 44
Beanstandung 73
Bearbeitungsfrist 11
Beratung 73
bereichsspezifischer Identifikator 22
Berufsschüler 26
Beschäftigtendatenschutz 64, 66
Beschränkung der Verarbeitung 55
Beschwerde 11
Bestattungsportal 69
Beteiligtentransparenzdokumentation 74
Betriebs- und Geschäftsgeheimnis 77
Bevölkerungszählung 65
Bildüberwachungsanlage 83
Bildungsministerium 65
Biometrie 31
biometrische Analyse 18
biometrische Daten 18, 31
biometrische Samples 32
biometrische Verfahren 18
BKA-Urteil 54
Bodycam 59
Brandschutz 71
Bring Your Own Device 66
BSI-Grundschutz 37
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit 12
Bußgeld 11, 19
Bußgeldverfahren 59
BYOD 66
Calliope mini 31
Cloud 7, 43
Computer-Forensik 20
Computerspiel 27
Computerviren 20
Cookies 46
Cybermobbing 27
DAkkS 43
Datenminimierung 34, 53
Datenpanne 11, 41, 72
Datenschutz durch datenschutzfreundliche Voreinstellungen 21
Datenschutz durch Technikgestaltung 21
Datenschutz- und IT-Sicherheitskonzept 38
Datenschutzaufsichtsbehörde wirksame Befugnisse eingeräumt 60
Datenschutzerklärung 38
Datenschutz-Folgenabschätzung 14, 38, 83
Datenschutz-Grundverordnung ... 17, 36, 38
Datenschutzkonferenz 20, 33, 36, 53
Datenschutzkonzept 83
Datenschutzmanagement 37
Datenübermittlung 33
Datenverarbeitung 67
Deutsche Akkreditierungsstelle 43
Deutschland-Cloud 35
Diagnosedaten 33
digitale Kompetenz 23, 30
Digitalisierung 65
Digitalisierung des Gesundheitswesens .. 18
Digitalisierungsprogramm 21
Diskriminierung 34
Dokumentationsplattform 74
DOMEA 39
Drittland 42
DS-GVO 17, 21, 38
Dunkelfeld 11
eAkte 39
E-Government-Basisdienst 39
E-Government-Gesetz 39
Eingabe 11
einheitlicher Identifikator 22
Einwilligung 38, 46, 68, 69

elektronische Kommunikation 72
Elternabend 25
Elterngespräch 29
E-Mail 72
E-Mail-Verschlüsselung 20
Ende-zu-Ende-Verschlüsselung 45
Erforderlichkeit 53
Erhebungsbeauftragter 65
Erhebungsstelle 65
Erste juristische Staatsprüfung 60
Europäische Kommission 30
Europäischer Datenschutzausschuss 14, 18, 32
Europäisches Parlament 19, 30
Festplatte 71
Finanzamt 63
Flugdrohne 70
Forensik 20
förmliche Abhilfemaßnahme 10
förmliche Beanstandung 76
FragDenStaat 79
Freiwilliges Soziales Jahr 30
Gebühr 80
Geschäftsgeheimnis 77
Geschlechtsklassifikation 32
Gesundheits-App 18
Gesundheitswebseite 18
Gewährleistungsziel 35, 36
Guideline 32
Haftungsrisiko 66
Hambacher Erklärung 18
Haushaltebefragung 65
Hello World 29
Hygienezustand 79
Identifikation 32
Identifizierung 22
Identität 32
Identitätsmanagement 22
Informationsfreiheit 79
Informationsfreiheitsgesetz ... 73, 78, 79, 84
Informationskostenverordnung 78, 80
Informationssystem der Polizei 59
Innenministerium 70
Innenministerkonferenz 22
Instant Messenger 20, 44
Integrität 72
Interessenvertretung 74
ISY 65
IT-Planungsrat 21
IT-PLR 21
JI-Richtlinie 55, 60
Jugend hackt 29
Justizvollzugsdatenschutzgesetz 60
Kind 23
Kinder 68
Kirche 19
Kirchensteuer 64
KI-System 18, 34
Kohärenzverfahren 10
kommunales Steueramt 64
Kommune 69
Komplexität 73
Konformitätsbewertungsprogramm 43
Kontaktdaten 44
Kontrollzuständigkeit 80
Kopie 60
Kosten 78, 81
Kostenbescheid 78
Krankenhaus 19, 44
Kultusministerkonferenz 23
Künstliche Intelligenz 17, 20, 34
Landesamt für innere Verwaltung 75
Landesjugendring 25
Landesjustizprüfungsamt 61
Landeskriminalamt 24, 25
Landesmedienanstalt 25
Landesrechnungshof 12
Landkreisverwaltung 70
Lebensmittelüberwachung 80
Lebenszyklus 35
Lehrerfortbildung 24
Lehrkraft 66
Lobbyregister 74
Löschkonzept 71
Löschung 44
Medienaktiv M-V 24, 27
Medienaneignung, ... 29
Medienanstalt 24
Medienbildung 23, 24
Medienerlebnis 29
Medienkompetenz 23, 28
Mediennutzung 29
medienpädagogische Angebote 29
Medienscouts MV 24, 25, 30
Meldedatenabgleich 53
Melderegister 65
Messenger 20, 44
Messenger-Dienst 19
Microsoft 33, 35
Ministerium für Energie, Infrastruktur und Digitalisierung Mecklenburg-Vorpommern 38

Mitglied 67
Mitgliederdaten 67
Mobile Device Management 45
modulare Fortbildung 29
MV-Serviceportal 37
Nordkirche 27
Normenhierarchie 70
Normenkontrollrat 22
Novellierung 73
Nutzerkonto 38
öffentlich-rechtlicher Rundfunk 19
Office365 36
Online-Zugangsgesetz 21, 37
Ordnungswidrigkeitenverfahren 70
OZG 37
Passwort 40, 41
Patch 45
peer-to-peer-Ansatz 25
Personalausstattung 12
Personalrat 67
Plakatkampagne 28
Planet49 46
Plattform 79
Polizei 59
Polizeipräsidium 82
Polizisten 59
postmortaler Datenschutz 69
Pre-Recording 59
Prüfungsakte 60
Raspberry Pi 31
Rechenschaftspflicht 42, 66
Recht am eigenen Bild 25
Rechtsstaatlichkeit 54
Register 74
Registermodernisierung 22
Restaurant 79
Risiko 35, 37
Rohdaten 35
Rostocker Straßenbahn AG 82
Rückkopplung 35
Rundfunkanstalt 54
Rundfunkdatenschutzbeauftragter 20
Rundfunkstaatsvertrag 53
Sample 32
Schadsoftware 20, 33
SchiLF 24
Schule 66
Schulgesetz 66
Schulsozialarbeiter 26
Schulträger 66
Schulverwaltungssoftware 65
Schutzbedarf 37
Schwärzung 75
SDM 19, 36
Selbstveränderung 35
Sensibilisierung 10
Sicherheits-Updates 45
Smartphone 44
Social-Plugin 45
SOG M-V 54
soziales Netzwerk 27
Sparkassen 76
Speicherbegrenzung 71
Speichermedien 71
Sperrvermerk 12
spezifische Aufsichtsbehörde 19
Sponsoring 76
Sprachassistent 33
Stadt Rostock 82
Stammzahlensystem 22
Stand der Technik 41
Standard-Datenschutzmodell 19, 21, 35, 36
Statistisches Bundesamt 65
Statistisches Landesamt 65
Steuerwesen 63
technische und organisatorische Maßnahmen 40
Technology Subgroup 14
Telemetriedaten 19, 33, 36
Tracking 7, 46
Trainingsdaten 35
Transparenz 74
Überwachungs- und Aufsichtsmaßnahmen 82
Umweltinformationen 79
Umweltinformationsgesetz 79
Universität 24
Unterauftragsverarbeiter 42
Untersagung 38
Update 45
Urheberrecht 25
Urteil Fashion ID 45
Verbraucherinformation 79
Verein 67
Vereinbarungen zu gemeinsamen Verantwortlichkeiten 38
Vereinsaktivität 67
Vereinsmitglieder 68
Verhältnismäßigkeit 71
Vermittler 73
Vermittlung 79, 84
Verschlüsselung 41

Verstorbene 69
Vertragslaufzeit 75
Vertragsunterlagen 75
Vertraulichkeit.....72
Verwaltungsakt.....10
Verwaltungsaufwand.....80
Verwaltungsdienstleistung 37
Verwaltungsgericht 11
Verwaltungsportal 39
Verwaltungsregister 65
Verzeichnis der Verarbeitungstätigkeiten 38, 67
Videokonferenzanlage.....21
Videoüberwachung 15, 31
Vorstand..... 67
Warnung 10, 55
Webseiten 45
Werbung 31
WhatsApp 44
Windows 10 ..... 19, 20, 33
Windows 7 33
Zensus 64
Zertifizierung 11, 42
Zertifizierungskriterien 43
Zwangsgeld..... 11