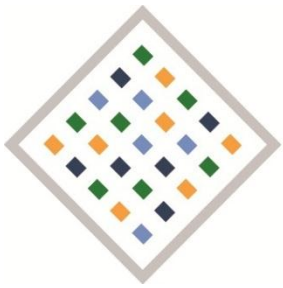

Der Landesbeauftragte
für Datenschutz und Informationsfreiheit
Mecklenburg-Vorpommern

Vierzehnter Tätigkeitsbericht zum Datenschutz

des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern

Berichtszeitraum: 1. Januar 2018 bis 31. Dezember 2018

Redaktion:

Der Landesbeauftragte für Datenschutz und Informationsfreiheit
Mecklenburg-Vorpommern

Postanschrift:
Schloss Schwerin
Lennéstraße 1
19053 Schwerin

Hausanschrift:
Werderstraße 74 a
19055 Schwerin

Telefon: +49 385 59494-0
Telefax: +49 385 59494-58
E-Mail: info@datenschutz-mv.de
Web: https://www.datenschutz-mv.de

Vorwort

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (LfDI MV) erstattet gemäß Artikel 59 Europäische Datenschutz-Grundverordnung (DS-GVO) jährlich einen Bericht über seine Tätigkeit.

Damit fallen mit dem Inkrafttreten der DS-GVO die Berichtszeiträume auseinander: Der Tätigkeitsbericht zum Datenschutz wird jährlich erstellt, der Tätigkeitsbericht zur Informationsfreiheit in Mecklenburg-Vorpommern weiterhin jedoch alle zwei Jahre.

Der vorliegende Tätigkeitsbericht zum Datenschutz umfasst den Zeitraum vom 1. Januar 2018 bis zum 31. Dezember 2018. Die hier dargestellten Vorgänge sollen einen Eindruck von der breit gefächerten Tätigkeit der Behörde als Beratungs-, Aufsichts- und Kontrollbehörde vermitteln. Innerhalb des Berichtszeitraumes hat sich mit dem Wirksamwerden der DS-GVO die Rechtsbasis für die Arbeit des LfDI MV grundlegend gewandelt, was sich teilweise im Bericht spiegelt.

Einige Beiträge schließen an Sachverhalte aus den Tätigkeitsberichten der vorherigen Berichtszeiträume an. Insofern könnte es hilfreich sein, in dem einen oder anderen Fall noch einmal auf diese Berichte zurückzugreifen.

Heinz Müller
Landesbeauftragter für Datenschutz
und Informationsfreiheit Mecklenburg-Vorpommern

Inhaltsverzeichnis

1 Empfehlungen

1.1 Zusammenfassung aller Empfehlungen

1. Wir empfehlen der Landesregierung, sich dafür einzusetzen, dass schnellstmöglich durch den Bundesrat ein Stellvertreter für den Europäischen Datenschutzausschuss (EDSA) gewählt wird, siehe Punkt 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, siehe Punkt 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, siehe Punkt 7.1.3.

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, siehe Punkt 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, siehe Punkt 9.1.2.

6. Wir empfehlen der Landesregierung, die entsprechenden Regelungen im KiföG M-V zu ändern, siehe Punkt 9.4.5.

1.2 Umsetzung der Empfehlungen des Dreizehnten Tätigkeitsberichtes

Lfd. Nr.:	Empfehlung	Umsetzungsstand	Gliederungspunkt im 13. TB
1	Wir empfehlen der Landesregierung angesichts von unüberschaubaren und ungewöhnlich schnellen digitalen Entwicklungen, die dringend erforderliche Vermittlung von Medienkompetenz über alle Altersgruppen hinweg prioritär zu behandeln. Informationelle Selbstbestimmung und Privatsphäre sind Grundrechte einer jeden Bürgerin und eines jeden Bürgers. Die Förderung von Medienkompetenz ist (mehr denn je) eine politische Querschnittsaufgabe.	Die „Kooperationsvereinbarung zur Förderung der Medienkompetenz in Mecklenburg-Vorpommern“ wird nach Kabinettbeschluss neu geschrieben. Die Digitale Agenda des Landes Mecklenburg-Vorpommern setzt sich ebenfalls mit der Medienbildung in unserem Land auseinander. Das ist sehr zu begrüßen. Doch die Akteure und Umsetzer in den Institutionen und Einrichtungen vor Ort benötigen verlässliche politische Rahmenbedingungen. Der gesamtgesellschaftliche Dialog und den vernetzenden Grundgedanken sehen wir weiterhin nicht umgesetzt.	4.1.5
2	Wir empfehlen der Landesregierung, bei der Planung, der Einrichtung und dem Betrieb von Verfahren zur Verarbeitung personenbezogener Daten die im Standard-Datenschutzmodell beschriebene Vorgehensweise evaluierend anzuwenden und uns über die Erfahrungen beim Umgang mit diesem Werkzeug zu berichten, um dadurch die Weiterentwicklung des Standard-Datenschutzmodells zu unterstützen.	Die im Standard-Datenschutzmodell (SDM) beschriebene Vorgehensweise wird in verschiedenen Bereichen der Landesverwaltung gut angenommen. So erfolgten erste Anpassungen vorhandener Sicherheitskonzepte an die Forderungen der DS-GVO unter Nutzung des SDM mit Unterstützung der DVZ-MV GmbH. Auch die Schutzbedarfsfeststellung und Risikoanalyse mit Schwellwertanalyse zur Datenschutzfolgenabschätzung für ServO.MV – Servicekonto wurde mit der SDM-Methodik durchgeführt. Ebenso wurden Datenschutzfolgenabschätzungen für den Einsatz von Bodycams bei der Polizei und für die Videoüberwachung des Marienplatzes in Schwerin mit Hilfe der Systematik des SDM durchgeführt.	5.1.1

3	Wir empfehlen der Landesregierung, sich für klare gesetzliche Regelungen im Hinblick auf die Einsatzvoraussetzungen, die Entwicklung, die Prüfung und die Verwendung von Algorithmen einzusetzen. Diese Regelungen dürfen nicht allein dem Markt überlassen werden. Unreguliert würde der Markt zu Lösungen tendieren, die die wirtschaftlichen Risiken der Anbieter minimieren, im Zweifel zu Lasten der Betroffenen.	Uns liegen keine Informationen zur Nutzung von Algorithmen oder von Anwendungen „Künstlicher Intelligenz“ vor.	5.1.6

2 Zahlen und Fakten

Eine exakte zahlenmäßige Erfassung unserer Arbeit war erst nach der Sommerpause umsetzbar. Die folgende Tabelle beleuchtet wichtige Arbeitsfelder; die Zahlen beziehen sich ausschließlich auf die Monate September bis Dezember, also einen Zeitraum von vier Monaten:

Prüfmaßnahmen und Sanktionen	1
Stellungnahmen und Empfehlungen	231
Meldungen nach Art. 33 DS-GVO (Datenschutzverletzungen)	36
Eingaben und Beschwerden	158
von Parlament/Regierung angeforderte Beratungen	15
anlassunabhängige Prüfungen und Untersuchungen	2
gemeldete behördliche Datenschutzbeauftragte	143
gemeldete betriebliche Datenschutzbeauftragte	294
europäische Verfahren einschl. Kohärenzverfahren	433
Veranstaltungen	70
Veranstaltungsteilnehmer ca.	2.960

Auffällig ist die geringe Zahl von Prüfungen und Untersuchungen. Zu dieser Kernaufgabe einer Aufsichts- und Kontrollbehörde waren wir angesichts der Arbeitsbelastung in anderen Bereichen und der völlig unzureichenden Personalausstattung nahezu gar nicht in der Lage.

3 Entwicklung der Behörde

Entscheidendes Ereignis für die Entwicklung der Behörde des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern im Berichtszeitraum war die Tatsache, dass die Europäische Datenschutz-Grundverordnung (DS-GVO) im Mai des Jahres unmittelbar geltendes Recht wurde.

Die Behörde veränderte dadurch ihren Charakter: Sie wurde von einer Opportunitätsbehörde nach nationalem Recht zu einer Exekutivbehörde, deren Rechte und Pflichten maßgeblich im europäischen Recht verankert sind.

Der Umfang der Aufgaben erweiterte sich stark; mehr als 50 neue Aufgaben kamen hinzu. Gleichzeitig führte das Wirksamwerden der DS-GVO zu einer sehr breiten öffentlichen Hysterie sowohl im öffentlichen wie im privaten Sektor. Zwar war die DS-GVO bereits 2016 auf EU-Ebene beschlossen und in Kraft gesetzt worden, um den Betroffenen Zeit zur Umstellung zu geben. Doch diese zwei Jahre blieben weitgehend ungenutzt. Und so konnte man im Mai 2018 den Eindruck gewinnen, das neue Recht sei über Nacht gekommen und stelle völlig neue Anforderungen. Doch dies ist unzutreffend; vielmehr knüpft die DS-GVO in vielen Bereichen an bestehendes deutsches Recht an.

Die von einigen Medien noch angeheizte Hysterie führte zu einem Ansturm von Anforderungen an die Datenschutzbeauftragten – auch in Mecklenburg-Vorpommern. Zu den neuen Aufgaben, die ihre Auswirkungen erst mit der Zeit entfalteten und entfalten, trat eine kaum zu bewältigende Nachfrage nach Information, Schulung und Beratung. Hinzu kam die Notwendigkeit der Verständigung und Abstimmung mit anderen Datenschutzbehörden in zahlreichen Einzelfragen des neuen Rechts.

Der Bedarf an Abstimmung wie der Bedarf an Schulung und Beratung ging im Laufe der Zeit wieder etwas zurück; gleichzeitig stieg aber die Inanspruchnahme der Behörde durch Privatpersonen, Vereine, Unternehmen etc. in verschiedenen Bereichen massiv an, was sicherlich auch darauf zurückzuführen ist, dass Datenschutz stärker ins öffentliche Bewusstsein gerückt war. In verschiedenen Arbeitsfeldern (Eingaben, Meldung von Datenpannen, Beschwerden u. a.) verdreifachte sich das Arbeitsaufkommen gegenüber dem Vorjahr. Eine Tendenzumkehr ist nicht zu erwarten.

Das stark gestiegene Arbeitsaufkommen sollte die Behörde mit einem unveränderten Personalbestand bewältigen. Zwar wurden im Haushaltsplan fünf neue Stellen geschaffen, was dazu führte, dass die befristeten Arbeitsverhältnisse von fünf bisher aus Aushilfskräfte-Mitteln beschäftigten Mitarbeiterinnen und Mitarbeitern in feste Arbeitsverhältnisse umgewandelt werden konnten. Dies war zweifellos positiv und hat die Behörde stabilisiert. Die Zahl der hier tätigen Beschäftigten wurde aber dadurch nicht erhöht, der Haushaltstitel für Aushilfskräfte entsprechend abgesenkt. Ein dramatisch gestiegenes Aufgabenvolumen soll also weiterhin mit unveränderter Beschäftigtenzahl bewältigt werden.

Alle Bemühungen um personelle Verstärkung – wenn auch nur temporär – sind gescheitert. Ein Papier des Landesrechnungshofes (LRH), das die veränderte Rechtslage völlig ignoriert – der LRH spricht offen davon, er habe die Behörde geprüft „wie jede andere auch“ – und das geänderte Arbeitsvolumen nicht zur Kenntnis nimmt, dient als Vorwand, einem Grundrecht die praktische Verwirklichung abzusprechen. Der LRH möchte insbesondere die Beratungstätigkeit so weit wie möglich reduzieren – in seinem Papierentwurf sogar vollständig beenden, was rechtlich schwierig wäre – und so mehr Personal verhindern.

Ein Blick über die Grenzen von Mecklenburg-Vorpommern hinaus zeigt, dass andere dies anders sehen. So stieg beispielsweise die Stellenzahl bei der Bundesbeauftragten für Datenschutz und Informationsfreiheit in der Amtszeit von Andrea Voßhoff vom Januar 2014 bis Januar 2019 von 87 auf 253,5. Zu beachten ist dabei, dass die Bundesbeauftragte bis auf wenige Bereiche nicht für die Privatwirtschaft zuständig ist; dies ist Aufgabe der Landesbeauftragten.

Angesichts dieser Fakten ist es nicht verwunderlich, dass der Landesbeauftragte für Datenschutz in Mecklenburg-Vorpommern seine gesetzlichen Aufgaben nur zu einem Teil erfüllen kann. Dies führt zunehmend zu Verärgerung bei betroffenen Bürgerinnen und Bürgern, vor allem aber dazu, dass die Aufgaben nach Art. 57 DS-GVO, insbesondere die Durchsetzung der DS-GVO, nur in Teilen möglich ist und die insbesondere von der Wirtschaft nachgefragte Beratung und Unterstützung, gerade von kleinen und mittleren Unternehmen (KMU), nicht erfolgen kann.

4 Zusammenarbeit auf europäischer Ebene

4.1 Europäischer Datenschutzausschuss (EDSA)

Am 25. Mai 2018 ist der Europäische Datenschutzausschuss (EDSA) an die Stelle der bisherigen Artikel-29-Datenschutzgruppe getreten. Er besteht wie diese aus dem Leiter einer Aufsichtsbehörde jedes Mitgliedstaates 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 (BR) als Stellvertreter einen Leiter der Aufsichtsbehörde eines Landes wählt. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) hat dem Bundesrat einen Vorschlag übermittelt. Eine Wahl ist bislang jedoch nicht erfolgt.

Anders als die Artikel-29-Datenschutzgruppe ist der EDSA eine Einrichtung der Europäischen Union (EU) 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. Auch hat er Leitlinien und Empfehlungen zur Auslegung einzelner Vorschriften der DS-GVO zu erstellen.

Bislang hat der EDSA unter https://edpb.europa.eu/edpb_de Leitlinien zu den Themen

- Recht auf Datenübertragbarkeit
- Datenschutzbeauftragte
- Federführende Aufsichtsbehörde
- Datenschutzfolgenabschätzung
- Meldung von Datenpannen
- Automatisierte Entscheidungen
- Geldbußen

- Einwilligung
- Transparenz

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.

Wir empfehlen der Landesregierung, sich dafür einzusetzen, dass schnellstmöglich durch den Bundesrat ein Stellvertreter für den Europäischen Datenschutzausschuss (EDSA) gewählt wird.

4.2 Gremien des Europäischen Datenschutzausschusses (EDSA)

4.2.1 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 den Datenschutz Niedersachsen wahr, im Vertretungsfalle wir. Die Sitzungen der Enforcement Subgroup finden etwa alle zwei Monate in Brüssel statt.

In der ersten Jahreshälfte 2018 erprobte die Enforcement Subgroup die neuen Verfahren für die Zusammenarbeit der Aufsichtsbehörden, unter anderem das Dringlichkeitsverfahren nach Art. 66 DS-GVO. Die Mitglieder der Arbeitsgruppe verschafften sich zudem einen Überblick über das in den einzelnen Mitgliedstaaten jeweils zur Anwendung kommende Verfahrensrecht.

Im Mittelpunkt stand jedoch die gemeinsame Bearbeitung grenzüberschreitender Fälle. Nach dem 25. Mai 2018 wurde deutlich, dass die Enforcement Subgroup zudem ein Forum darstellt, in dem konkrete Fragen zur Anwendung der Vorschriften in der DS-GVO über die Zusammenarbeit der Aufsichtsbehörden schnell und unbürokratisch geklärt werden können.

Gegen Ende des Berichtszeitraumes begann die Arbeit an einem Strategiepapier für den EDSA zur Durchsetzung der DS-GVO. Eine Verständigung der europäischen Aufsichtsbehörden über grundlegende strategische Fragen könnte eine wertvolle Ergänzung zu den in Art. 60 ff. DS-GVO geregelten Verfahren der Kooperation und Kohärenz darstellen.

4.2.2 Technology Subgroup

Die Artikel-29-Gruppe wurde vor vielen Jahren als zentrales Koordinierungsgremium für die datenschutzrechtliche Aufsicht innerhalb der Europäischen Union (EU) eingerichtet. Ähnlich dem Arbeitskreis „Technische und organisatorische Datenschutzfragen“ (AK Technik), siehe Punkt 5.3, auf nationaler Ebene, diente die Technology Subgroup im internationalen Kontext als Beratungs- und Unterstützungsgremium lange Zeit der Artikel-29-Gruppe. Inzwischen ist diese Arbeitsgruppe ein offizielles Gremium (Expert-Group) des Europäischen Datenschutzausschusses (EDSA), in dem Aktivitäten aller europäischen Datenschutzaufsichtsbehörden koordiniert werden und der mit Geltung der Europäischen Datenschutz-Grundverordnung (DS-GVO) die Artikel-29-Gruppe abgelöst hat. Um die Synergieeffekte der sich überschneidenden Themen in der Technology Subgroup und dem AK Technik sinnvoll zu nutzen, sind wir als ständiger Vertreter der deutschen Landesdatenschutzbeauftragten Mitglied der Tech-

nology 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 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. Daher lag im Berichtszeitraum der Fokus der Technology Subgroup besonders in der Erstellung von Leitlinien, die sich auf zentrale technische und organisatorische Aspekte der DS-GVO beziehen und diese dabei näher erläutern und zugleich Umsetzungshinweise liefern. Neben den bereits veröffentlichten Leitlinien zur Datenübertragbarkeit [1]gemäß Art. 20 DS-GVO und zur Datenschutzfolgenabschätzung (DSFA)[2] gemäß Art. 35 DS-GVO, siehe dazu auch Dreizehnter Tätigkeitsbericht, Punkt 8.3, wurden inzwischen auch die Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten[3] gemäß Art. 33 und die Leitlinien zur Akkreditierung[4] gemäß Art. 43 verabschiedet.

4.3 Europäische Zusammenarbeit mit dem 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, wir sind weiterhin für die Entgegennahme von Beschwerden über eine angeblich rechtswidrige Datenverarbeitung beispielsweise durch Facebook zuständig. 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 Binnenmarktes, nicht nur im Bereich des Datenschutzes, unterstützt.

Vom 25. Mai 2018 bis zum Jahresende 2018 fand in 619 Fällen über IMI eine Verständigung über die federführende Aufsichtsbehörde statt. 257 dieser Vorverfahren mündeten in einem Fallregistereintrag. 16 Entscheidungsentwürfe federführender Aufsichtsbehörden wurden bislang über IMI an die betroffenen Aufsichtsbehörden verteilt. Davon ging eine einzige Entscheidung ohne Weiteres durch. Ein Entwurf wurde zurückgezogen, alle anderen Entwürfe

1 https://www.datenschutzkonferenz-online.de/media/wp/20170405_wp242_rev01.pdf
2 https://www.datenschutzkonferenz-online.de/media/wp/20171004_wp248_rev01.pdf
3 https://www.datenschutzkonferenz-online.de/media/wp/20180206_wp250_rev01.docx
4 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_1_2018_certification_public_consultation_en.pdf

sind noch in Bearbeitung. Wir haben bislang in fünf Beschwerden über grenzüberschreitende Verarbeitungen ein IMI-Verfahren eingeleitet.

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 der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, statt.

Die 95. Datenschutzkonferenz im April 2018 stand erwartungsgemäß im Zeichen der Europäischen Datenschutz-Grundverordnung (DS-GVO), die wenige Wochen später in ganz Europa gelten würde. Die Konferenz musste unter anderem Festlegungen zur Zusammenarbeit der Aufsichtsbehörden untereinander treffen und auch klären, wie mit dem Europäischen Datenschutzausschuss (EDSA), siehe Punkt 4.1, und der Zentralen Anlaufstelle gemäß § 17 Abs. 1 Bundesdatenschutzgesetz (BDSG) zusammengearbeitet werden soll. Der Bundesgesetzgeber hat dazu in Kapitel 5 des neuen BDSG zwar Vorgaben gemacht. Diese recht abstrakten Vorgaben musste die Konferenz nun mit einem entsprechenden Konzept in praktische Verfahrensweisen umsetzen. Dazu gehörten auch Details der unterschiedlichen Zuständigkeiten von Aufsichtsbehörden im sogenannten Kohärenzverfahren (internationale Zusammenarbeit), das in Kapitel VII der DS-GVO festgelegt ist. Schließlich waren Anpassungen der Gremienstruktur der Konferenz (also deren Arbeitskreise und Arbeitsgruppen) an die internationalen Gremien des EDSA erforderlich. In der Frühjahrskonferenz begannen die Mitglieder zudem, die Geschäftsordnung der Konferenz an die Gegebenheiten der DS-GVO anzupassen. Diskutiert wurde auch über die Möglichkeiten, Einfluss darauf zu nehmen, wie der Stellvertreter des Gemeinsamen Vertreters der deutschen Aufsichtsbehörden im EDSA (§ 17 BDSG) bestimmt wird.

Neben diesen organisatorischen Fragen wurden auch zahlreiche fachliche Datenschutzaspekte besprochen. So wurden Orientierungshilfen zu „Online-Lernplattformen im Schulunterricht“[5], zu „Whistleblowing-Hotlines“[6] und zur „Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung“[7] beschlossen und eine Entschließung zum „Facebook-Datenskandal“[8] sowie eine „Positionsbestimmung zur Anwendbarkeit des Telemediengesetzes für nichtöffentliche Stellen ab dem 25. Mai 2018“[9] verabschiedet. Schließlich wurde eine überarbeitete Version des Standard-Datenschutzmodells[10] beschlossen, siehe Punkt 7.1.5.

In der 96. Datenschutzkonferenz im November 2018 konnten bereits erste Erfahrungen der Anwendung der DS-GVO und der internationalen Zusammenarbeit ausgetauscht werden. Nicht überraschend war, dass die Zusammenarbeit zwischen allen Ebenen weiter optimiert und verbessert werden muss. Die Konferenz bat deshalb ihren Arbeitskreis Organisation und Struktur, Verbesserungsvorschläge zur Organisation der Zusammenarbeit der deutschen Aufsichtsbehörden untereinander und mit den europäischen Aufsichtsbehörden zu erarbeiten. Als unbefriedigend hatte sich zudem herausgestellt, dass der Bundesrat von seiner Befugnis nach § 17 BDSG nach wie vor keinen Gebrauch gemacht und immer noch keinen Stellvertreter für

5 https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Broschueren/OH-Lernplattformen.pdf
6 https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Broschueren/OH-Whistleblowing-Hotlines-neu.pdf
7 https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Broschueren/OH_Werbung.pdf
8 https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/95-Ent-FB-Datenskandal.pdf
9 https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/95-Position-TMG.pdf
10 https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V_1_1.pdf

den EDSA gewählt hatte. Bis zum Ende des Berichtszeitraumes hat der Bundesrat die dringend erforderliche Wahl nicht durchgeführt. In der Herbstkonferenz konnte schließlich die neue Geschäftsordnung abschließend beraten und einstimmig verabschiedet werden[11].

Die Fülle der Themen, die unter den deutschen Aufsichtsbehörden regelmäßig abgestimmt werden muss, hat gezeigt, dass die zwei turnusmäßigen Datenschutzkonferenzen keinen ausreichenden Zeitrahmen bieten. Deshalb wurden wie schon in den Jahren davor auch in diesem Berichtszeitraum vier zusätzliche Sonderkonferenzen durchgeführt. In den Sonderkonferenzen wurden ausschließlich Themen behandelt, die aus der Anwendung und Durchsetzung der DS-GVO resultieren.

Ein Schwerpunkt dieser Sitzungen war beispielsweise die Abstimmung einer Liste von Verarbeitungsvorgängen, für die eine Datenschutzfolgenabschätzung (DSFA) gemäß Art. 35 Abs. 1 DS-GVO durchzuführen ist. Wie auf den Homepages aller Aufsichtsbehörden findet sich auch in unserem Internetangebot nun die abgestimmte Liste für den nichtöffentlichen Bereich[12].

Beraten wurde auch die Rolle der Aufsichtsbehörden bei der Evaluation der DS-GVO, denn die Europäische Kommission muss gemäß Art. 97 Abs. 1 DS-GVO erstmalig zum 25. Mai 2020 einen entsprechenden Bericht vorlegen, in den nach unserer Auffassung insbesondere die Erfahrungen der Datenschutzaufsichtsbehörden einfließen sollen.

5.2 Kurzpapiere zum vorläufigen Verständnis der DS-GVO

Zum vorläufigen Verständnis der Europäischen Datenschutz-Grundverordnung (DS-GVO) hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) seit Juli 2017 die folgenden Kurzpapiere veröffentlicht:

- Kurzpapier Nr. 1 Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO
- Kurzpapier Nr. 2 Aufsichtsbefugnisse / Sanktionen
- Kurzpapier Nr. 3 Verarbeitung personenbezogener Daten für Werbung
- Kurzpapier Nr. 4 Datenübermittlung in Drittländer
- Kurzpapier Nr. 5 Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO
- Kurzpapier Nr. 6 Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO
- Kurzpapier Nr. 7 Marktortprinzip: Regelungen für außereuropäische Unternehmen
- Kurzpapier Nr. 8 Maßnahmenplan „DS-GVO“ für Unternehmen
- Kurzpapier Nr. 9 Zertifizierung nach Art. 42 DS-GVO
- Kurzpapier Nr. 10 Informationspflichten bei Dritt- und Direkterhebung
- Kurzpapier Nr. 11 Recht auf Löschung / „Recht auf Vergessenwerden“
- Kurzpapier Nr. 12 Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern

[11] https://www.datenschutzkonferenz-online.de/media/dskb/20180905_dskb_geschaeftsordnung.pdf

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

- Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO
- Kurzpapier Nr. 14 Beschäftigtendatenschutz
- Kurzpapier Nr. 15 Videoüberwachung nach der Datenschutz-Grundverordnung
- Kurzpapier Nr. 16 Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DS-GVO
- Kurzpapier Nr. 17 Besondere Kategorien personenbezogener Daten
- Kurzpapier Nr. 18 Risiko für die Rechte und Freiheiten natürlicher Personen
- Kurzpapier Nr. 19 Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO

Mit der Veröffentlichung des Kurzpapiers Nr. 19 wurde dieses Projekt der Datenschutzkonferenz im Mai 2018 abgeschlossen. Wir haben uns, soweit uns dies zeitlich möglich war, an der Erarbeitung der Kurzpapiere beteiligt und werden im Folgenden auch unseren Anteil an der Überarbeitung und Aktualisierung der Papiere übernehmen.

Die Kurzpapiere sind auf der Internetseite des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern unter www.datenschutz-mv.de zu finden.

5.3 AK Technik

Seit mehr als 25 Jahren leitet der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern den Arbeitskreis „Technische und organisatorische Datenschutzfragen“ (AK Technik) der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz).

Über das Vertrauen der Datenschutzkonferenz, dass sie uns in einem besonders wichtigen Teilaspekt des Datenschutzes schon über eine so lange Zeit eine maßgebliche Rolle übertragen hat, freuen wir uns sehr. Die Leitung des AK Technik sehen wir daher als eine unserer Schwerpunktaufgaben an und berichten, wie in jedem Tätigkeitsbericht, zuletzt im Dreizehnten Tätigkeitsbericht unter Punkt 8, zum AK Technik.

Im Dreizehnten Tätigkeitsbericht hatten wir prognostiziert, dass die Europäische Datenschutz-Grundverordnung (DS-GVO) und die Digitalisierung der Verwaltung in Deutschland eine zunehmende Koordinierung der Aktivitäten der Aufsichtsbehörden im technischen Bereich erfordern werden. Wie die folgende, lediglich schlaglichtartige Schilderung der letzten zwei Sitzungen des AK Technik zeigt, hat sich diese Prognose vollständig bestätigt.

Die **70. Sitzung** des AK Technik fand im Frühjahr 2018 auf Einladung des Deutschen Zentrums für Luft- und Raumfahrt (DLR) in Neustrelitz statt. In verschiedenen Vorträgen informierten uns die Mitarbeiter des DLR zu den Themen Datenmanagement, Maritime Sicherheit, Kommunikation und Navigation. Insbesondere bei der Besichtigung der Bereiche Datenempfang und Archiv konnten wir uns mit technischen und organisatorischen Maßnahmen vertraut machen, die einen sicheren Umgang mit großen Datenbeständen ermöglichen und insbesondere deren Verfügbarkeit, Integrität und Vertraulichkeit sicherstellen. Zu dieser Sitzung waren auch Mitarbeiter des Robert-Koch-Instituts eingeladen, um mit den Mitgliedern des Arbeitskreises technische Details des Elektronischen Melde- und Informationssystems für den Infektionsschutz (DEMIS) zu beraten. Schließlich wurde auch die Version 1.1 des Standard-Datenschutzmodells (SDM), siehe Punkt 7.1.5, abschließend beraten, die dann von der 95. Datenschutzkonferenz verabschiedet wurde, siehe Punkt 5.1.

Nachdem der designierte Konferenzvorsitzende für das Jahr 2019 darüber informiert hatte, dass er für die Zeit seines Vorsitzes das Thema „Künstliche Intelligenz“ als Schwerpunktthema ausgewählt habe, baten wir die Technische Universität Kaiserslautern um Unterstützung. Zur **71. Sitzung** im Herbst 2018 luden uns Wissenschaftler des Lehrstuhls Robotersysteme aus dem Fachbereich Informatik der Universität ein, um uns einen Einblick in die Forschung zu autonomen Systemen und insbesondere zu autonomen Fahrzeugen zu gewähren. Die Diskussion mit den Wissenschaftlern machte deutlich, wie schwierig die Prüfung der äußerst komplexen Steuerungssysteme autonomer Systeme ist. Insbesondere in selbstlernenden Systemen wäre kaum Transparenz bzw. Prüfbarkeit herstellbar und es könne nur schwer entschieden werden, ob die Datenbasis für den Lernvorgang sinnvoll ausgewählt ist. Mit Blick auf die Forderungen der DS-GVO stellten die Wissenschaftler fest, dass viele Algorithmen und ihre algorithmischen Entscheidungsfindungen nur schwer oder gar nicht nachvollziehbar sein können und die Transparenz daher vielfach nicht gegeben sei. Ein weiteres Schwerpunktthema der Sitzung war die Verschlüsselung von E-Mails. Die Mitglieder diskutierten den ersten Entwurf einer Orientierungshilfe und versuchten zu klären, welche Technologien inzwischen als Stand der Technik im Sinne des Art. 32 DS-GVO angesehen werden müssen und folgerichtig von Verantwortlichen beim Versand von E-Mails einzusetzen sind, siehe Punkte 7.2.1 und 7.2.2. In dieser Sitzung wurden auch Fragen des Einsatzes von privaten Endgeräten von Schülerinnen und Schülern sowie Lehrkräften im schulischen Umfeld beraten. Die Kultusministerkonferenz (KMK) war an verschiedene Arbeitskreise der Datenschutzkonferenz mit der Bitte um Unterstützung bei der Umsetzung ihrer Strategie zur „Bildung in der digitalen Welt“ herangetreten.

5.4 IT-Planungsrat

Turnusmäßige Sitzungen

Der IT-Planungsrat[13] (IT-PLR) wurde als zentrales Gremium für die föderale Zusammenarbeit in der Informationstechnik etabliert. Die Errichtung des IT-PLR und die Ziele der Zusammenarbeit sind im IT-Staatsvertrag festgelegt, den Bund und Länder zur Umsetzung des Artikel 91 c Grundgesetz (GG) geschlossen haben. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) hat uns in unserer Eigenschaft als Vorsitzendem des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ (AK Technik), siehe Punkt 5.3, das Mandat zur Beratung des IT-PLR aus der Sicht der Landesbeauftragten für den Datenschutz erteilt, siehe auch Zehnter Tätigkeitsbericht, Punkt 3.2.7.

Im Berichtszeitraum haben wir sowohl an den vorbereitenden Sitzungen auf der Ebene der Abteilungsleiter als auch an allen sechs turnusmäßigen Sitzungen teilgenommen. Wir versuchen auf diese Weise, einerseits den IT-PLR auf die datenschutzrechtlichen Aspekte seiner zahlreichen Projekte und Anwendungen[14] aufmerksam zu machen und andererseits die Datenschutzkonferenz über die Arbeit des IT-PLR zu informieren.

Im folgenden Abschnitt berichten wir über die Themen „Digitalisierungsprogramm des Bundes“ und „Portalverbund“. Diese Themen sind inzwischen zu Schwerpunktthemen in der Arbeit des IT-PLR geworden und weisen besonders enge Bezüge zur Tätigkeit der Datenschutzaufsichtsbehörden auf.

[13] https://www.it-planungsrat.de/DE/Home/home_node.html
[14] https://www.it-planungsrat.de/DE/Projekte/projekte_node.html

Ausgewählte Aspekte der Tätigkeit

Seit seiner 20. Sitzung im Juni 2016 befasst sich der IT-PLR mit dem Digitalisierungsprogramm für die öffentliche Verwaltung von Bund, Ländern und Kommunen. Das Onlinezugangsgesetz (OZG) verpflichtet Bund und Länder, bis Ende 2022 ihre Verwaltungsleistungen auch elektronisch über Verwaltungsportale anzubieten. Das OZG ist somit der rechtliche Rahmen, an dem sich der IT-PLR bei der Planung und Umsetzung seines Digitalisierungsprogramms orientiert, siehe auch Dreizehnter Tätigkeitsbericht, Punkt 7.2. Im Oktober 2016 hat der IT-PLR die Einrichtung des Koordinierungsprojektes „Portalverbund“[15] beschlossen. Mit dem Portalverbund soll der Zugang zu digitalisierten Verwaltungsleistungen bundesweit ermöglicht werden. Im März 2017 wurde dann folgerichtig das Koordinierungsprojekt „Digitalisierungsprogramm“[16] eingerichtet.

In die Diskussionen zum Digitalisierungsprogramm hat sich im Jahr 2017 auch der Nationale Normenkontrollrat (NKR) eingeschaltet. In der 24. Sitzung des IT-PLR im Oktober 2017 hat der Vorsitzende des NKR seine Studie mit dem Titel „Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren.“[17] vorgestellt. Ein Kerngedanke dieser Studie ist die Modernisierung der deutschen Registerlandschaft durch Schaffung einer gesamtstaatlichen Infrastruktur für digitalen Registerzugriff. Im Zusammenhang mit der Modernisierung der deutschen Registerlandschaft empfiehlt der NKR, dass bestimmte Basisdaten von Bürgern und Unternehmen nur einmal mitgeteilt werden müssen („Once Only“-Prinzip). Der NKR hat darüber hinaus angeregt, datenschutzkonforme Identifikationsnummern für Personen, Unternehmen sowie Gebäude, Wohnungen und Flurstücke zu schaffen und zu nutzen.

Das Bundesinnenministerium hat dem IT-Planungsrat inzwischen die „Leitlinien für eine Modernisierung der Registerlandschaft“ und den „Vorschlag für die Verbesserung des Identitätsmanagements als Teil der Registermodernisierung“ vorgelegt. Es ist davon auszugehen, dass der IT-PLR diesen Dokumenten Anfang 2019 zustimmt und damit den Weg freimacht für einen dauerhaft eingerichteten, zentralen Personenbestand (Kerndatensystem) und für die Einführung eines sogenannten Identifikators zum zuverlässigen Auffinden von Datensätzen einer Person in verschiedenen Registern.

Das Bundesverfassungsgericht hat schon im Volkszählungsurteil von 1983 der Einführung und Verarbeitung derartiger Personenkennzeichen sehr enge Schranken auferlegt, da sie massiv in den Schutzbereich des Rechts auf informationelle Selbstbestimmung betroffener Bürgerinnen und Bürger eingreifen. Die Europäische Datenschutz-Grundverordnung (DS-GVO) ermöglicht den Mitgliedstaaten mit Artikel 87 zwar, die Implementierung und Verarbeitung von nationalen Kennziffern zu regeln, fordert aber eine Verwendung unter Wahrung geeigneter Garantien für die Rechte und Freiheiten der Betroffenen gemäß der DS-GVO.

Unsere Aufgabe im IT-PLR wird es daher sein, gemeinsam mit den Aufsichtsbehörden von Bund und Ländern darauf hinzuwirken, dass insbesondere die Datenschutz-Grundsätze aus Art. 5 DS-GVO sowie die Regelungen aus Art. 25 der DS-GVO zur datenschutzgerechten Gestaltung bei der Umsetzung des Digitalisierungsprogramms beachtet werden.

[15] https://www.it-planungsrat.de/DE/Projekte/Koordinierungsprojekte/Portalverbund/Portalverbund_node.html

[16] https://www.it-planungsrat.de/DE/Projekte/Koordinierungsprojekte/Digitalisierungsprogramm/DigPro_node.html

[17] https://www.normenkontrollrat.bund.de/resource/blob/72494/476004/12c91fffb877685f4771f34b9a5e08fd/2017-10-06-download-nkr-gutachten-2017-data.pdf

6 Projekte

6.1 Datenschutz als Bildungsauftrag

Bereits seit dem Elften Tätigkeitsbericht, Punkt 2 und folgende, haben wir über unsere unterschiedlichen Aktivitäten im Bereich der Medienbildung und Medienkompetenzförderung sowie der Sensibilisierung aller Altersgruppen zum datenschutzbewussten Umgang mit persönlichen Daten berichtet. Die dort genannten Projekte wurden in diesem Berichtszeitraum weitergeführt sowie weitere Initiativen gestartet[18].

Ausgehend von der bis heute uneingeschränkt gültigen Rechtsprechung des Bundesverfassungsgerichtes zum Grundrecht auf informationelle Selbstbestimmung und nach Artikel 57 Abs. 1 Ziffer b der Europäischen Datenschutz-Grundverordnung (DS-GVO)[19] ist es nach wie vor eine der gesetzlichen Kernaufgaben unserer Behörde, über den Datenschutz und seine praktische Umsetzung in geeigneter Weise, das heißt zielgruppenorientiert, zeitnah und umfänglich, zu informieren und mit diesen notwendigen Informationen im Hinblick auf die rasante Entwicklung unserer medial geprägten Gesellschaft aufzuklären. Ein besonderes Augenmerk soll dabei auf spezifische Angebote für Kinder und Jugendliche gelegt werden (ebd.).

Die Digitalisierung durchdringt alle Bereiche der Gesellschaft und verändert grundlegend die Lebens- und Berufswelt aller Bürgerinnen und Bürger in unserem Bundesland. Die rasante Entwicklung erfordert von jedem Einzelnen eine stetige Auseinandersetzung sowie sich kontinuierlich weiterentwickelnde Kompetenzen. Nur kritische und informierte Nutzerinnen und Nutzer sind in der Lage, die Vor- und Nachteile der digitalen Kultur einzuschätzen. Dies erfordert lebenslanges Lernen und eine grundlegende Medienbildung. Medienkompetenz ist also der Schlüssel für die Teilhabe und die Entwicklung einer aktiven und selbstbewussten Rolle in der Gesellschaft. 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 Medienbildung eine Grundvoraussetzung für eine gelingende Persönlichkeitsentwicklung, das Verständnis von Demokratie, für gesellschaftliche Teilhabe und die Entwicklung einer Ausbildungs- und Erwerbsfähigkeit.

Die digitalen Medien haben Einzug in die Familien und Zimmer aller Heranwachsenden gehalten. Damit stellt sich bei unvoreingenommener Betrachtung die Frage nicht mehr, ob Medienbildung und Medienkompetenzvermittlung ein notwendiger Baustein auf dem Bildungsweg der Kinder und Jugendlichen sein sollte, sondern es stellt sich nur noch die Frage, wie dieser Baustein möglichst zeitnah und in geeigneter Form in die Lebenswelt der Heranwachsenden eingefügt werden kann.[20] Dieses Vorhaben ist als eine gesamtgesellschaftliche Aufgabe zu betrachten.

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

[18] Tage ethischer Orientierung (TEO) – protect privacy: Dein Klick, Deine Verantwortung; Medien-Familie-Verantwortung;“ Jugend hackt“ in MV; Kooperation mit „Jugend im Landtag“ und „Jugend fragt nach“

[19] „Unbeschadet anderer in dieser Verordnung dargelegter Aufgaben muss jede Aufsichtsbehörde in ihrem Hoheitsgebiet
b) die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung sensibilisieren und sie darüber aufklären. Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder; […]“

[20] http://www.kmk.org/bildung-schule/allgemeine-bildung/faecher-und-unterrichtsinhalte/weitere-unterrichtsinhalte/medienbildung-in-der-schule.html

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.

6.1.1 Aktuelles zum Projekt „MedienscoutsMV“

Der Projektstart erfolgte im Juni 2012. Das „MedienscoutsMV“-Projekt wird seither unterstützt von der Landeskoordinierungsstelle für Suchtthemen Mecklenburg-Vorpommern (LAKOST MV), dem Landesjugendring Mecklenburg-Vorpommern (LJR MV), dem Landeskriminalamt Mecklenburg-Vorpommern (LKA MV), der Medienanstalt Mecklenburg-Vorpommern (MMV) und deren Online-Selbsthilfeplattform juuuport sowie der Computer-SpielSchule Greifswald (CSG).

Die Konzeptidee liegt auf dem peer-to-peer-Ansatz. Jugendliche können anhand dieser Methode ihr Wissen unmittelbar an andere Jugendliche (und bisweilen auch an Lehrkräfte 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. Sie lernen zudem eine Auswahl an methodischen Konzepten zur Umsetzung von Workshops, Vorträgen und Projekttagen kennen und können sich darin sofort üben. Gleichzeitig steht ihnen das Expertenteam im Nachgang der Ausbildung dauerhaft zur Verfügung, um Hilfe und Unterstützung zu leisten. Einmal jährlich werden alle bereits ausgebildeten MedienscoutsMV zu einem Update-Treffen eingeladen, um sich auszutauschen, neue Themen zu besprechen und aktuelle Trends zu diskutieren.

Bisher wurden in 13 Ausbildungswochenenden seit 2012 rund 400 MedienscoutsMV landesweit ausgebildet. Durch den peer-to-peer-Ansatz ist es dem Gemeinschaftsprojekt möglich, das Wissen zu multiplizieren. Jährlich erreichen die MedienscoutsMV rund 3.500 Schülerinnen und Schüler.

Wenn es Anmeldungen von Schülerinnen und Schülern einer Schule gibt, dann bieten wir auch einem Erwachsenen (Lehrerin/Lehrer oder Schulsozialarbeiterin/Schulsozialarbeiter) an, sich ebenfalls als MedienscoutsMV ausbilden zu lassen. Dadurch sind an Schulen richtige „MedienscoutsMV-AG“ entstanden, die sich regelmäßig treffen und Projekttage planen. Dies bedeutet für die Jugendlichen ebenso wie für die betreuenden Erwachsenen neben ihren schulischen Aufgaben einen zusätzlichen Aufwand. Es gibt Schulen, an denen es einen spürbaren Nachweis für die hohe Wertschätzung und Anerkennung dieses ehrenamtlichen Engagements seitens der Lehrerschaft und der Schulleitung gibt. Es gibt jedoch auch immer wieder Schulen, wo dies leider nicht der Fall ist. Es wäre wünschenswert, wenn jede Schule, an der es MedienscoutsMV gibt, die Chancen erkennen könnte, welches Wissen und ehrenamtliches Engagement von den Jugendlichen und gegebenenfalls betreuenden Erwachsenen ausgeht.

Das Projekt wird durch die bereitgestellten Mittel des Landtages sowie durch eine finanzielle Beteiligung des Landeskriminalamtes Mecklenburg-Vorpommern und der Medienanstalt Mecklenburg-Vorpommern finanziert. Die finanzielle Ausstattung des Projektes MedienscoutsMV ist seit 2012 gleichbleibend.

Jeder Schülerin und jedem Schüler wird eine kostenfreie Teilnahme ermöglicht. Aus unseren Erfahrungen zeigt sich immer wieder, dass sonst Jugendliche aus finanzschwächeren Familien nicht teilnehmen könnten.

Der Erfolg dieses bundesweit beachteten Projektes setzt auch weiterhin voraus, dass mindestens die strukturelle, organisatorische und finanzielle Basis für diese außerschulische Kooperation erhalten bleibt. Letztlich genießt das in unserem Land praktizierte Kooperationsmodell

mit vielen sehr unterschiedlichen und vor allem außerschulischen Kooperationspartnern nach wie vor eine bundesweite Aufmerksamkeit, gilt es doch als besonders kostensparend und effizient.

Es ist zu vermerken, dass es einen stetigen Anstieg der Teilnehmerzahlen gibt, der dazu führte, dass wir im Jahr 2018 in jedem Durchgang bereits 10 Teilnehmende mehr ausgebildet haben. Die Nachfrage ist noch einmal gestiegen. Es gibt Wartelisten, und interessierte Jugendliche müssen auf den nächst folgenden Ausbildungslehrgang vertröstet werden. Das kann dazu führen, dass die Jugendlichen eine weitere Anreise in Kauf nehmen müssen.

Mit den aktuellen Teilnehmerzahlen hat das Projekt bereits die Grenze des Möglichen überschritten. Es stehen keine weiteren finanziellen Mittel bereit, um die höheren Kosten von Übernachtung und Verpflegung durch die gestiegenen Teilnehmerzahlen zu decken. Darüber hinaus gibt es weder beim LfDI MV noch bei den Kooperationspartnern hinreichend strukturelle und finanzielle Voraussetzungen, um beispielsweise die Zahl der Ausbildungsdurchgänge zu erhöhen oder gegebenenfalls zielgruppenspezifisch anzupassen. Weder die bereits im Dreizehnten Tätigkeitsbericht, Punkt 4.1.1, angesprochene Weiterentwicklung des Projektes noch die Initiierung einer datenschutzgerechten Kommunikationsplattform für die MedienscoutsMV wurde im Berichtszeitraum 2018 umgesetzt.

Interessierte können sich informieren unter: www.medienscouts-mv.de.

6.1.2 Netzwerk „Medienaktiv M-V“

Das landesweite Netzwerk für Medienbildung in Mecklenburg-Vorpommern „Medienaktiv M-V“ wird vom Landesjugendring Mecklenburg-Vorpommern (LJR MV), der Landeskoordinierungsstelle für Suchtthemen Mecklenburg-Vorpommern (LAKOST MV), dem Landeskriminalamt Mecklenburg-Vorpommern (LKA MV), dem Kompetenzzentrum und Beratungsstelle für exzessive Mediennutzung und Medienabhängigkeit Schwerin der Evangelischen Suchtkrankenhilfe Mecklenburg-Vorpommern, der Medienanstalt Mecklenburg-Vorpommern (MMV) und unserer Behörde organisiert.

Den bundesweit beispielgebenden Charakter des Netzwerkes hat „Medienaktiv M-V“ auch weiterhin inne. Nach unseren Erkenntnissen aus bundesweiten Arbeitsgruppen zum Thema sind jedoch auch die anderen Bundesländer auf dem Weg, sich institutionsübergreifend zu vernetzen, und treiben Konzepte zur Medienkompetenzvermittlung aktiv voran.

Das Netzwerk unterstützt den Wissenstransfer aktiv, so dass andere Bundesländer von unseren Erkenntnissen und der Zusammenarbeit profitieren. So hat sich Thüringen ein Beispiel an der „Kooperationsvereinbarung zur Förderung der Medienkompetenz in Mecklenburg-Vorpommern“ und den „Medienpolitischen Forderungen an die zukünftige Arbeit der Landesregierung“ unseres Netzwerkes genommen und im Jahr 2017 die „Landeskooperationsvereinbarung zur nachhaltigen Weiterentwicklung von Medienkompetenz in Thüringen“ aufgesetzt. Möchte das Land Mecklenburg-Vorpommern jedoch weiterhin diese bundesweite Vorreiterrolle behalten, bedarf es entsprechender Maßnahmen:

- enge und ressortübergreifende Zusammenarbeit im Sinne der „Kooperationsvereinbarung zur Förderung der Medienkompetenz in Mecklenburg-Vorpommern“,
- konkrete Unterstützung für die Vernetzung möglichst aller medienpädagogisch Wirkenden in Mecklenburg-Vorpommern und die Stärkung des Netzwerkes „Medienaktiv M-V“,
- die verstärkte Einbindung von Familienarbeit zur Stärkung der Medienkompetenz,

- niederschwellige Angebote der Medienbildung, angefangen bei der frühkindlichen Bildung und verstanden als lebenslanges Lernen, das sich wie ein roter Faden durch viele Bildungsangebote zieht,
- Medienbildung verstanden als fächerintegrativer Ansatz,
- verbindliche Einführung von Standards zur schulischen Medienbildung (Curriculum),
- die Schulung von Lehrkräften und pädagogischen Fachkräften, unter anderem durch die Einführung von verpflichtenden Elementen der Medienbildung bereits in der Ausbildung/im Studium sowie weiterführend in der Fort- und Weiterbildung von Erzieherinnen und Erziehern sowie Lehrerinnen und Lehrern (in allen Phasen der Ausbildung),
- eine moderne und im internationalen Vergleich angemessene technische Ausstattung von Schulen,
- die konsequente praktische Umsetzung des Kinder- und Jugendmedienschutzes,
- die Stärkung der Medienbildung von Eltern und Senioren.

Um den politischen Diskurs zu begleiten, fand auch im Jahr 2018 der „Medienpolitische Abend“ des Netzwerkes statt. Die Resultate einer Chancen- und Risikoanalyse in den verschiedenen Arbeitsfeldern (außerschulisch, schulisch, Kooperation im Land, Seniorinnen und Senioren etc.) bilden die Grundlage für das medienpolitische Handeln des Netzwerkes „Medienaktiv M-V“.

Die Frühjahrstagung des Netzwerkes „Digitale Kompetenzen – lernen, leben und arbeiten in Mecklenburg-Vorpommern“ wurde erstmals in Kooperation mit dem Ministerium für Energie, Infrastruktur und Digitalisierung Mecklenburg-Vorpommern veranstaltet. Durch diese Kooperation wurde es möglich, das breite Spektrum der Akteure im Land und bundesweit allen Interessierten vorzustellen. Die Frühjahrstagung hat Ideen, Chancen und Entwicklungsmöglichkeiten vorgestellt. Im Fokus standen Angebote und Initiativen, die beim Erwerb von digitalen Kompetenzen Hilfe leisten. Die Frühjahrstagung wurde unterstützt von der Universität Rostock und den Industrie- und Handelskammern (IHK) in Mecklenburg-Vorpommern. Diese Zusammenarbeit hat gezeigt, dass institutionsübergreifendes Handeln im Sinne der Präambel der „Kooperationsvereinbarung zur Förderung der Medienkompetenz in Mecklenburg-Vorpommern“ als gesamtgesellschaftliche Aufgabe umsetzbar ist.

Die Herbsttagung des Netzwerkes folgte dem Beispiel. Die Zusammenarbeit mit dem Landkreis Mecklenburgische Seenplatte ermöglichte eine Durchführung in Neubrandenburg. Die Herbsttagung vermittelte ganz praktisches Wissen zum Einsatz digitaler Lernmittel.

Das Netzwerk „Medienaktiv M-V“ will die Vernetzung aller Akteure im Land voranbringen und den Dialog mit Politik, Verwaltung und Wirtschaft weiter ausbauen. Ziel ist es, der digitalen Spaltung der Gesellschaft entgegenzuwirken und eine solide Basis für ein selbstbestimmtes und lebenslanges Lernen in Mecklenburg-Vorpommern zu schaffen.

Das Netzwerk „Medienaktiv M-V“ zeigt, dass die strukturelle Vernetzung in einem präventiven Sinne Suchthilfe, Polizei, Datenschutz, Jugendhilfe u. v. m. verbinden kann. Für die Vernetzung bedarf es einer verbindlichen Struktur und eines ressortübergreifenden Aus-

tauschs. Die Struktur des Netzwerkes vereint sehr viel Fachwissen und ein hohes Engagement der Akteure, das mit Blick auf den reinen Bildungssektor kaum genutzt wird.[21]

Das Netzwerk „Medienaktiv M-V“ hat sich aus der Arbeit heraus und vor allem auch aus den Bedarfen heraus gebildet. Mittlerweile verfügt es über einen hohen Bekanntheitsgrad in Mecklenburg-Vorpommern und darüber hinaus. Das führt jedoch auch dazu, dass die Anfragen nach Unterstützung sich erhöhen. Andere Bundesländer schauen nach Mecklenburg-Vorpommern, wie hier die Zusammenarbeit zwischen so vielen verschiedenen Akteuren funktionieren kann. Auf Nachfragen aus dem Bundesgebiet informieren wir alle interessierten Institutionen dazu.

Die Vernetzung innerhalb Mecklenburg-Vorpommerns aufrechtzuerhalten und stetig neue Netzwerkpartner einzubinden übernimmt der LfDI MV maßgeblich. Da keine strukturelle Unterstützung dafür vorhanden ist, bleibt das Engagement der Akteure der Medienbildung in Mecklenburg-Vorpommern das Hauptpotenzial des Netzwerkes.

Alle neuen Erkenntnisse, weitere Kooperationen und mögliche Schritte, wie wir uns als Bundesland der Digitalisierung unserer Gesellschaft stellen können, um damit gesellschaftliche Teilhabe, Demokratiebildung und Chancengleichheit herzustellen, werden wir weiter im Netzwerk „Medienaktiv M-V“ im Dialog mit Politik erörtern.

6.1.3 Medienkompetenz in Mecklenburg-Vorpommern

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (LfDI MV) wurde als Experte eingeladen zur öffentlichen Anhörung des Sozialausschusses des Landtages Mecklenburg-Vorpommern zum Thema „Medienbildung für junge Leute im Kontext der Digitalisierung“ im Rahmen der Reihe „Jung sein in Mecklenburg-Vorpommern“.

Sowohl in der schriftlichen Stellungnahme des LfDI MV[22] als auch in der mündlichen Anhörung[23] wurde klar, dass eine separate Betrachtung von schulischer Medienbildung und außerschulischer Medienbildung nicht förderlich ist. Darauf verweisen auch die Stellungnahmen der Jugendlichen und anderen Vertreter.[24] Die außerschulische Medienbildung muss ein fester Bestandteil der außerschulischen Kinder- und Jugendbildung sein, verstanden als gleichberechtigter Part zu schulischer Medienbildung und Elternarbeit.

Die außerschulische Medienbildung bietet viel Potenzial für Partizipation und Demokratiebildung gleichermaßen. Dies wird ebenfalls in der Strategie der Kultusministerkonferenz (KMK) „Bildung in der digitalen Welt“ hervorgehoben[25]. Dabei ist dringend darauf zu achten, dass das bisherige quantitative Gefälle von Medienbildungsprojekten zwischen den Landesteilen aufgehoben wird. Aufgrund der Fläche von Mecklenburg-Vorpommern ergeben sich auch daraus spezielle Herausforderungen.

Positiv werten wir die zunehmende Sensibilisierung für das Thema der Medienkompetenzförderung und Medienbildung. Dabei bleibt es weiterhin eine große Herausforderung, wie dies zeitnah und flächendeckend für Mecklenburg-Vorpommern umgesetzt werden kann. Dabei

[21] gl. DR7/340-3, Stellungnahme des LfDI MV zur öffentlichen Anhörung des Sozialausschusses des Landtags M-V „Medienbildung für junge Leute im Kontext der Digitalisierung“ im Rahmen der Reihe „Jung sein in Mecklenburg-Vorpommern“

[22] DR 7/340-3

[23] Video der öffentlichen Anhörung „Medienbildung für junge Leute im Kontext der Digitalisierung https://www.youtube.com/watch?v=n4gBx9CpIJg

[24] DR 7/340-9neu

[25] KMK Strategie „Bildung in der digitalen Welt“, Kompetenzbereiche für den Unterricht, S. 27

wäre es wünschenswert, wenn der gesamtgesellschaftliche Blick mit allen Institutionen eingenommen werden kann. Die öffentliche Anhörung hat dabei gezeigt, wer die tragenden Pfeiler der Medienbildung in Mecklenburg-Vorpommern sind. Das Engagement der Expertinnen und Experten im Land und die Vernetzung durch „Medienaktiv M-V“ tragen umfangreich und dauerhaft dazu bei. Es benötigt jedoch politische Rahmenbedingungen, die durch die Digitale Agenda des Landes jetzt aufgenommen wurden. Das begrüßen wir sehr. Und gleichzeitig benötigt es einen Dialog in unserer Gesellschaft, um diese gesamtgesellschaftliche Aufgabe umsetzen zu können.

Zwar impliziert der Begriff Medienbildung die Zuständigkeit von einem Ressort. Doch sehen wir im Kontext der gesamtgesellschaftlichen Aufgabe hier keine alleinige Aufgabe eines Ressorts. So vernetzt, wie unsere digitale Gesellschaft aufgebaut ist, müssen die politischen Rahmenbedingungen mit den handelnden Akteuren ebenfalls Vernetzung schaffen. Hier sehen wir noch viele ungenutzte Potenziale.

In mehreren Stellungnahmen wird ebenfalls auf die „Kooperationsvereinbarung zur Förderung der Medienkompetenz in Mecklenburg-Vorpommern“ als notwendiges und wichtiges Instrument verwiesen. Die Neuschreibung bietet die Möglichkeit, klare Handlungsfelder zu definieren.

Die Landesregierung Mecklenburg-Vorpommern räumt mit der „Kooperationsvereinbarung zur Förderung der Medienkompetenz in Mecklenburg-Vorpommern“ der Förderung von Medienbildung und Medienkompetenz einen hohen Stellenwert ein. Die Vereinbarung wurde 2015 von der Staatskanzlei des Landes Mecklenburg-Vorpommern, dem Ministerium für Inneres und Sport Mecklenburg-Vorpommern, dem Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern, dem Ministerium für Arbeit, Gleichstellung und Soziales Mecklenburg-Vorpommern, dem Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern sowie der Medienanstalt Mecklenburg-Vorpommern unterzeichnet. Darin ist vereinbart, dem Kabinett einen Evaluationsbericht bis Ende 2018 vorzulegen, um von den Ergebnissen und den Erfahrungen bei der Umsetzung der Vereinbarung zu berichten.

Die oben genannten Unterzeichnenden bzw. ihre Vertretungen bilden die Arbeitsgruppe „Meko 1“. Alle weiteren direkten Akteure bzw. Projektpartner der Kooperationsvereinbarung bilden die Arbeitsgruppe „Meko 2“. Dies sind aktuell das Institut für Qualitätsentwicklung Mecklenburg-Vorpommern (IQ MV), die Landesarbeitsgemeinschaft Medien Mecklenburg-Vorpommern (LAG Medien), der Landesjugendring Mecklenburg-Vorpommern (LJRMV), die Landeskoordinierungsstelle für Suchtthemen Mecklenburg-Vorpommern (LAKOST), das Landeskriminalamt Mecklenburg-Vorpommern (LKA M-V) und der Landesrat für Kriminalitätsvorbeugung (LfK), der Landesseniorenbeirat Mecklenburg-Vorpommern (LSB) sowie die Universität Greifswald (hier: Lehrstuhl für Praktische Theologie, Religionspädagogik, Medienpädagogik).

Neben den Arbeitsgruppen „AG Digitale Schule“ und „AG Frühkindliche Medienbildung“, wo der LfDI MV seine inhaltlichen Kompetenzen einbringt, gehörte 2018 auch die Stellungnahme zur Evaluation der Kooperationsvereinbarung zu unseren Aufgaben. Die Federführung liegt bei der Staatskanzlei Mecklenburg-Vorpommern, was der LfDI MV sehr begrüßt, so dass die Koordination und Zuarbeit aller Ressorts und Unterzeichner gewährleistet wird. Zusammenfassend wird im Bericht die vernetzende Arbeit[26] vor allem durch das Netzwerk „Medienaktiv M-V“ gestützt. Das Fazit des Berichtes ist, dass eine Fortschreibung begrüßt wird. Sie bietet die Möglichkeit, noch nicht abgeschlossene Projekte fortzuführen. Gleichzeitig

[26] vgl. Kooperationsvereinbarung zur Förderung der Medienkompetenz in M-V, Punkt IV, Nr. 1

können neue Ziele definiert werden, wie beispielsweise die Einführung verpflichtender Elemente der Medienbildung in den Fachdidaktiken im Lehramtsstudium und in allen weiteren pädagogischen Studiengängen der Universitäten des Landes.

Der LfDI MV hält das persönliche Engagement der Akteure und damit direkten Umsetzer der Kooperationsvereinbarung für die Grundlage der gelingenden Vermittlung von Medienbildung in Mecklenburg-Vorpommern. In unserer Stellungnahme heißt es weiter: Wir fordern eine stetige Auseinandersetzung mit der digitalen Kultur und sehen weite Ziele der Dritten Kooperationsvereinbarung als noch nicht erreicht. Vor allem die fehlende Planungsmöglichkeit unterstütze nicht das Ziel der Landesregierung, „ein flächendeckendes und generationenübergreifendes Angebot zum Erwerb von Medienkompetenz zu unterbreiten“[27] Der LfDI MV sieht hier einen erhöhten Handlungsbedarf. Auch die Stellungnahmen anderer Unterzeichner sehen noch Optimierungspotenzial auf vielen Ebenen. Gleichzeitig ist das Resümee der Dritten Vereinbarung, dass es Projekte und Maßnahmen gibt, die gut umgesetzt werden konnten. Oftmals wird dabei nicht „auf das vorhandene Fachwissen [Anm. der direkten Akteure und Umsetzer] im Land zurückgegriffen und genutzt“[28]. Diese aktiven Lösungen könnten die Vierte Vereinbarung mit greifbaren Umsetzungsstrategien füllen. Ein weiterer Diskussionspunkt bleibt die Schaffung einer ressortunabhängigen vernetzenden Stelle, die die Aktivitäten, Projekte und Umsetzungsschritte koordiniert.

Die Inhalte der neuen Kooperationsvereinbarung werden im Jahr 2019 erarbeitet. Die ressortübergreifende und vernetzende Arbeit mit „Medienaktiv M-V“ bleibt eine bestehende Aufgabe. In der Vierten Kooperationsvereinbarung sollten jedoch neue und weiterführende klare Aufgaben enthalten sein, die auch personell und finanziell bedacht werden müssen. Gleichzeitig haben wir den Wunsch geäußert, dass es weitere Unterzeichner geben sollte. Durch den Wechsel der Zuständigkeit für das Thema „Gesundheit“ sehen wir das Ministerium für Wirtschaft, Arbeit und Gesundheit Mecklenburg-Vorpommern als einen neuen Unterzeichner. Ebenfalls wünschenswert ist, als neuen Unterzeichner das Ministerium für Energie, Infrastruktur und Digitalisierung Mecklenburg-Vorpommern mit aufzunehmen. Der LfDI MV ist der Meinung, dass es auch weitere Themen wie den Verbraucherschutz zu betrachten gilt. Insgesamt spiegelt sich hier die vernetzende Arbeitsweise unserer Behörde wider.

6.1.4 Freiwilliges Soziales Jahr „Demokratie/Politik“ beim Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern – ein Erfahrungsbericht

Mein Tätigkeitsfeld beim Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern umfasst den Bereich „Datenschutz als Bildungsaufgabe“. Das bedeutet, dass ich das Projekt „MedienscoutsMV“, die Netzwerkarbeit von „Medienaktiv M-V“ und die Zusammenarbeit mit Landtag, Ausschüssen und Ministerien begleite.

Als FSJlerin habe ich in den ersten vier Monaten das „MedienscoutsMV“-Wochenende im November 2018 intensiv mit vorbereitet und durchgeführt. Die dazugehörige Webseite wurde von mir stets im Angebot „News“ aktualisiert und einige Inhalte wurden neu formuliert. Mein Beitrag beinhaltet hier vor allem die Beantwortung von E-Mails, das Durchführen von Telefonaten, die Recherche zu relevanten Themen und die Erarbeitung von Briefen. Auch die Begleitung zu externen Veranstaltungen wie Planungstreffen, Anhörungen im Landtag und Referate/Projektarbeit in Schulen, bei denen ich auch inhaltliche Aspekte hinzufügte, zählten bisher schon zu meinem Aufgabenbereich. Die Mitgestaltung der letzten Gruppen-Englischstunde in der Behörde, Protokollführung bei einer thematischen Mitarbeiterversamm-

[27] vgl. Kooperationsvereinbarung zur Förderung der Medienkompetenz in M-V, Präambel
[28] vgl. Kooperationsvereinbarung zur Förderung der Medienkompetenz in M-V, Punkt III

lung, die Anfertigung von (Veranstaltungs-)Mappen und thematischen FAQ`s für Kolleginnen und Kollegen machen ebenso eine Vielzahl meiner Aufgaben aus. Auch die inhaltliche Vorbereitung für die Verfilmung von „Datenschutz im Kindergarten“ zählt dazu.

Darüber hinaus führte ich mehrere Umfragen bei den Datenschutzbehörden bundesweit durch.

Im landesweiten Netzwerk der Medienbildung „Medienaktiv M-V“ werden thematische Veranstaltungen und medienpolitische Themen umgesetzt. Meine Aufgabe besteht darin, die intensive Arbeit des Landesdatenschutzbeauftragten im Netzwerk zu unterstützen.

Im Rahmen einer „Task Force“-Sitzung steuerte ich den inhaltlichen Einstieg mittels zweier Vorträge bei. Die Jugendwebsite „YoungData.de“ und die klick-safe Broschüre „Ich bin öffentlich ganz privat“ überprüfte ich auf Aktualität und entwarf neue Inhalte. Ebenso unterstütze ich inhaltlich die AG zum Thema „Medienbildung im Bereich der frühkindlichen Bildung“, Inhalte eines Praxiskapitels, und die Anhörung „Jung sein in MV – Medienbildung im Kontext der Digitalisierung in MV“ im Sozialausschuss mit Ideen.

Für die Frühjahrstagung des Netzwerkes „Medienaktiv M-V“ ist wieder ein medienpolitisches Thema gewählt worden. Damit will das Netzwerk die „Kooperationsvereinbarung zur Förderung der Medienkompetenz in Mecklenburg-Vorpommern“ aktiv in der Evaluation und Neuschreibung begleiten. Der aktive Austausch mit Unterzeichnern, Ministerien und dem Landtag MV steht dabei im Vordergrund.

Die Kinder- und Jugendarbeit in Bezug auf Medien bereitet mir sehr viel Freude, ebenso wie das Erlernen von Verwaltungsgrundlagen, wie zum Beispiel der Umgang mit Fragen und Einwänden von den Behörden Mecklenburg-Vorpommerns. Die bisherige Arbeit und das erlernte Wissen möchte ich in meine zukünftigen Tätigkeiten mit einfließen lassen.

6.2 Umsetzung der DS-GVO in der Arztpraxis

Überfüllte Wartezimmer, Bürokratie ohne Ende und dann auch noch das: die Europäische Datenschutz-Grundverordnung (DS-GVO). Nicht zuletzt, weil Anfang 2018 einige geschäftstüchtige externe Datenschutzbeauftragte und Anwälte Ärztinnen und Ärzte mit der Androhung von Bußgeldern in Millionenhöhe in Angst und Schrecken versetzt hatten.

Schulungen des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (LfDI MV) sollten über die Anforderungen der DS-GVO informieren und Hinweise zur Umsetzung geben. Ergänzt wurden diese Maßnahmen durch die „Notfallsprechstunde DS-GVO für Gesundheitsberufe“, immer montags von 17:00 – 19:00 Uhr, die auch 2019 fortgesetzt wird.

Bei der Organisation der Schulungen gab es eine sehr gute Zusammenarbeit mit der Ärztekammer Mecklenburg-Vorpommern (ÄK MV) und mit der Kassenärztlichen Vereinigung Mecklenburg-Vorpommern (KV MV). Als hilfreich erwiesen sich auch Beiträge im Ärzteblatt Mecklenburg-Vorpommern. Die Ärztekammer hatte damit ermöglicht, unkompliziert Beiträge unmittelbar an Ärztinnen und Ärzte im Land zu richten und einfache Tipps zur Umsetzung der DS-GVO in der Arztpraxis zu geben.

6.3 Projekt „Umgang mit Patientendaten in den Krankenhäusern Mecklenburg-Vorpommerns (UPDK)“

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (LfDI MV) hat als Aufsichtsbehörde für den Datenschutz gemäß Art. 57 Abs. 1 Europäische Datenschutz-Grundverordnung (DS-GVO) unter anderem maßgebliche Entwicklungen zu verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere

die Entwicklung der Informations- und Kommunikationstechnologien sowie deren Anwendung.

Mit der am 25. Mai 2018 in Kraft getretenen DS-GVO und hieraus entstandenen Unsicherheiten bei der Anwendung der neuen Rechtsnormen intensivierte der LfDI MV seine Informations- und Beratungsangebote für die Krankenhäuser und universitätsmedizinischen Einrichtungen in Mecklenburg-Vorpommern und initiierte für diesen Bereich auch verschiedene Projekte, um den Stand der Umsetzung nach den Vorgaben der DS-GVO insbesondere beim Umgang mit Patientendaten festzustellen und zu erfahren, wo besonderer Handlungsbedarf im Hinblick auf Information und Beratung in diesem Bereich besteht.

Von Januar 2018 bis Dezember 2019 führt der LfDI MV ein Projekt „Umgang mit Patientendaten in den Krankenhäusern Mecklenburg-Vorpommerns (UPDK)“ durch. Ziele des Projektes sind das Erfassen des IST-Zustandes in Bezug auf datenschutzrechtliche Fragestellungen, das Erfassen von Schwierigkeiten bei der Umsetzung der DS-GVO und das Feststellen von erforderlichen datenschutzrechtlichen Handlungsbedarfen.

Das Projekt wird 2019 fortgeführt. Die Ergebnisse werden in einem Projekt-Bericht dokumentiert. Weitere Informationen sind zu finden unter:

https://www.datenschutz-mv.de/datenschutz/Projekte/UPDK/.

7 Technik und Organisation

7.1 Neue Technologien

7.1.1 Einsatz von funkbasierten digitalen Messzählern

Regelmäßig erreichen uns Petitionen zum Austausch von alten analogen Wasser- und Wärmezählern durch neue digitale Zähler, die ihre Werte drahtlos per Funk übertragen.

Bereits in der Vergangenheit haben wir diese Technologie untersucht, da mit ihrer sekundengenauen Erfassung von Verbrauchswerten eine Profilbildung über das Verhalten der Verbraucherinnen und Verbraucher möglich wird, siehe dazu auch Zwölfter Tätigkeitsbericht, Punkt 4.1.7. Denn die Zählerdaten geben nicht nur Aufschluss über den gesamten Verbrauch, sondern lassen auch Rückschlüsse auf Anwesenheits- und Abwesenheitszeiten sowie auf das Nutzungsverhalten der Verbraucherinnen und Verbraucher zu.

Beim Einsatz solcher Funkzähler sind daher angemessene technische und organisatorische Maßnahmen zum Schutz der zu verarbeitenden Verbrauchsdaten zu treffen. Hierzu zählt insbesondere, dass dem im Datenschutz verankerten Gebot der Datenminimierung Rechnung getragen wird, indem schon im Vorfeld die Übertragung der Verbrauchsdaten auf das tatsächlich erforderliche beschränkt wird. So ist ein monatlich konsolidierter Verbrauchswert ausreichend und eine Profilbildung ist unter diesen Umständen nicht mehr möglich. Weiterhin muss sichergestellt werden, dass nur berechtigte Personen auf die Verbrauchsdaten zugreifen können, entsprechend sind die Daten bei ihrer Übertragung nach dem Stand der Technik zu verschlüsseln.

Nicht zu vergessen bleibt aber auch die notwendige Transparenz den Verbraucherinnen und Verbrauchern gegenüber. So müssen diese hinreichend über die Verarbeitung ihrer Verbrauchsdaten sowie über ihre Auskunfts- oder Berichtigungsansprüche aufgeklärt werden.

7.1.2 Positionspapier „Biometrische Analyse“

Das Thema „Biometrische Gesichtserkennung für Werbezwecke“, siehe auch Zwölfter Tätigkeitsbericht, Punkt 5.9.2., beschäftigt die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder auch weiterhin.

Auf ihrer 2. Sonderkonferenz am 21. Juni 2017 hatte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) den Arbeitskreis „Technische und organisatorische Datenschutzfragen“ (AK Technik, siehe Punkt 5.3) und die Arbeitsgruppe „Videoüberwachung“ des Arbeitskreises „Wirtschaft“ damit beauftragt, sich mit dem Thema „Verarbeitung von Daten durch Sensorik und Videotechnik und deren datenschutzrechtliche Einordnung“ zu befassen. Zu diesem Zweck wurde unter unserer Leitung die Unterarbeitsgruppe (UAG) „Biometrische Analyse“ eingesetzt.

In ihren ersten Sitzungen ließ sich die UAG mehrere Gesichtserkennungssysteme vorstellen. Zudem bat die UAG Professor Dr. Christoph Busch, Hochschule Darmstadt, Norwegian University of Science and Technology, Technical University of Denmark, um eine Bewertung der Verarbeitung biometrischer Daten im Lichte der Europäischen Datenschutz-Grundverordnung (DS-GVO). Die UAG beschloss, nicht einzelne Produkte oder Verfahren zu bewerten, sondern eine Orientierungshilfe mit Bewertungskriterien zu erarbeiten, mit deren Hilfe dann einzelne Verfahren bewertet bzw. Empfehlungen zur datenschutzgerechten Ausgestaltung gegeben werden können. Da die bearbeiteten Fragestellungen sich als komplex und zudem teilweise als umstritten herausstellten, erstreckte sich die Arbeit an diesem Papier über acht Sitzungen, so dass die UAG nunmehr zu insgesamt neun Sitzungen zusammengekommen ist.

Biometrische Daten definiert Art. 4 Nr. 14 DS-GVO als „mit speziellen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten“. Lichtbilder werden nach Erwägungsgrund 51 nur dann von der Definition des Begriffs „biometrische Daten“ erfasst, wenn sie mit speziellen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen.

In diesem Zusammenhang stellt sich die Frage, ob ein in einer Videoaufnahme enthaltenes Gesichtsbild als ein biometrisches Datum im Sinne des Art. 4 Nr. 14 DS-GVO einzustufen ist. Dafür spricht zunächst der Wortlaut des Art. 4 Nr. 14 DS-GVO, der „Gesichtsbilder“ als ein Beispiel für biometrische Daten aufführt. Unterstützt wird diese Auffassung auch durch die Ausführungen von Professor Dr. Busch, nach denen Aufnahmen handelsüblicher Videokameras zur biometrischen Identifizierung von Personen geeignet sind. Dagegen spricht der Umstand, dass biometrische Daten nach Art. 4 Nr. 14 DS-GVO „mit speziellen Verfahren gewonnen“ werden müssen. Besonders schutzbedürftig wären danach nicht schon biometrische Samples, also die analogen oder digitalen Repräsentationen biometrischer Charakteristika, sondern erst die biometrischen Merkmale, also Zahlen oder markante Kennzeichen, die aus einem biometrischen Sample extrahiert wurden und zum Vergleich verwendet werden können.

Allerdings sind bereits in dem biometrischen Sample alle für den Vergleich erforderlichen Informationen vorhanden. Bei einer entsprechenden Qualität dürfte daher schon das in einer Videoaufnahme enthaltene Gesichtsbild als ein biometrisches Datum im Sinne des Art. 4 Nr. 14 DS-GVO einzustufen sein. Das würde bedeuten, dass bei einer einfachen Videoüberwachung mit Hilfe handelsüblicher Videokameras biometrische Daten verarbeitet werden. Um eine Verarbeitung zum Zwecke der eindeutigen Identifizierung einer natürlichen Person im Sinne des Art. 9 Abs. 1 DS-GVO würde es sich dabei jedoch nur dann handeln, wenn die-

se Daten für eine biometrische Identifizierung eingesetzt werden. Damit wäre der Betrieb einer einfachen Videoüberwachungsanlage ohne Gesichtserkennungsfunktion nach Art. 6 und nicht nach Art. 9 DS-GVO zu beurteilen. Abschließend geklärt sein werden diese Fragen jedoch erst nach Verabschiedung der Orientierungshilfe durch die Datenschutzkonferenz.

7.1.3 Zugang zu Online-Verwaltungsleistungen in Mecklenburg-Vorpommern

Mit dem Onlinezugangsgesetz (OZG) hat der Bundesgesetzgeber die Weichen in Richtung einer datenschutzgerechten Digitalisierung und Präsentation von Verwaltungsleistungen in Landesportalen gestellt, siehe auch Dreizehnter Tätigkeitsbericht, Punkt 7.2. Im Berichtszeitraum haben wir das Projekt in unserem Land hierzu begleitet. In diesem Projekt wirken das Ministerium für Energie, Infrastruktur und Digitalisierung Mecklenburg-Vorpommern als das für landesweite IT-Projekte zuständige Ressort, die landeseigene DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH (DVZ) als Auftragnehmer, der Zweckverband Elektronische Verwaltung in Mecklenburg-Vorpommern (eGo-MV) sowie Landesbehörden und Stadt- und Gemeindeverwaltungen zusammen.

Zentraler Punkt der Beratungen mit dem Ministerium war die Frage nach einer tragfähigen Rechtsgrundlage und Verfahrensgestaltung. Das OZG fordert von Bund und allen Ländern, Stellen zu bestimmen, die die Einrichtung der Nutzerkonten anbieten und die die Registrierung der Nutzerkonten vornehmen, § 7 OZG, siehe dazu auch Punkt 5.5.2. Hierzu ist unserer Meinung nach eine Regelung per Landesgesetz erforderlich, die noch nicht existiert. Ohne eine solche Regelung darf das Ministerium das Portal weder betreiben noch vom DVZ betreiben lassen. In dem Portal sollen Daten aus Anträgen an verschiedene Verwaltungen, Bescheiddaten und anderen personenbezogenen Daten verarbeitet werden. Dies ist mit der Möglichkeit der Kenntnisnahme personenbezogener Daten durch das Ministerium und durch den Auftragsverarbeiter verbunden und bedarf daher einer Rechtsgrundlage, die den Anforderungen von Art. 6 Abs. 1 lit. e i. V. m. Abs. 3 Europäische Datenschutz-Grundverordnung (DS-GVO) genügen muss.

Sobald die Rechtsgrundlage vorliegt, müssen die am Verfahren beteiligten Stellen eine Vereinbarung nach Art. 26 DS-GVO – Gemeinsam für die Verarbeitung Verantwortliche – schließen. Weil sie das Verfahren gemeinsam gestalten und dessen Zwecke bzw. Mittel festlegen, werden sie kraft Gesetzes gemeinsam Verantwortliche und müssen die Vorschriften des Art. 26 DS-GVO einhalten. Zu beachten ist, dass Art. 26 DS-GVO nicht zur Verarbeitung personenbezogener Daten berechtigt, siehe auch Punkt 9.1.3. Das DVZ ist Auftragsverarbeiter im Sinne von Art. 28 DS-GVO und wird aufgrund eines Vertrages tätig. Es ist kein Partner dieser Vereinbarung nach Art. 26 DS-GVO.

Daneben haben wir Hinweise zu einer datensparsamen und transparenten Gestaltung von Verarbeitungen gegeben. So muss die Information über Verwaltungsleistungen und die dazu nötigen Anträge ohne Anmeldung oder anderweitige Identifikation möglich sein. Die dauerhafte Speicherung von Anträgen oder Nachrichten der Verwaltung muss ins Belieben der Nutzerinnen und Nutzer gestellt werden. Auch Zwischeninformationen, Bescheide oder andere Dokumente dürfen nur dann über das Portal zur Verfügung gestellt werden, wenn die Betroffenen dies wünschen. Ferner haben wir Anregungen gegeben, wie Informationen nach Art. 13 DS-GVO zu geben sind. Werden personenbezogene Daten bei Betroffenen erhoben, so sind nach dieser Vorschrift die Betroffenen über ihre Rechte sowie über die Zwecke der Verarbeitung und die für die Verarbeitung Verantwortlichen zu informieren.

Unsere Beratung war zum Ende des Berichtszeitraumes noch nicht abgeschlossen. Auch die Frage nach der Rechtsgrundlage für das Verfahren war noch nicht befriedigend geklärt.

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.

7.1.4 Entwicklungen bei Microsoft und der Deutschland-Cloud

Mit Fragen der Datenschutzkonformität der Deutschland-Cloud der Firma Microsoft und dem dazugehörigen Treuhändermodell haben sich die deutschen Datenschutzaufsichtsbehörden schon im letzten Berichtszeitraum intensiv befasst, siehe Dreizehnter Tätigkeitsbericht, Punkte 8.1 und 8.2. Um diese Cloud-Strukturen datenschutzrechtlich bewerten zu können, haben die Aufsichtsbehörden umfassende Kataloge mit juristischen und technischen Fragen zum Betrieb der Deutschland-Cloud erstellt und Microsoft zur Beantwortung vorgelegt.

Auf Antworten mussten die Aufsichtsbehörden teilweise monatelang warten, da offenbar eine aufwendige microsoftinterne Abstimmung mit dem Hauptsitz in Redmond (USA) erforderlich war. Bevor die Aufsichtsbehörden die Antworten von Microsoft ausgewertet hatten, gab Microsoft bekannt, dass der Betrieb der Deutschland-Cloud eingestellt werden soll. Seit dem 1. September 2018 bietet Microsoft keine Neuverträge für die Deutschland-Cloud mehr an. Microsoft hat angekündigt, stattdessen eigene Rechenzentren in Deutschland zu bauen, aus denen Cloud-Dienste für deutsche Kundinnen und Kunden angeboten werden sollen. Damit stehen die Aufsichtsbehörden vor grundlegend geänderten Voraussetzungen zur datenschutzrechtlichen Bewertung von Cloud-Angeboten der Firma Microsoft. Das betrifft sowohl rechtliche als auch technische Fragestellungen. Um technische Aspekte bewerten zu können, müssen jedoch zunächst die rechtlichen Rahmenbedingungen geklärt und ausgewertet werden. Diese Aufgabe hat der Arbeitskreis Verwaltungsmodernisierung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) übernommen. Dort wurde die strategische Entscheidung getroffen, zunächst die juristischen Aspekte der Auftragsverarbeitung zu bewerten. Zu diesem Zweck untersucht der Arbeitskreis zunächst alle von Microsoft zur Verfügung gestellten Verträge und befragt Microsoft bei Unklarheiten. Erste Antworten von Microsoft sind bereits eingegangen und werden durch den Arbeitskreis Verwaltungsmodernisierung ausgewertet.

Angesichts der rechtlichen und technischen Komplexität der Cloud-Angebote der Firma Microsoft ist nicht damit zu rechnen, dass eine abschließende datenschutzrechtliche Bewertung kurzfristig vorliegen wird.

7.1.5 Das Standard-Datenschutzmodell (SDM)

Über das Standard-Datenschutzmodell (SDM) als Methode zur Datenschutzberatung und -prüfung auf der Basis der Gewährleistungsziele Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Transparenz und Intervenierbarkeit haben wir bereits mehrfach berichtet. Im Dreizehnten Tätigkeitsbericht, Punkt 5.1.1, konnten wir über die Verabschiedung der Version 1.0 des SDM durch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) im November 2016 informieren.

Schon zu diesem Zeitpunkt war klar, dass weitere Anpassungen des SDM an die Europäische Datenschutz-Grundverordnung (DS-GVO) erforderlich sein werden. Einen wichtigen Meilenstein konnten die Autoren des SDM mit der Verabschiedung der Version 1.1 durch die Datenschutzkonferenz im April 2018 verzeichnen. Diese Version enthält nun keine Bezüge mehr zum „alten“ Datenschutzrecht, sondern stützt sich nun ausschließlich auf die DS-GVO. So wurde der ehemalige Abschnitt Schutzbedarf grundlegend überarbeitet. Im überarbeiteten neuen Abschnitt wurde der zentrale Begriff des Risikos der DS-GVO eingeführt und ein ers-

ter Versuch unternommen, die Begriffe Schutzbedarf und Risiko in ein praktikables Verhältnis zu setzen. Dies ist deshalb besonders wichtig, weil eine Verbindung zwischen der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlenen Grundschutz-Methodik[29] und der dort geforderten Schutzbedarfsfeststellung einerseits und der in der DS-GVO verankerten Risikoanalyse andererseits hergestellt werden muss. Denn die „Leitlinie zur Gewährleistung der Informationssicherheit in der Landesverwaltung von Mecklenburg-Vorpommern“ (IS-Leitlinie M-V [30]) schreibt als Mindestsicherheitsniveau den BSI-Grundschutz und somit eine Schutzbedarfsfeststellung vor, die DS-GVO hingegen verlangt eine Risikoabschätzung, beispielsweise im Zusammenhang mit der Datenschutzfolgenabschätzung (DSFA) nach Art. 35 DS-GVO.

Die Weiterentwicklung des SDM hat sich in der Praxis bereits bewährt. So wurde die für den Einsatz von Bodycams bei der Polizei erforderliche DSFA mit Hilfe der Systematik des SDM durchgeführt, siehe Punkt 9.1.2. Nicht zuletzt dadurch konnte die Polizei eine vollständige DSFA vorlegen, die alle Anforderungen der DS-GVO erfüllt und für sämtliche Verarbeitungsrisiken angemessene und erforderliche technische und organisatorische Maßnahmen auflistet.

Trotz aller Erfolge sind weitere Überarbeitungen und Anpassungen des SDM an die DS-GVO erforderlich. Dabei wird die Erarbeitung des Referenz-Maßnahmenkatalogs sicher noch eine längere Zeit in Anspruch nehmen. Dennoch empfehlen wir die Anwendung und Erprobung des SDM schon jetzt. Das Kapitel 7 des SDM enthält einen generischen Maßnahmenkatalog, der solange zur Auswahl von Einzelmaßnahmen genutzt werden kann, bis die Referenz-Maßnahmenkataloge vorliegen.

Um einen ersten Eindruck vom Inhalt und von der Struktur des Referenz-Maßnahmenkatalogs zu vermitteln, haben sich einige Aufsichtsbehörden zusammengeschlossen, um Vorentwürfe einzelner Bausteine des Katalogs zu erarbeiten und als Testversionen zu veröffentlichen. Ende August 2018 wurden auf diesem Wege die Bausteine „Aufbewahrung“, „Planung und Spezifikation“, „Dokumentation“, „Protokollierung“, „Trennung“, „Löschen und Vernichten“ und „Datenschutzmanagement“ veröffentlicht31. Wir weisen auch an dieser Stelle nochmals darauf hin, dass diese Bausteine noch nicht in der Datenschutzkonferenz abgestimmt worden sind. Wir empfehlen den Anwendern aber dennoch, diese Bausteine zu testen und uns ihre Erfahrungen bei der Erprobung der Bausteine mitzuteilen (z. B. unter sdm@datenschutz-mv.de) und somit zur Weiterentwicklung von Methode und Maßnahmen beizutragen.

Um auf dem aktuellen Stand zu SDM zu bleiben, empfehlen wir den Bezug des SDM-Newsletters32. Dieser Newsletter informiert SDM-Interessierte immer dann, wenn ein berichtenswertes Ereignis im Kontext des SDM anzukündigen ist oder stattgefunden hat.

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.

[29] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html
[30] http://www.cio.m-v.de/static/CIO/Dateien/ISMS/IS-Leitlinie.pdf
[31] https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/
[32] https://datenschutzzentrum.de/mailinglisten/#sdm

7.2 Kommunikation und neue Medien

7.2.1 Wenn E-Mails nicht verschlüsselt werden

Seit vielen Jahren weisen wir darauf hin, dass E-Mails mit schutzbedürftigen Inhalten verschlüsselt werden sollen, denn eine E-Mail ist in Bezug auf die Sicherheit mit einer Postkarte zu vergleichen: Was man einer Postkarte nicht anvertrauen würde, sollte man auch nicht per E-Mail versenden. Dennoch werden E-Mails auch mit sensiblen Daten noch sehr oft unverschlüsselt versendet.

Es ist keinesfalls immer kriminelle Energie erforderlich, um unberechtigt Zugang zu Inhalten unverschlüsselter E-Mails zu erhalten. Manchmal spielt der Zufall eine Rolle, um zu verdeutlichen, dass eine unverschlüsselte E-Mail erhebliche Risiken etwa für die Vertraulichkeit personenbezogener Daten in sich birgt.

Wir erhielten den Hinweis eines Bürgers, dass er eine offensichtlich nicht für ihn bestimmte E-Mail von einer öffentlichen Stelle des Landes erhalten habe. Die E-Mail hatte als Anlage eine Liste von Personen mit deren Namen, Anschriften, Personalausweisnummern, Kfz-Kennzeichen und Hinweise auf deren Sicherheitsüberprüfungen durch die Bundespolizei. Der richtige Adressat der E-Mail war bis auf die Schreibweise eines Umlautes namensgleich mit dem falschen Empfänger. Die Absenderin hatte versehentlich die Schreibweise des falschen Empfängers gewählt, so dass dieser die E-Mail erhielt. Dies zeigt, dass keinesfalls immer kriminelle Energie im Spiel ist, wenn der Inhalt vertraulicher E-Mails an falsche Adressaten gelangt. Ein einfacher Adressierungsfehler reicht mitunter aus.

Die Europäische Datenschutz-Grundverordnung (DS-GVO) fordert in Art. 32 technische und organisatorische Maßnahmen, um die Sicherheit der Verarbeitung personenbezogener Daten zu gewährleisten, und nennt ausdrücklich die Verschlüsselung. E-Mail-Versendern stehen verschiedene Möglichkeiten der Verschlüsselung zur Verfügung:

Als eine Möglichkeit kommt eine Inhalts- oder Ende-zu-Ende-Verschlüsselung in Frage, bei der der Absender verschlüsselt und nur der Empfänger entschlüsseln kann. Zwei Standards haben sich etabliert: S/MIME (Secure/Multipurpose Internet Mail Extensions, definiert in RFC 5751) und OpenPGP (Pretty Good Privacy, definiert in RFC 4880). Diese Standards sind seit vielen Jahren bekannt und werden von Fachleuten als Stand der Technik eingestuft[33]. Dennoch sind sie für den Versand von E-Mails noch wenig verbreitet. Beim Versand besonders schutzbedürftiger Daten oder bei regelmäßigen Übermittlungen von personenbezogenen Daten zwischen gleichbleibenden Kommunikationspartnern wäre eine solche Verschlüsselung aber verhältnismäßig und daher prinzipiell erforderlich.

Als zweite Möglichkeit kommt eine verschlüsselte Übertragung von E-Mails (Transportverschlüsselung) in Frage. Dabei werden jeweils die Transportwege der E-Mails verschlüsselt, also zwischen dem Absender und dessen Mail-Server, zwischen den weiteren an der Übertragung beteiligten Mail-Servern und zwischen dem Mail-Server des Empfängers und dem Empfänger selbst. Diese Art der Verschlüsselung bietet einen geringeren Vertraulichkeitsschutz als eine Inhaltsverschlüsselung, denn die Mails liegen auf den Mail-Servern unverschlüsselt vor. Als Standard hat sich hier TLS (Transport Layer Security) etabliert. Er sollte jedenfalls in der Version 1.2 (definiert in RFC 5246) eingesetzt werden, auch wenn inzwischen TLS 1.3 als offizieller Standard verabschiedet ist. Dessen Praxiseinsatz ist aber noch keine Realität. Auf technische Details soll hier nicht weiter eingegangen werden, umfassende Empfehlungen zu TLS liefert beispielsweise die Technische Richtlinie TR-02102-2, Teil 2 des BSI, siehe

[33] https://www.teletrust.de/publikationen/broschueren/stand-der-technik/

Punkt 7.2.2. Auch dieser Standard ist seit vielen Jahren bekannt und zählt zum Stand der Technik.

Im vorliegenden Fall verfügten weder Absender noch Empfänger über eine Infrastruktur zum verschlüsselten Versand von E-Mails. Um dennoch den Schutz von per E-Mail gesendeten Daten zu gewährleisten, hatte die Behördenleitung der öffentliche Stelle ihre Beschäftigten angewiesen, personenbezogene Daten vor dem E-Mail-Versand mit einer speziellen Software zu verschlüsseln und dann als Anlage zu versenden. Der Versand von symmetrisch verschlüsselten Anhängen (z. B. AES-verschlüsselte Zip-Archive oder AES-verschlüsselter Dokumente, wie sie von gängiger Büro-, Dateikonversions- und Archivsoftware erstellt werden können) steht dann der Ende-zu-Ende-Verschlüsselung gleich, wenn die zur Entschlüsselung benötigten Passwörter nur dem Absender und den befugten Empfängern bekannt sind und sicher (über einen anderen Kanal, beispielsweise per Brief, SMS, Messenger oder telefonisch) übergeben und verwahrt werden. Die entsprechende Dienstanweisung enthielt derartige Vorgaben für die bei diesem Verfahren erforderliche Übermittlung des Entschlüsselungspasswortes an den Empfänger. Die Absenderin hatte diese Anweisungen jedoch ignoriert und eine E-Mail mit unverschlüsseltem Anhang versendet.

Der Datenschutzverstoß war somit nicht der Behördenleitung zuzurechnen, sondern ausschließlich der Mitarbeiterin, die entgegen den Anweisungen sensible Inhalte unverschlüsselt übermittelt hatte. Die Behördenleitung hat den Vorfall zum Anlass genommen, den Beschäftigten spezifische Schulungen zum Datenschutz anzubieten.

Wir nehmen diesen Datenschutzverstoß erneut zum Anlass, Verantwortliche in Verwaltung und Wirtschaft aufzufordern, bei der elektronischen Übermittlung personenbezogener Daten Verschlüsselungsverfahren nach dem Stand der Technik einzusetzen. Nur so werden sie künftig in der Lage sein, die Grundsätze der Europäischen Datenschutz-Grundverordnung (DS-GVO) für die Verarbeitung personenbezogener Daten, Art. 5 DS-GVO, insbesondere im Hinblick auf Integrität und Vertraulichkeit zu gewährleisten.

7.2.2 Anforderungen an die Verschlüsselung von E-Mails

Im Berichtszeitraum haben wir vermehrt Anfragen dazu erhalten, wie E-Mails richtig zu verschlüsseln sind.

E-Mails werden zur Übertragung von personenbezogenen Daten verschiedener Sensibilität genutzt und zwar sowohl im Rahmen regelmäßiger als auch sporadischer Kontakte. Zum Ende des Berichtszeitraumes sind die deutschen Datenschutzaufsichtsbehörden dabei, eine abgestimmte Position zum Thema E-Mail-Verschlüsselung zu erarbeiten. Federführendes Gremium ist der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ (AK Technik), siehe Punkt 5.3. Wir vertreten in diesem Abstimmungsprozess und den anfragenden Personen und Stellen gegenüber folgende Position:

Für die Übermittlung personenbezogener Daten per E-Mail gelten die Anforderungen der Europäischen Datenschutz-Grundverordnung (DS-GVO), insbesondere die Pflicht zur Auswahl geeigneter technischer und organisatorischer Maßnahmen, Art. 24 Abs. 1 DS-GVO, und zur Gewährleistung der Sicherheit der Verarbeitung, Art. 32 DS-GVO. Die DS-GVO stellt dabei auf den Stand der Technik ab. Hierfür stehen mehrere Technologien zur Auswahl, die jeweils verschiedene Eigenschaften haben:

- Bei Ende-zu-Ende-Verschlüsselung verschlüsselt der Absender den Inhalt einer E-Mail und nur der beabsichtigte Empfänger kann ihn wieder entschlüsseln. Inhalte von E-Mails können so auf der gesamten Transportkette zwischen Absender und Empfän-

ger nicht von Unbefugten zur Kenntnis genommen werden. Beispiele sind die Standards OpenPGP und S/MIME (RFC4880 und RFC5751).

- Die Verbindungsverschlüsselung wirkt jeweils auf den Transportverbindungen zwischen den verschiedenen Servern, die die E-Mails auf ihrem Weg zwischen Absender und Empfänger entgegennehmen und weiter verteilen. Auf den Servern selbst liegen die E-Mails unverschlüsselt vor; ob sie von Unbefugten eingesehen werden können, hängt von den Schutzmaßnahmen ab, die die beteiligten Dienstleister ergreifen. Solche Verfahren basieren in der Regel auf TLS, siehe Punkt 7.2.5.

Zu beachten ist jedoch, dass die genannten Verfahren zur Ende-zu Ende-Verschlüsselung ausschließlich den Inhalt der E-Mails schützen, nicht aber die der Verbindungsdaten in den Kopfzeilen. Die Verbindungsverschlüsselung wirkt stattdessen auf die gesamte E-Mail einschließlich der Verbindungsdaten in den Kopfzeilen.

Stand der Technik ist nach unserer Auffassung die Ende-zu-Ende-Verschlüsselung. Grundsätzlich sollte daher bei der Übermittlung von E-Mails immer eine Ende-zu-Ende-Verschlüsselung angestrebt werden. Um auch einen Schutz der Verbindungsdaten zu gewährleisten, ist eine Kombination beider Ansätze empfehlenswert.

Die DS-GVO enthält in Art. 9 Abs. 1 einen Katalog von besonders sensiblen und damit besonders schutzbedürftigen Kategorien personenbezogener Daten. Dazu gehören Gesundheitsdaten, Art. 9 Abs. 1 i. V. m. Art. 4 Nr. 15. Wir gehen davon aus, dass wir und alle anderen Aufsichtsbehörden für die Übermittlung solcher besonders sensiblen Daten künftig die Ende-zu-Ende-Verschlüsselung einfordern werden, wobei sicher noch eine Übergangszeit eingeräumt werden muss.

Da es in der Praxis in absehbarer Zeit noch immer nicht durchgängig möglich sein wird, eine Ende-zu-Ende-Verschlüsselung durchzusetzen, wäre bei der Übermittlung von Daten, die nicht in den Katalog des Art. 9 DS-GVO fallen, auch eine Transportverschlüsselung hinnehmbar. Dabei sind aber in jedem Fall eine Verschlüsselung (mindestens) nach TLS 1.2 und eine Initiierung mit STARTTLS zu fordern. Es ist sicherzustellen, dass nicht nur die TLS-Verschlüsselung der E-Mail-Eingangsserver sicher konfiguriert ist, sondern dass auch Techniken zum Schutz vor Manipulationen des E-Mail-Versands, insbesondere DANE (DNS-Based Authentication of Named Entities, vgl. RFC 7672) unterstützt werden. Mit DANE können die E-Mail-Eingangsserver prüfen, ob eingehende verschlüsselte Verbindungen aus zuverlässigen Quellen stammen. Diese Anforderung muss entweder bei der Auswahl und Beauftragung des E-Mail-Providers oder aber bei der Konfiguration der eigenen Server berücksichtigt werden, siehe auch Dreizehnter Tätigkeitsbericht, Punkt 5.2.1.

Zu den Vorteilen von TLS 1.3, siehe Punkt 7.2.5, zur Konfiguration von TLS 1.2 haben wir uns im Zwölften Tätigkeitsbericht, Punkt 5.8.2, geäußert.

In der Praxis muss sichergestellt werden, dass die Transportverschlüsselung bei der Übertragung auch wirklich greift. Darüber hinaus müssen die beteiligten E-Mail-Anbieter dem Telekommunikationsgesetz (TKG) unterliegen und damit zu zusätzlichen technischen und organisatorischen Maßnahmen verpflichtet sein. Dazu gehören zum Beispiel die deutschen Provider Posteo, Web.de und GMX. Letzteres ist erforderlich, weil die E-Mails bei den Anbietern kurzzeitig unverschlüsselt vorliegen.

Verantwortliche, die in großem Stil personenbezogene Daten verschicken (beispielsweise zum Rechnungsversand), sollten Nutzenden die Möglichkeit der Ende-zu-Ende-Verschlüsselung nach den verbreiteten Standards OpenPGP oder S/MIME anbieten und dazu

einen entsprechenden öffentlichen Schlüssel bereithalten. Dann liegt es ausschließlich an deren Kommunikationspartnern, ob verschlüsselt kommuniziert wird oder nicht. Unsere Behörde bietet beispielsweise OpenPGP an (siehe Punkt 9 in unserer Datenschutzerklärung – https://www.datenschutz-mv.de/datenschutzerklaerung).

Alternativ zu den genannten Verfahren können andere verfügbaren Technologien berücksichtigt werden. So bieten auch verschlüsselte PDF- und ZIP-Dateien eine Ende-zu-Ende-Verschlüsselung, siehe Punkt 7.2.1. Die Sicherheit dieser Verfahren hängt von der Sicherheit der Passwörter ab, die hierzu eingesetzt werden. Deshalb muss so ein Passwort nicht nur hinreichend stark sein, sondern auch auf einem alternativen sicheren Weg übermittelt werden, beispielsweise per Brief, Instant Messenger mit ausreichender Verschlüsselung oder telefonisch, bei geringerem Schutzbedarf auch per SMS. Die ZIP-Archive und die PDF-Dateien müssen überdies mit hinreichend starken Verfahren verschlüsselt werden, wie AES-128 oder AES-256. Dies ist bei einigen alten Versionen der oben genannten Technologien nicht gegeben. Bei allen Verfahren, bei denen E-Mail-Anlagen verschlüsselt werden, fehlt zudem jegliche Integritätssicherung: Nur der Inhalt der Dateien selbst ist verschlüsselt und die einzelnen Dateien in verschlüsselten Anhängen können unbemerkt ausgetauscht werden.

7.2.3 Überarbeitung der Webseite des LfDI MV

Die Webseite des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (LfDI MV) ist ein wichtiges Informations- und Kontaktangebot für die öffentliche Verwaltung, für Unternehmen und nicht zuletzt auch für die Bürgerinnen und Bürger des Landes.

Um den Anforderungen durch sich verändernde Rahmenbedingungen gerecht zu werden, etwa die Darstellung auf kleineren Displaygrößen durch mobile Endgeräte wie Tablets oder Smartphones, haben wir bereits im Jahr 2017 eine notwendige technische Umstellung vorgenommen, siehe dazu Dreizehnter Tätigkeitsbericht, Punkt 3.1.1.

Mit Blick auf die Anwendbarkeit der Europäischen Datenschutz-Grundverordnung (DS-GVO) ab dem 25. Mai 2018 sind jedoch auch inhaltlich neue Anforderungen sowohl für die Verwaltung und die Unternehmen als auch für uns als Behörde hinzugekommen, von denen wir einige auf der Webseite abgebildet haben. Hierzu zählen Mitteilungs- und Meldepflichten, die sich für die öffentliche Verwaltung und für Unternehmen durch die DS-GVO ergeben, wie die Mitteilung von Datenschutzbeauftragten gemäß Art. 37 Abs. 7 DS-GVO oder die Meldung einer Datenpanne durch das verantwortliche Unternehmen gemäß Art. 33 Abs. 1 DS-GVO. Darüber hinaus können sich aber jederzeit auch die Bürgerinnen und Bürger des Landes an uns wenden und mögliche Datenschutzverstöße melden.

Wichtig ist in allen Fällen die Gewährleistung einer sicheren Übertragung der personenbezogenen Daten Betroffener und im Fall einer Beschwerde auch die Möglichkeit einer anonymen Mitteilung. Da sich eine verschlüsselte Ende-zu-Ende-Kommunikation leider noch immer nicht flächendeckend durchgesetzt hat, siehe dazu Punkte 7.2.1 und 7.2.2, haben wir als Alternative hierzu einige Kontaktformulare[34] auf der Webseite bereitgestellt, welche die Inhalte an uns verschlüsselt übermitteln und im Falle einer Beschwerde auch eine anonyme Meldung ermöglichen.

[34] https://www.datenschutz-mv.de/datenschutz/DS-GVO/Formulare/

7.2.4 Datenschutz auf Webseiten

Uns erreichen vermehrt Petitionen mit Fragen rund um die Datenschutzerklärungen auf Webseiten. Wir möchten dies zum Anlass nehmen, um auf die aktuelle Rechtssituation einzugehen.

Die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und somit auch den Datenschutz auf Webseiten soll künftig die ePrivacy-Verordnung regeln. Sie wird in Teilen der Europäischen Datenschutz-Grundverordnung (DS-GVO) und dem Telemediengesetz (TMG) vorgehen. Das Gesetzgebungsverfahren zur ePrivacy-Verordnung hat sich jedoch erheblich verzögert. Um Verantwortlichen bis zum Inkrafttreten der Verordnung die Anwendung des TMG zu erleichtern, hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) am 26. April 2018 eine Positionsbestimmung zur Anwendbarkeit des TMG für nichtöffentliche Stellen ab dem 25. Mai 2018 veröffentlicht[35].

In der Positionsbestimmung wird dargestellt, dass Teile des Abschnitts 4 des TMG im Lichte der geltenden DS-GVO nicht mehr anwendbar sind. Dies betrifft zum einen die Rechtsgrundlagen zur Datenverarbeitung bei der Bereitstellung von Telemedien (u. a. Webseiten). Sie werden zurzeit durch entsprechende Regelungen der DS-GVO ersetzt. Insbesondere ist hier Art. 6 Abs. 1 f DS-GVO zu nennen. Dort ist geregelt, dass die Verarbeitung personenbezogener Daten zulässig sein kann, wenn sie zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist. Diese Vorschrift kann als Rechtsgrundlage zur Datenverarbeitung bei der Bereitstellung von Webseiten herangezogen werden. Wichtig ist in diesem Zusammenhang der Hinweis, dass die Verarbeitungen zur Bereitstellung von Webseiten erforderlich sein müssen, um die angefragten Dienste zur Verfügung zu stellen. Hierbei kommt es besonders auf die vernünftigen Erwartungen der Betroffenen zur Verarbeitung ihrer personenbezogen Daten an.

Mit der DS-GVO haben sich auch die Informationspflichten für Webseitenbetreiber in den Datenschutzerklärungen geändert. Diese ergeben sich nunmehr aus Art. 13 DS-GVO. Für Webseitenbetreiber stellt dies nach unserer Auffassung eine Vereinfachung dar. So ist in Art. 13 klar normiert, welche Informationen den Betroffenen bereitgestellt werden müssen.

Auch zum Ende des Berichtszeitraumes war nicht absehbar, wann das Gesetzgebungsverfahren zur ePrivacy-Verordnung abgeschlossen sein wird.

7.2.5 Der Verschlüsselungsstandard TLS 1.3

Viele Internet-Dienste nutzen den Verschlüsselungsstandard Transport Layer Security (TLS). Dieser Standard beschreibt ein Protokoll zur Verbindungsverschlüsselung, die mittlerweile bei Web-Services nahezu allgegenwärtig genutzt wird. Andere Anwendungen wie die Transportsicherung von E-Mails, siehe Punkt 7.2.2, oder die Verschlüsselung von Internet-Telefonie sind vielleicht weniger bekannt, aber genauso wichtig. Im Berichtszeitraum ist die neue Version 1.3 dieses Standards erschienen. Die Neufassung ist, wie für Internet-Standards üblich, als Request for Comment (RFC) 8446 erschienen und frei verfügbar[36]. Sie enthält zahlreiche Verbesserungen gegenüber der Vorgängerversion 1.2 aus dem Jahre 2008.

- TLS 1.3 hat stets die Eigenschaft „Perfect Forward Secrecy“ (PFS, siehe auch Zwölfter Tätigkeitsbericht, Punkt 5.8.2). Sollten also die privaten Schlüssel des Servers in

[35] https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/95-Position-TMG.pdf
[36] https://www.rfc-editor.org/rfc/rfc8446.txt

falsche Hände fallen, dann können früher mitgeschnittene Verbindungen nicht entschlüsselt werden.

- Die verwendeten kryptographischen Verfahren sind umfassend modernisiert worden. So ist RSA nicht mehr zum Schlüsselaustausch zugelassen, weil es PFS nicht unterstützt. Stattdessen gibt es modernere, sichere und effiziente Verfahren zum Schlüsselaustausch wie ECDHE. Andere Verfahren wie die Hash-Verfahren MD5a und SHA-1 und die Stromchiffre RC4 sind längst gebrochen und deshalb in TLS 1.3 gestrichen worden.

- Kryptographische Algorithmen müssen auch in sicherer Weise verwendet werden. Da es in der Vergangenheit mehrfach Sicherheitsprobleme mit dem Betriebsmodus Cipher Block Chaining (CBC) gab, darf er in TLS 1.3 nicht mehr verwendet werden. Stattdessen stehen sichere Verfahren mit den Bezeichnungen GCM und CCM zur Verfügung. Als angreifbar hat sich auch der bislang verwendete Ansatz erwiesen, die zum Integritätsschutz verwendeten Daten an den Klartext anzuhängen und erst das Ergebnis zu verschlüsseln. Auch dies wurde in TLS 1.3 korrigiert.

Das Europäische Institut für Telekommunikationsnormen (European Telecommunications Standards Institute, ETSI), ein europäisches Standardisierungsgremium, hat mit eTLS 1.3 eine abgeschwächte Version von TLS 1.3 entwickelt. Dieser unterläuft gezielt die Eigenschaft PFS und gestattet das nachträgliche Entschlüsseln der Datenverbindungen, indem er zum Schlüsselaustausch genutztes Schlüsselmaterial nicht nur länger als zum Verbindungsaufbau erforderlich verwendet, sondern auch dessen dauerhafte Speicherung unterstützt. Deshalb ist der Einsatz von eTLS 1.3 aus Datenschutzsicht abzulehnen.

Software, die TLS 1.3 unterstützt, durchdringt den Markt immer mehr. Da TLS vor Version 1.2 einige protokollimmanente Schwächen aufweist, sollten ältere Versionen als 1.2 ohnehin nicht mehr verwendet werden, siehe auch Zwölfter Tätigkeitsbericht, Punkt 5.8.2.

Angesichts der vielen Vorteile von TLS 1.3 gegenüber den älteren Protokollfassungen empfehlen wir Betreibern von Internetdiensten, möglichst bald das neue Protokoll zu unterstützen.

7.3 Videoüberwachung

7.3.1 Einsatz von Videokameras und Webcams

Auf weiterhin sehr hohem Niveau liegt die Anzahl der Petitionen zum Einsatz von Videokameras. An den rechtlichen Voraussetzungen für den Einsatz von Videokameras hat sich mit der Europäischen Datenschutz-Grundverordnung (DS-GVO) grundsätzlich nichts geändert.

Maßgebliche Zulässigkeitsnorm ist Art. 6 Abs. 1 lit. f DS-GVO, der die Videoüberwachung mit regelt. Hiernach ist die Videoüberwachung nur zulässig, wenn die Verarbeitung von personenbezogenen Daten zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, nicht überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Ein berechtigtes Interesse kann grundsätzlich angenommen werden, wenn der Zweck im Schutz vor Einbrüchen, Vandalismus oder Diebstählen besteht, sofern eine tatsächliche Gefahrenlage nachgewiesen wurde.

Voraussetzung ist, dass die Videoüberwachung tatsächlich für die Erreichung des festgelegten Zwecks geeignet und auch erforderlich ist. Die Erforderlichkeit ist nur dann gegeben, wenn

der Zweck nicht genauso mit einem „milderen“ (also in die Rechte des Betroffenen weniger einschneidenden) Mittel erreicht werden kann. Nicht selten ist es für den Zweck ausreichend, die Überwachung auf Zeiträume außerhalb der Geschäftszeiten oder auf die Nachtstunden zu begrenzen. Alternativen können auch im zusätzlichen Einbau von Sicherheitsschlössern, dem Einsatz von Überwachungspersonal oder einer Umzäunung bestehen, sofern diese Mittel wirtschaftlich und organisatorisch zumutbar sind.

Auch wenn nach diesen Maßstäben eine Erforderlichkeit gegeben ist, ist die Videoüberwachung nur dann zulässig, wenn zusätzlich in einer Abwägung zwischen den berechtigten Interessen des Verantwortlichen und den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Person letztere nicht überwiegen. Grundsätzlich unzulässig sind Überwachungsmaßnahmen, die die Intimsphäre verletzen, beispielsweise im Fall von Saunen, Toiletten oder Duschkabinen. Schutzwürdige Interessen überwiegen zudem häufig dort, wo Menschen kommunizieren, essen und trinken oder sich erholen, beispielsweise in den Sitzbereichen von Restaurants, Parks etc.

Grundsätzlich muss eine Information zur Videoüberwachung im Rahmen des Art. 13 DS-GVO erfolgen. Nach Art. 17 Abs. 1 lit. a DS-GVO sind die Daten unverzüglich zu löschen, sofern sie für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind. Bei Aufzeichnungen zu Beweiszwecken ist das in der Regel nach 48 Stunden der Fall (in begründeten Einzelfällen, z. B. an Wochenenden, nach 72 Stunden).

Beim Einsatz von Webcams, die Live-Aufnahmen ins Internet übertragen und dadurch einer unbestimmten Zahl von Personen weltweit zugänglich machen, ist zu beachten, dass diese nur dann datenschutzrechtlich zulässig sind, wenn auf den Bildern ein Personenbezug nicht herstellbar ist.

8 Datenschutz in Wirtschaft und Vereinen

8.1 Anfragen zur Datenschutz-Grundverordnung (DS-GVO)

Eine wahre Flut von Anfragen erreichte uns bereits in den Monaten März, April und Mai 2018 im Vorfeld des Inkrafttretens der Europäischen Datenschutz-Grundverordnung (DS-GVO) und in den Monaten direkt nach deren Inkrafttreten ab Mai bis September 2018.

Sowohl aus der Wirtschaft als auch von Vereinen und Privatpersonen mussten täglich, teilweise im 10-Minuten-Takt, Anfragen zur neuen Rechtsgrundlage beantwortet werden. Dabei reichte das Spektrum von den Formerfordernissen der Informationen nach Art. 13 und 14 DS-GVO und der Benennungspflicht von betrieblichen Datenschutzbeauftragten gemäß Art. 37 DS-GVO i. V. m. § 38 Bundesdatenschutzgesetz (BDSG) über die Anforderungen an eine rechtmäßige Videoüberwachung bis hin zur korrekten Form von Einwilligungserklärungen und der zu erwartenden Bußgeldpraxis der Aufsichtsbehörde vor dem Hintergrund erheblich erhöhter Bußgeldsummen nach der DS-GVO.

Da wir bereits im Vorfeld versucht hatten, eine Vielzahl von Fragen durch koordinierte Veranstaltungen mit den entsprechenden Dachverbänden der Wirtschaft gebündelt klarzustellen, war die riesige Menge der Anfragen auch insofern bemerkenswert.

Festzustellen war ferner, dass viele kommerzielle Anbieter in Datenschutzangelegenheiten ebenso Schulungsveranstaltungen anboten, die jedoch teilweise zu Verunsicherungen bei den Schulungsteilnehmern und weiterem Klarstellungsbedarf durch unsere Behörde geführt haben. Die Flut der Anfragen – verbunden mit einem ebenso großen Anstieg entsprechender Petitionen und Meldungen von Datenpannen – hat zu einem erheblichen Rückstau in der Bearbeitung dieser Fälle geführt, weil unsere Behörde im Gegensatz zu anderen Länderauf-

sichtsbehörden mit Inkrafttreten der DS-GVO keinerlei zusätzliche Stellen bewilligt bekam. Diese personellen Kapazitätsprobleme wurden noch verstärkt durch die Tatsache, dass viele Rechtsbegriffe und neue Verfahrensabläufe erst zwischen den Länderaufsichtsbehörden und auf Bundes- und EU-Ebene neu abgestimmt werden müssen. Gleiches gilt für die teilweise veränderte rechtliche Situation in speziellen datenschutzrechtlichen Fachgebieten, beispielsweise der Videoüberwachung, den Sanktionen der Aufsichtsbehörde und den modifizierten Anforderungen im Versicherungs- und Auskunfteienbereich.

Trotz dieser insgesamt doch recht konfusen Situation im Jahr des Inkrafttretens der DS-GVO haben wir uns über das stark gestiegene Interesse am Datenschutz gefreut, das sich ebenfalls in der erwähnten großen Zahl von Anfragen widerspiegelt. Noch mehr freuen würden wir uns über eine personelle Verstärkung, die uns in die Lage versetzt, diesem stark gestiegenen Interesse der Bürgerinnen und Bürger und der Wirtschaft unsererseits gerecht werden zu können.

8.2 Meldung von Datenpannen

Datenpannen mussten auch nach dem alten Bundesdatenschutzgesetz (BDSG) gemeldet werden, wenn personenbezogene Daten besonderer Art, die einem Berufsgeheimnis unterlagen, sich auf strafbare Handlungen oder Ordnungswidrigkeiten bezogen oder Informationen zu Bank- oder Kreditkartenkonten enthielten und Dritten unrechtmäßig zur Kenntnis gelangt waren sowie schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohten.

Diese Meldepflicht wurde mit der Europäischen Datenschutz-Grundverordnung (DS-GVO) ausgeweitet und ist nicht mehr auf die oben genannten Kategorien beschränkt. Eine Meldepflicht tritt im Falle einer Verletzung des Schutzes personenbezogener Daten ein. Weiterhin hat sich mit der DS-GVO die Höhe der möglichen Bußgelder erhöht. Waren nach dem alten BDSG dreihunderttausend Euro für nicht gemeldete Datenpannen möglich, sind es nach der DS-GVO bis zu zwanzig Millionen Euro.

Die Ausweitung der Meldepflicht und die Erhöhung des möglichen Bußgeldrahmens dürften zwei Gründe dafür sein, dass sich die Anzahl der Meldungen stark erhöht hat. So wurden uns im Rahmen des alten BDSG vom 1. Januar 2018 bis zum 24. Mai 2018 nur 4 Datenpannen gemeldet, allerdings 56 im Rahmen der DS-GVO vom 25. Mai 2018 bis zum 31. Dezember 2018.

8.3 Schulungen für die Wirtschaft

Zur Vorbereitung auf die zu erwartenden vielen Fragen zur Europäischen Datenschutz-Grundverordnung (DS-GVO) wurden von uns bereits im Vorfeld des Inkrafttretens der DS-GVO Informationsveranstaltungen organisiert und durchgeführt. Um in möglichst großem Maße Synergieeffekte zu nutzen, haben wir uns mit den drei Industrie- und Handelskammern (IHK) in Mecklenburg-Vorpommern in Verbindung gesetzt, um eine zentrale Großveranstaltung durchzuführen. Durch die über die Industrie- und Handelskammern breit gestreuten Einladungen konnten wir eine Vielzahl von Wirtschaftsunternehmen erreichen, so dass es sich um eine insgesamt sehr gelungene Auftaktveranstaltung handelte.

Eine Vielzahl von Fragen wurde darüber hinaus im Erfahrungsaustauschkreis (ERFA-Kreis) der Gesellschaft für Datenschutz und Datensicherheit (GDD) für eine größere Zahl von Unternehmen und kommunaler Einrichtungen wie Stadtwerken etc. beantwortet.

Gut besucht waren auch Schulungen für den Bauernverband Mecklenburg-Vorpommern und den Verband Norddeutscher Wohnungsunternehmen, bei denen Datenschutzfragen für diese spezifischen Bereiche beantwortet wurden.

Für Mecklenburg-Vorpommern als Tourismusland wichtig war ferner die umfangreiche Schulung für einen großen Verband der Campingplätze im Lande, bei dem ebenfalls viele Unsicherheiten und Besorgnisse hinsichtlich der neuen Regelungen der DS-GVO ausgeräumt werden konnten.

Bei allen Veranstaltungen war neben den vielen fachlichen Fragen auch immer wieder die Sorge über mögliche Bußgelder vor dem Hintergrund des erheblich erhöhten Bußgeldrahmens nach der DS-GVO erkennbar. Wir haben jeweils deutlich gemacht, dass die Datenschutzaufsichtsbehörde in Mecklenburg-Vorpommern sich primär in ihrer Unterstützungs- und Beratungsfunktion sieht. Höhere Bußgelder werden in den Fällen verhängt, wo eine Kooperation mit der Aufsichtsbehörde von dem jeweiligen Unternehmen abgelehnt wird. Diese Aussage konnte allerdings nur mit der Einschränkung getroffen werden, dass zurzeit auf europäischer Ebene nähere Durchführungsbestimmungen sowohl zum Prozedere als auch zur Höhe von Bußgeldern in Vorbereitung sind, an die auch der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern gebunden sein wird. Soweit wir in die jeweiligen Abstimmungsprozesse einbezogen sind, werden wir auch weiterhin versuchen, derartige Regularien so zu beeinflussen, dass der Wirtschaftsstruktur in Mecklenburg-Vorpommern mit einer Vielzahl von sehr kleinen Unternehmen und Betrieben Rechnung getragen werden kann.

8.4 Zusätzliche Einwilligungen einholen?

Die Einwilligung ist eine von mehreren möglichen Rechtsgrundlagen des Katalogs in Art. 6 Europäische Datenschutz-Grundverordnung (DS-GVO), auf die eine Datenverarbeitung bzw. Datenübermittlung gestützt werden kann.

In vielen Fällen ist jedoch die Datenverarbeitung bereits aufgrund eines Vertrages durch eine andere Rechtsgrundlage (nämlich Art. 6 Abs. 1 b DS-GVO) abgedeckt.

In derartigen Fällen wurden jedoch oft (um „sicherzugehen“) zusätzliche Einwilligungen von den jeweiligen Vertragspartnern eingeholt. Dies kann bei diesen zu dem Missverständnis führen, man könne die erteilten Einwilligungen mit Wirkung für die Zukunft widerrufen, wodurch die wirksame Rechtsgrundlage für eine Datenverarbeitung entfallen würde, obwohl eine solche in dem geschlossenen Vertrag nach Art. 6 Abs. 1 b DS-GVO tatsächlich existiert.

Mit Blick auf den Grundsatz der Transparenz und Fairness gemäß Art. 5 Abs. 1 a DS-GVO ist jedoch ein Wechseln zwischen Einwilligungen und anderen Rechtsgrundlagen grundsätzlich unzulässig.

In weiteren Fällen wurden schriftliche Informationsblätter gemäß Art. 13 DS-GVO mit schriftlich erteilten Einwilligungen nach Art. 6 Abs. 1 a DS-GVO vermischt und dabei übersehen, dass eine Einwilligung nach Art. 13 DS-GVO nicht erforderlich ist, sondern es sich um eine reine Information handelt, die lediglich zu dokumentieren ist.

Sofern jedoch eine Einwilligung als Rechtsgrundlage vorliegt, muss sie freiwillig und informiert erteilt worden sein. Außerdem muss ein Hinweis gemäß Art. 7 Abs. 3 Satz 3 darüber erfolgt sein, dass die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen werden kann.

Für die Verarbeitung besonderer Kategorien von Daten (Gesundheitsdaten, genetische Daten etc.) ist gemäß Art. 9 Abs. 2 a DS-GVO eine ausdrückliche Einwilligung hierfür erforderlich, konkludente Handlungen sind also insofern ausgeschlossen.

Art. 8 DS-GVO enthält darüber hinaus besondere Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft.

Einwilligungen, die nicht den dargestellten Anforderungen genügen, sind unwirksam und können nicht als Rechtsgrundlage für eine Datenverarbeitung herangezogen werden.

8.5 „Datenschutzerklärung“ nach Art. 13 DS-GVO

Im Rahmen der uns vorliegenden Anfragen und Beschwerden bei der Anwendung der Europäischen Datenschutz-Grundverordnung (DS-GVO) haben wir festgestellt, dass bei den Verantwortlichen vielerorts Unsicherheit und zum Teil auch Unwissenheit herrscht, obwohl sich an den Grundsätzen der Datenverarbeitung nichts geändert hat. Man benötigt nach wie vor eine Rechtsgrundlage oder die Einwilligung für die Datenverarbeitung. Ausgeweitet wurden die Informationspflichten, die in Art. 13 und 14 DS-GVO geregelt sind. Diese sollen den Betroffenen einen Überblick über die Verarbeitung ihrer Daten verschaffen und sie über ihre Rechte aufklären.

Vielfach wird diese reine Information mit anderen Klauseln vermischt und unter dem Begriff „Datenschutzerklärung“ den Betroffenen zur Unterschrift vorgelegt. Ein einem Fall legte der Arbeitgeber seinen Beschäftigten eine solche „Datenschutzerklärung“ vor. Diese enthielt neben den Informationen nach Art. 13 DS-GVO eine Belehrung über die Schweigepflicht, eine Einwilligungsklausel in die Verwendung von Bild- und Tonaufnahmen der Beschäftigten und eine Einwilligungsklausel in die Verarbeitung der Beschäftigtendaten. Ein Petent, der diese „Datenschutzerklärung“ nicht unterschrieben hatte, meldete sich bei uns, da sein Arbeitgeber seine Gehaltzahlung zurückhielt mit der Begründung, dass er diese nicht leisten könne, weil der Petent die Datenschutzerklärung nicht unterschrieben habe und er ohne Einwilligung die Beschäftigtendaten nicht verarbeiten dürfe.

Nach unserem zunächst telefonischen Kontakt zum Arbeitgeber wurde dem Petenten sein Gehalt gezahlt. Im danach geführten Schriftverkehr wurde die „Datenschutzerklärung“ durch den betrieblichen Datenschutzbeauftragten entwirrt und von den falschen Klauseln, den Einwilligungen und Belehrungen getrennt. Es wurde dem Arbeitgeber erklärt, dass er für die Verarbeitung der erforderlichen Beschäftigtendaten keine Einwilligung benötigt, da es hierfür eine Rechtsgrundlage nach Art. 6 Abs. 1 lit. b DS-GVO i. V. m. § 26 Bundesdatenschutzgesetz (BDSG) gibt. Es wurde weiter erklärt, dass, sofern Einwilligungen eingeholt werden sollen, diese freiwillig sein müssen und dass er sich zu Dokumentations- und Nachweiszwecken die Aushändigung von Belehrungen oder Informationen (z. B. nach Art. 13) mit Unterschrift bestätigen lassen kann, diese dann aber keine Einwilligungen darstellen.

8.6 Hilfe für Vereine vor Ort

Unser Land braucht ehrenamtliches Engagement. Doch die Unsicherheit, die vielerorts in Vereinen zum Thema Europäische Datenschutz-Grundverordnung (DS-GVO) vorherrschte, brachte selbst langjährig in den Vorständen Aktive zum Grübeln.

Für den Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (LfDI MV) war diese Unsicherheit Anlass, im Rahmen von Veranstaltungen zur Umsetzung der DS-GVO im Verein zu informieren und auch ganz konkret Hilfestellung zu geben. So wurden beispielhaft Verzeichnisse von Verarbeitungstätigkeiten ausgefüllt, Formulare zur Erfüllung der Informationspflichten entworfen oder erklärt, wie sich ein Verein richtig verhält, wenn es doch zu einer Datenpanne kommen sollte.

Die Veranstaltungen wurden von der Stiftung für Ehrenamt und bürgerschaftliches Engagement in Mecklenburg Vorpommern organisiert. Nur diese gute Zusammenarbeit mit der Stiftung machte es letztlich möglich, dass trotz der knappen Personalausstattung beim LfDI MV viele der Veranstaltungen, verbunden mit langen Reisezeiten und arbeitnehmertauglichen Terminen, auch am späteren Abend realisiert werden konnten.

8.7 Orientierungshilfe für Vereine

Die Europäische Datenschutz-Grundverordnung (DS-GVO) stellt Vereine vor große Herausforderungen: Brauchen wir einen Datenschutzbeauftragten? Müssen wir von unseren Vereinsmitgliedern Einwilligungen einholen, um deren Daten im Verein verarbeiten zu dürfen? Dürfen wir Fotos vom letzten Fußballturnier auf unsere Homepage stellen?

Fragen über Fragen, die sich Vereine stellen. Doch damit nicht genug: Verzeichnisse müssen ausgefüllt und Formulare entworfen werden. Die ganze Datenverarbeitung im Verein ist zu prüfen.

Der Landtag Mecklenburg-Vorpommern hatte die Stiftung für Ehrenamt und bürgerschaftliches Engagement in Mecklenburg-Vorpommern und den Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (LfDI MV) gebeten, den Vereinen im Land für diese Aufgabe eine Orientierungshilfe an die Hand zu geben. Gemeinsam wurde ein Leitfaden für Vereine zur DS-GVO entwickelt, der seit Oktober 2018 unter www.ehrenamtsstiftung-mv.de und www.datenschutz-mv.de kostenlos zum Download zur Verfügung steht. Eine Druckversion kann ebenfalls kostenlos angefordert werden.

Der Leitfaden ist unterteilt: In Teil 1, „DS-GVO light“, finden Vereine einen Praxisratgeber für die schnelle Orientierung mit häufig gestellten Fragen, Checklisten und Mustern. Es gibt unter anderem Formulierungsbeispiele für die Einwilligung in die Verarbeitung von Gesundheitsdaten oder für Infoblätter, mit denen die Vereine ihrer Informationspflicht gegenüber ihren Mitgliedern nachkommen können.

Wer es ganz genau wissen will, kann in Teil 2 vertiefende Informationen nachlesen. Während kleinere Vereine im ersten Teil alle wesentlichen Informationen finden, können vor allem größere Vereine mit komplexeren Fragestellungen vom zweiten Teil profitieren. Der zweite Teil basiert mit freundlicher Genehmigung des Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg auf der Orientierungshilfe „Datenschutz im Verein nach der Datenschutz-Grundverordnung (DS-GVO) – Informationen über die datenschutzrechtlichen Rahmenbedingungen beim Umgang mit personenbezogenen Daten in der Vereinsarbeit“ aus Baden-Württemberg. Unser Dank gilt den Kolleginnen und Kollegen aus Baden-Württemberg, dass wir ihr Material nutzen durften. Nur so war es trotz des knappen Personals beim Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern und der Arbeitsauslastung möglich, kurzfristig einen Leitfaden zu verfassen, der den Bedürfnissen aller Vereine gerecht wird.

8.8 Datenschutz im Ehrenamt

Eine Petentin schilderte uns, dass sie sich ehrenamtlich bei der Betreuung von Flüchtlingsfamilien engagiert. Im Zusammenhang mit dieser Tätigkeit erhielt sie vom zuständigen Jugendamt eine E-Mail, in der die Betreuung einer Flüchtlingsfamilie durch die Petentin ausführlich beschrieben und auch mögliche Versäumnisse ihrerseits erwähnt wurden. Die E-Mail wurde vom Jugendamt unverschlüsselt an die dienstliche Adresse der Petentin gesandt, so dass alle Kolleginnen und Kollegen die Möglichkeit hatten, den Inhalt zur Kenntnis zu nehmen. Darüber hinaus wurde die E-Mail „cc“ auch an den Bürgermeister gesandt. Die Petentin bat uns, den Sachverhalt datenschutzrechtlich zu prüfen.

Wir haben die Anfrage zum Anlass genommen und das Jugendamt um Stellungnahme zu dem Sachverhalt gebeten. Das Jugendamt begründete das Vorgehen mit dem Hinweis auf Kindeswohlgefährdung sowie mit dem Argument, dass die Petentin nicht ausdrücklich darauf hingewiesen hatte, dass die Antwort nicht an ihre Dienstadresse gesendet werden soll. Außerdem war dem Jugendamt eine andere Adresse der Petentin nicht bekannt. Eine entsprechende

Rechtsgrundlage für die Übermittlung der in Rede stehenden Daten an den Arbeitgeber konnte uns das Jugendamt nicht nennen und es hat auch nicht dargelegt, warum die E-Mail dem Bürgermeister zur Kenntnis gesandt wurde.

Die im Schreiben des Jugendamtes angeführte Begründung für den Versand sensibler Sozialdaten per E-Mail konnten wir aus datenschutzrechtlicher Sicht nicht akzeptieren. Allein der Hinweis auf eine mögliche Kindeswohlgefährdung genügt im datenschutzrechtlichen Sinne nicht, um die zum Teil sensiblen Daten der Petentin so zu versenden, dass die Mitarbeiterinnen und Mitarbeiter oder der Bürgermeister diese zur Kenntnis nehmen können. Auch das Argument, dass dort nur die dienstliche Adresse der Petentin bekannt war, reicht nicht, um die Übermittlung zu rechtfertigen. So hätte das Schreiben ohne Weiteres auch per Post an die dienstliche Anschrift der Petentin mit dem Hinweis „persönlich“ gesandt werden können. Es war daher nicht nachvollziehbar, warum die Übermittlung per Post offenbar nicht in Erwägung gezogen wurde.

Im Verhältnis der Europäischen Datenschutz-Grundverordnung (DS-GVO) zu den Sozialgesetzbüchern (SGB) ist davon auszugehen, dass zunächst die Regelungen der DS-GVO gelten, die aber durch nationale Gesetze spezifiziert werden. Deshalb können für die Verarbeitung (hierzu gehört auch das Übermitteln von Sozialdaten) die Rechtsgrundlagen aus den §§ 67 ff. Sozialgesetzbuch Zehntes Buch (SGB X) sowie auch die Bestimmungen des Sozialgesetzbuches Achtes Buch (SGB VIII) herangezogen werden. Grundsätzlich ist die Übermittlung von Sozialdaten durch die Sozialleistungsträger (hier das Jugendamt) nur zulässig, soweit die Vorschriften des SGB X oder eine andere Rechtsvorschrift in diesem Gesetzbuch (z. B. SGB VIII) es erlauben oder anordnen. Eine Rechtsgrundlage, auf die die Übermittlung der in Rede stehenden Daten hätte gestützt werden können, ist im Sozialgesetzbuch nicht enthalten.

Dies teilten wir dem Jugendamt mit, das daraufhin einräumte, dass die Intention der Kontaktaufnahme vom Mitarbeiter des Jugendamtes und der Petentin darin bestand, auf die aus Sicht des Jugendamtes nicht förderlichen Unterstützungshandlungen der Petentin hinsichtlich einer Kontaktaufnahme zweier Familien kritisch hinzuweisen. Es räumte ein, dass es nicht ausreichend geprüft hat, ob der Versand der E-Mail an die dienstliche Adresse der Petentin und insbesondere auch die Weiterleitung an den Bürgermeister gegen datenschutzrechtliche Vorgaben verstoßen könnte. Bei korrekter Prüfung hätte dieser Irrtum vermieden werden können und müssen. Insofern bedauerte der Mitarbeiter des Jugendamtes sein Agieren und entschuldigte sich hierfür in aller Form.

Der Sachverhalt wurde auch mit dem Datenschutzbeauftragten des Landkreises ausgewertet und zum Anlass genommen, die Mitarbeiterinnen und Mitarbeiter nochmals auf die Einhaltung der datenschutzrechtlichen Bestimmungen hinzuweisen. Sofern eine Mitarbeiterin oder ein Mitarbeiter sich nicht sicher ist, ob das Handeln mit den datenschutzrechtlichen Bestimmungen vereinbar ist, wird empfohlen, den Datenschutzbeauftragten des Landkreises hinzuzuziehen.

9 Datenschutz in verschiedenen Rechtsgebieten

9.1 Polizei / Ordnungswesen

9.1.1 Umsetzung der JI-Richtlinie

Die Richtlinie 2016/680 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr wurde am 27. April 2016 ausgefertigt und am 4. Mai 2016 im Amtsblatt der Europäischen Union verkündet. Nach Art. 63 Abs. 1 JI-

Richtlinie war vorgesehen, dass die Richtlinie bis zum 6. Mai 2018 in nationales Recht umgesetzt werden sollte.

Die Umsetzung dieser Richtlinie ist in Mecklenburg-Vorpommern nur insoweit erfolgt, als im § 3 Landesdatenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) die entsprechende Anwendung der Europäischen Datenschutz-Grundverordnung (DS-GVO) geregelt worden ist. Die erforderliche Umsetzung in den Fachgesetzen, insbesondere dem Sicherheits- und Ordnungsgesetz (SOG M-V) und dem Strafvollzugsgesetz (StVollzG M-V) steht bis heute aus.

9.1.2 Pilotprojekt zum Einsatz von Bodycams bei der Polizei

Das Landesamt für zentrale Aufgaben und Technik der Polizei, Brand- und Katastrophenschutz Mecklenburg-Vorpommern (LPBK M-V) trat im April mit der Bitte an uns heran, das Pilotprojekt zum „Einsatz körpernah getragener Aufnahmegeräte durch die Polizei“, bekannt als Bodycams, zu begleiten.

Der Einsatz solcher Aufnahmetechniken ist auch in vielen anderen Bundesländern in der Erprobungsphase. Begründet wird der Einsatz unter anderem damit, dass die bewusste Wahrnehmung einer Aufzeichnung eine deeskalierende Wirkung haben soll.

Im Gegensatz zu einigen anderen Bundesländern ist in Mecklenburg-Vorpommern neben der Bild- auch eine Tonaufzeichnung zulässig, § 32a Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommern (SOG M-V). Zudem soll der Einsatz in Wohnräumen möglich sein. Damit erfolgt ein starker Eingriff in das Grundrecht auf die Unverletzlichkeit der Wohnung, welches sich aus Artikel 13 des Grundgesetzes (GG) ergibt. Weiterhin ist in Mecklenburg-Vorpommern auch eine sogenannte Pre-Recording-Funktion von 60 Sekunden vorgesehen. Bei der Technik werden im Standby-Modus der Kamera permanent die vergangenen 60 Sekunden zwischengespeichert. Es ist vorgesehen, dass der Träger der Kamera das Pre-Recording schon bei bloßem Verdacht auf eine Gefährdung aktivieren darf. Es steht zu befürchten, dass diese niederschwellige Hürde zu einer kontinuierlichen Speicherung von Bild und Ton auf Vorrat führen wird. Es muss also schon zu Beginn der Pilotphase kritisch festgehalten werden, dass zum Erreichen des angestrebten Ziels gleich mit der maximal möglichen Eingriffsintensität gearbeitet wird, anstatt zu versuchen, das Ziel mit einer stufenweisen Erhöhung der Eingriffsschwelle zu erreichen.

Da es sich bei den Aufnahmen um teils sehr sensible Daten handelt, ist deren Absicherung mit entsprechend hohen Anforderungen an die technischen und organisatorischen Maßnahmen verbunden. So müssen die Aufzeichnungen verschlüsselt und manipulationssicher erstellt und aufbewahrt werden. Zudem dürfen die Daten nicht über den vorgesehenen Zweck hinaus genutzt werden. Daher haben wir die Nutzung der Aufzeichnungen für Aus- und Fortbildungszwecke abgelehnt.

Da sich bei dem geplanten Verfahren hohe Risiken für die Rechte und Freiheiten der betroffenen Personen ergeben, war es erforderlich, eine Datenschutzfolgenabschätzung (DSFA) gemäß Art. 35 Europäische Datenschutz-Grundverordnung (DS-GVO) durchzuführen. Dabei hat sich das LPBK weitgehend auf die von uns bereitgestellten Hilfsmittel gestützt. Nicht zuletzt dadurch konnte das LPBK eine vollständige DSFA vorlegen, die alle Anforderungen der DS-GVO erfüllt und für sämtliche Verarbeitungsrisiken angemessene und erforderliche technische und organisatorische Maßnahmen auflistet.

Bereits vor dem Abschluss des Pilotprojektes scheint absehbar zu sein, dass Bodycams früher oder später flächendeckend in Mecklenburg-Vorpommern eingesetzt werden sollen. Eine entsprechende Rechtsgrundlage mit flankierenden Regelungen zu den umstritten Punkten, wie die Möglichkeit einer Aufzeichnung in Wohnräumen sowie die von uns kritisierte Nutzung

von Aufzeichnungen zu Aus- und Fortbildungszwecken, wurde zum Zeitpunkt dieses Berichtes mit der geplanten Novellierung des SOG M-V bereits vorbereitet, siehe dazu auch Punkt 9.1.1.

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.

9.1.3 Fox-112

Bereits seit 2014 beraten wir das Landesamt für zentrale Aufgaben und Technik der Polizei, Brand- und Katastrophenschutz Mecklenburg-Vorpommern (LPBK M-V) sowie Gemeinden bei der landesweiten Einführung der Feuerwehr-Verwaltungssoftware Fox-112. Diese Software soll Feuerwehren und Feuerwehrverbände bei Verwaltungsaufgaben einschließlich des Berichtswesens unterstützen. Es handelt sich dabei um eine webbasierte Lösung.

Während der Beratung haben wir insbesondere auf folgende Punkte hingewirkt:

- Der Umfang der verarbeiteten Daten war an das rechtlich Zulässige anzupassen. Maßgeblich ist hier das Brandschutz- und Hilfeleistungsgesetz Mecklenburg-Vorpommern (BrSchG M-V).

- Es musste ein leistungsfähiger Dienstleister mit dem technischen Betrieb der zentralen Komponenten gefunden und beauftragt werden, der die Anforderungen an die Auftragsverarbeitung nach Art. 28 Europäische Datenschutz-Grundverordnung (DS-GVO) erfüllt. Auch mit dem Softwareentwickler ist ein Vertrag nach diesen Regularien erforderlich, weil die Wartung durch den Entwickler im Einzelfall den Zugriff auf personenbezogene Daten erfordert.

- Wir haben zahlreiche Hinweise gegeben, wie die Anforderungen an die Sicherheit der Verarbeitung (Art. 32 DS-GVO) zu gewährleisten ist. Hierbei haben wir uns am Standard-Datenschutzmodell (SDM, siehe Punkt 7.1.5) und an der Grundschutzmethodik des Bundesamtes für Sicherheit in der Informationstechnik (BSI) orientiert.

- Darüber hinaus haben wir darauf aufmerksam gemacht, dass die Träger der Feuerwehren und das LPBK „gemeinsam für die Verarbeitung Verantwortliche“ im Sinne von Art. 26 DS-GVO sind. Sowohl die jeweiligen Gemeinden als auch das LPBK legen Zwecke bzw. Mittel der Verarbeitung fest. Dies macht sie von Gesetzes wegen zu „gemeinsam Verantwortlichen“. Sie müssen daher insbesondere eine Vereinbarung nach den Anforderungen des Art. 26 DS-GVO schließen. Art. 26 DS-GVO gibt den Beteiligten jedoch keine Befugnis zur Verarbeitung der Daten. Haben die Beteiligten Zugriff auf personenbezogene Daten, benötigen sie hierfür eine gesetzliche Erlaubnis. Im Falle von Fox-112 besteht diese in Art. 6 Abs. 1 lit. e DS-GVO in Verbindung mit § 28 BrSchG M-V. Diese gestattet nicht nur den Feuerwehren die Verarbeitung bestimmter personenbezogener Daten, sondern auch dem LPBK den Betrieb der zentralen Komponenten.

Zum Ende des Berichtszeitraumes stand die Inbetriebnahme des Verfahrens noch aus.

9.1.4 Neue Zuständigkeit für den LfDI MV: Bußgeldverfahren gegen Polizeibeamte

Seit Inkrafttreten der Europäischen Datenschutz-Grundverordnung (DS-GVO) ist der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (LfDI MV)

zuständig für Bußgeldverfahren gegen Polizeibeamte, die aus Datenschutzverletzungen der Polizisten in ihrem Dienstverhältnis resultieren. Bislang lag die Zuständigkeit hierfür im Ministerium für Inneres und Europa Mecklenburg-Vorpommern.

Wir hatten es dabei mit unerfreulichen Fällen zu tun:

In zwei Fällen haben Polizeibeamte ihre Dienststellung ausgenutzt, um an die Kontaktdaten minderjähriger Mädchen zu gelangen. In einem Fall hatte sich eine 15jährige Jugendliche, die sich wegen der Erstattung einer Strafanzeige wegen der ungewollten Veröffentlichung von Bildern im Internet, die sie beim Sex zeigen, in Begleitung einer Betreuerin auf das Polizeirevier begeben. Im Nachgang wurde sie von dem Polizeibeamten, der sie auf dem Revier in Empfang genommen hatte und dem der Sachverhalt zuerst geschildert wurde, per SMS angeschrieben und zu einem Fotoshooting eingeladen. Besonders gravierend ist dabei, dass diese Jugendliche sexuell freizügig in Erscheinung getreten und psychisch instabil gewesen ist. Sie hatte sich mit der Bitte um Hilfe an die Polizei gewandt. Im Ergebnis war sie aber erneuten Avancen ausgesetzt.

In einem anderen Fall hat ein Ermittler in einem Verfahren wegen Kindesmissbrauchs eine 13jährige Zeugin des Missbrauchsverfahrens im Anschluss an eine Zeugenvernehmung auf What`sApp kontaktiert. Die Handynummer hatte er sich im Nachgang der Vernehmung mit dem Hinweis verschafft, diese würde möglicherweise noch für Nachfragen benötigt. Am selben Tag hat der Polizeibeamte mit dem Mädchen einen Chat auf What`sApp begonnen und hat in dessen Verlauf diesem 13jährigen Mädchen sexuelle Avancen gemacht.

Schließlich hat ein weiterer Polizeibeamter seine Dienststellung ausgenutzt, um ein Strafverfahren gegen seinen Sohn zu verhindern. Er hatte im Dienst von einer Strafanzeige gegen seinen Sohn Kenntnis erlangt. Mit diesem Wissen und mit dem Hinweis auf seine Dienststellung hat er sich dann per What´sApp an die Erstatterin der Strafanzeige gewandt, um sie zur Rücknahme der Anzeige zu bewegen. Die Erstatterin der Strafanzeige, eine 16jährige Jugendliche, hatte den Sohn des Polizeibeamten angezeigt, weil dieser sie und ihren Vater bedroht hatte, nachdem sie die Beziehung zu ihm beendet hatte. Der Polizeibeamte hat in dem Verlauf des What´sApp-Chats versucht, die Jugendliche in bedrohlicher Form zur Rücknahme der Strafanzeige zu bewegen.

9.2 Justiz

9.2.1 Verwarnung gegen das OLG Rostock wegen mangelhafter Faxnutzung

Wir haben gegen das Oberlandesgericht (OLG) Rostock eine Verwarnung ausgesprochen, weil dort die Datensicherheit bei der Nutzung des Telefax-Gerätes nicht eingehalten wurde.

Eine Petentin hatte sich an uns gewandt, weil in zwei Fällen Beschlüsse des OLG in Strafsachen auf ihrem Faxgerät angekommen waren. Es handelte sich um die vollständigen Beschlüsse in Strafvollstreckungsverfahren wegen Totschlags und anderer Delikte. Die Petentin hat diese Beschlüsse an verschiedene Institutionen in Deutschland und an die russische Botschaft versendet.

Wir haben das OLG um Stellungnahme gebeten. Nach dem Schriftverkehr mussten wir davon ausgehen, dass beide Faxe irrtümlich und damit fehlerhaft an die Petentin versendet wurden. Im Gegensatz zur Briefpost handelt es sich beim Telefax um eine Art offener Zustellung. Deshalb müssen bei einem Versand von personenbezogenen Daten per Fax Maßnahmen getroffen werden, die verhindern, dass bei der Übertragung dieser Daten unbefugt gelesen, kopiert, verändert oder gelöscht wird. Bei Telefaxen kommt es immer wieder zu Fehlerübertragungen. Als häufigste Ursache dafür ist meist menschliches Versagen verantwortlich, etwa

nicht erkannte Tippfehler bei der Eingabe der Zielnummer. Die Verantwortlichen sollten vor dem Versand von schutzwürdigen Daten mit dem Telefax-Dienst prüfen, ob diese Versandart wirklich erforderlich ist und nicht eine andere Versandart angemessener ist.

Wir haben das OLG aufgefordert, die Datensicherheit bei dem Telefax-Dienst zu verbessern. Insbesondere bei der Übertragung von Telefaxen mit besonders schutzwürdigem Inhalt kann eine Fehlzustellung gravierende Folgen für den Absender, Empfänger und Betroffenen haben. Deshalb sollte zumindest in diesen Fällen eine unverschlüsselte Datenübertragung unterbleiben oder einem für den besonderen Schutz dieser besonderen Daten speziellem Verfahren unterzogen werden.

9.3 Kommunales

9.3.1 Vollzeitstellen für behördliche Datenschutzbeauftragte in größeren Verwaltungen

Seit Jahren ist festzustellen, dass gerade den behördlichen Datenschutzbeauftragten größerer Verwaltungen nicht der für ihre Aufgabenerfüllung erforderliche Zeitanteil zur Verfügung steht. Nicht ganz unbeachtlich ist dabei auch der Umstand, dass die Datenschutzbeauftragten oft nicht nur für den Bereich ihrer Kernverwaltung, sondern beispielsweise auch für nachgeordnete Bereiche, zum Beispiel Schulen, oder kommunale Eigenbetriebe mitverantwortlich sind.

Von daher haben wir schon seit geraumer Zeit immer wieder die Empfehlung ausgesprochen, die Datenschutzbeauftragten mit dem für ihre Aufgabenerfüllung notwendigen Zeitanteil auszustatten. Ähnlich hat dieses auch der Rechts- und Verfassungsausschuss des Landkreistages Mecklenburg-Vorpommern gesehen, der im Zuge der Kreisgebietsreform in seiner Sitzung vom 28.04.2011 für einen hauptamtlichen Datenschutzbeauftragten votiert hat. Dieses wurde in der Folge jedoch nur im Landkreis Vorpommern-Greifswald umgesetzt.

Im Zuge der Umsetzungen der mit der Europäischen Datenschutz-Grundverordnung (DS-GVO) verbundenen Maßnahmen wurde deutlich, dass die vorgenannte Forderung aktueller ist denn je.

Exemplarisch hierfür sind beispielsweise allein die Umsetzung der notwendigen Dokumentations- und Informationspflichten oder auch die Mitwirkung an e-Government-Projekten, zum Beispiel Einführung der e-Akte, und deren Umsetzung (vor allem bezogen auf technische und organisatorische Maßnahmen zu nennen.

Um den Aufgaben und der damit verbundenen verstärkten Rolle der Datenschutzbeauftragten innerhalb der Verwaltung gerecht werden zu können, haben wir gegenüber den Landkreisen, kreisfreien und großen kreisangehörigen Städten die Empfehlung ausgesprochen, die Zeitanteile der behördlichen Datenschutzbeauftragten jeweils auf eine Vollzeitstelle anzuheben.

Nach uns vorliegenden Informationen sind der Landkreis Vorpommern-Rügen sowie die Hansestädte Rostock und Greifswald dieser Empfehlung gefolgt. Die Hansestadt Wismar sowie der Landkreis Ludwiglust-Parchim wollen externe Dienstleister mit der Aufgabenwahrnehmung beauftragen.

9.3.2 Angriff auf das Ratsinformationssystem einer Kommune

Art. 33 Europäische Datenschutz-Grundverordnung (DS-GVO) sieht eine Meldepflicht auftretender Datenpannen vor. Konkret hat der Verantwortliche spätestens nach 72 Stunden uns die Verletzung und nähere Informationen hierzu, die sich aus der vorgenannten Vorschrift ergeben, mitzuteilen.

Im Berichtszeitraum erhielten wir eine große Zahl derartiger Meldungen, die unterschiedliche Gründe hatten. Unter anderem wurden wir darüber in Kenntnis gesetzt, dass das Ratsinformationssystem einer Amtsverwaltung soweit gehackt wurde, dass ein unerlaubter Zugriff auf personenbezogene Daten, die Inhalt nichtöffentlicher Beschlussvorlagen und Protokolle waren, nicht ausgeschlossen werden konnte. Der Vorfall wurde uns indes erst 14 Tage nach Bekanntwerden und damit verspätet gemeldet. Dieses haben wir gegenüber der Amtsverwaltung entsprechend kritisiert.

Die Amtsverwaltung stellte fest, dass sämtliche Unterlagen der Sitzungen, welche im Zeitraum der Jahre 2012 – 2018 stattfanden, betroffen waren. Als Sofortmaßnahmen wurden alle Zugänge zu dieser Plattform deaktiviert. Ebenso wurden die betroffenen Gemeindevertreter über diese Datenpanne informiert. Da aber nicht nur sie, sondern auch eine Vielzahl von Personen, deren personenbezogene Daten in den Beschlussvorlagen beziehungsweise Protokollen enthalten waren, betroffen waren, mussten auch diese entsprechend informiert werden. Grund hierfür ist das mit der Datenpanne verbundene hohe Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen. Dieses Risiko resultiert allein schon daraus, dass beispielsweise Anträge über Stundung, Niederschlagung und Erlass betroffen waren und Inhalt dieser Beschlussvorlagen insbesondere auch Angaben über wirtschaftliche Verhältnisse der jeweiligen Antragsteller enthielten.

Aufgrund der Vielzahl der betreffenden Unterlagen und gesehen auf den sechsjährigen Zeitraum wurde in Abstimmung mit uns entschieden, dass eine Einzelbenachrichtigung aller betroffener Person mit einem unverhältnismäßigen Aufwand verbunden sei, so dass von dem Instrumentarium des Art. 34 Abs. 3 lit. c) DS-GVO Gebrauch gemacht wurde und die betroffenen Personen über eine öffentliche Bekanntmachung informiert wurden.

In Auswertung dieses Vorfalls hat die Amtsverwaltung von sich aus entschieden, künftig auf den weiteren Einsatz des Ratsinformationssystems zu verzichten.

9.3.3 Mitwirkungspflichten bei der Erhebung einer Kurabgabe

Im Zusammenhang mit dem Wirksamwerden der Europäischen Datenschutz-Grundverordnung (DS-GVO) im Mai 2018 wurde immer wieder die Rechtmäßigkeit der Verarbeitung personenbezogener Daten für die Erhebung von Kurabgaben in Frage gestellt.

Auch mit Wirksamkeit der DS-GVO hat sich an dem allgemeinen Grundsatz, dass personenbezogene Daten unter anderem dann verarbeitet werden dürfen, wenn eine Rechtsgrundlage dies erlaubt oder der Betroffene eingewilligt hat, nichts geändert. Als eine solche Rechtsgrundlage kommt auch das Kommunalabgabengesetz Mecklenburg-Vorpommern (KAG M-V) in Verbindung mit den jeweiligen kommunalen Kurabgabensatzungen in Betracht.

In einem uns vorliegenden Fall sah die gemeindliche Kurabgabensatzung unter anderem eine Kurabgabenpflicht für Inhaber von Bootsliegeplätzen vor. Anders als bei den Quartiergebern wurde der vorgenannte Personenkreis jedoch nicht zur Mitwirkung verpflichtet. Das KAG M-V verweist bezüglich der Erhebung von Kommunalabgaben (zu denen unter anderem die Fremdenverkehrs- und Kurabgabe gehören) auf die Vorschriften der Abgabenordnung (AO).

Nach § 93 Abs. 1 AO unterliegen Beteiligte und andere Personen einer Auskunftsverpflichtung. Aufgrund dieser Vorschrift sind beispielsweise auch Inhaber von Bootsliegeplätzen zur Mitwirkung bei der Erhebung einer Kurabgabe verpflichtet.

Aus Gründen der Normenklarheit und Transparenz haben wir der betroffenen Verwaltung empfohlen, in der Kurabgabensatzung vollständige Regelungen bezüglich etwaiger Mitwirkungsverpflichtungen zu treffen.

9.4 Bildung / Schule / Kita

9.4.1 Schulgesetz M-V

Seit dem 25. Mai 2018 ist die Europäische Datenschutz-Grundverordnung (DS-GVO) anzuwenden. Die erforderlichen Anpassungen der Spezialgesetze in den verschiedensten Bereichen sind noch nicht überall abgeschlossen.

Sehr erfreulich ist es daher, dass das Schulgesetz unseres Landes (SchulG M-V) fristgerecht an die DS-GVO angepasst wurde. Wesentliche Regeln zum Umgang mit personenbezogenen Daten enthält der neu gefasste § 70 SchulG M-V. Die datenschutzrechtlichen Vorgaben in den Absätzen 1 bis 5 sind jedoch noch sehr allgemein. Das Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern als oberste Schulbehörde des Landes wurde daher in Abs. 6 dieser Norm ermächtigt, durch eine Rechtsverordnung diese Absätze näher zu bestimmen. Wir unterstützen ausdrücklich, den Anwendenden des Schulgesetzes mit dieser Rechtsverordnung, der Schuldatenschutzverordnung – Schul-DSVO M-V, die Auslegung des Schulgesetzes zu erleichtern.

Bis zum Ende des Berichtszeitraumes hat das Ministerium noch keine überarbeitete Schul-DSVO vorgelegt.

9.4.2 Private Technik von Lehrkräften im Unterricht

Mit Inkrafttreten des neuen Schulgesetzes für das Land Mecklenburg-Vorpommern (SchulG M-V), siehe auch Punkt 9.4.1, findet eine neue Regelung zur Bereitstellung von Datenverarbeitungsanlagen für Lehrkräfte und sonstiges Schulpersonal Anwendung. Das Schulgesetz legt fest, dass künftig der Schulträger Lehrkräften und sonstigem Schulpersonal Datenverarbeitungsanlagen zur Verfügung stellen soll, wenn auf diesen personenbezogene Daten zu dienstlichen Zwecken verarbeitet werden. Das bisherige Gesetz war in dieser Klarheit nicht formuliert.

Mit Schreiben vom 25. Mai 2018 informierte das Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern alle Schulleitungen des Landes mit einer mehrseitigen Handreichung über das neue Schulgesetz. In dieser Handreichung wurde den Schulleitungen nun aber mitgeteilt, dass es in begrenzten Ausnahmefällen doch zulässig sei, private Datenverarbeitungsanlagen zu dienstlichen Zwecken zu nutzen. Voraussetzung dafür wäre, dass der Schulträger keine Geräte zur Verfügung stellen könne, die die notwendigen Sicherheitsanforderungen erfüllen, und er somit den neuen gesetzlichen Verpflichtungen nicht nachkommen könne. Als Anlage war dieser Handreichung das Muster einer sogenannten Datenschutzerklärung beigefügt. Lehrkräfte sollten damit in Kenntnis gesetzt werden, dass ein Verstoß gegen die Bestimmungen der Europäischen Datenschutz-Grundverordnung (DS-GVO) sowie anderer einschlägiger Rechtsvorschriften mit Bußgeldern und strafrechtlichen Sanktionen geahndet werde und dies auch Schadensersatzforderungen sowie dienst- oder arbeitsrechtliche Konsequenzen zur Folge haben könne. Durch Unterschrift sollten sie die Kenntnisnahme bestätigen.

Angesichts der Tatsache, dass die Schulträger in absehbarer Zeit kaum in der Lage sein würden, datenschutzgerecht konfigurierte Geräte zu Verfügung zu stellen, war zu befürchten, dass sich das Regel-Ausnahme-Verhältnis ins Gegenteil umkehren würde und das Haftungsrisiko bei Verstößen gegen die Datenschutzregelungen zu Unrecht auf die Unterzeichnenden übertragen werden sollte.

Nachdem die Schulleitungen diese Handreichung erhalten hatten, wandte sich der Lehrerhauptpersonalrat im Juni 2018 mit der Bitte an uns, die Hinweise des Ministeriums daten-

schutzrechtlich zu bewerten. Wir haben daraufhin Kontakt mit dem Ministerium aufgenommen, um die datenschutzrechtlichen Belange der Angelegenheit zu klären. Ziel des von uns angebotenen Meinungsaustausches war es, die Handreichung zur dienstlichen Nutzung privater Datenverarbeitungsanlagen durch Lehrkräfte vom Bildungsministerium grundlegend überarbeiten zu lassen.

Bis zum Ende des Berichtszeitraumes haben die Schulleitungen jedoch noch keine überarbeitete Handreichung vom Ministerium erhalten.

9.4.3 Arbeitsgruppe „Digitale Schule“ und das Kooperative Projekt „Schul-IT“

Um die „Kooperationsvereinbarung zur Förderung der Medienkompetenz in Mecklenburg-Vorpommern“ von April 2015, siehe auch Punkt 6.1.3, umzusetzen, wurde unter anderem die Arbeitsgruppe „Digitale Schule“ gegründet. Bereits im Dreizehnten Tätigkeitsbericht, Punkt 6.8.1, haben wir hierzu ausführlich berichtet und auch dargestellt, warum es zu zeitlichen Verzögerungen bei der inhaltlichen Arbeit der Arbeitsgruppe kam.

Ein Ziel der Arbeitsgruppe „Digitale Schule“ ist es, einen Orientierungsrahmen für eine nachhaltige Strategie zur angemessenen Ausstattung der Schulen mit Informationstechnik zu erarbeiten. Dieser Rahmen soll der Landesregierung und den kommunalen Schulträgern als Entscheidungsgrundlage dienen.

Die Federführung der Arbeitsgruppe „Digitale Schule“ hat 2017 das Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern übernommen. Damit die Arbeitsgruppe ihr oben genanntes Ziel erreichen kann und um inhaltliche Fragen möglichst praxisnah zu bearbeiten wurde vereinbart, die Zielstellung innerhalb eines zu gründenden Projektes und am Beispiel von Musterschulen anzugehen. Da die Arbeitsgruppe „Digitale Schule“ auf Grund fehlender Rechtspersönlichkeit keine Fördermittel für das anstehende Projekt beantragen konnte, wurde hierfür ein Projektträger gesucht. Im 4. Quartal 2017 übernahm der Landkreis Vorpommern-Greifswald die Projektträgerschaft und beantragte die nötigen Fördermittel. Nach Bewilligung der Mittel konnte dann das Kooperative Projekt „Schul-IT“ gestartet werden. Die Projektteilnehmer haben bereits im Berichtszeitraum einen Muster-Medienentwicklungsplan für Schulträger erarbeitet. Zudem wurde im Rahmen des Projektes eine Handreichung zur Erarbeitung von Medienbildungskonzepten entwickelt. Zurzeit werden Prozessuntersuchungen zu einzelnen Datenverarbeitungsschritten in Schulen durchgeführt. An den so veranschaulichten Prozessen können datenschutzrechtliche Fragestellungen identifiziert und zielgerichtet bearbeitet werden.

Das Kooperative Projekt „Schul-IT“ wird im Jahr 2019 weitergeführt.

9.4.4 Schul-Cloud des Hasso-Plattner-Instituts (HPI)

Die Entwicklung der Schul-Cloud des Hasso-Plattner-Instituts (HPI) begleiten wir bereits seit einigen Jahren gemeinsam mit einigen anderen Datenschutzaufsichtsbehörden, siehe auch Dreizehnter Tätigkeitsbericht, Punkt 6.8.2. Im Rahmen der Begleitung des Projektes hatte uns das HPI darüber informiert, dass auch eine Schule in Mecklenburg-Vorpommern am Testbetrieb der Schul-Cloud teilnimmt.

Mit einem Informationsbesuch an dieser Schule wollten wir uns über die Details in der Praxis informieren. Allerdings mussten wir vor Ort feststellen, dass an dieser Schule der Testbetrieb noch nicht begonnen hatte. Die Schulleitung war verunsichert, welche datenschutzrechtlichen Unterlagen erforderlich und von wem in welcher Qualität zu erstellen waren. Dies betraf beispielsweise das Verzeichnis von Verarbeitungstätigkeiten, das Datenschutz- und Sicherheitskonzept oder die schon für den Testbetrieb erforderlichen Einwilligungserklärungen.

Rückblickend auf nun schon einige Jahre der Begleitung des Projektes war festzustellen, dass die Befassung der Aufsichtsbehörden mit der HPI-Schul-Cloud im Berichtszeitraum insbesondere wegen einiger vom HPI verursachter Informationsdefizite optimierungsbedürftig war. Um das gemeinsame Vorgehen der beteiligten Aufsichtsbehörden zu koordinieren, hat der Arbeitskreis Schulen und Bildungseinrichtungen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) eine Arbeitsgruppe eingesetzt. Diese soll sich mit anstehenden Fragen zur HPI-Schul-Cloud befassen und dem Arbeitskreis Bericht erstatten.

Wir beteiligen uns an der Arbeit des neu eingerichteten Gremiums, um unsere langjährigen Erfahrungen im Bereich des Einsatzes moderner Informationstechnik an Schulen einzubringen und um auf diese Weise das HPI-Schul-Cloud-Projekt auch weiterhin zu unterstützen.

9.4.5 Datenschutz in der Kindertagespflege

Der Landesverband für Kindertagespflege Mecklenburg-Vorpommern e. V. hat sich mit einer Problematik an uns gewandt, die unter anderem datenschutzrechtliche Folgen nach sich zieht.

Ausgangspunkt ist die Tatsache, dass die Einziehung der Elternbeiträge durch die Kindertagespflegepersonen erfolgt. Der Landesverband ist der Auffassung, dass der örtliche Träger der Jugendhilfe für den Einzug der Elternbeiträge verantwortlich sei und die vollständige Vergütung an die Tagespflegepersonen zu zahlen ist. Verschiedene öffentliche Träger sind der Auffassung, dass die Tagespflegepersonen die Elternbeiträge selbst einziehen müssen und berufen sich auf die Vorschriften des Kindertagesförderungsgesetzes Mecklenburg-Vorpommern (KiföG M-V) zum Elternbeitrag und die Grundsätze der Finanzierung.

Die somit in Mecklenburg-Vorpommern praktizierte Handhabung der Einziehung der Elternbeiträge durch die Kindertagespflegepersonen zieht eine datenschutzrechtliche Problematik nach sich. Die Kindertagespflegepersonen erhalten bei dieser Verfahrensweise Kenntnis darüber, welche Personen eine finanzielle Förderung durch die örtlichen Träger der Jugendhilfe erhalten. Die Eltern stellen zunächst den Antrag auf Kostenbeteiligung beim Jugendamt und erhalten anschließend eine Information bzw. eine Genehmigung vom Jugendamt und geben diese dann an die Tagespflegeeinrichtung weiter. Nur so erhalten die Kindertagespflegepersonen überhaupt Kenntnis über die Betreuungszeit der Tageskinder. Gleichzeitig werden ihnen damit jedoch beispielsweise auch Informationen über das Arbeitsverhältnis der Eltern sowie deren Vergütung und Berechnung für die Genehmigung der Betreuung zur Kenntnis gegeben.

Trotz der Informationen und Empfehlungen des Bundesministeriums für Familie, Senioren, Frauen und Jugend (BMFSFJ) dahingehend, dass der Elternbeitrag vom Jugendamt einzuziehen ist, wird jedoch an dieser Praxis festgehalten und damit aus datenschutzrechtlicher Sicht die Frage nach der Erforderlichkeit der Kenntnis der Kindertagespflegepersonen über die finanzielle Förderung der Eltern durch die örtlichen Träger der Jugendhilfe aufgeworfen.

Aus datenschutzrechtlicher Sicht ist es nicht erforderlich, dass die Kindertagespflegepersonen entsprechende Informationen über die Eltern vom Jugendamt erhalten.

Wir empfehlen der Landesregierung, die entsprechenden Regelungen im KiföG M-V zu ändern.

9.4.6 Datenschutz in Kita, Hort und Grundschule

Beratung und Fortbildung

Mit dem 25. Mai 2018 und der verbindlichen Einführung der Europäischen Datenschutz-Grundverordnung (DS-GVO) stieg unter anderem die Nachfrage zu Schulungen für Verantwortliche in Kindertageseinrichtungen, Horten und Grundschulen. Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (LfDI MV) schult bereits seit 2012 regelmäßig in Kooperation mit der Bildungsstätte Schabernack, Zentrum für Praxis und Theorie der Jugendhilfe e. V. Güstrow[37], zu dem Thema „Datenschutz und Privatsphäre".

Im Jahr 2018 gab es vier Veranstaltungen, die sich thematisch entweder an die pädagogischen Fachkräfte in Kita, Hort, Grundschule oder an Bereiche der Jugendhilfe wie Schulsozialarbeit oder offene Jugendarbeit richteten. Da der Bedarf weiterhin hoch ist, werden diese Ganztagesfortbildungen auch in 2019 weiter angeboten. Zusätzlich stieg auch die Anzahl der telefonischen Beratungen. Teilweise kommen immer wieder die gleichen Fragen auf. Aus diesem Grund nahm der LfDI MV auch eine Anfrage von AV1 Pädagogikfilme an, die zum Ziel hatte, eine DVD mit dem Titel „Datenschutz in der Kita" zu erstellen. Diese DVD kann genutzt werden, um Mitarbeiterinnen und Mitarbeiter zu Fragen des Datenschutzes zu sensibilisieren. Sowohl die DVD als auch unsere Ganztagsfortbildungen sind geprägt von einer hohen Fachlichkeit mit ganz praktischen Alltagsanwendungen.

In allen Beratungen und Fortbildungen wurde klar, dass eine große Verunsicherung bei den pädagogischen Fachkräften herrscht. Dies ist teilweise der übertriebenen Berichterstattung geschuldet und auch den äußerst kritischen Nachfragen und Anmerkungen der Eltern. Wir begrüßen sehr, dass Eltern die Rechte ihrer Kinder wahren. Dazu hat die Einführung der DS-GVO sicherlich beigetragen. Viele Träger sind allein durch ihre Größe bereits mit einem Datenschutzbeauftragten ausgestattet. Eltern sollten sich in erster Linie bei fachlichen Fragen zum Datenschutz an diese wenden. Die Pädagoginnen und Pädagogen vor Ort sind primär zur Erfüllung des Bildungs- und Erziehungsauftrages sowie der Betreuung der Kinder zuständig.

Geburtstagskalender

Eine häufige Frage war, ob noch Geburtstagskalender mit Fotos im Raum (Kita, Hort und/oder Klassenraum) hängen dürfen. Diese Frage ist mit ja zu beantworten. Das Gesetz zur Förderung von Kindern in Kindertageseinrichtungen und in Kindertagespflege, Kindertagesförderungsgesetz (KiföG M-V), bildet die gesetzliche Grundlage für die Kindertageseinrichtungen und Kindertagespflege in Mecklenburg-Vorpommern. Demnach ist die Ausgestaltung des pädagogischen Konzeptes den Trägern der Einrichtungen freigestellt, sofern sie den Zielen des KiföG M-V und den damit verbundenen Verordnungen entspricht. Aus pädagogischer Sicht ist dies ein wichtiger Bestandteil zur Förderung der Gruppengemeinschaft und zur Wertschätzung für das Geburtstagskind. Es fördert die sozialen Beziehungen innerhalb der Kindergruppe, KiföG M-V. Darüber hinaus lassen sich mit dem Kalender natürlich auch weitere Lerninhalte vermitteln. Wir empfehlen den Einrichtungen diesbezüglich immer, die Eltern aktiv nach einem Foto des Kindes für den Geburtstagskalender im Gruppenraum zu fragen. Sollte es wirklich einmal einen besonders schweren Fall von zum Beispiel häuslicher Gewalt oder ähnliches geben, wo die schutzwürdigen Interessen des Kindes überwiegen, dann werden die Personensorgeberechtigten die Fachkräfte sicherlich separat ansprechen. Dies wäre dann ein Einzelfall, wo man gemeinsam mit Eltern und Einrichtung schauen kann, wie man beides vereint bekommt.

[37] vgl. ab dem Elftem Tätigkeitsbericht

Fotoerlaubnis/Fotofreigabe

Weiterhin erhalten wir viele Fragen zum Thema der Fotoerlaubnis/Fotofreigabe. Hierzu ist zu sagen, dass nach den Regelungen der DS-GVO die Fotoerlaubnis hinreichend konkret und für jeden Zweck einzeln, z.B. Weitergabe an andere Eltern, Veröffentlichung auf der Homepage, in der Presse usw., wählbar sein muss. Das heißt ganz praktisch, dass die Eltern einzeln die verschiedenen Wege der Veröffentlichung auswählen können. Diese Vorgehensweise war bereits vor dem 25. Mai 2018 erforderlich.

Portfoliomappen

In Bezug auf die Ausgestaltung der Portfoliomappen der Kinder regen wir an, die „Verordnung über die inhaltliche Ausgestaltung und Durchführung der individuellen Förderung“ (BeDoVO M-V) mit dem konkreten Beispiel, dass Fotos ebenfalls zur Dokumentation gehören, zu erweitern. Die alltagsintegrierte Beobachtung und Dokumentation des kindlichen Entwicklungsprozesses hat ihre gesetzliche Grundlage in § 1 Abs. 5 KiföG M-V. Dem zugehörig ist die BeDoVo M-V, die die Verfahren festlegt. Mit der hinreichenden Konkretisierung in Bezug auf die Verwendung von Fotos können bereits im Vorfeld Unsicherheiten bei allen pädagogischen Fachkräften ausgeräumt werden.

Mit Blick auf die Wahrung der partnerschaftlichen Zusammenarbeit zwischen Eltern und Einrichtung empfehlen wir den Dialog, ohne dabei den Datenschutz als Instrument der Verunsicherung zu nutzen.

10 Presse- und Öffentlichkeitsarbeit

Die Entwicklung im Bereich des Datenschutzes erforderte auch in diesem Berichtszeitraum eine breite Presse- und Öffentlichkeitsarbeit der Behörde des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (LfDI MV). Dies betraf insbesondere die Entwicklung aufgrund des Wirksamwerdens der Europäischen Datenschutz-Grundverordnung (DS-GVO) am 25. Mai 2018. Vielen Anfragen, Wünschen nach Unterstützung, Beratung, Information konnte nicht in gewünschtem Umfang nachgekommen werden, da das dafür benötigte Personal in der Behörde vom Landtag verweigert wurde.

Zum Thema DS-GVO gab es im Berichtszeitraum zahlreiche Presse-Anfragen und Interview-Wünsche. Auch im Rahmen eines Pressegespräches zum neu gefassten Landesdatenschutzgesetz (DSG M-V) wurden Fragen beantwortet und Hintergründe erläutert.

Von den zahlreichen Aktivitäten im Bereich der Presse- und Öffentlichkeitsarbeit im Berichtszeitraum ist nachfolgend eine Auswahl genannt.

Tätigkeitsbericht

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern hat regelmäßig einen Bericht über seine Tätigkeit vorzulegen. In diesen Berichten finden sich im Wesentlichen die Entwicklungen in den Bereichen Datenschutz und Informationsfreiheit sowie beispielhaft auch Sachverhalte, die in den Berichtszeiträumen aktuell waren oder zu denen viele Petitionen und Anfragen oder auch Beratungsersuchen eingegangen sind.

Anfang 2018 wurden die Tätigkeitsberichte zum Datenschutz und zur Informationsfreiheit in Mecklenburg-Vorpommern für die Jahre 2016/2017 vorgelegt. Interessierte finden die Berichte auf der Internetseite des LfDI MV unter www.datenschutz-mv.de.

Tag der offenen Tür

Im Berichtszeitraum beteiligte sich die Behörde des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern wie auch schon all die Jahre zuvor am „Tag der offenen Tür“ des Landtages Mecklenburg-Vorpommern. Mit Flyern zu aktuellen Themen und weiteren Materialien informierte der Landesbeauftragte zu den Themen Datenschutz und Informationsfreiheit und beantwortete Fragen der Besucherinnen und Besucher. Ein Informationsschwerpunkt war das Thema „Datenschutz und Bildung“, siehe auch Punkt 6.1.

Informationsveranstaltungen, Schulungen, Beratungen, Vorträge

Die Presse- und Öffentlichkeitsarbeit der Behörde war im Berichtszeitraum insbesondere geprägt durch sehr viele Veranstaltungen zum Thema DS-GVO. Es wurden sowohl eigene als auch in Kooperation mit anderen Partnern organisierte Veranstaltungen durchgeführt oder es wurde auf Veranstaltungen zur DS-GVO informiert, die extern organisiert wurden. Wichtige Partner beispielsweise waren dabei die Ärztekammer Mecklenburg-Vorpommern, die Stiftung für Ehrenamt und bürgerschaftliches Engagement in Mecklenburg-Vorpommern, die Industrie- und Handelskammern und Wirtschaftsverbände.

Die Veranstaltungen waren teils öffentlich, teils an die eigene Mitgliedschaft gerichtet, und sie waren häufig als Abendveranstaltung, teilweise aber auch als Tagesveranstaltung organisiert. Darüber hinaus gab es auch zahlreiche Veranstaltungen für die Mitarbeiterinnen und Mitarbeiter von Behörden auf Landes- wie auf kommunaler Ebene. Auch mehrere Veranstaltungen für Kleingartenvereine wurden durchgeführt. Ein Landtagsabgeordneter organisierte in seinem Wahlkreis eine Veranstaltung zur DS-GVO. Darüber hinaus gab es auch wieder einige Seminare zum Datenschutz an den Hochschulen des Landes und am Kommunalen Studieninstitut Mecklenburg-Vorpommern.

Von September bis Dezember 2018 sind so 70 Veranstaltungen mit rund 3.000 Teilnehmenden durchgeführt worden, von denen viele auch Multiplikatoren waren. Viele der Teilnehmenden waren in besonderer Weise betroffen, so allein mehrere hundert Ärztinnen und Ärzte, da sich im Bereich des Gesundheitswesens ein erhöhter Informations- und Beratungsbedarf aufgrund der DS-GVO ergab, siehe beispielsweise Punkte 6.2, 8.1, 8.3, 8.6 und 8.7.

Broschüre und Veranstaltungen für Vereine

Auf Bitte des Landtages Mecklenburg-Vorpommern hat der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern in Zusammenarbeit mit der Stiftung für Ehrenamt und bürgerschaftliches Engagement in Mecklenburg-Vorpommern eine Informationsbroschüre für Vereine erarbeitet. Der Leitfaden „Datenschutz – Orientierungshilfe für Vereine in Mecklenburg-Vorpommern“ informiert über die Anforderungen des neuen Datenschutzrechts und gibt praktische Hilfe bei der Umsetzung. Der Ehrenamtsstiftung sei an dieser Stelle noch einmal für die sehr gute Zusammenarbeit gedankt.

Darüber hinaus gab es Unterstützung für die Vereine in Mecklenburg-Vorpommern mit der Vortragsreihe „Datenschutz – Tipps und Tricks zur Umsetzung“. In den Veranstaltungen wurde erläutert, was genau im Verein aufgrund der neuen Regelungen zu tun ist. Hier wurde der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern ebenfalls von der Stiftung für Ehrenamt und bürgerschaftliches Engagement in Mecklenburg Vorpommern unterstützt, siehe auch Punkte 8.6 und 8.7.

Änderungen auf der Webseite

Die Webseite des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (www.datenschutz-mv.de) ist ein wichtiges Informations- und Kontaktangebot für die Bürgerinnen und Bürger, die öffentliche Verwaltung, für Unternehmen, Institutionen, Vereine. Bereits 2017 wurden erforderliche technische Umstellungen vorgenommen. Mit Blick auf die Anwendbarkeit der DS-GVO ab dem 25. Mai 2018 sind jedoch auch inhaltlich neue Anforderungen hinzugekommen, von denen einige auf der Webseite abgebildet sind, siehe auch Punkt 7.2.3.

11 Abkürzungsverzeichnis

AK Technik	Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
AO	Abgabenordnung
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BMFSFJ	Bundesministerium für Familie, Senioren, Frauen und Jugend
BMI	Bundesministerium des Innern
BMWi	Bundesministerium für Wirtschaft
BrSchG M-V	Brandschutz- und Hilfeleistungsgesetz Mecklenburg-Vorpommern
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
CBC	Cipher Block Chaining
CSG	ComputerSpielSchule Greifswald
DANE	DNS-Based Authentication of Named Entities
DEMIS	Arbeitskreis Technische Details des elektronischen Melde- und Informationssystems für den Infektionsschutz
DNS	Domain Name System
DSG M-V	Landesdatenschutzgesetz Mecklenburg-Vorpommern
DS-GVO	Europäische Datenschutz-Grundverordnung
DSFA	Datenschutzfolgenabschätzung
DSK	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
DVZ M-V GmbH	Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH
EDSA	Europäischer Datenschutzausschuss
eGo-MV	Zweckverband Elektronische Verwaltung in Mecklenburg-Vorpommern

ERFA-Kreis	Erfahrungsaustauschkreis
EU	Europäische Union
eTLS	Enterprise Transport Layer Security
ETSI	European Telecommunications Standards Institute
GDD	Gesellschaft für Datenschutz und Datensicherheit
GG	Grundgesetz
HPI	Hasso-Plattner-Institut
HTTPS	Hypertext Transport Protocol Secure
IHK	Industrie- und Handelskammer
IQ M-V	Institut für Qualitätsentwicklung Mecklenburg-Vorpommern
IP	Internet Protocol
IT-PLR	IT-Planungsrat
KAG M-V	Kommunalabgabengesetz Mecklenburg-Vorpommern
KiföG M-V	Kindertagesförderungsgesetz Mecklenburg-Vorpommern
KMK	Kultusministerkonferenz
KMU	Kleine und mittlere Unternehmen
LAG Medien M-V	Landesarbeitsgemeinschaft Medien Mecklenburg-Vorpommern
LAKOST MV	Landeskoordinierungsstelle für Suchtthemen Mecklenburg-Vorpommern
LfK	Landesrat für Kriminalitätsvorbeugung
LJR MV	Landesjugendring Mecklenburg-Vorpommern
LKA MV	Landeskriminalamt Mecklenburg-Vorpommern
LPBK MV	Landesamt für zentrale Aufgaben und Technik der Polizei, Brand- und Katastrophenschutz Mecklenburg-Vorpommern
LRH MV	Landesrechnungshof Mecklenburg-Vorpommern
LSB MV	Landesseniorenbeirat Mecklenburg-Vorpommern
LT-Drs.	Landtags-Drucksache
MMV	Medienanstalt Mecklenburg-Vorpommern
NKR	Nationaler Normenkontrollrat

OZG	Onlinezugangsgesetz
PFS	Perfect Forward Secrecy
RFC	Request for Comment
RSA	Rivest, Shamir und Adleman
SchulDSVO M-V	Schuldatenschutzverordnung Mecklenburg-Vorpommern
SchulG M-V	Schulgesetz Mecklenburg-Vorpommern
SGB	Sozialgesetzbuch
SOG M-V	Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommern
TLS	Transport Layer Security
TMG	Telemediengesetz
UAG	Unterarbeitsgruppe
UPDK	Umgang mit Patientendaten in den Krankenhäusern Mecklenburg-Vorpommerns
WWW	World Wide Web

12 Stichwortverzeichnis